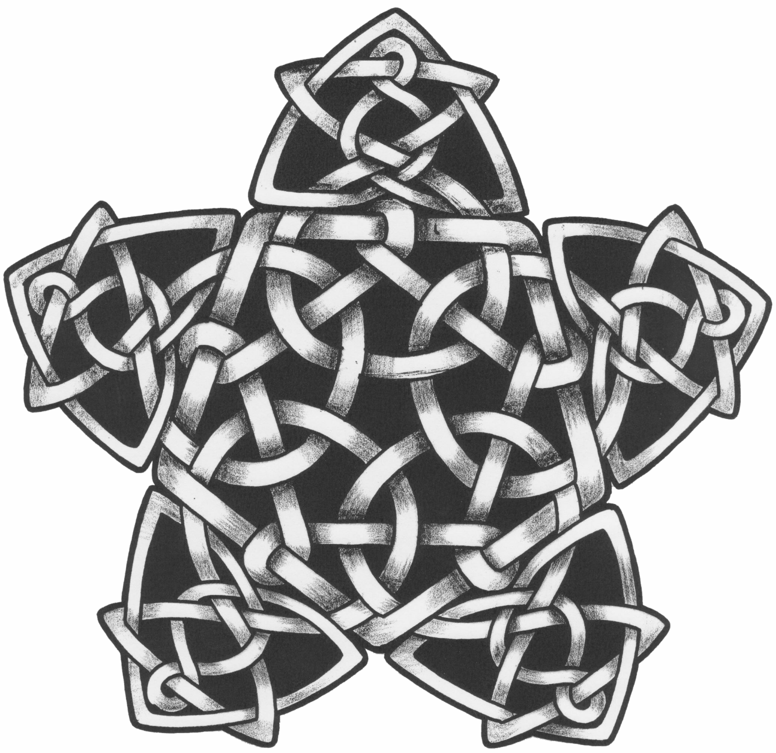
Cours de
Mathématiques Supérieures



Florian Bouguet

TABLE DES MATIÈRES

Première partie

Le Dernier Maître de $\mathbb{R}$

CHAPITRE 1

GROUPES, ANNEAUX ET CORPS

What is purple and commutes ? An abelian grape.

Classic joke

Un ensemble quelconque est une collection d'éléments, sans ordre et sans relations entre eux. C'est pour organiser tout cela qu'on parle de structure d'un ensemble. Dans ce premier chapitre, on va découvrir trois types structures algébriques fondamentales : les groupes, les anneaux et les corps.

On verra que des ensembles qui ont la même structure se "comportent" de la même façon et obéissent aux mêmes règles. C'est l'essence même des mathématiques de définir des règles abstraites pour savoir comment manipuler des ensembles, des fonctions, des éléments...On va donc découvrir quelles sont les règles précises gérant les calculs que l'on a l'habitude de faire en pratique.

En tant que premier chapitre de l'année, ce chapitre ne nécessite pas vraiment de pré-requis. Il est simplement nécessaire d'avoir quelques rudiments de mathématiques, de logique, et de théorie des ensembles et des applications.

I Groupes

1. Loi de composition interne

On rappelle que le produit cartésien de deux ensembles E et F est l'ensemble des couples d'éléments de E et F :

$$E \times F = \{(x, y) \,/ x \in E, y \in F\}.$$

On pourra noter $E^2 = E \times E$.

Définition 1.1 *Loi de composition interne*

Soit E un ensemble non-vide. On appelle *loi de composition interne sur* E sur E toute application $f : E^2 \to E$.

Exemple 1.2 :

1. $\begin{array}{ccc} \mathbb{N}^2 & \to & \mathbb{N} \\ (n,m) & \mapsto & n+m \end{array}$ est une loi de composition interne sur $\mathbb{N}$.
2. $\begin{array}{ccc} (\mathbb{R}^*)^2 & \to & \mathbb{R}^* \\ (x,y) & \mapsto & \dfrac{x}{y} \end{array}$ est une loi de composition interne sur $\mathbb{R}^*$.

$\diamondsuit$

Dans la suite, on notera toujours le composé de x et y par un symbole (généralement $\star$) qui représente la loi de composition interne. Par exemple, on dira que $+$ est une loi de composition interne sur $\mathbb{N}$ ou que $\div$ est une loi de composition interne sur $\mathbb{R}^*$. C'est un abus totalement admis.

Vérifier que $\star$ est une loi de composition interne sur E revient donc à vérifier que

$$\forall (x,y) \in E^2, \quad x \star y \in E.$$

Exemple 1.3 :
L'opération $-$ n'est pas une loi de composition interne sur $\mathbb{N}$. En revanche, $-$ est une loi de composition interne sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$. $\diamondsuit$

Définition 1.4

Soit E un ensemble non-vide et $\star$ une loi de composition interne sur E. On dit que $\star$ est *associative* si

$$\forall x,y,z \in E, \quad (x \star y) \star z = x \star (y \star z).$$

On dit que $\star$ est *commutative* si

$$\forall x,y \in E, \quad x \star y = y \star x.$$

On dit que $\star$ *admet un élément neutre* si

$$\exists e \in E, \forall x \in E, \quad e \star x = x \star e = x.$$

Si une loi est associative, on n'a plus besoin d'écrire de parenthèses puisque l'ordre dans lequel on fait les opérations n'a pas d'importance.

L'élément neutre, s'il existe, ne dépend pas de x. Autrement dit, il faut bien faire attention à l'ordre des quantificateurs dans cette définition.

Exemple 1.5 :
La loi $\div$ n'est ni associative ni commutative dans $\mathbb{R}^*$:

$$\frac{3}{2} = 1 \div (2 \div 3) \neq (1 \div 2) \div 3 = \frac{1}{6}, \quad 1 \div 2 \neq 2 \div 1.$$

$\diamondsuit$

Proposition 1.6

Soit E un ensemble non-vide muni d'une loi de composition interne $\star$. Si $\star$ possède un élément neutre, alors il est unique.

Démonstration : Soient $e, e' \in E$ deux éléments neutres pour $\star$. Alors on a

$$e = e \star e' = e'.$$

Donc $e = e'$. □

Définition/Proposition 1.7 *Inverse*

Soient E un ensemble non-vide et $\star$ une loi de composition interne sur E possédant un élément neutre e. Soit $x \in E$. On dit que x est *inversible pour la loi* $\star$ si

$$\exists y \in E, \quad x \star y = y \star x = e.$$

De plus, si $\star$ est associative, alors s'il existe, y est unique, on l'appelle *inverse de* x, et on note $y = x^{-1}$.

On dit aussi que x est *inversible à gauche* s'il existe $y \in E$ tel que $y \star x = e$, et *inversible à droite* s'il existe $y \in E$ tel que $x \star y = e$.

On notera que la notion d'inversibilité dépend de la loi de composition interne considérée. En pratique, si il n'y a pas de risque de confusion, on ne précisera pas cette loi.

Pour montrer qu'un élément est inversible et déterminer son inverse, il faut trouver un même inverse à gauche et inverse à droite. D'autre part, il est sous-entendu que $x^{-1} \in E$: en toute rigueur, on devrait dire "x est inversible pour $\star$ dans E".

Démonstration : Il faut juste prouver l'unicité de l'inverse. Soit $x \in E$ inversible. Supposons qu'il existe $y, y' \in E$ tels que

$$x \star y = y \star x = x \star y' = y' \star x = e.$$

On a alors, si $\star$ est associative,

$$y = y \star e = y \star (x \star y') = (y \star x) \star y' = e \star y' = y'.$$

□

Exemple 1.8 :

1. On considère l'ensemble $\mathbb{Z}$. $+$ est une loi de composition interne sur $\mathbb{Z}$ car

   $$\forall x, y \in \mathbb{Z}, \quad x + y \in \mathbb{Z}.$$

   - $+$ est commutative car $\forall x, y \in \mathbb{Z}, x + y = y + x$.
   - $+$ est associative car $\forall x, y, z \in \mathbb{Z}, (x + y) + z = x + y + z = x + (y + z)$.
   - $+$ possède un élément neutre $e = 0$, car $\forall x \in \mathbb{Z}, 0 + x = x = x + 0$.
   - Soit $x \in \mathbb{Z}$. Alors x est inversible car $x + (-x) = -x + x = 0$, et donc $x^{-1} = -x$.
2. $\times$ est une loi de composition interne sur $\mathbb{Z}^*$ qui est associative, commutative et qui possède un élément neutre $e = 1$. Les seuls éléments inversibles de $\mathbb{Z}^*$ sont -1 et 1 (ils sont leurs propres inverses), car

   $$\forall x \in \mathbb{Z} \setminus \{-1, 0, 1\}, \quad \frac{1}{x} \in \mathbb{Q} \setminus \mathbb{Z}$$

3. $\div$ est une loi de composition interne sur $\mathbb{R}^*$ qui n'est pas commutative, pas associative et qui ne possède pas d'élément neutre.

$\diamondsuit$

Exercice 1.9 :
Soit E l'ensemble des applications de $\mathbb{N}$ dans $\mathbb{N}$.

1. Montrer que $\circ$ est une loi de composition interne sur E.
2. $\circ$ est-elle commutative ? Associative ?
3. Montrer que $\circ$ possède un élément neutre.
4. (a) Montrer que $f \in E$ est inversible à gauche si, et seulement si f est injective.
   (b) Montrer que f est inversible à droite si, et seulement si, f est surjective.
5. Quels sont les éléments inversibles de E ?

Réponse

1. Soient $f, g \in E$. Puisque $g(\mathbb{N}) \subseteq \mathbb{N}$, $f \circ g$ est bien définie et $(f \circ g)(\mathbb{N}) \subseteq N$, donc $f \circ g \in E$.
2. $\circ$ n'étant évidemment pas commutative, on va exhiber un contre-exemple. Posons

$$f : \begin{array}{ccc} \mathbb{N} & \rightarrow & \mathbb{N} \\ n & \rightarrow & n+1 \end{array}, \quad g : \begin{array}{ccc} \mathbb{N} & \rightarrow & \mathbb{N} \\ n & \rightarrow & n^2 \end{array}.$$

   Par définition, $f, g \in E$ et $f \circ g(1) = f(1) = 2$. Par contre, $g \circ f(1) = g(2) = 4$, donc $f \circ g \neq g \circ f$. Donc $\circ$ n'est pas commutative.
3. On a, pour tout $f \in E$, et pour tout $n \in \mathbb{N}$,

$$\mathrm{Id} \circ f(n) = \mathrm{Id}(f(n)) = f(n), \quad f \circ \mathrm{Id}(n) = f(n), \quad \mathrm{Id} \circ f = f \circ \mathrm{Id} = f.$$

   Donc Id est l'élément neutre de $\circ$.
4. Soit $f \in E$.
   (a) Supposons que f soit inversible à gauche, c'est-à-dire qu'il existe $g \in E$ telle que $g \circ f = \mathrm{Id}$. Soient $x, y \in \mathbb{N}$. Alors

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

   Donc f est injective. Réciproquement, supposons que f soit injective. Pour tout $y \in f(\mathbb{N})$, il existe un unique antécédent x vérifiant $f(x) = y$. On peut noter $g(y) = x$. Alors

$$\forall x \in \mathbb{N}, \quad g(f(x)) = x$$

   car x est un antécédent de $y = f(x)$.
   (b) Supposons que f soit inversible à droite, c'est-à-dire qu'il existe $g \in E$ telle que $f \circ g = \mathrm{Id}$. Soit $y \in \mathbb{N}$. Alors

$$f(g(y)) = y,$$

   donc y admet un antécédent par f. Donc f est surjective. Réciproquement, supposons que f soit surjective. Pour tout $y \in \mathbb{N}$, il existe $x \in \mathbb{N}$ tel que $f(x) = y$. Notons $g(y) = x$. Alors

$$\forall y \in \mathbb{N}, f(g(y)) = y,$$

   car $g(y)$ est un antécédent de y par f.
5. Soit $f \in E$. On déduit des questions précédentes que :

$$\begin{aligned} f \text{ est inversible} &\iff f \text{ est inversible à gauche et à droite} \iff f \text{ est injective et surjective} \\ &\iff f \text{ est bijective.} \end{aligned}$$

$\diamondsuit$

Exemple 1.10 :

On considère $\mathcal{F}(\mathbb{N},\mathbb{N})$ muni de la loi de composition interne $\circ$. Soient $f, g : \mathbb{N} \to \mathbb{N}$ telles que

$$f : n \to n+1, \quad g : n \to \begin{cases} n-1 & \text{si } n \geq 1 \\ 0 & \text{si } n = 0 \end{cases}$$

Pour tout $n \in \mathbb{N}$, on a

$$g \circ f(n) = g(n+1) = n+1-1 = n, \quad f \circ g(n) = \begin{cases} n & \text{si } n \geq 1 \\ 1 & \text{si } n = 0 \end{cases}$$

Donc g est inversible à droite et f est inversible à gauche. D'après l'exercice 1.9, puisque f et g ne sont pas bijectives, elles ne sont pas inversibles. ♢

Proposition 1.11

Soit E un ensemble non-vide muni d'une loi de composition interne associative admettant un élément neutre e. Soient $x, y \in E$. Alors

(i) Si x est inversible, alors x^{-1} est inversible et $\left(x^{-1}\right)^{-1} = x$.
(ii) Si x et y sont inversibles, alors $x \star y$ est inversible et $(x \star y)^{-1} = x^{-1} \star y^{-1}$.

Démonstration : (i) Supposons que $x \in E$ soit inversible. On a alors

$$x \star x^{-1} = x^{-1} \star x = e.$$

Donc x^{-1} est inversible et $\left(x^{-1}\right)^{-1} = x$.

(ii) Supposons que x et y soient inversibles. Alors on a

$$(x \star y) \star \left(y^{-1} \star x^{-1}\right) = x \star y \star y^{-1} \star x^{-1} = x \star e \star x^{-1} = x \star x^{-1} = e.$$

De même, $\left(y^{-1} \star x^{-1}\right) \star (x \star y) = e$ donc $x \star y$ est inversible et $(x \star y)^{-1} = x^{-1} \star y^{-1}$.

□

2. Structure de groupe

Définition 1.12 *Groupe*

Soit G un ensemble non-vide muni d'une loi de composition interne $\star$. On dit que le couple $(G, \star)$ est un *groupe* si

(i) $\star$ est associative
(ii) $\star$ possède un élément neutre
(iii) tout élément de G est inversible (pour la loi $\star$).

Si de plus $\star$ est commutative, alors on dit que $(G, \star)$ est un groupe *commutatif* (ou *abélien*[1]).

Remarque 1.13 : Pour montrer que $(G, \star)$ est un groupe, on démontrera les points suivants :

0) $\star$ est bien une loi de composition interne sur G et G est non-vide.
1) $\star$ est associative.
2) on trouve un élément $e \in G$ tel que pour tout $x \in G$, $x \star e = e \star x = x$. Alors e est bien l'élement neutre de $\star$.

1. Niels Henrik Abel (1802-1829) : Mathématicien norvégien.

3) pour tout x dans G, on trouve un élément $y \in G$ tel que $x \star y = y \star x = e$. Alors $y = x^{-1}$.
4) On étudie si $(G, \star)$ est commutatif ou pas.

Attention à l'ordre des quantificateurs dans les points 2) et 3). $\diamondsuit$

Dans la suite, on dira souvent par abus "G est un groupe". Cela ne pose aucun problème, à condition qu'il n'y ait aucune ambiguïté sur la loi $\star$ pour laquelle $(G, \star)$ est un groupe. On verra de tels exemples plus tard.

Proposition 1.14 *Groupes de référence*
Les ensembles suivants sont des groupes commutatifs :

$$\begin{array}{cccc} (\mathbb{Z},+) & (\mathbb{Q},+) & (\mathbb{R},+) & (\mathbb{C},+) \\ & (\mathbb{Q}^*,\times) & (\mathbb{R}^*,\times) & (\mathbb{C}^*,\times) \end{array}$$

Démonstration : Montrons que $(\mathbb{Q}^*, \times)$ est un groupe. On démontre de la même manière tous les autres résultats.

0) Soient $a, b \in \mathbb{Q}^*$. Alors $ab \in Z$ donc $\times$ est bien une loi de composition interne sur $\mathbb{Q}^*$. De plus, $1 \in \mathbb{Q}^*$ donc $Q^* \neq \emptyset$.
1) Soient $a, b, c \in \mathbb{Q}^*$. Alors par définition de la multiplication, $(ab)\,c = a\,(bc)$ donc $\times$ est associative sur $\mathbb{Q}^*$.
2) Pour tout $a \in \mathbb{Q}^*$, on a
$$a \times 1 = 1 \times a = a.$$
Donc $\times$ admet pour élément neutre $1 \in \mathbb{Q}^*$.
3) Soit $a \in \mathbb{Q}^*$. Alors
$$a \times \frac{1}{a} = \frac{1}{a} \times a = 1.$$
Puisque $\frac{1}{a} \in \mathbb{Q}^*$, l'élément a est bien inversible pour $\times$ dans $\mathbb{Q}^*$.

Donc $(\mathbb{Q}^*, \times)$ est un groupe.

4) Pour tous $a, b \in \mathbb{Q}^*$, on a bien $ab = ba$.

Donc $(\mathbb{Q}^*, \times)$ est un groupe commutatif. Et en fait, puisque $\times$ est commutative sur $\mathbb{Q}^*$, on avait juste besoin de vérifier que

$$\forall a \in \mathbb{Q}^*, \quad a \times \frac{1}{a} = 1, \quad 1 \times a = a$$

$\square$

Il est important de remarquer que $(\mathbb{N}, +)$, $(\mathbb{Q}, \times)$ et $(\mathbb{Z}^*, \times)$ ne sont pas des groupes. En effet :

- 0 ne possède pas d'inverse pour $\times$ (dans n'importe quel ensemble).
- 1 ne possède pas d'inverse pour $+$ dans $\mathbb{N}$ (car $-1 \notin \mathbb{N}$).
- 2 ne possède pas d'inverse pour $\times$ dans $\mathbb{Z}^*$ (car $\frac{1}{2} \notin \mathbb{Z}^*$).

Proposition 1.15

Les ensembles $\left(\mathbb{R}^{\mathbb{N}},+\right)$ et $(\mathcal{F}(\mathbb{R},\mathbb{R}),+)$ sont des groupes commutatifs.

Démonstration : On va montrer que $(\mathcal{F}(\mathbb{R},\mathbb{R}),+)$ est un groupe, où l'on définit

$$\forall f,g\in\mathcal{F}(\mathbb{R},\mathbb{R}),\quad f+g:x\mapsto f(x)+g(x).$$

0) Tout d'abord, puisque $(\mathbb{R},+)$ est un groupe, $+$ est bien une loi de composition interne sur $\mathcal{F}(\mathbb{R},\mathbb{R})$. De plus, cet ensemble est non-vide car $\mathrm{Id}_{\mathbb{R}}\in\mathcal{F}(\mathbb{R},\mathbb{R})$.
1) Soient $f,g,h\in\mathbb{R}$. Alors, pour tout $x\in\mathbb{R}$,

$$((f+g)+h)(x)=(f(x)+g(x))+h(x)=f(x)+(g(x)+h(x))=(f+(g+h))(x),$$

donc $(f+g)+h=(f+(g+h))$ donc $+$ est associative sur $\mathcal{F}(\mathbb{R},\mathbb{R})$.
2) Puisque $+$ est commutative sur $\mathbb{R}$, il est clair que $+$ est commutative sur $\mathcal{F}(\mathbb{R},\mathbb{R})$.
3) Notons $f_0:x\mapsto 0$. Alors $f_0\in\mathcal{F}(\mathbb{R},\mathbb{R})$ et

$$\forall f\in\mathcal{F}(\mathbb{R},\mathbb{R}),\quad f+f_0=f_0+f=f.$$

4) Soit $f\in\mathcal{F}(\mathbb{R},\mathbb{R})$. Notons $g:x\mapsto -f(x)$. Alors

$$f+g=g+f=f_0.$$

Donc f est inversible pour $+$.

Donc $(\mathcal{F}(\mathbb{R},\mathbb{R}),+)$ est un groupe commutatif. On montre de la même façon que $\left(\mathbb{R}^{\mathbb{N}},+\right)$ est un groupe commutatif. □

Proposition 1.16

Soit E un ensemble non-vide. Notons $\sigma(E)=\{f:E\to E/f \text{ est une bijection}\}$. Alors $(\sigma(E),\circ)$ est un groupe. De plus, si E possède au moins trois éléments distincts, alors $(\sigma(E),\circ)$ n'est pas commutatif.

Démonstration : Tout d'abord, $\sigma(E)$ n'est pas vide car $\mathrm{Id}_E\in\sigma(E)$.

0) Soient $f,g\in\sigma(E)$. Alors $f\circ g$ est une application de E dans E (elle est bien définie car $g(E)\subseteq E$). De plus, pour tout $y\in E$, il existe $x'\in E$ tel que $f(x')=y$, et il existe $x\in E$ tel que $g(x)=x'$. Alors

$$f\circ g(x)=f(x')=y.$$

Donc $f\circ g$ est surjective. De plus, pour tous $x_1,x_2\in E$, puisque f et g sont injectives,

$$f(g(x_1))=f(g(x_2))\Rightarrow g(x_1)=g(x_2)\Rightarrow x_1=x_2.$$

Donc $f\circ g$ est injective donc bijective. Donc $\circ$ est bien une loi de composition interne sur $\sigma(E)$.
1) Soient $f,g,h\in\sigma(E)$. Pour tout $x\in E$, on a

$$f\circ(g\circ h)(x)=f(g\circ h(x))=f(g(h(x)))=(f\circ g)(h(x))=(f\circ g)\circ h(x),$$

donc $f\circ(g\circ h)=(f\circ g)\circ h$, donc $\circ$ est associative.
2) On sait que $\mathrm{Id}_E\in\sigma(E)$, et, pour tout $f\in\sigma(E)$,

$$\forall x\in\mathbb{E},\quad f\circ\mathrm{Id}_E(x)=f(x)=\mathrm{Id}_E\circ f(x),\quad f\circ\mathrm{Id}_E=f=\mathrm{Id}_E\circ f$$

Donc $\circ$ admet Id_E pour élément neutre.

3) Soit $f \in \sigma(E)$. Puisque f est bijective, f admet une bijection réciproque f^{-1} vérifiant

$$f \circ f^{-1} = f^{-1} \circ f = \mathrm{Id}_E .$$

De plus, f^{-1} est aussi une bijection donc $f^{-1} \in \sigma(E)$. Donc f est inversible pour $\circ$ dans $\sigma(E)$.

Enfin, supposons que E possède au moins trois éléments distincts a, b, c. Soient $f, g \in \sigma(E)$ définies par

$$\forall x \in E, \quad f(x) = \begin{cases} b & \text{si } x = a \\ a & \text{si } x = b \\ x & \text{sinon} \end{cases}, \quad g(x) = \begin{cases} c & \text{si } x = b \\ b & \text{si } x = c \\ x & \text{sinon} \end{cases}.$$

Alors

$$f \circ g(b) = f(c) = c, \quad g \circ f(b) = g(a) = a, \quad f \circ g \neq g \circ f.$$

Donc $(\sigma(E), \circ)$ n'est pas commutatif. □

On tire de cette propriété une remarque importante : il existe des groupes non-commutatifs. En fait, en dehors des lois habituelles, la plupart des lois de composition interne ne sont pas commutatives. On verra d'autres exemples plus tard (notamment l'ensemble des matrices, au second semestre).

A partir de maintenant, on pourra utiliser sans démonstration que les lois $+$, $\times$ et $\circ$ sont associatives (et que $+$ et $\times$ sont commutatives) dans les ensembles usuels.

Proposition 1.17

Soit $(G, \star)$ un groupe et soient $x, y \in G$. Alors

$$\left(x^{-1}\right)^{-1} = x, \quad (x \star y)^{-1} = y^{-1} \star x^{-1}.$$

C'est exactement la proposition 1.11. On fera attention à l'ordre si G n'est pas un groupe commutatif.

3. Sous-groupes

Une fois que l'on connaît certains groupes de référence, certains de leurs sous-ensembles peuvent hériter de cette structure. C'est le principe des sous-groupes.

Définition/Proposition 1.18 *Sous-groupe*

Soit $(G, \star)$ un groupe et soit $H \subseteq G$. On note e l'élément neutre de G. On dit que H est *un sous-groupe de* G si

(i) H est non-vide.
(ii) $\forall x, y \in H, x \star y \in H$. On dit que H est *stable par* $\star$.
(iii) $\forall x \in H, x^{-1} \in H$. On dit que H est *stable par inverse*.

Dans ce cas, $(H, \star)$ est un groupe. De plus, $e \in H$ et e est aussi l'élément neutre de H.

Démonstration : Il faut montrer que $(H, \star)$ est un groupe.

0) D'abord, H est non-vide, d'après (i), et $\star$ est une loi de composition interne sur H d'après (ii).
1) Puisque $\star$ est associative sur G, elle est encore associative sur H.

2) Soit $x \in H$. Alors $x^{-1} \in H$ et donc $e = x \star x^{-1} \in H$. Donc $\star$ admet e pour élément neutre dans H.
3) Enfin, d'après (iii), pour tout $x \in H$, $x^{-1} \in H$ et donc x possède un inverse pour $\star$ dans H.

Donc $(H, \star)$ est un groupe. On a montré au passage que $e \in H$ et que c'est l'élément neutre de H. $\square$

Un sous-groupe de G est simplement un autre groupe H inclus dans G et qui possède une structure de groupe "compatible" avec celle de G (autrement dit, G et H sont des groupes pour la même loi).

$(\mathbb{R}^*, \times)$ n'est pas un sous-groupe de $(\mathbb{R}, +)$.

Remarque 1.19 : En pratique, pour montrer qu'un ensemble est un groupe, on montrera presque tout le temps qu'il s'agit d'un sous-groupe d'un groupe connu. C'est pourquoi il est important de connaître les groupes de référence. On utilisera en général la propriété suivante. $\diamondsuit$

Proposition 1.20

H est un sous-groupe de G si, et seulement si,

0) $H \subseteq G$.
1) $e \in H$.
2) $\forall x, y \in H, x \star y^{-1} \in H$.

On peut remplacer la propriété (iii) par "$x^{-1} \star y \in H$" : la preuve est exactement la même.

Démonstration : H est non-vide et $H \subseteq G$, il reste donc à prouver que H est stable par produit et par inverse en utilisant la propriété :

$$(P) \quad : \quad \forall x, y \in H, \quad x \star y^{-1} \in H$$

Puisque $e \in H$, pour tout $y \in H$, on applique (P) à e et y, donc $e \star y^{-1} = y^{-1} \in H$ donc H est stable par inverse. Ensuite, pour tous $x, y \in H$, $y^{-1} \in H$ et on applique (P) à x et y^{-1}. Donc

$$x \star \left(y^{-1}\right)^{-1} = x \star y \in H,$$

donc H est stable par $\star$. $\square$

Exemple 1.21 :
$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ et $(\mathbb{R}, +)$ sont des sous-groupes de $(\mathbb{C}, +)$. $\diamondsuit$

Exercice 1.22 :
Montrer que $\left(\mathbb{R}_+^*, \times\right)$ est un sous-groupe de $(\mathbb{R}^*, \times)$.

Réponse

$(\mathbb{R}^*, \times)$ est un groupe de référence dont l'élément neutre est 1. De plus, $1 \in \mathbb{R}_+^*$ et

$$\mathbb{R}_+^* =]0, +\infty[\subseteq]-\infty, 0[\cup]+\infty[= \mathbb{R}^*$$

par définition. Enfin, pour tous $xy \in \mathbb{R}_+^*$, on a

$$xy^{-1} = \frac{x}{y} > 0,$$

donc $\left(\mathbb{R}_+^*, \times\right)$ est bien un sous-groupe de $(\mathbb{R}^*, \times)$.

$\diamondsuit$

Exercice 1.23 :
Soit $(G, \star)$ un groupe. Quel est le plus petit sous-groupe de G ?

Réponse

On va montrer que $H = \{e\}$ est un sous-groupe de G, où e est l'élément neutre de G. Il ne peut évidemment pas y en avoir de plus petit car un sous-groupe est non-vide. $e \in H$ et H est inclus dans G par définition. De plus, $e \star e^{-1} = e \in H$, donc H est un sous-groupe de G.

$\diamondsuit$

Proposition 1.24

Soit $(G, \star)$ un groupe commutatif. Alors tout sous-groupe de $(G, \star)$ est commutatif.

La preuve est évidente. Ce qui est intéressant, c'est que la réciproque est fausse. En effet, si E est un ensemble contenant au moins trois éléments distincts, alors $(\sigma(E), \circ)$ est un groupe non-commutatif. En revanche, $\{\mathrm{Id}_E\}$ est un sous-groupe de $\sigma(E)$ qui est évidemment commutatif.

Exercice 1.25 :
On pose

$$\mathbb{U} = \{z \in \mathbb{C} / |z| = 1\}.$$

Montrer que $(\mathbb{U}, \times)$ est un groupe. Est-il commutatif ?

Réponse

On va montrer que $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

0) Par définition, $U \subseteq \mathbb{C}^*$ (car $0 \notin U$).
1) $|1| = 1$ donc $1 \in \mathbb{U}$.
2) Soient $z, z' \in \mathbb{U}$. Alors

$$|z \times z'| = |z| \times |z'| = 1,$$

donc $zz' \in \mathbb{U}$, donc $\mathbb{U}$ est stable par $\times$.
3) Soit $z \in \mathbb{U}$. Alors

$$\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1,$$

donc $\frac{1}{z} \in \mathbb{U}$, donc $\mathbb{U}$ est stable par inverse.

Donc $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$, c'est donc un groupe. De plus, puisque $(\mathbb{C}^*, \times)$ est commutatif, alors $(\mathbb{U}, \star)$ est aussi commutatif.

$\diamondsuit$

Proposition 1.26

Soit $(G, \star)$ un groupe. Si H_1 et H_2 sont deux sous-groupes de G alors $H_1 \cap H_2$ est un sous-groupe de G.

Démonstration : Notons e l'élément neutre de G et $K = H_1 \cap H_2$.

0) Puisque $e \in H_1$ et $e \in H_2$ alors $e \in K$. De plus, $K \subseteq H_1 \subseteq G$.
1) Soient $x, y \in K$. Alors, pour tout $i \in [\![1,2]\!]$, $x, y \in H_i$ donc $x \star y^{-1} \in H_i$ donc $x \star y^{-1} \in K$.

□

En fait, l'intersection quelconque (éventuellement infinie) de sous-groupes de G est encore un sous-groupe de G. La démonstration est identique.

L'union de deux sous-groupes n'est en général pas un sous-groupe.

4. Morphismes de groupe

Dans cette section, on introduit un type d'applications très importantes : les morphismes. Un morphisme (ou homomorphisme) est une "application qui respecte les structures" de ses ensembles de départ et d'arrivée. C'est donc tout naturellement qu'on définit les morphismes de groupe.

Définition 1.27 *Morphisme de groupe*
Soient $(G, \star)$ et $(H, \circledast)$ deux groupes, et $f : G \to H$. On dit que f est un *morphisme de groupes* si

$$\forall x, y \in G, \quad f(x \star y) = f(x) \circledast f(y).$$

Définition 1.28 *Types de morphismes*
Soit f un morphisme de groupes de $(G, \star)$ dans $(H, \circledast)$.

(i) On dit que f est un endomorphisme si $G = H$.
(ii) On dit que f est un isomorphisme si f est aussi une bijection.
(iii) On dit que f est un automorphisme si $G = H$ et si f est aussi une bijection.

On retiendra : "automorphisme = endomorphisme + isomorphisme".[2]

Pour parler de morphismes de groupes, on vérifiera d'abord que $f : G \to H$ et que G et H sont bien des groupes.

Exemple 1.29 :
Montrons que la fonction exp est un morphismes de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{R}^*, \times)$. D'abord, $\mathbb{R}$ et $\mathbb{R}^*$ sont bien des groupes pour les opérations annoncées. Ensuite,

$$\forall x, y \in \mathbb{R}, \quad \exp(x + y) = \exp(x) \exp(y).$$

On pourra remarquer que $\exp : \mathbb{R} \to \mathbb{R}_+^*$ est un isomorphisme entre $(\mathbb{R}, +)$ et $\left(\mathbb{R}_+^*, \times\right)$. ◇

Exemple 1.30 :
Si G est un groupe, alors Id_G est un morphisme de groupes. C'est même un automorphisme. ◇

Exercice 1.31 :
Soit $E =]-1, 1[$ et $\star$ définie par

$$\forall x, y \in E, \quad x \star y = \frac{x + y}{1 + xy}.$$

2. "Endo" signifie "dans, dedans". "Iso" signifie "égal, pareil". "Auto" signifie "sur soi-même".

1. Montrer que $(E, \star)$ est un groupe abélien.
2. Montrer que la fonction $f : x \mapsto \dfrac{e^x - e^{-x}}{e^x + e^{-x}}$ est un morphisme de groupes entre $(\mathbb{R}, +)$ et $(E, \star)$.

Réponse

1. La loi $\star$ étant plutôt exotique, pas question de parler de sous-groupes ici. On montre que E est un groupe par définition :
   0) $E \neq \emptyset$ et, pour tout $y \in E$, la fonction $\varphi : x \mapsto \dfrac{x+y}{1+xy}$ est strictement croissante sur $[-1, 1]$ (montrer qu'elle est dérivable et calculer φ'). De plus $\varphi(1) = 1$ et $\varphi(-1) = -1$ donc
   $$\forall x, y \in E, \quad x \star y \in]-1, 1[= E.$$
   $\star$ est donc bien une loi de composition interne.
   1) Il est clair que $x \star y = \dfrac{x+y}{1+xy} = \dfrac{y+x}{1+yx} = y \star x$ donc $\star$ est commutative sur E.
   2) Soient $x, y, z \in E$. On a
   $$x \star (y \star z) = x \star \frac{y+z}{1+yz} = \frac{x + \frac{y+z}{1+yz}}{1 + \frac{xy+xz}{1+yz}} = \frac{x+y+z+xyz}{xy+xz+yz}.$$
   Cette expression est symétrique en x et z donc
   $$x \star (y \star z) = z \star (y \star x) = (y \star x) \star z = (x \star y) \star z,$$
   donc $\star$ est associative.
   3) On a, pour tout $x \in E$,
   $$0 \star x = x \star 0 = \frac{x+0}{1+x \times 0} = x,$$
   donc $(E, \star)$ admet 0 pour élément neutre.
   4) Pour tout $x \in E$, on a
   $$x \star (-x) = \frac{x-x}{1-x^2} = 0,$$
   donc x admet $-x$ comme inverse pour la loi $\star$.

   On en déduit que $(E, \star)$ est un groupe abélien.
2. Soit $x \in \mathbb{R}$. On a alors $f(x) = \dfrac{e^{2x} - 1}{e^{2x} + 1}$. Alors il est évident que $f(x) < 1$ et $f(x) > -1$. Donc $f : \mathbb{R} \to E$. De plus, on sait que $(\mathbb{R}, +)$ et $(E, \star)$ sont des groupes. Enfin, on a, pour tous $x, y \in \mathbb{R}$,
   $$\begin{aligned} f(x) \star f(y) &= \frac{\frac{e^x - e^{-x}}{e^x + e^{-x}} + \frac{e^y - e^{-y}}{e^y + e^{-y}}}{1 + \frac{(e^x - e^{-x})(e^y - e^{-y})}{(e^x + e^{-x})(e^y + e^{-y})}} = \frac{(e^x - e^{-x})(e^y + e^{-y}) + (e^x + e^{-x})(e^y - e^{-y})}{(e^x + e^{-x})(e^y + e^{-y}) + (e^x - e^{-x})(e^y - e^{-y})} \\ &= \frac{2 e^x e^y - 2 e^{-x} e^{-y}}{2 e^x e^y + 2 e^{-x} e^{-y}} = \frac{e^{x+y} - e^{-x-y}}{e^{x+y} + e^{-x-y}} = f(x+y). \end{aligned}$$
   Donc f est un morphisme de groupes. On pourrait même montrer que c'est un isomorphisme.

$\diamondsuit$

Proposition 1.32

Soit f un morphisme de groupes de $(G, \star)$ dans $(H, \circledast)$, de neutres respectifs e_G et e_H. Alors

(i) $f(e_G) = e_H$.

(ii) Pour tout $x \in G$, $f\left(x^{-1}\right) = f(x)^{-1}$.
(iii) Pour tous $n \in \mathbb{N}^*$, et $x_1, \ldots, x_n \in G$,

$$f(x_1 \star \cdots \star x_n) = f(x_1) \circledast \cdots \circledast f(x_n).$$

Démonstration : (i) On a

$$e_H \circledast f(e_G) = f(e_G) = f(e_G \star e_G) = f(e_G) \circledast f(e_G),$$

on en déduit donc que

$$e_H = e_H \circledast f(e_G) \circledast f(e_G)^{-1} = f(e_G) \circledast f(e_G) \circledast f(e_G)^{-1} = f(e_G).$$

(ii) Pour tout $x \in G$, on a

$$f(x) \circledast f\left(x^{-1}\right) = f\left(x \star x^{-1}\right) = f(e_G) = e_H.$$

De même, $f\left(x^{-1}\right) \circledast f(x) = e_H$ donc $f(x)^{-1} = f\left(x^{-1}\right)$.
(iii) Récurrence directe sur $n \in \mathbb{N}^*$.

□

Proposition 1.33

Soient $(G, \star), (H, \circledast), (K, \diamond)$ trois groupes. Soient $f : G \to H$ et $g : H \to K$ deux morphismes de groupes. Alors

(i) $g \circ f$ est un morphisme de groupes de G dans K.
(ii) Si f est un isomorphisme, alors f^{-1} est un isomorphisme de groupes de K dans G.

Démonstration : (i) G et K sont bien des groupes et $g \circ f : G \to K$. De plus, pour tous $x, x' \in G$, on a

$$\begin{aligned} g \circ f(x \star x') &= g(f(x \star x')) = g(f(x) \circledast f(x')) = g(f(x)) \diamond g(f(x')) \\ &= g \circ f(x) \diamond g \circ f(x'), \end{aligned}$$

donc $g \circ f$ est un morphisme de groupes.
(ii) $f^{-1} : H \to G$ est bien définie car f est bijective, et H et G sont des groupes. De plus, on sait que f^{-1} est bijective, il reste donc à montrer que c'est un morphisme. Soient $y, y' \in H$. On sait qu'il existe $x, x' \in G$ tels que $f(x) = y, f(x') = y'$, et on a

$$f(x \star x') = f(x) \circledast f(x') = y \circledast y', \quad f^{-1}(y \circledast y') = f^{-1} \circ f(x \star x') = x \star x' = f^{-1}(y) \star f^{-1}(y').$$

Donc f^{-1} est un isomorphisme.

□

Définition 1.34 *Noyau et image*

Soit f un morphisme de groupes de $(G, \star)$ dans $(H, \circledast)$. On appelle *noyau de* f l'ensemble

$$\ker(f) = \{x \in G / f(x) = e_H\} = f^{-1}(\{e_H\}).$$

On appelle *image de* f l'ensemble

$$\operatorname{Im}(f) = \{y \in H / \exists x \in G, f(x) = y\} = f(G).$$

Théorème 1.35

Soit f un morphisme de groupes de $(G, \star)$ dans $(H, \circledast)$. Alors

(i) $\ker f$ est un sous-groupe de G.
(ii) $\mathrm{Im}\,(f)$ est un sous-groupe de H.
(iii) f est injective si, et seulement si, $\ker f = \{e_G\}$.

Démonstration : (i) Par définition, $\ker f \subseteq G$ et $e_G \in \ker f$ car $f(e_G) = e_H$. De plus, pour tous $x, x' \in \ker f$, on a

$$f\left(x \star (x')^{-1}\right) = f(x) \circledast f\left((x')^{-1}\right) = f(x) \circledast f(x')^{-1} = e_H \circledast e_H^{-1} = e_H,$$

donc $x \star (x')^{-1} \in \ker f$ donc $\ker f$ est un sous-groupe de G.

(ii) Par définition, $\mathrm{Im}\, f \subseteq H$ et $e_H \in \mathrm{Im}\, f$ car $f(e_G) = e_H$. De plus, pour tous $y, y' \in \mathrm{Im}\, f$, il existe $x, x' \in G$ tels que $f(x) = y$, $f(x') = y'$, et alors

$$f\left(x \star (x')^{-1}\right) = f(x) \circledast f\left((x')^{-1}\right) = f(x) \circledast f(x')^{-1} = y \circledast (y')^{-1},$$

donc $y \circledast (y')^{-1} \in \mathrm{Im}\, f$ donc $\mathrm{Im}\, f$ est un sous-groupe de H.

(iii) Supposons que f est injective. On veut montrer que $\ker f = \{e_G\}$, mais on a déjà vu que $e_G \in \ker f$. Soit $x \in \ker f$. On a $f(x) = e_H = f(e_G)$. Puisque f est injective, on en déduit que $x = e_G$ et donc $\ker f \subseteq \{e_G\}$, donc $\ker f = \{e_G\}$. Réciproquement, supposons que $\ker f = \{e_G\}$ et soient $x, x' \in G$ tels que $f(x) = f(x')$. Alors

$$f(x) \circledast f\left((x')^{-1}\right) = f(x') \circledast f\left((x')^{-1}\right) = f(x') \circledast f(x')^{-1} = e_H, \quad f\left(x \star (x')^{-1}\right) = e_H.$$

Donc $x \star (x')^{-1} \in \ker f$ donc $x \star (x')^{-1} = e_G$ donc

$$x = x \star (x')^{-1} \star x' = x'.$$

Donc f est injective.

□

On peut donc caractériser l'injectivité ou la surjectivité à l'aide du noyau ou de l'image (rappelons que, par définition, f est surjective si, et seulement si, $\mathrm{Im}\, f = H$).

Remarque 1.36 : Une manière standard, et souvent rapide, de montrer qu'un ensemble est un groupe est de le voir comme le noyau ou l'image d'un morphisme de groupe. Par exemple, cela permet de démontrer rapidement que $\left(\mathbb{R}_+^*, \times\right)$ est un sous-groupe de $(\mathbb{R}^*, \times)$: c'est l'image de exp. ♢

⚠ On a toujours les inclusion $\{e_G\} \subseteq \ker f$ et $\mathrm{Im}\, f \subseteq H$.

Exercice 1.37 :
Soit $p \in \mathbb{N}^*$ et $f : \mathbb{Z} \to \mathbb{Z}$ définie par $f : n \mapsto pn$.

1. Montrer que f est un endomorphisme du groupe $(\mathbb{Z}, +)$.
2. Démontrer que f est injective.
3. Démontrer que l'ensemble des multiples de p, noté $p\mathbb{Z}$, est un groupe pour l'addition.

Réponse

1. L'application f est un endomorphisme du groupe $(\mathbb{Z}, +)$, car $(\mathbb{Z}, +)$ est bien un groupe et, pour tous $n, m \in \mathbb{Z}$,
$$f(n) + f(m) = pn + pm = p(n+m) = f(n+m).$$
2. Soit $x \in \mathbb{Z}$. Alors, puisque $p \neq 0$,
$$x \in \ker f \iff f(x) = 0 \iff px = 0 \iff x = 0,$$
donc $\ker f = \{0\}$ donc f est injective.
3. Par définition, $p\mathbb{Z} = \{pn \in \mathbb{Z} / n \in \mathbb{Z}\} = \operatorname{Im} f$. Puisque f est un morphisme, on en déduit que $(\operatorname{Im} f, +)$ est un sous-groupe de $(\mathbb{Z}, +)$. Donc $(p\mathbb{Z}, +)$ est un groupe.

$\diamondsuit$

Exemple 1.38 :

Sur le même principe, on peut montrer facilement que $f : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{U} \\ x & \mapsto & \mathrm{e}^{ix} \end{array}$ est un morphisme surjectif entre les groupes $(\mathbb{R}, +)$ et $(\mathbb{U}, \times)$. On en déduit que $\ker f = 2\pi\mathbb{Z}$ est un sous-groupe de $\mathbb{R}$. $\diamondsuit$

Exemple 1.39 :

Encore sur le même principe, on peut montrer que pour tout $a > 0$, $f : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{U} \\ n & \mapsto & a^n \end{array}$ est un morphisme injectif entre les groupes $(\mathbb{Z}, +)$ et $(\mathbb{R}^*, \times)$. $\diamondsuit$

5. Compléments

5.1. Notation additive et notation multiplicative

Proposition 1.40 *Notation multiplicative*

Soit $(G, \star)$ un groupe muni d'un élément neutre e, et soit $x \in G$. On note, pour tout $n \in \mathbb{N}^*$,
$$x^0 = e, \quad x^n = \underbrace{x \star \cdots \star x}_{n \text{ fois}}, \quad x^{-n} = \underbrace{x^{-1} \star \cdots \star x^{-1}}_{n \text{ fois}}$$
On a alors, pour tous $p, q \in \mathbb{Z}$,
$$x^p \star x^q = x^{p+q}, \quad (x^p)^q = x^{pq}, \quad (x^p)^{-1} = x^{-p}.$$

La démonstration est évidente. On retiendra que cela fonctionne comme pour les puissances de nombres réels (cas où $\star$ est $\times$). C'est ce qu'on appelle la notation multiplicative, qu'on peut utiliser lorsqu'on est suffisamment à l'aise avec les notions considérées. Alors e joue le rôle de 1 et on se permet de ne pas noter la loi lorsqu'il n'y a pas d'ambiguïté.

Comme on vient de le remarquer, pour effectuer des exercices théoriques, on ne précisera pas toujours la loi pour un groupe abstrait G, et on utilise alors la notation additive ou la notation multiplicative[3] :

3. Ceci est lié au fait que la plupart des ensembles sont vus comme des groupes pour $+$ ou $\times$.

	Notation actuelle	Notation additive	Notation multiplicative
Loi	$\star$	$+$	$\times$
Neutre	e	0	1
Inverse	x^{-1}	$-x$	x^{-1}
Abélien	?	Oui	?

Dans les chapitres suivants, on rencontrera des ensembles où la multiplication n'est pas commutative (l'exemple principal étant les matrices). Par contre, l'addition sera toujours commutative dans les ensembles que l'on considère, c'est pourquoi on réservera la notation additive aux groupes abéliens, et la notation multiplicative aux groupes peut-être pas commutatif, ou non-commutatifs. La notation multiplicative est donc choisie en générale, et permet en plus de ne même pas écrire la loi :

$$\forall x \in G, \quad 1x = x1 = x, \quad xx^{-1} = x^{-1}x = 1.$$

Ces abus de notation sont particulièrement utiles lorsqu'on a plusieurs groupes abstraits, chacun munis d'une loi différente...

5.2. Table d'un groupe

Lorsqu'un groupe est fini, on peut être amené à dresser sa table. Cela permet notamment de simplifier les calculs à venir, et de déterminer si le groupe est abélien.

Exercice 1.41 :
Soit $G = \{x_0, \dots, x_5\}$ un groupe à six éléments d'élément neutre x_0. Compléter sa table :

$\star$	x_0	x_1	x_2	x_3	x_4	x_5
x_0						
x_1			x_4			
x_2		x_5		x_4	x_3	
x_3		x_4				
x_4			x_1		x_5	x_0
x_5				x_1		

$\diamondsuit$

Réponse

$\star$	x_0	x_1	x_2	x_3	x_4	x_5
x_0	x_0	x_1	x_2	x_3	x_4	x_5
x_1	x_1	x_0	x_4	x_5	x_2	x_3
x_2	x_2	x_5	x_0	x_4	x_3	x_1
x_3	x_3	x_4	x_5	x_0	x_1	x_2
x_4	x_4	x_3	x_1	x_3	x_5	x_0
x_5	x_5	x_2	x_3	x_1	x_0	x_4

II Anneaux et corps

On va voir que les anneaux sont des groupes plus évolués : ils disposent d'une seconde loi de composition interne.

1. Structure d'anneau

Définition 2.1 *Distributivité*

Soit E un ensemble muni de deux lois de composition interne $+$ et $\times$. On dit que $\times$ est *distributive* par rapport à $+$ si

$$\forall x, y, z \in E, \quad (x+y) \times z = x \times z + y \times z, \quad x \times (y+z) = x \times y + x \times z.$$

On parle parfois de distributivité à gauche ou à droite si une seule de ces conditions est vérifiée.

Définition 2.2 *Anneau*

Soit A un ensemble muni de deux lois de composition interne $+$ et $\times$. On dit que $(A, +, \times)$ est un *anneau* si

(i) $(A, +)$ est un groupe commutatif.
(ii) $\times$ est associative
(iii) $\times$ admet un élément neutre.
(iv) $\times$ est distributive par rapport à $+$.

Si de plus $\times$ est commutative, alors on dit que $(A, +, \times)$ est un anneau *commutatif*.

Selon certains ouvrages plus anciens, l'existence d'un élément neutre pour $\times$ n'est pas requise (notion de *pseudo-anneau*). Attention de bien vérifier la définition choisie par votre livre favori.

L'ordre des lois est important : $(A, \star, \diamond)$ ne signifie pas la même chose que $(A, \diamond, \star)$.

Remarque 2.3 : Contrairement aux groupes, les notations des anneaux sont relativement standards : on utilise généralement les notations additives et multiplicatives. Sauf indication contraire, les neutres des lois $+$ et $\times$ seront notés respectivement 0_1 et 1_A. ♢

Dans un anneau quelconque $(A, +, \times)$, les éléments ne commutent pas et ne sont pas inversibles pour la loi $\times$. Cette absence d'inverse multiplicatif est la principale différence avec les groupes. Puisque tous les éléments de A admet un inverse pour $+$, on ne parlera d'éléments inversibles que par rapport à la loi $\times$.

Proposition 2.4 *Anneaux de référence*

Les ensembles suivants sont des anneaux commutatifs :

$$(\mathbb{Z}, +, \times), \quad (\mathbb{Q}, +, \times), \quad (\mathbb{R}, +, \times), \quad (\mathbb{C}, +, \times),$$

$$\left(\mathbb{R}^{\mathbb{N}}, +, \times\right), \quad (\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \times), \quad \left(\mathcal{C}^0(\mathbb{R}, \mathbb{R}), +, \times\right).$$

L'ensemble $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \circ)$ n'est pas un anneau, car $\circ$ n'est pas distributive pour $+$. Dommage, il s'agissait d'un bon candidat pour donner un exemple d'anneau non-commutatif (voir exercice 2.7).

Proposition 2.5 *Règles de calcul dans un anneau*

Soit $(A, +, \times)$ un anneau. Alors

(i) 0_A est *absorbant* pour $\times$:

$$\forall x \in A, \quad x \times 0_A = 0_A \times x = 0_A.$$

(ii) Règle des signes :

$$\forall x, y \in A, \quad (-x) \times y = x \times (-y) = -(x \times y), \quad (-x) \times (-y) = x \times y.$$

(iii) Soient $x, y \in A$. Si x et y commutent, alors ils vérifient la formule du binôme :

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

Démonstration : (i) Soit $x \in A$. Alors on a

$$x \times 0_A = x \times (0_A + 0_A) = x \times 0_A + x \times 0_A, \quad x \times 0_A - x \times 0_A = x \times 0_A + x \times 0_A - x \times 0_A, \quad 0_A = x \times 0_A.$$

De même, $0_A \times x = 0_A$.

(ii) D'après le point (i), pour tous $x, y \in A$,

$$0_A = x \times 0_A = x \times (y - y) = x \times y + x \times (-y), \quad -(x \times y) = x \times (-y).$$

De même, $(-x) \times y = -(x \times y)$. On a ensuite

$$(-x) \times (-y) = -(x \times (-y)) = -(-(x \times y)) = x \times y.$$

(iii) Soient $x, y \in A$, on suppose que x et y commutent. On montre la formule du binôme par récurrence sur n. Rappelons la formule de Pascal : $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$.

Initialisation : On a $(x+y)^0 = 1 = \sum_{k=0}^{0} \binom{0}{0} x^0 y^{0-k}$.

Hérédité : Supposons que la formule soit vraie pour un certain rang $n \in \mathbb{N}$. On a alors, puisque x et y commutent,

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)(x+y)^n = (x+y) \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n+1-k} \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} x^k y^{n+1-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n+1-k} \\
&= x^{n+1} + y^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) x^k y^{n+1-k} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{n+1-k}.
\end{aligned}$$

La formule du binôme est donc vraie au rang $n+1$, ce qui achève cette récurrence.

□

⚠ Soit $(A, +, \times)$ un anneau. Soient $x, y \in A$. Alors

$$x \times y = 0 \not\Rightarrow x = 0 \text{ ou } y = 0.$$

En effet, on a un contre-exemple en considérant de $A = \mathcal{F}(\mathbb{R}, \mathbb{R})$, $f = \mathbb{1}_{]0,+\infty[}$ et $g = \mathbb{1}_{]-\infty,0[}$.

Définition 2.6 *Anneau intègre*

Soit $(A, +, \times)$ un anneau. On dit que A est *intègre* si

$$\forall a, b \in A, \quad a \times b = 0 \not\Rightarrow a = 0 \text{ ou } b = 0.$$

Exercice 2.7 :
On note E l'ensemble des endomorphismes de groupe de $(\mathbb{C}, +)$.

1. Montrer que $(E, +, \circ)$ est un anneau.
2. Montrer que E est un anneau non-commutatif.
Indication : on pourra remarquer que les applications de la forme $z \mapsto \alpha \mathfrak{Re}(z) + \beta \mathfrak{Im}(z) + i(\gamma \mathfrak{Re}(z) + \delta \mathfrak{Im}(z))$ sont des endomorphismes de groupe de $\mathbb{C}$.

Réponse

1. $E \neq \emptyset$ car $\mathrm{Id}_{\mathbb{C}} \in E$. Exactement comme dans le cas de la proposition 1.15, on montre que $(E, +)$ est un groupe abélien. Rien de difficile de ce côté-là, c'est la structure d'anneau qui nous intéresse. D'après la proposition 1.33, si $f, g \in E$ alors $f \circ g$ est aussi un endomorphisme de $\mathbb{C}$, donc $\circ$ est une loi de composition interne pour E. De plus, $\mathrm{Id}_{\mathbb{C}} \in E$ et on a

$$\forall f \in E, \quad f \circ \mathrm{Id}_{\mathbb{C}} = \mathrm{Id}_{\mathbb{C}} \circ f = f,$$

donc $\mathrm{Id}_{\mathbb{C}}$ est l'élément neutre pour la loi $\circ$. De plus, on a déjà vu que $\circ$ est associative. Il reste donc à montrer que $\circ$ est distributive par rapport à $+$. Soient $f, g, h \in E$. Alors, pour tout $x \in G$,

$$(f + g) \circ h(x) = (f + g)(h(x)) = f(h(x)) + g(h(x)) = f \circ h(x) + g \circ h(x),$$
$$f \circ (g + h)(x) = f(g(x) + h(x)) = f(g(x)) + f(h(x)) = f \circ g(x) + f \circ h(x),$$

car f est un morphisme de groupe. On en déduit que $(E, +, \circ)$ est un anneau.

2. Soit $f, g : \mathbb{C} \to \mathbb{C}$ définies pour tout $z \in \mathbb{C}$, en notant $a = \mathfrak{Re}(z)$ et $b = \mathfrak{Im}(z)$, par

$$f(a + ib) = a + b + ib, \quad g(a + ib) = a + i(a + b).$$

On vérifie sans problème que f et g sont des endomorphismes de groupe de $\mathbb{C}$. De plus, on a

$$f \circ g(1) = f(1 + i) = 2 + i, \quad g \circ f(1) = g(1) = 1 + i, \quad f \circ g \neq g \circ f.$$

On en déduit que E n'est pas un anneau commutatif.

◇

Remarque 2.8 : Il est important de bien comprendre pourquoi $(E, +, \circ)$ est un anneau alors que $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +\circ)$ n'en est pas un. Cet exemple prouve l'existence d'anneaux non-commutatifs, et fonctionne en remplaçant $\mathbb{C}$ par un groupe abélien[4] quelconque ; en général, $(E, +, \circ)$ n'est pas un anneau commutatif. ◇

2. Structure de corps

Définition 2.9 *Corps*

Soit $(A, +, \times)$ un anneau non-réduit à $\{0\}$. Si tout élément de $A \setminus \{0\}$ est inversible, alors on dit que $(A, +, \times)$ est un *corps*.

4. Il est important que G soit abélien, sans quoi $(E, +)$ n'est pas abélien, et on ne pourra pas avoir d'anneau par définition.

Proposition 2.10 *Corps de référence*
Les ensembles suivants sont des corps commutatifs :

$$(\mathbb{Q},+,\times)\,,\quad (\mathbb{R},+,\times)\,,\quad (\mathbb{C},+,\times)\,.$$

Il est important de noter quels ensembles mentionnés dans la proposition 2.4 sont des corps et lesquels n'en sont pas (et pour quelle raison).

Remarque 2.11 : On retiendra

$$\text{Corps} \Rightarrow \text{Anneau} \Rightarrow \text{Groupe}$$

Attention, on parle ici de la loi $+$ (la première loi de l'anneau ou du corps) : si $(A,+,\times)$ est un anneau, alors $(A,\times)$ n'est pas un groupe [5] ! En effet, 0_A ne peut pas avoir d'inverse pour la loi $\times$ car il est absorbant.

Par définition, on a donc

$$(A,+,\times) \text{ est un corps} \quad \Longleftrightarrow \quad (A^*,\times) \text{ est un groupe},$$

où l'on a noté $A^* = A \setminus \{0_A\}$ (qui est non-vide par hypothèse). ♢

On pourra noter qu'un corps est un cas particulier d'anneau intègre (grâce à l'existence de l'inverse pour les éléments non-nuls).

3. Sous-anneaux et sous-corps

Comme pour les groupes, un sous-anneau d'un anneau A est un anneau inclus dans A héritant de la même structure. Commençons par une remarque importante.

Remarque 2.12 (*Anneau nul*) : Soit A un ensemble réduit à un seul élément, qu'on peut toujours noter 0_A. On définit naturellement

$$0_A + 0_A = 0_A, \quad 0_A \times 0_A = 0_A.$$

Alors l'ensemble $(\{0_A\},+,\times)$ possède une structure d'anneau : on l'appelle *l'anneau nul*. C'est le seul anneau pour lequel $1_A = 0_A$ (le neutre pour $+$ et le neutre pour $\times$ sont égaux). Il a une structure particulière qui nous oblige à faire un peu attention lorsqu'on parle de sous-anneau. ♢

Définition/Proposition 2.13 *Sous-anneau*
Soit $(A,+,\times)$ un anneau, et soit $B \subseteq A$. On dit que B est un *sous-anneau de* A si

(i) $1_A \in B$
(ii) Pour tous $x,y \in B$, $x - y \in B$.
(iii) Pour tous $x,y \in B$, $x \times y \in B$. On dit que B est *stable par* $\times$.

Dans ce cas, $(B,+,\times)$ est un anneau.

Cela revient à vérifier que

$$\forall x,y \in B, \quad 1_A \in B, \quad x+y \in B, \quad x \times y \in B, \quad -x \in B.$$

Puisqu'on veut que B et A aient la même structure, on impose la condition (i) pour ne pas considérer $\{0_A\}$ comme un sous-anneau de A. Les conditions (i) et (ii) entrainent que $(B,+)$ est aussi un sous-groupe de $(A,+)$.

5. Du moins, lorsque A n'est pas l'anneau nul.

Proposition 2.14

Soit $(A, +, \times)$ un anneau. Si B_1 et B_2 sont deux sous-anneaux de A alors $B_1 \cap B_2$ est un sous-anneau de A.

Exercice 2.15 :
On considère l'ensemble $A = \mathbb{Z}[i\sqrt{2}] = \{a + bi\sqrt{2} \in \mathbb{C} / \, (a, b) \in \mathbb{Z}^2\}$.

1. Montrer que A est un anneau. Est-il commutatif ? A est-il un corps ?
2. Soient $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ et $z = a + bi\sqrt{2}$. Montrer que z est inversible dans A si, et seulement si, $|z|^2 = 1$.
   Indication : on pourra déterminer, s'il existe, l'inverse de z dans $\mathbb{C}$.
3. Déterminer les éléments inversibles de A.

Réponse

1. Par définition, $A \subseteq \mathbb{C}$, on va donc montrer que $(A, +, \times)$ est un sous-anneau de $(\mathbb{C}, +, \times)$ (qui est bien un anneau, c'est même un corps). D'abord, $1 \in \mathbb{C}$ car $1 = 1 + 0 \times i\sqrt{2}$ et $1, 0 \in \mathbb{Z}$. Soient $z, z' \in A$. Il existe $a, b, a', b' \in \mathbb{Z}$ tels que $z = a + bi\sqrt{2}$ et $z' = a' + b'i\sqrt{2}$. Alors
$$z - z' = a + bi\sqrt{2} - a' - b'i\sqrt{2} = (a - a') + (b - b')\, i\sqrt{2},$$
et $a - a' \in \mathbb{Z}$ et $b - b' \in \mathbb{Z}$, donc $z - z' \in A$. De plus,
$$zz' = \left(a + bi\sqrt{2}\right)\left(a' + b'i\sqrt{2}\right) = aa' - 2bb' + ab'i\sqrt{2} + a'bi\sqrt{2},$$
et $(aa' - 2bb') \in \mathbb{Z}$ et $(ab' + a'b) \in \mathbb{Z}$, donc $zz' \in A$. Donc A est bien un sous-anneau de $\mathbb{C}$. De plus, $\mathbb{C}$ est un anneau commutatif ($\times$ est commutative sur $\mathbb{C}$) donc A est aussi un anneau commutatif. Enfin, A n'est pas un corps car il possède des éléments non-inversibles. Par exemple, $2 = 2 + 0i\sqrt{2} \in A$. L'inverse de 2 existe dans $\mathbb{C}$ et $2^{-1} = \dfrac{1}{2} \notin A$.
2. On suppose que $(a, b) \neq (0, 0)$, c'est-à-dire que $z \neq 0$. Supposons que z soit inversible dans A, alors il existe $z' = a' + b'i\sqrt{2} \in A$ vérifiant $zz' = 1$. On a alors
$$1 = |zz'|^2 = |z|^2|z'|^2, \quad |z|^2 = a^2 + 2b^2 \in \mathbb{N}, \quad |z'|^2 = (a')^2 + 2\,(b')^2 \in \mathbb{N}.$$
Donc $|z|^2 = |z'|^2 = 1$. Réciproquement, supposons que $|z|^2 = 1$. Or, on sait que $z\overline{z} = |z|^2 = 1$. De plus, $\overline{z} = a - bi\sqrt{2} \in A$. Donc z est inversible et $z^{-1} = \overline{z}$.
3. Soit $z = a + bi\sqrt{2} \in A$. On déduit de la question précédente que
$$z \text{ est inversible dans } A \iff |z|^2 = 1 \iff |z| = 1 \iff z = \pm 1.$$
En effet, si $|a| \geq 2$ alors $|z| \geq 2$ et si $b \neq 0$ alors $|z| \geq \sqrt{2}$. Les éléments inversibles de A sont donc 1 et -1.

◊

Définition/Proposition 2.16 *Sous-corps*

Soit $(\mathbb{L}, +, \times)$ un anneau, et soit $\mathbb{K} \subseteq \mathbb{L}$. On dit que $\mathbb{K}$ est un *sous-corps de* $\mathbb{L}$ si

(i) $1_{\mathbb{L}} \in \mathbb{K}$
(ii) Pour tous $x, y \in \mathbb{K}$, $x - y \in \mathbb{K}$.
(iii) Pour tous $x, y \in \mathbb{K}$, $x \times y^{-1} \in \mathbb{K}$.

Dans ce cas, $(\mathbb{K}, +, \times)$ est un corps.

Cela revient à vérifier que

$$\forall x, y \in \mathbb{K}, \quad 1_{\mathbb{L}} \in \mathbb{K}, \quad x + y \in \mathbb{K}, \quad x \times y \in \mathbb{K}, \quad -x \in \mathbb{K}, \quad x^{-1} \in \mathbb{K}.$$

Proposition 2.17

Soit $\mathbb{L}$ un corps. Si $\mathbb{K}_1$ et $\mathbb{K}_2$ sont deux sous-anneaux de $\mathbb{L}$ alors $\mathbb{K}_1 \cap \mathbb{K}_2$ est un sous-anneau de $\mathbb{L}$.

En fait, l'intersection quelconque (éventuellement infinie) de sous-anneaux ou de sous-corps est encore un sous-anneau ou un sous-corps. En revanche, l'union n'est en général pas un sous-anneau ou un sous-corps.

4. Morphismes d'anneaux et morphismes de corps

Dans le cas des groupes, on a vu qu'un morphisme de groupes est une application entre deux groupes préservant cette structure, c'est-à-dire compatible avec la loi $\star$. Les morphismes d'anneaux et de corps obéissent à la même logique et sont donc compatibles avec les lois $+$ et $\times$.

Définition 2.18 *Morphisme d'anneau et morphisme de corps*

Soient $(A, +, \times)$ et $(B, \oplus, \otimes)$ deux anneaux, et $f : A \to B$. On dit que f est un ***morphisme d'anneaux*** si

(i) $f(1_A) = 1_B$
(ii) Pour tous $x, y \in A$, $f(x + y) = f(x) \oplus f(y)$.
(iii) Pour tous $x, y \in A$, $f(x \times y) = f(x) \otimes f(y)$.

On dira que f est un ***morphisme de corps*** si f est un morphisme d'anneaux entre A et B et si A et B sont des corps.

Pour parler de morphisme (d'anneaux ou de corps), comme dans le cas des groupes, on vérifiera d'abord que $f : A \to B$ et que A et B sont bien des anneaux ou des corps.

Exemple 2.19 :
La conjugaison est un automorphisme de corps de $\mathbb{C}$. En effet, $\mathbb{C}$ est un corps et

$$\overline{1} = 1, \quad \forall x, y \in \mathbb{C}, \quad \overline{x + y} = \overline{x} + \overline{y}, \quad \overline{x \times y} = \overline{x} \times \overline{y}, \quad \overline{\overline{x}} = x.$$

$\diamondsuit$

Attention, l'application nulle n'est pas un morphisme d'anneaux (sauf si B est l'anneau nul). Par contre Id_A est bien un endomorphisme de l'anneau A.

Proposition 2.20

Soit f un morphisme entre les anneaux $(A, +, \times)$ et $(B, \oplus, \otimes)$. Alors f est un morphisme de groupes entre les groupes $(A, +)$ et $(B, \oplus)$. De plus, si $x \in A$ est inversible, alors $f(x)$ est inversible dans B et

$$f(x)^{-1} = f\left(x^{-1}\right).$$

Démonstration : Il est évident que f est un morphisme de groupes lorsqu'on considère A et B comme des groupes. Soit $x \in A$ et supposons que x soit inversible (pour $\times$). Alors on a

$$f(x) \otimes f\left(x^{-1}\right) = f\left(x \times x^{-1}\right) = f(1_A) = 1_B,$$

donc $f(x)$ est inversible et $f(x)^{-1} = f\left(x^{-1}\right)$. $\square$

Il n'est donc pas nécessaire de faire attention au contexte lorsqu'on parle de "morphisme" (cela dépend simplement de la meilleure structure possible dont on peut munir A et B).

⚠ La définition de noyau et d'image reste la même pour les morphismes d'anneaux. Si $f : A \to B$ est un morphisme d'anneaux, alors

$$\ker f = \{x \in A / f(x) = 0_B\}, \quad \operatorname{Im} f = \{y \in B / \exists x \in A, f(x) = y\}.$$

Proposition 2.21

Soit f un morphisme entre les anneaux $(A, +, \times)$ et $(B, \oplus, \otimes)$. Alors

(i) $\ker f$ n'est pas un sous-anneau de A, sauf si B est l'anneau nul.
(ii) $\operatorname{Im}(f)$ est un sous-anneau de B.
(iii) f est injective si, et seulement si, $\ker f = \{0_A\}$.

Démonstration : (i) Si $B \neq \{0_B\}$, alors $f(1_A) = 1_B \neq 0_B$ donc $1_A \notin \ker f$. Donc $\ker f$ n'est pas un sous-anneau de A.
(ii) Par définition, $\operatorname{Im} f \subseteq B$ et $1_B \in \operatorname{Im} f$ car $f(1_A) = 1_B$. De plus, pour tous $y, y' \in \operatorname{Im} f$, il existe $x, x' \in A$ tels que $f(x) = y, f(x') = y'$, et alors

$$y \ominus y' = f(x) \ominus f(x') = f(x - x') \in \operatorname{Im} f, \quad y \otimes y' = f(x) \otimes f(x') = f(x \times x') \in \operatorname{Im} f,$$

donc $\operatorname{Im} f$ est un sous-anneau de B.
(iii) f est un morphisme d'anneaux donc f est un morphisme de groupes, cette propriété est donc évidente.

$\square$

Et si B est un corps, est-ce que $\operatorname{Im} f$ est un sous-corps de B ?

Proposition 2.22

Soient A, B, C trois anneaux. Soient $f : A \to B$ et $g : B \to C$ deux morphismes d'anneaux. Alors

(i) $g \circ f$ est un morphisme entre les anneaux A et B.
(ii) Si f est un isomorphisme, alors f^{-1} est un isomorphisme entre les anneaux B et A.

Démonstration : (i) A et C sont bien des anneaux et $g \circ f : A \to C$. De plus, pour tous $x, x' \in A$, on a

$$\begin{aligned} g \circ f(1_A) &= g(1_B) = 1_C, \\ g \circ f(x + x') &= g(f(x) + f(x')) = g(f(x)) + g(f(x')) = g \circ f(x) + g \circ f(x'), \\ g \circ f(xx') &= g(f(x) \times f(x')) = g(f(x)) \times g(f(x')) = g \circ f(x) \times g \circ f(x'). \end{aligned}$$

donc $g \circ f$ est un morphisme de groupes.

(ii) $f^{-1} : B \to A$ est bien définie car f est bijective, et B et A sont des anneaux. De plus, on sait que f^{-1} est bijective, il reste donc à montrer que c'est un morphisme (d'anneaux). Puisque $f(1_A) = 1_B$, on a $f^{-1}(1_B) = 1_A$. Soient $y, y' \in B$. On sait qu'il existe $x, x' \in A$ tels que $f(x) = y$, $f(x') = y'$, et alors

$$f(x + x') = f(x) + f(x') = y + y', \quad f^{-1}(y) + f^{-1}(y') = x + x' = f^{-1}(y + y'),$$

et

$$f(xx') = f(x) \times f(x') = yy', \quad f^{-1}(y) \times f^{-1}(y') = xx' = f^{-1}(yy'),$$

donc f^{-1} est un isomorphisme d'anneaux.

$\square$

À connaître à la fin du chapitre

Groupes

- Connaître les bases de groupes : règles de calcul, groupes de référence.
- Faire attention à la commutativité.
- Savoir montrer qu'un ensemble est un sous-groupe d'un groupe connu.
- Savoir montrer qu'une application est un morphisme de groupes, et déterminer son noyau ou son image.

Anneaux

- Connaître les bases des anneaux et des corps : règles de calcul, anneaux et corps de référence.
- Faire attention à l'inversibilité.
- Savoir montrer qu'un ensemble est un sous-anneau d'un anneau connu.
- Savoir montrer qu'une application est un morphisme d'anneaux.

Pour aller plus loin

- Espace vectoriel.
- Anneau des matrices.
- Groupe $\mathbb{Z}/n\mathbb{Z}$.

La théorie des groupes est encore un domaine très actif de recherche en mathématiques. Il existe de nombreux types de groupes (groupes de Lie, groupes de Galois, groupes quotients, etc.) qui sont tous très loin de notre niveau actuel.

CHAPITRE 2

ENSEMBLES ORDONNÉS

Ce chapitre, bien que relativement abstrait au début, permet de construire les ensembles de nombres bien connus, de $\mathbb{N}$ à $\mathbb{R}$ en passant par $\mathbb{Z}$ et $\mathbb{Q}$. Leur structure repose de manière fondamentale sur la notion d'ensemble ordonné. Cela nous permettra également de déduire les premières propriétés importantes de ces ensembles de nombres.

I Relation d'ordre

1. Généralités

Définition 1.1

Soit E un ensemble. Une *relation binaire*, ou *relation* est un sous-ensemble $\mathcal{R} \subseteq E \times E$. Pour $(x, y) \in E^2$, on écrira $x\mathcal{R}y$ lorsque $(x, y) \in \mathcal{R}$ et $x\not{\mathcal{R}}y$ sinon.

Une définition équivalente est de voir une relation $\mathcal{R}$ comme une proposition $P(x, y)$ dépendant de deux variables $x, y \in E$; on note alors $x\mathcal{R}y$ si $P(x, y)$ est vraie.

Dans la suite, on oubliera la notion de sous-ensemble de E^2 pour se concentrer exclusivement sur la notation $x\mathcal{R}y$.

Définition 1.2 *Types de relations*

On dit qu'une relation binaire $\mathcal{R}$ est

- *réflexive* si pour tout $x \in E, x\mathcal{R}x$.
- *transitive* si pour tous $x, y, z \in E, (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow (x\mathcal{R}z)$.
- *symétrique* si pour tous $x, y \in E, (x\mathcal{R}y) \Rightarrow (y\mathcal{R}x)$.
- *antisymétrique* si pour tous $x, y \in E, (x\mathcal{R}y \text{ et } y\mathcal{R}x) \Rightarrow (x = y)$.

Exemple 1.3 :
Considérons $E = \mathbb{R}$ et la relation d'inégalité $\mathcal{R} = " \leq "$. Soient $x, y, z \in \mathbb{R}$. Alors

- $\mathcal{R}$ est réflexive, car $x \leq x$.
- $\mathcal{R}$ est transitive, car si $x \leq y$ et $y \leq z$, alors il est clair que $x \leq z$.

- $\mathcal{R}$ est antisymétrique, car si $x \leq y$ et $y \leq x$, alors $x = y$.

$\diamondsuit$

Exemple 1.4 :
Considérons $E = \mathbb{R}$ et la relation $x\mathcal{R}y \iff y = x + 1$. Soient $x, y, z \in \mathbb{R}$. Alors

- $\mathcal{R}$ n'est pas réflexive, car $x \neq x + 1$.
- $\mathcal{R}$ n'est pas transitive, car si $y = x + 1$ et $z = y + 1$, alors $z \neq x + 1$.
- $\mathcal{R}$ n'est pas symétrique, car il est impossible que $x\mathcal{R}y$ et $y\mathcal{R}x$ ($\mathcal{R}$ est donc par contre antisymétrique).

$\diamondsuit$

Exercice 1.5 :
Montrer que si $\mathcal{R}$ est une relation symétrique et antisymétrique, alors

$$\forall (x, y) \in E^2, x\mathcal{R}y \Rightarrow x = y.$$

Quelles sont les relations vérifiant cette propriété ? $\diamondsuit$

2. Relation d'ordre

Définition 1.6 *Ordre*
Soit E un ensemble. Une relation binaire $\mathcal{R}$ est appelée *relation d'ordre*, ou *ordre*, si elle est réflexive, transitive et antisymétrique.

Un *ensemble ordonné* est un couple $(E, \preceq)$ où E est un ensemble et $\preceq$ un ordre sur E.

Dans la suite, pour plus de commodité, on notera les ordres abstraits $\preceq$ au lieu de $\mathcal{R}$.

Exemple 1.7 (*Relations d'ordre fondamentales*) :

- L'ordre usuel $\leq$ sur $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.
- L'inclusion $\subseteq$ sur $\mathscr{P}(E)$.
- La divisibilité $|$ sur $\mathbb{N}$, où, pour tous $p, q \in \mathbb{N}$,

$$p|q \iff \exists k \in \mathbb{N}, pk = q.$$

Montrons que $(\mathscr{P}(E), \subseteq)$ est un ensemble ordonné. Soient $A, B, C \in \mathscr{P}(E)$. Alors

- $\subseteq$ est réflexive, car $A \subseteq A$.
- $\subseteq$ est transitive, car si $A \subseteq B$ et $B \subseteq C$, alors que $A \subseteq C$.
- $\subseteq$ est antisymétrique, car si $A \subseteq B$ et $B \subseteq A$, alors $A = B$.

$\diamondsuit$

Pour tout ensemble ordonné $(E, \preceq)$, on peut définir l'ordre strict par la relation

$$\forall x, y \in E, \quad x \prec y \iff x \preceq y \text{ et } x \neq y,$$

et l'ordre inverse par la relation

$$\forall x, y \in E, \quad x \succeq y \iff y \preceq x.$$

Au sens de la définition 1.6, $\succeq$ est une relation d'ordre, mais $\prec$ n'est pas réflexif.

2.1. Ordre total

Définition 1.8 *Eléments comparables*
Soit $(E, \preceq)$ un ensemble ordonné. Soit $x, y \in E$. On dit que x et y sont ***comparables*** si soit $x \preceq y$, soit $y \prec x$.

Définition 1.9 *Ordre total*
Soit $(E, \preceq)$ un ensemble ordonné. On dit que l'ordre $\preceq$ est ***total*** si tous les éléments de E sont deux à deux comparables. On dit alors que $(E, \preceq)$ est ***totalement ordonné***. Si ce n'est pas le cas, on dit que $\preceq$ est ***partiel*** et que $(E, \preceq)$ est ***partiellement ordonné***.

Exemple 1.10 :

- $(\mathbb{R}, \leq)$ est un ensemble totalement ordonné.
- $(\mathbb{N}, |)$ est partiellement ordonné, car 2 et 3 ne sont pas comparables.
- $(\mathscr{P}(\mathbb{R}), \subseteq)$ est partiellement ordonné, $\{x\}$ et $\{y\}$ n'étant pas comparables dès que $x \neq y$.

$\diamondsuit$

Exercice 1.11 :
Soit $E = \mathcal{F}(\mathbb{R}, \mathbb{R})$ et, $\forall f, g \in E$, on définit $f \preceq g \iff \forall x \in \mathbb{R}, f(x) \leq g(x)$. Montrer que $\preceq$ est un ordre sur E. Est-il total ? $\diamondsuit$

Exemple 1.12 (*Ordres sur* $\mathbb{R}^2$) :
On définit l'ordre produit sur $\mathbb{R}^2$ comme la relation binaire :

$$(x_1, x_2) \preceq_{\mathrm{P}} (y_1, y_2) \iff \begin{cases} x_1 \leq y_1 \\ x_2 \leq y_2 \end{cases} .$$

On définit l'ordre lexicographique sur $\mathbb{R}^2$ comme la relation binaire :

$$(x_1, x_2) \preceq_{\mathrm{L}} (y_1, y_2) \iff \left| \begin{array}{l} x_1 < y_1 \\ x_1 = y_1 \text{ et } x_2 \leq y_2. \end{array} \right. .$$

L'ordre produit est partiel, car $(0, 1)$ et $(1, 0)$ ne sont pas comparables. L'ordre lexicographique est total, mais impose de "donner plus d'importance" à une coordonnée spécifique (ici, la première coordonnée) : il s'agit de l'ordre du dictionnaire. $\diamondsuit$

2.2. Sous-ensembles d'un ensemble ordonné

Dans toute cette section, on considère $(E, \preceq)$ un ensemble ordonné et $A \subseteq E$.

Définition 1.13 *Majorant et minorant*
Soit $m \in E$. On dit que m est un *majorant* de A si, pour tout $x \in A$, $x \preceq m$. On dit que m est un *minorant* de A si, pour tout $x \in A$, $m \preceq x$. On note respectivement $\mathrm{Majo}(A)$ et $\mathrm{Mino}(A)$ les ensembles de majorants et de minorants de A.

A est dite *majorée* (dans E) si elle possède (au moins) un majorant, *minorée* si elle possède un minorant, et *bornée* si elle possède un minorant et un majorant.

Ces définitions coïncident avec les notions usuelles de majoration et de minoration sur $\mathbb{R}$. Notons qu'un majorant ou un minorant doivent être comparables à tous les éléments de A.

Exemple 1.14 :
On considère l'ensemble ordonné $(\mathbb{R}, \leq)$ et $A =]2,3]$. Alors $\text{Mino}(A) =]-\infty, 2]$ et $\text{Majo}(A) = [3, +\infty[$. ♢

Définition 1.15 *Maximum et minimum*

On appelle *maximum* (ou *plus grand élément*) de A tout élément m de A tel que, pour tout $x \in A, x \preceq m$.
On appelle *minimum* (ou *plus petit élément*) de A tout élément m de A tel que, pour tout $x \in A, m \preceq x$.

On notera qu'un maximum [1] (resp. minimum) de A est un majorant (resp. minorant) de A qui appartient à A.

Proposition 1.16 *Unicité du maximum et du minimum*

(i) Si A admet un maximum, alors il est unique ; on le note alors $\max(A)$.
(ii) Si A admet un minimum, alors il est unique ; on le note alors $\min(A)$.

Démonstration : Supposons que A admette au moins un maximum. Soient m et m' deux maxima de A. On a $m \in A$ et $m' \in \text{Majo}(A)$, donc $m \preceq m'$. Par symétrie des hypothèses, $m' \preceq m$ et donc, par antisymétrie de la relation d'ordre, $m = m'$. La démonstration de (ii) est identique. □

Exemple 1.17 :
Dans le cadre de l'exemple précédent, il est clair que $\max A = 3$. Supposons que A admette un minimum qu'on note $\min A = a$. Alors $a > 2$ et, pour tout $\varepsilon \in]0, a-2[$, $2 < a - \varepsilon < a$ donc $a - \varepsilon \in A$, ce qui est impossible. Donc A n'admet pas de minimum ♢

Exemple 1.18 :
Soit E un ensemble à quatre éléments distincts tel que $E = \{a,b,c,d\}$, et considérons l'ensemble ordonné $(\mathscr{P}(E), \subseteq)$ et $\mathcal{A} = \{\{a,b\},\{b\},\{a,c\}\}$. Alors

- $\text{Mino}(\mathcal{A}) = \{\emptyset\}$.
- $\text{Majo}(\mathcal{A}) = \{\{a,b,c\},\{a,b,c,d\}\}$.

$\mathcal{A}$ est donc bornée, mais ne possède ni minimum ni maximum. ♢

Définition 1.19

On dit que A admet une *borne supérieure* (dans E) si $\text{Majo}(A)$ admet un minimum. Dans ce cas, cet élément est appelé borne supérieure de A et est noté $\sup(A)$. On dit que A admet une *borne inférieure* (dans E) si $\text{Mino}(A)$ admet un maximum. Dans ce cas, cet élément est appelé borne inférieure de A et est noté $\inf(A)$.

Sous réserve d'existence, on peut donc écrire

$$\sup(A) = \min(\text{Majo}(A)) = \min\{m \in E | \forall x \in A, x \preceq m\},$$
$$\inf(A) = \max(\text{Mino}(A)) = \max\{m \in E | \forall x \in A, m \preceq x\}.$$

On en déduit immédiatement l'unicité de la borne inférieure et la borne supérieure (si elles existent).

Exemple 1.20 :
Dans le cadre de l'exemple précédent, on a vu que A n'admettait pas de minimum. En revanche, il admet une borne inférieure et $\inf(A) = 2$. En effet, il est clair que $2 \in \text{Mino}(A)$. De plus, supposons qu'il existe

1. Le pluriel de *maximum* est *maxima* (on emploie souvent, à tort, *maximums*). Idem pour *minimum*.

$m \in \text{Mino}(A)$ tel que $m > 2$. Alors $m \in A$, ce qui est impossible car on a vu que $B \cap \text{Mino}(A) = \emptyset$ (ce qui est équivalent à dire que B ne possède pas de minimum). Donc $\inf(A) = \max(\text{Mino}(A)) = 2$. ♢

On retiendra qu'un ensemble n'a pas forcément de maximum ou de minimum, de borne supérieure ou de borne inférieure.

Proposition 1.21 *Cas d'égalité*

(i) Si A admet un maximum, alors A admet une borne supérieure et $\sup A = \max A$.
(ii) Si A admet un minimum, alors A admet une borne inférieure et $\sup A = \max A$.

Démonstration : On traite juste (i). Pour tout $m \in \text{Majo}(A), \max A \preceq m$ car $\max A \in A$ et $\max A \in \text{Majo}(A)$. Donc $\max A = \min \text{Majo}(A) = \sup A$. □

Proposition 1.22 *Cas des ensembles inclus*

Soit $B \subseteq E$ tel que $A \subseteq B$. Sous réserve d'existence, on a

(i) $\max A \preceq \max B$.
(ii) $\min B \preceq \min A$.
(iii) $\sup A \preceq \sup B$.
(iv) $\inf B \preceq \inf A$.

Démonstration : Démontrons (i). Par définition, $\max A \in A \subseteq B$ et donc $\max A \preceq \max B$. La démonstration de (ii) est similaire pour les minima. Pour (iii), on notera que $\text{Majo}(B) \subseteq \text{Majo}(A)$ et que $\sup A = \min \text{Majo}(A), \sup B = \min \text{Majo}(B)$ et (iv) se traite de la même façon. □

2.3. Applications monotones

Définition 1.23

Soit $(A, \preceq_A)$ et $(B, \preceq_B)$ deux ensembles ordonnés et une application $f : A \mapsto B$. On dit que

- f est *croissante* si $\forall a, a' \in A, a \preceq_A a' \Rightarrow f(a) \preceq_B f(a')$.
- f est *strictement croissante* si $\forall a, a' \in A, a \prec_A a' \Rightarrow f(a) \prec_B f(a')$.
- f est *décroissante* si $\forall a, a' \in A, a \preceq_A a' \Rightarrow f(a') \preceq_B f(a)$.
- f est *strictement décroissante* si $\forall a, a' \in A, a \prec_A a' \Rightarrow f(a') \prec_B f(a)$.
- f est *monotone* (resp. *strictement monotone*) si f est croissante ou décroissante (resp. strictement croissante ou strictement décroissante).

Exercice 1.24 :
Soit E un ensemble et $\mathcal{P} = \{A \in \mathscr{P}(E) / |A| < +\infty\}$. Montrer que l'application

$$f : \begin{array}{ccc} \mathcal{P} & \to & \mathbb{N} \\ A & \mapsto & |A| \end{array}$$

est croissante. Est-elle strictement croissante ? ♢

3. Relation d'équivalence

Définition 1.25 *Relation d'équivalence*
Une relation binaire $\mathcal{R}$ est appelée *relation d'équivalence* si elle est réflexive, transitive et symétrique.

Exemple 1.26 :

- Sur $E = \mathbb{R}$, définissons $x\mathcal{R}y \Leftrightarrow \cos(x) = \cos(y)$. La relation $\mathcal{R}$ est une relation d'équivalence.
- Sur $E = \mathbb{Z}$, définissons $n\mathcal{R}m \Leftrightarrow n - m$ est pair. La relation $\mathcal{R}$ est une relation d'équivalence.

$\diamondsuit$

II Entiers naturels, principe de récurrence

1. Ensemble des entiers naturels

Définition/Théorème 2.1 *Ensemble* $\mathbb{N}$ *- Admis*
Il existe un ensemble $\mathbb{N}$, appelé *ensemble des entiers naturels*, tel que

- $\mathbb{N}$ est non-vide et muni d'une relation d'ordre $\leq$.
- $\mathbb{N}$ n'est pas majoré.
- Toute partie non-vide de $\mathbb{N}$ admet un minimum.
- Toute partie non-vide et majorée de $\mathbb{N}$ admet un maximum.

On munit $\mathbb{N}$ des opérations $+$ et $\times$, telles que

- $+$ et $\times$ sont compatibles avec $\leq$:

$$\forall n, p, q \in \mathbb{N}, \quad \left\{ \begin{array}{ccc} p \leq q & \Rightarrow & p + n \leq q + n \\ 0 \leq p, 0 \leq q & \Rightarrow & 0 \leq pq \end{array} \right. .$$

- $+$ et $\times$ sont associatives, commutatives, et $\times$ est distributive par rapport à $+$.
- $+$ admet un élément neutre, noté 0.
- Pour tous $n, p, q \in \mathbb{N}, (x + n = y + n) \Rightarrow (x = y)$.
- $\times$ admet un élément neutre, noté 1.
- Pour tous $n, p, q \in \mathbb{N}, (x \times n = y \times n$ et $n \neq 0) \Rightarrow (x = y)$.

Dans la suite, on pourra donc manipuler les entiers de $\mathbb{N}$ comme on en avait l'habitude. On notera, pour $p, q \in \mathbb{N}$,

$$[\![p, q]\!] = \left\{ \begin{array}{ll} \{k \in \mathbb{N} / p \leq k \leq q\} & \text{si } p \leq q \\ \emptyset & \text{si } p > q \end{array} \right. .$$

Corollaire 2.2
$(\mathbb{N}, \leq)$ est totalement ordonné, et $\mathbb{N}$ n'admet pas de maximum.

Démonstration : Soient $p, q \in \mathbb{N}$. Alors $\{p, q\}$ est minorée et admet donc un minimum, par exemple p. Alors $p \leq q$.

$\mathbb{N}$ n'étant pas majoré, il n'admet pas de maximum. $\square$

2. Principe de récurrence

2.1. Récurrence simple

On rappelle qu'un prédicat P sur $\mathbb{N}$ est une proposition $P(n)$ dépendant de l'entier $n \in \mathbb{N}$.

Théorème 2.3 *Récurrence*
Soit P un prédicat sur $\mathbb{N}$. On a alors équivalence entre

(i) $\forall n \in \mathbb{N}, P(n)$.
(ii) $P(0)$ et $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$.

Démonstration : $\boxed{(i) \Rightarrow (ii)}$ Supposons que $P(n)$ pour tout $n \in \mathbb{N}$. Alors en particulier $P(0)$. De plus, pour tout $n \in \mathbb{N}$, on a $P(n)$ et $P(n+1)$, donc $P(n) \Rightarrow P(n+1)$.

$\boxed{(i) \Rightarrow (ii)}$ Supposons que $P(0)$ et $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$. Notons

$$A = \{n \in \mathbb{N} / \neg P(n)\}$$

et supposons par l'absurde que $A \neq \emptyset$. Alors A admet un minimum noté $\min A = n_0$. Puisque $P(0), n_0 > 0$. Par définition du minimum, $n_0 - 1 \notin A$ donc $P(n_0 - 1)$. Par hypothèse, il s'en suit que $P(n_0)$, ce qui est impossible. Donc $A = \emptyset$, ce qui entraîne (i). $\square$

Pour rappel, une preuve par récurrence nécessite quatre étapes.

1. Introduction. On énonce clairement quelle propriété $P(n)$ on souhaite démontrer par récurrence (et le type de récurrence).
2. Initialisation. On démontre $P(0)$.
3. Hérédité. On suppose $P(n)$ pour un certain rang $n \in \mathbb{N}$ et on montre $P(n+1)$.
4. Conclusion. On annonce que le raisonnement est terminé et qu'on a démontré $P(n)$ pour tout $n \in \mathbb{N}$.

Exemple 2.4 :
Montrons par récurrence simple que, pour tout $n \in \mathbb{N}$, on a

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

$\boxed{\text{Initialisation}}$ On a

$$\sum_{k=0}^{0} k = 0 = \frac{0 \times 1}{2},$$

donc la propriété est vraie au rang 0.

$\boxed{\text{Hérédité}}$ Soit $n \in \mathbb{N}$ et supposons que la propriété est vraie au rang n. Alors

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

La propriété est donc vraie au rang $n+1$.

Conclusion On a donc démontré par récurrence que

$$\forall n \in \mathbb{N}, \sum_{k=0}^{n} k = \frac{n(n+1)}{2}.$$

♢

2.2. Autres types de récurrence

Dans toute cette partie, on considère P un prédicat sur $\mathbb{N}$ et $n_0 \in \mathbb{N}$. Etudions quelques corollaires du principe de récurrence simple.

Corollaire 2.5 *Récurrence "retardée"*
On a équivalence entre

(i) $\forall n \geq n_0, P(n)$.
(ii) $P(n_0)$ et $\forall n \geq n_0, P(n) \Rightarrow P(n+1)$.

Démonstration : Le résultat étant évident si $n_0 = 0$, on suppose $n_0 > 0$. On applique alors le théorème de récurrence simple à la propriété

$$Q(n): \quad P(n+n_0).$$

Variante : on l'applique à la propriété

$$Q(n): \quad n < n_0 \text{ ou } P(n).$$

□

Exercice 2.6 :
Montrer que pour tout entier $n \geq 6, 6n+7 \leq 2^n$. ♢

Parfois, on a besoin de supposer un peu plus que $P(n)$ pour démontrer la propriété au rang suivant. C'est par exemple le cas lorsqu'on a une relation entre $P(n), P(n+1)$ et $P(n+2)$.

Corollaire 2.7 *Récurrence double*
On a équivalence entre

(i) $\forall n \geq n_0, P(n)$.
(ii) $P(n_0), P(n_0+1)$ et $\forall n \geq n_0, (P(n) \text{ et } P(n+1)) \Rightarrow P(n+2)$.

Démonstration : On applique le théorème de récurrence (simple ou "retardée") à la propriété

$$Q(n): \quad P(n) \text{ et } P(n+1).$$

□

Exemple 2.8 :
Soit (u_n) la suite définie par

$$u_0 = u_1 = 3, \quad u_{n+2} = u_{n+1} + 2u_n.$$

Montrons par récurrence double que, pour tout $n \in \mathbb{N}, u_n = 2^{n+1} + (-1)^n$.

$\boxed{\text{Initialisation}}$ On a

$$u_0 = 3 = 2^1 - 1, \quad u_1 = 3 = 2^2 - 1.$$

donc la propriété est vraie au rangs 0 et 1.

$\boxed{\text{Hérédité}}$ Soit $n \in \mathbb{N}$ et supposons que la propriété est vraie au rangs n et $n+1$. Alors

$$\begin{aligned} u_{n+2} &= u_{n+1} + 2u_n = 2^{n+2} + (-1)^{n+1} + 2\left(2^{n+1} + (-1)^n\right) \\ &= 2^{n+2} + 2^{n+2} + (-1)^n = 2^{n+3} + (-1)^{n+2}. \end{aligned}$$

La propriété est donc vraie au rang $n+2$.

$\boxed{\text{Conclusion}}$ On a donc démontré par récurrence que $\forall n \in \mathbb{N}, u_n = 2^{n+1} + (-1)^n$. ♢

On peut généraliser ce principe à des récurrences d'ordre $p \geq 1$.

Corollaire 2.9 *Récurrence d'ordre k*

Soit $p \in \mathbb{N}^*$. On a équivalence entre

(i) $\forall n \geq n_0, P(n)$.
(ii) $\forall k \in [\![n_0, n_0 + p - 1]\!], P(k)$ et $\forall n \geq n_0, (\forall k \in [\![0, p-1]\!], P(n+k)) \Rightarrow P(n+p)$.

On notera que l'initialisation d'une récurrence double comporte *deux* étapes : la vérification de $P(n_0)$ et celle de $P(n_0 + 1)$. Plus généralement, l'initialisation d'une récurrence d'ordre p comporte p étapes.

Corollaire 2.10 *Récurrence forte*

On a équivalence entre

(i) $\forall n \geq n_0, P(n)$.
(ii) $P(n_0)$ et $\forall n \geq n_0, (\forall k \in [\![n_0, n]\!], P(k)) \Rightarrow P(n+1)$.

Démonstration : On applique le théorème de récurrence à la propriété

$$Q(n): \quad \forall k \in [\![n_0, n]\!], P(k).$$

□

Exercice 2.11 :
Soit (u_n) la suite définie par

$$u_0 \in \mathbb{R}, \quad \forall n \in \mathbb{N}, u_{n+1} = \sum_{k=0}^{n} u_k.$$

Montrer que, pour tout $n \in \mathbb{N}^*, u_n = 2^{n-1} u_0$. ♢

Corollaire 2.12 *Récurrence finie et récurrence descendante*
Soit $n_1 \geq n_0$. On a équivalence entre

(i) $\forall n \in [\![n_0, n_1]\!], P(n)$.
(ii) $P(n_0)$ et $\forall n \in [\![n_0, n_1 - 1]\!], P(n) \Rightarrow P(n+1)$.
(iii) $P(n_1)$ et $\forall n \in [\![n_0 + 1, n_1]\!], P(n) \Rightarrow P(n-1)$.

Démonstration : Il est clair que $(i) \Rightarrow (ii)$ et $(i) \Rightarrow (iii)$. Pour démontrer $(ii) \Rightarrow (i)$, on applique le théorème de récurrence simple à la propriété

$$Q(n): \quad P(n) \text{ ou } n < n_0 \text{ ou } n \geq n_1.$$

Pour démontrer $(iii) \Rightarrow (i)$, on applique le théorème de récurrence finie à la propriété

$$Q(n): \quad P(n_1 - n).$$

□

⚠ Une récurrence permet de prouver un résultat proposé dans l'énoncé ("Montrer que..."), mais ne permet pas de l'établir si l'on n'a aucune idée a priori ("Calculer...").

III Entiers relatifs, nombres rationnels

1. Anneau des entiers relatifs

Définition/Théorème 3.1 *Ensemble $\mathbb{Z}$ - Admis*
Il existe un anneau $(\mathbb{Z}, +, \times)$, appelé *ensemble des entiers relatifs*, tel que

- $\mathbb{N}$ est inclus dans $\mathbb{Z}$.
- $\mathbb{Z}$ est commutatif et intègre.
- Les lois $+$ et $\times$ prolongent celles de $\mathbb{N}$.

On munit $\mathbb{Z}$ d'une relation d'ordre $\leq$ prolongeant celle de $\mathbb{N}$ et telle que

- $+$ et $\times$ sont compatibles avec $\leq$:

$$\forall n, p, q \in \mathbb{Z}, \quad \begin{cases} p \leq q & \Rightarrow \quad p + n \leq q + n \\ 0 \leq p, 0 \leq q & \Rightarrow \quad 0 \leq pq \end{cases}.$$

- Pour tous $n \in \mathbb{N}, p, q \in \mathbb{Z}, (p \leq q) \Rightarrow (np \leq nq)$.
- $\mathbb{N} = \{z \in \mathbb{Z} / 0 \leq z\}$ et $\mathbb{Z} = \mathbb{N} \sqcup \{-n / n \in \mathbb{N}^*\} = \mathbb{N} \sqcup \{z \in \mathbb{Z} / z < 0\}$.

Dans la suite, on pourra maintenant manipuler les entiers positifs ou négatifs comme on en a l'habitude. On en profite pour étendre la notation $[\![p, q]\!]$ au cas où $p, q \in \mathbb{Z}$.

Théorème 3.2 *Maximum et minimum dans $\mathbb{Z}$*

(i) Toute partie non-vide et minorée de $\mathbb{Z}$ admet un minimum.
(ii) Toute partie non-vide et majorée de $\mathbb{Z}$ admet un maximum.

Démonstration : Soit $A \subseteq \mathbb{Z}$, qu'on suppose non-vide et minorée. Soit $m \in \mathrm{Mino}\,(A)$ et considérons $A' = \{z - m/z \in A\}$. Alors, il est clair que $A' \subseteq \mathbb{N}$ et A' est non-vide, donc admet un minimum a'. Alors $a' + m \in A \cap \mathrm{Mino}\,(A)$ donc $\min A = a' + m$. D'où (i).

Supposons $A \subseteq Z$ non-vide et minorée. On définit cette fois-ci $A' = \{-z/z \in A\}$. Alors A' est une partie non-vide et minorée de $\mathbb{Z}$, donc $\min A' = a'$. On peut alors vérifier que $\max A = -a'$, d'où (ii). □

Corollaire 3.3

$(\mathbb{Z}, \leq)$ est totalement ordonné.

Démonstration : Soient $p, q \in \mathbb{Z}$. On distingue trois cas :

- si $p, q \in \mathbb{N}$, p et q sont comparables car $(\mathbb{N}, \leq)$ est totalement ordonné.
- si $p < 0, q < 0$ alors $\{p, q\}$ est une partie non-vide et majorée de $\mathbb{Z}$, et admet donc un maximum.
- si $p < 0 \leq q$, alors par transitivité $p \leq q$ (le cas $q < 0 \leq p$ étant traité de manière identique).

□

Théorème 3.4 *Caractérisation des ensembles finis de* $\mathbb{Z}$

Soit A une partie non-vide de $\mathbb{Z}$. Alors

$$|A| < +\infty \iff A \text{ est bornée.}$$

⚠ La notation $|A| < +\infty$ ou $\#A < +\infty$ est un abus de notation signifiant "A est un ensemble fini".

Démonstration : $\boxed{\Rightarrow}$ Notons $n = |A|$. Alors $A = \{z_1, \dots z_n\}$ et, puisque $\mathbb{Z}$ est totalement ordonné, on peut supposer que

$$z_1 < z_2 < \cdots < z_n.$$

Alors $\min A = z_1, \max A = z_n$ donc A est minorée et majorée (donc bornée).

$\boxed{\Leftarrow}$ Soit $(a, b) \in \mathrm{Mino}\,(A) \times \mathrm{Majo}\,(A)$. Donc tout $z \in A$ vérifie $a \leq z \leq b$, donc $z \in [\![a, b]\!]$, donc $A \subseteq [\![a, b]\!]$. Par croissance de $A \mapsto |A|$, il s'en suit que

$$|A| \leq a - b + 1 < +\infty.$$

□

2. Corps des nombres rationnels

Définition 3.5 *Ensemble* $\mathbb{Q}$

On appelle *ensemble des nombres rationnels* l'ensemble

$$\mathbb{Q} = \left\{ \frac{p}{q}, (p, q) \in \mathbb{Z} \times \mathbb{N}^* \right\}.$$

On munit $\mathbb{Q}$ des lois $+$ et $\times$ usuelles et de la relation d'ordre $\leq$ qui prolongent celles de $\mathbb{Z}$, où

$$\forall (p_1, q_1), (p_2, q_2) \in \mathbb{Z} \times \mathbb{N}^*, \quad \frac{p_1}{q_1} \leq \frac{p_2}{q_2} \iff p_1 q_2 \leq p_2 q_1.$$

Théorème 3.6 *Structure de $\mathbb{Q}$ - Admis*

$(\mathbb{Q}, +, \times)$ est un corps commutatif et $(Q, \leq)$ est totalement ordonné.

IV Nombres réels

1. Corps des nombres réels

Définition/Théorème 4.1 *Ensemble $\mathbb{R}$ - Admis*

Il existe un corps commutatif $(\mathbb{R}, +, \times)$, appelé *ensemble des nombres réels*, tel que

- $\mathbb{Q}$ est inclus dans $\mathbb{R}$.
- Les lois $+$ et $\times$ prolongent celles de $\mathbb{Q}$.

On munit $\mathbb{R}$ d'une relation d'ordre $\leq$ prolongeant celle de $\mathbb{Q}$ et telle que

- $+$ et $\times$ sont compatibles avec $\leq$.
- $(\mathbb{R}, \leq)$ vérifie la propriété de la borne supérieure : toute partie non-vide et majorée de $\mathbb{R}$ admet une borne supérieure.

On appelle *nombre irrationnel* tout élément de $\mathbb{R} \setminus \mathbb{Q}$.

On notera que $(\mathbb{Q}, \leq)$ ne vérifie pas ce théorème de la borne supérieure. En effet, $\{x \in \mathbb{Q} / x^2 \leq 2\}$ n'admet pas de borne supérieure (dans $\mathbb{Q}$).

2. Borne supérieure et borne supérieure dans $\mathbb{R}$

Pour rappel, si $(E, \preceq)$ est un ensemble ordonné et $A \subseteq E$, alors la borne supérieure de A est le minimum des majorants de A et on a

$$\sup(A) = \min(\mathrm{Majo}(A)) = \min\{m \in E / \forall x \in A, x \preceq m\}.$$

De même, sous réserve d'existence,

$$\inf(A) = \max(\mathrm{Mino}(A)) = \max\{m \in E / \forall x \in A, x \succeq m\}.$$

Enfin, on rappelle que $\mathbb{R}$ vérifie le théorème suivant.

Théorème 4.2 *Propriété de la borne supérieure*

Toute partie non-vide et majorée de $\mathbb{R}$ admet une borne supérieure.

Corollaire 4.3 *Propriété de la borne inférieure*
Toute partie non-vide et minorée de $\mathbb{R}$ admet une borne inférieure.

Démonstration : Soit $A \subseteq \mathbb{R}$ une partie non-vide admettant un minorant $m \in \text{Mino}(A)$. Considérons $A' = \{-x \in \mathbb{R}/x \in A\}$. Alors A' est non-vide et majorée par $-m$, elle admet donc une borne supérieure. Notons $a' = \sup A'$ et montrons que $a = -a'$ est la borne supérieure de A. Pour tout $x \in A$, puisque $a' = \sup A'$, on a

$$-x \leq a', \quad x \geq -a' = a$$

donc $a \in \text{Mino}(A)$. Maintenant, pour tout $m \in \text{Mino}(A)$, $-m \in \text{Majo}(A')$

$$-m \geq a', \quad m \leq a.$$

Donc $a = \max \text{Mino}(A) = \inf(A)$. $\square$

Proposition 4.4 *Caractérisation*
Soit A une partie non-vide et majorée de $\mathbb{R}$. On a alors équivalence entre :

(i) $M = \sup(A)$.
(ii) M majore A et

$$\forall \varepsilon > 0, \exists x \in A, M - \varepsilon < x \leq M.$$

On notera que l'inégalité stricte $M - \varepsilon < x$ peut-être changée en inégalité large sans problème. En revanche, il n'est pas question de transformer $x \leq M$ en $x < M$. Pour s'en convaincre, considérer $A = \{1, 2\}$ et $\varepsilon = 1/2$.

Démonstration : $\boxed{(i) \Rightarrow (ii)}$ Par définition, $M \in \text{Majo}(A)$. D'autre part, soit $\varepsilon > 0$. Alors $M - \varepsilon < M$ donc $M - \varepsilon$ n'est pas un majorant de A. Autrement dit, il existe $x \in A$ tel que $M - \varepsilon < x$ et $x \leq M$.

$\boxed{(ii) \Rightarrow (i)}$ Soit $M' \in \text{Majo}(A)$. Supposons par l'absurde que $M' < M$ et notons $\varepsilon = M - M'$. On peut donc trouver $x \in A$ tel que

$$M' = M - \varepsilon < x \leq M,$$

ce qui est impossible. Donc $M \leq M'$ et $M = \min(Majo(A)) = \sup(A)$. $\square$

Proposition 4.5 *Caractérisation*
Soit A une partie non-vide et minorée de $\mathbb{R}$. On a alors équivalence entre :

(i) $m = \inf(A)$.
(ii) m minore A et

$$\forall \varepsilon > 0, \exists x \in A, m \leq x < m + \varepsilon.$$

Démonstration : On applique la propriété précédente à $\{-x/x \in A\}$. □

Ces caractérisations de la borne supérieure et de la borne supérieure sont fondamentales. On verra la caractérisation séquentielle au prochain chapitre.

3. Valeur absolue

Définition 4.6 *Valeur absolue*
Soit $x \in \mathbb{R}$. On appelle *valeur absolue* de x le nombre réel positif $\max\{-x, x\}$.

Proposition 4.7
Soient $x, y \in \mathbb{R}$. Alors

(i) $|-x| = |x|$.
(ii) $x \leq |x|$.
(iii) $|x| = 0 \iff x = 0$.
(iv) $|x \times y| = |x| \times |y|$.
(v) Si $x \neq 0$, $|x^{-1}| = |x|^{-1}$.

Proposition 4.8 *Inégalité triangulaire*
Soient $x, y, z \in \mathbb{R}$. Alors

(i) $|x + y| \leq |x| + |y|$ avec égalité si, et seulement si, x et y ont même signe.
(ii) $|x - y| \leq |x - z| + |z - y|$ avec égalité ssi, $x \leq z \leq y$ ou $y \leq z \leq x$.

Démonstration : $\boxed{(i)}$ On a

$$\begin{aligned} |x+y|^2 &= (x+y)^2 = x^2 + y^2 + 2xy = |x|^2 + |y|^2 + 2xy \qquad (\text{car } z^2 = |z|^2) \\ &\leq |x|^2 + |y|^2 + 2|xy| = |x|^2 + |y|^2 + 2|x||y| = (|x| + |y|)^2 \end{aligned}$$

Par croissance de la fonction $x \mapsto \sqrt{x}$ sur $\mathbb{R}_+$, on conclut à l'inégalité (i). En reprenant le calcul précédent, on voit que l'inégalité se transforme en égalité dès que $xy = |xy|$, c'est-à-dire $xy \geq 0$, ou encore x et y ont même signe.

$\boxed{(ii)}$ Il suffit d'appliquer l'inégalité (i) à $x - z$ et $z - y$. □

Il convient d'interpréter cette inégalité géométriquement : le plus court chemin pour aller de x à y est en ligne droite, et non en faisant un détour par z.

Corollaire 4.9
Soient $x, y \in \mathbb{R}$. Alors

(i) $|x| - |y| \leq |x - y|$.
(ii) $\big||x| - |y|\big| \leq |x + y|$.

Démonstration : $\boxed{(i)}$ On applique l'inégalité (i) du théorème précédent à $x-y$ et y.

$\boxed{(ii)}$ On applique l'inégalité (i) à x et $-y$. Alors

$$|x|-|y| = |x| - |-y| \leq |x+y|.$$

Par symétrie des hypothèses, on a aussi $|y|-|x| \leq |x+y|$ et on en déduit (ii). □

4. Partie entière

Définition/Proposition 4.10 *Partie entière*

Soit $x \in \mathbb{R}$. Il existe un unique $E(x) \in \mathbb{Z}$ tel que

$$E(x) \leq x < E(x)+1.$$

Cet entier relatif $E(x)$ est appelé *partie entière* de x.

D'autres notations usuelles pour la partie entière : $[x]$ ou $\lfloor x \rfloor$.

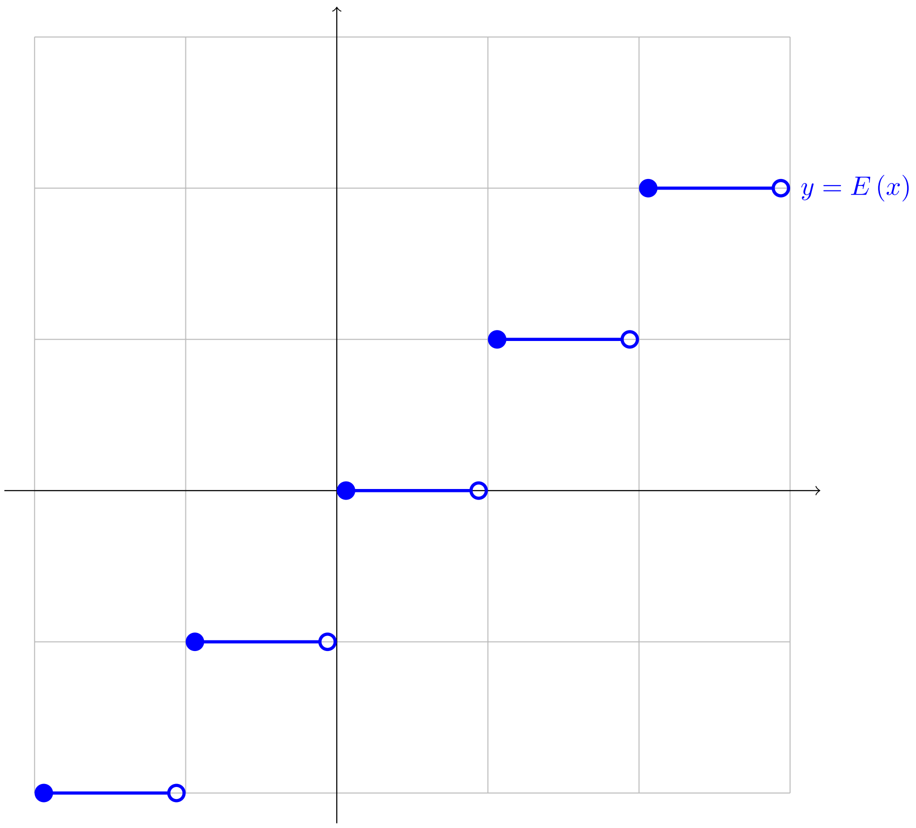
Démonstration : Considérons $A = \{n \in \mathbb{Z}/n \leq x\}$. Alors A est une partie non-vide et majorée de $\mathbb{Z}$, et admet donc un maximum, qu'on note naturellement $E(x)$. Par définition, $E(x)+1 \notin A$ et donc

$$E(x) \leq A < E(x)+1.$$

□

On notera que $E(x)$ est l'entier immédiatement inférieur à x. Donc

$$E(3,1) = 3, \quad E(-3,1) = -4.$$



Proposition 4.11

(i) E est croissante sur $\mathbb{R}$.

(ii) Pour tout $x \in \mathbb{R}$, $E(x) = \max\{n \in \mathbb{Z}/n \leq x\}$.

(iii) Pour tous $x \in \mathbb{R}$ et $n \in \mathbb{N}$, $E(n + x) = n + E(x)$.

Démonstration : $\boxed{(i)}$ Soient $x, y \in \mathbb{R}$ tels que $x \leq y$. Alors $E(x) \leq x \leq y$ et, puisque $E(y) = \{n \in \mathbb{Z}/n \leq y\}$, $E(x) \leq E(y)$.

$\boxed{(ii)}$ Déjà vu dans la preuve de l'existence et de l'unicité de $E(x)$.

$\boxed{(iii)}$ On a $E(x) \leq x < E(x) + 1$ donc $n + E(x) \leq n + x < n + E(x) + 1$. On en déduit que $E(n + x) = n + E(x)$. □

Exemple 4.12 :
Montrons que, pour tous $x, y \in \mathbb{R}$,

$$E(x) + E(y) \leq E(x + y) \leq E(x) + E(y) + 1.$$

$\boxed{E(x) + E(y) \leq E(x + y)}$ $E(x) \leq x, E(y) \leq y$ donc $E(x) + E(y) \leq x + y$ donc $E(x) + E(y) \leq E(x + y)$.

$\boxed{E(x + y) \leq E(x) + E(y) + 1}$ On a

$$\begin{aligned} E(x + y) &= E(E(x) + E(y) + (x - E(x)) + (y - E(y))) \\ &= E(x) + E(y) + E((x - E(x)) + (y - E(y))) \\ &\leq E(x) + E(y) + 1 \end{aligned}$$

car $(x - E(x)) + (y - E(y)) < 2$. ◇

5. Intervalles

Définition 4.13 *Ensemble* $\overline{\mathbb{R}}$

On appelle *droite numérique achevée* l'ensemble $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$, où $+\infty$ et $-\infty$ sont deux symboles, non-réels, tels que $\max \overline{\mathbb{R}} = +\infty$ et $\min \overline{\mathbb{R}} = -\infty$. On note alors

$$\forall x \in \mathbb{R}, -\infty < x < +\infty, \quad \overline{\mathbb{R}} = [-\infty, +\infty].$$

On munit $\overline{\mathbb{R}}$ de $+$ et $\times$ qui sont commutatives et prolongent l'addition et la multiplication sur $\mathbb{R}$ de manière usuelle (lorsqu'on calcule les limites) avec les trois formes indéterminées suivantes :

$$(+\infty) + (-\infty), \quad (+\infty) \times 0, \quad (-\infty) \times 0.$$

On munit enfin $\overline{\mathbb{R}}$ d'un ordre (total) $\leq$ qui prolonge celui de $\mathbb{R}$.

Introduire la droite numérique achevée permettra de parler plus tard de limites dans $\overline{\mathbb{R}}$, c'est-à-dire de limites finies ou infinies.

Définition/Proposition 4.14 *Intervalles - Admis*

Soit $I \subseteq \overline{\mathbb{R}}$. On dit que I est un *intervalle* de $\overline{\mathbb{R}}$ si, pour tous $x, y \in I$ tels que $x \leq y, [x, y] \subseteq I$. I est un intervalle si, et seulement si, il existe $a, b \in \overline{\mathbb{R}}$ tels que

$$I = \begin{cases} [a,b] & = \{x \in \overline{\mathbb{R}} / a \leq x \leq b\} \\ [a,b[& = \{x \in \overline{\mathbb{R}} / a \leq x < b\} \\ ]a,b] & = \{x \in \overline{\mathbb{R}} / a < x \leq b\} \\ ]a,b[& = \{x \in \overline{\mathbb{R}} / a < x < b\} \end{cases}.$$

Les intervalles de $\mathbb{R}$ sont définis de la même manière, en excluant les cas $[-\infty, b]$, $[-\infty, b[$, $[a, +\infty]$ et $]a, +\infty]$.

6. Densité

Définition 4.15 *Densité*

Soit $A \subseteq \mathbb{R}$. On dit que A est dense dans $\mathbb{R}$ si,

$$\forall x, y \in \mathbb{R}, x < y, \exists a \in A, x < a < y.$$

Proposition 4.16

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

Démonstration : Soient $x, y \in \mathbb{R}, x < y$.

$\boxed{\text{Densité de } \mathbb{Q}}$ Idée : prendre q suffisamment grand tel que $q(y-x) > 1$. L'intervalle $]qx, qy[$ étant de longueur plus grande que 1, on pourra y trouver un entier relatif p, et donc $pq^{-1} \in]x, y[$. Posons donc $q = E\left((y-x)^{-1}\right) + 1$. Alors

$$\frac{1}{y-x} < q, \quad qy > qx + 1.$$

Posons $p = E(qx) + 1$. On a premièrement

$$p > qx, \quad \frac{p}{q} > x.$$

Deuxièmement, on a

$$p \leq qx + 1 < qy, \quad \frac{p}{q} < y$$

et donc $pq^{-1} \in]x, y[$.

$\boxed{\text{Densité de } \mathbb{R} \setminus \mathbb{Q}}$ $\mathbb{Q}$ étant dense dans $\mathbb{R}$, il existe $a, b \in \mathbb{Q}$ tels que $x < a < b < y$. Posons

$$r = a + \frac{b-a}{\sqrt{2}}.$$

Alors $a < r < b$, car $\sqrt{2} > 1$, et r est irrationnel. En effet, sinon on aurait

$$\sqrt{2} = \frac{b-a}{r-a} \in \mathbb{Q}$$

ce qui est impossible. Donc $r \in \mathbb{R} \setminus \mathbb{Q}$ qui est dense dans $\mathbb{R}$. $\square$

CHAPITRE 3

SUITES NUMÉRIQUES

CHAPITRE 4

ARITHMÉTIQUE DES ENTIERS

La principale application de ce chapitre est la cryptographie. En effet, les idées de base du chiffrement RSA reposent sur l'arithmétique modulaire, les nombres premiers, l'algorithme d'Euclide et le théorème de Bézout. Les résultats obtenus dans ce chapitre permettent également de résoudre certains types d'équations diophantiennes, et de comprendre les mécaniques de bases gouvernant les anneaux factoriels ou euclidiens. [1]

Avant toute chose, il est nécessaire de convenir d'une façon d'écrire les entiers.

Définition/Proposition 0.1 *Ecriture en base b - Admis*
Soit $b \geq 2$. Pour tout entier $n \in \mathbb{N}^*$, $\exists! r \in \mathbb{N}, \exists! (a_0, \dots, a_r) \in [\![0, b-1]\!]^r$,

$$n = \sum_{k=0}^{r} a_k p^k, \quad a_r \neq 0.$$

Cette décomposition est appelée *écriture en base b* de n et on note

$$n = \underline{a_r \dots a_0}_b \text{ ou } n = \overline{a_r \dots a_0}^b$$

La base 10, ou *écriture décimale*, est la base que nous utilisons habituellement pour nos calculs. Un ordinateur, suivant les besoins, utilisera la base 2, ou *binaire*, ou la base 16, ou *hexadécimale*. Lorsque $b > 10$, on utilise les lettres pour remplacer les chiffres manquants après le 9 $(A = 10, B = 11, \dots)$.

Sauf indication contraire, la base utilisée dans ce cours sera la base décimale.

Exemple 0.2 :
Considérons $n = 61$. Alors $n = 32 + 16 + 8 + 4 + 1$ et $n = 3 \times 16 + 13 \times 1$, donc

$$\underline{61}_{10} = \underline{111101}_2 = \underline{3D}_{16}.$$

◊

1. Notions évidemment largement hors-programme en classe préparatoire.

I Divisibilité

1. Congruence

Définition 1.1 *Multiple et diviseur*

Soient $a, b \in \mathbb{Z}$. On dit que a *divise* b si

$$\exists k \in \mathbb{Z}, \quad ak = b.$$

Dans ce cas, on note $a|b$ et on dit que b est un *multiple* de a, ou que a est un *diviseur* de b. On note l'ensemble des multiples de a

$$a\mathbb{Z} = \{z \in \mathbb{Z}/a|z\} = \{na \in \mathbb{Z}/n \in \mathbb{Z}\}.$$

Exemple 1.2 :

3 est un diviseur de -12 car $3 \times (-4) = -12$. ♢

Proposition 1.3

(i) La relation $|$ est réflexive et transitive sur $\mathbb{Z}$.

(ii) $\forall a, b \in \mathbb{Z}$,

$$a|b \iff a|(-b) \iff (-a)|b.$$

(iii) $\forall a \in \mathbb{Z}, 1|a, a|a, a|0$.

(iv) $\forall a \in \mathbb{Z}, 0|a \iff a = 0$.

(v) $\forall a, b, n \in \mathbb{Z}$,

$$(n|a \text{ et } n|b) \iff (\forall u, v \in \mathbb{Z}, n|(au + bv)).$$

(vi) $\forall a, b \in \mathbb{Z}$,

$$a|b \iff b\mathbb{Z} \subseteq a\mathbb{Z}.$$

(vii) $\forall a, b \in \mathbb{Z}$,

$$(a|b \text{ et } b|a) \iff a = \pm b.$$

(viii) $\forall a, b \in \mathbb{N}$,

$$a|b \Rightarrow a \leq b.$$

On notera que le point (ii) nous assure que le signe d'un nombre n'influe pas dans la relation de divisibilité. Cela nous permet de nous ramener la plupart du temps au cadre des entiers naturels. On pourra alors remarquer que, d'après (i) et (vii), la relation $|$ restreinte à $\mathbb{N}$ est un ordre, comme on l'a déjà vu au chapitre 2.

Démonstration : Les point $(i), (ii), (iii), (iv)$ sont évidents car, pour tous $a, b \in \mathbb{Z}$,

$$1 \times a = a, \quad b \times 0 = 0.$$

$\boxed{(v)}$ La réciproque est claire en choisissant $(u, v) = (1, 0)$ et $(0, 1)$, et

$$\begin{aligned} (n|a \text{ et } n|b) &\Rightarrow \exists p, q \in \mathbb{Z}, \quad np = a, nq = b \\ &\Rightarrow \exists p, q \in \mathbb{Z}, \forall u, v \in \mathbb{Z} \quad n(pu + qv) = au + bv \\ &\Rightarrow n|(au + bv) \end{aligned}$$

$\boxed{(vi)}$ L'implication est claire par transitivité de la relation $|$. La réciproque est évidente en remarquant que $b \in b\mathbb{Z}$.

$\boxed{(vii)}$ On se contente de montrer l'implication, la réciproque est évidente. Si que $a|b$ et $b|a$, alors il existe $p, q \in \mathbb{Z}$ tels que $ap = b$ et $bq = a$. Donc $apq = a$ et $a(pq-1) = 0$. Si $a = 0$, alors $b = 0$ d'après (ii). Sinon, $pq - 1 = 0$ (car $\mathbb{Z}$ est intègre) et par suite $q = \pm 1$ (car les inversibles de $\mathbb{Z}$ sont 1 et -1). Dans tous les cas, $a = qb = \pm b$. $\square$

Définition 1.4 *Congruence*
Soient $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$. On dit que a est *congru* à b modulo n, si $n|(b-a)$. On note alors

$$a \equiv b \ [n] \quad \text{ou } a \equiv b \pmod{n}.$$

En pratique, on utilisera souvent le critère suivant :

$$a \equiv b \ [n] \iff \exists k \in \mathbb{Z}, \quad a = b + nk.$$

Exemple 1.5 :
Soient $a, b \in \mathbb{Z}$. Remarquons que

$$a \equiv b \ [2] \iff \exists k \in \mathbb{Z}, a = b + 2k \iff a \text{ et } b \text{ sont de même parité.}$$

$\diamondsuit$

Exemple 1.6 :
Si $n = 3$, remarquons que $17 \equiv 2 \ [3]$ car $3|(17-2)$, ou car $17 = 2 + 3 \times 5$.

Si $n = 10$, remarquons que $17 \equiv 7 \ [10]$. $\diamondsuit$

On tire de cet exemple deux remarques :

- La congruence dépend bien entendu du modulo.
- Un nombre est congru modulo 10 à son dernier chiffre (en base 10).

Proposition 1.7
Soit $n \in \mathbb{N}^*$ fixé. Alors

(i) La relation $\equiv$ est une relation d'équivalence sur $\mathbb{Z}$.
(ii) $\forall a \in \mathbb{Z}, a \equiv 0 \ [n] \iff n|a \iff a \in n\mathbb{Z}$.
(iii) $\forall a, b, c, d \in \mathbb{Z}$,

$$(a \equiv b \ [n] \text{ et } c \equiv d \ [n]) \Rightarrow \begin{cases} a + c \equiv b + d \ [n] \\ a - c \equiv b - d \ [n] \\ ac \equiv bd \ [n] \end{cases}.$$

(iv) $\forall a, b \in \mathbb{Z}$,

$$a \equiv b \ [n] \iff \forall k \in \mathbb{N}, \quad a^k \equiv b^k \ [n].$$

Démonstration : $\boxed{(i)}$ Soient $a, b, c \in \mathbb{Z}$ tels que $a \equiv b \ [n]$ et $b \equiv c \ [n]$. Alors $n|0 = a - a$ donc $a \equiv a \ [n]$, donc $\equiv$ est réflexive. De plus, $n|(a-b)$ donc $b \equiv a \ [n]$, donc $\equiv$ est symétrique. Enfin,

$$\exists k, k' \in \mathbb{Z}, \quad a = b + kn, b = c + k'n,$$

donc $a = c + (k + k')\, n$ donc $a \equiv c \ [n]$, donc $\equiv$ est transitive. Il s'agit donc bien d'une relation d'équivalence sur $\mathbb{Z}$.

$\boxed{(ii)}$ Evident par définition.

$\boxed{(iii)}$ Soient $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b \ [n]\,, c \equiv d \ [n]$. Alors il existe $k, k' \in \mathbb{Z}$ tels que $a = b + kn, c = d + k'n$. Alors

$$a + c = b + d + (k + k')\, n, ac = bd + (kd + k'b + kk')\, n,$$

et donc $a + c \equiv b + d \ [n]\,, ac \equiv bd \ [n]$.

$\boxed{\text{iv)}}$ La réciproque est évidemment vraie en prenant $k = 1$. Pour l'implication, soient $a, b \in \mathbb{Z}$ tels que $a \equiv b \ [n]$ et $k \in \mathbb{N}$. Alors, en utilisant k fois (iii) (à écrire proprement à l'aide d'une récurrence), on obtient

$$\prod_{i=1}^{k} a \equiv \prod_{i=1}^{k} b \ [n]\,, \quad a^k \equiv b^k \ [n]\,.$$

$\square$

On a vu au point (iii) que la relation de congruence modulo n était compatible avec l'addition et la multiplication, c'est-à-dire qu'elle se comporte bien avec $+, -, \times$. En revanche, on ne peut pas diviser dans une relation de congruence en général. En effet, si $pa \equiv pb \ [n]$ alors il existe $k \in \mathbb{Z}$ tel que $pa = pb + kn$. On a $a = b + \dfrac{k}{p} n$, et il faudrait s'assurer que p est un diviseur de k, ce qui n'est en général pas possible. On verra à la fin du cours qu'il suffit en quelque sorte de s'assurer que p ne divise pas n.[2]

Corollaire 1.8

Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Alors a^n est pair si, et seulement si, a est pair.

Démonstration : Il est clair que

$$a \equiv 0 \ [2] \Rightarrow a^n \equiv 0 \ [2]\,, \quad a \equiv 1 \ [2] \Rightarrow a^n \equiv 1 \ [2]\,.$$

$\square$

Exemple 1.9 :
Montrons qu'un nombre est divisible par 3 si, et seulement si, la somme de ses chiffres est divisible par 3. Soit $n \in \mathbb{N}$. Alors il existe $r \in \mathbb{N}, a_0, \ldots, a_r \in [\![0, 9]\!]$,

$$n = \underline{a_r \ldots a_0}_{10} = \sum_{k=0}^{r} a_k 10^k,$$

c'est l'écriture en base 10 de n. Notons que $10 \equiv 1 \ [3]$. Alors

$$n \equiv 0 \ [3] \iff \sum_{k=1}^{r} a_k 10^k \equiv 0 \ [3] \iff \sum_{k=1}^{r} a_k 1^k \equiv 0 \ [3] \iff \sum_{k=1}^{r} a_k \equiv 0 \ [3]\,.$$

$\diamondsuit$

Exercice 1.10 :
Déterminer des critères similaires permettant de tester si un nombre entier est un multiple de 9 ou un multiple de 11.

2. Ou plus exactement, que p et n sont premiers entre eux.

Réponse

$\boxed{\text{Divisibilité par 9}}$ Soit $n = \underline{a_r \dots a_0}_{10} \in \mathbb{N}$. Puisque $10 \equiv 1 \ \ [9]$, on a encore

$$n \equiv 0 \ \ [9] \iff \sum_{k=1}^{r} a_k 10^k \equiv 0 \ \ [9] \iff \sum_{k=1}^{r} a_k 1^k \equiv 0 \ \ [9] \iff \sum_{k=1}^{r} a_k \equiv 0 \ \ [9]\,.$$

Donc un nombre est divisible par 9 si, et seulement si, la somme de ses chiffres est divisible par 9.

$\boxed{\text{Divisibilité par 11}}$ Puisque $10 \equiv -1 \ \ [11]$, on a

$$n \equiv 0 \ \ [11] \iff \sum_{k=1}^{r} a_k 10^k \equiv 0 \ \ [11] \iff \sum_{k=1}^{r} (-1)^k a_k \equiv 0 \ \ [11]\,.$$

♢

2. Nombres premiers

Définition 1.11 *Nombre premier*

Un entier naturel p est dit *premier* s'il admet exactement deux diviseurs dans $\mathbb{N}$: 1 et p. On note $\mathcal{P}$ l'ensemble des nombres premiers. Un entier non-premier est dit *composé*.

D'après la définition, 1 n'est pas premier (car il admet un seul diviseur dans $\mathbb{N}$).

Exemple 1.12 :
Les nombres $2, 3, 5, 7, 11, 13, 17, 19, 23$ sont premiers. Les nombres $8, 15, 21$ sont composés. ♢

Lemme 1.13

Tout entier naturel $n \geq 2$ admet au moins un diviseur premier.

Démonstration : Montrons par une récurrence forte que tout entier $n \geq 2$ admet un diviseur premier.D'abord, 2 est premier, et $2|2$ donc la propriété est vraie pour $n_0 = 2$. Ensuite, soit $n \geq 2$ et supposons la propriété vraie pour tout $k \in [\![2, n]\!]$. Alors, si $n+1$ est premier (comme pour l'initialisation de la récurrence), $n+1$ admet un diviseur premier. Sinon, $n+1$ admet au moins un diviseur $k \in [\![2, n]\!]$ et k admet lui-même un diviseur premier (par hypothèse de récurrence). Par transitivité, $n+1$ admet donc un diviseur premier. □

Proposition 1.14

Tout entier naturel $n \geq 2$ est composé si, et seulement si, il admet un diviseur premier $p \leq \sqrt{n}$.

Démonstration : La réciproque étant évidente, on s'intéresse à l'implication directe. Soit un entier $n \geq 2$ composé. Puisque n n'est pas premier, il existe $p, q \in [\![2, n-1]\!]$ tels que $n = pq$. Il est clair que $p \leq \sqrt{n}$ ou $q \leq n$ (sinon on aurait $pq > n$). Supposons donc que $p \leq n$. Alors p admet un diviseur premier p' et $p' \leq p \leq \sqrt{n}$. □

Ce critère est fondamental pour déterminer si un nombre n est premier ou pas : on s'intéresse à ses diviseurs compris entre 1 et $\sqrt{n}$.

Exemple 1.15 :
127 est-il un nombre premier ? Remarquons que $121 < 127 < 144$ donc $\sqrt{121} < 12$. Les seuls diviseurs premiers à tester sont donc $2, 3, 5, 7, 11$.

- 127 est impair donc $2 \not| 127$.
- $1 + 2 + 7 = 10$ et 10 n'est pas un multiple de 3 donc $3 \not| 127$.
- 127 ne finit ni par un 0 ni par un 5 donc $5 \not| 127$.
- On remarque que $7 \times 18 = 126$ et $7 \times 19 = 133$ donc $7 \not| 127$.
- $1 - 2 + 7 = 6$ et 6 n'est pas un multiple de 11 donc $11 \not| 127$.

Donc 127 est premier. ♢

On mentionnera une technique ancienne et efficace pour déterminer les nombres premiers : le crible d'Eratosthène.

Théorème 1.16
L'ensemble des nombres premiers $\mathcal{P}$ est infini.

Démonstration : Supposons, par l'absurde, que $\mathcal{P}$ soit fini. Alors il existe $n \in \mathbb{N}^*$ tel que $\mathcal{P} = \{p_1, \ldots, p_n\}$. Posons $p = \prod_{i=1}^{n} p_i + 1.$. Notons que $p > \max(p_1, \ldots, p_n)$ donc $p \notin \mathcal{P}$. Supposons (par l'absurde encore une fois) qu'il existe $k \in [\![1, n]\!]$, tel que $p_k | p$, alors

$$p = p_k \left(\prod_{i \neq k} p_i + \frac{1}{p_k} \right), \quad \frac{1}{p_k} \notin \mathbb{N}.$$

Donc p n'admet aucun diviseur premier : impossible. □

Théorème 1.17 *Décomposition en produit de facteurs premiers*
Soit un entier naturel $n \geq 2$. Alors $\exists! r \in \mathbb{N}^*, \exists! (p_1, \ldots p_r) \in \mathcal{P}^r, \exists! (\alpha_1, \ldots \alpha_r) \in (\mathbb{N}^*)^r$ tels que $p_1 < \cdots < p_r$ et

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}.$$

Le théorème précédent est parfois appelé "théorème fondamental de l'arithmétique"[3], car il donne une façon de construire tout entier à l'aide des nombres premiers, qui font office de "briques élémentaires".

En relâchant la condition $p_1 < \cdots < p_r$, cette écriture en produit de nombres premiers est unique à l'ordre près des facteurs.

3. Ce résultat est la principale raison pour laquelle il est convenu que 1 n'est pas premier : sinon la décomposition ne serait plus unique.

Corollaire 1.18

Soit un $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Alors $\exists! r \in \mathbb{N}^*, \exists! (p_1, \dots p_r) \in \mathcal{P}^r, \exists! (\alpha_1, \dots \alpha_r) \in (\mathbb{N}^*)^r$ tels que $p_1 < \cdots < p_r$ et

$$n = \pm \prod_{i=1}^{r} p_i^{\alpha_i}.$$

On remarquera que si $n = \pm 1$, en prenant $r = 0$ le produit est vide et vaut par convention 1. On peut donc écrire cette décomposition mais elle n'est plus unique.

Pour démontrer ces résultats, [4] nous aurons besoin du lemme d'Euclide, qui ne sera énoncé qu'à la fin de la partie suivante. Admettons la preuve pour le moment.

II Division euclidienne

1. Division euclidienne

Définition/Théorème 2.1 *Division euclidienne*

Soient $a \in \mathbb{Z}, b \in \mathbb{N}^*$. Alors $\exists! (q, r) \in \mathbb{Z} \times [\![0, b-1]\!]$,

$$a = bq + r.$$

Les entiers q et r sont appelés respectivement *quotient* et *reste* dans la division euclidienne de a par b.

On a unicité à condition de supposer bien sûr que $0 \leq r < b$. On notera que r est l'unique entier de $[\![0, b-1]\!]$ tel que $a \equiv r \quad [b]$.

Démonstration : Remarquons que

$$a = bq + r \iff \frac{a}{b} = q + \frac{r}{b}.$$

On pose donc $q = E(a/b)$ et $r = a - bq$. Alors

$$q \leq \frac{a}{b} < q + 1, \quad 0 \leq \frac{a}{b} - q = \frac{r}{b} < 1, \quad 0 \leq r < b.$$

On a donc existence du couple (q, r). Supposons que $a = bq + r = bq' + r'$ avec $r, r' \in [\![0, b-1]\!]$. Alors

$$0 = b(q - q') + (r - r'), \quad r' - r = b(q - q') \in b\mathbb{Z}.$$

Puisque $-b < r' - r < b$, on en déduit que $r' - r = 0$ et donc $q' - q = 0$. $\square$

Exemple 2.2 :
Effectuons la division euclidienne de 97 par 7.

$$\begin{array}{rr|ll} 9 & 7 & 7 & \\ \cline{3-4} 2 & 7 & 1 & 3 \\ & 6 & & \end{array}$$

On a donc $97 = 7 \times 13 + 6$, donc le quotient vaut 13 et le reste vaut 6. $\diamondsuit$

4. Plus précisément, pour démontrer l'unicité de la décomposition.

Proposition 2.3
Soient $a \in \mathbb{Z}, b \in \mathbb{N}^*$ et r le reste dans la division euclidienne de a par b. Alors $a \equiv r \ [b]$.

La division euclidienne est un outil très puissant, aussi bien en théorie qu'en pratique. Il faut savoir effectuer une division euclidienne à la main, et appliquer le résultat théorique.

2. PGCD et PPCM

Définition/Proposition 2.4 *PGCD et PPCM*
Soient $a, b \in \mathbb{Z}, a \neq 0, b \neq 0$.

(i) L'ensemble des diviseurs communs de a et b admet un maximum strictement positif. Il est appelé *plus grand commun diviseur* (ou PPCM) de a et b et est noté $a \wedge b$ ou $\operatorname{pgcd}(a, b)$.
(ii) L'ensemble des multiples communs strictement positifs de a et b admet un minimum. Il est appelé *plus petit commun multiple* (ou PPCM) de a et b et est noté $a \vee b$ ou $\operatorname{ppcm}(a, b)$.

Par convention, on posera pour tout $a \in \mathbb{Z}$: $a \wedge 0 = a$ et $a \vee 0 = 0$.

Démonstration : L'ensemble des diviseurs communs de a et b est une partie non-vide (car 1 en fait partie) et majorée (par $|a|$) de $\mathbb{Z}$, et admet donc un maximum. De même, l'ensemble des multiples communs strictement positifs de a et b est une partie non-vide (car $|ab|$ en fait partie) de $\mathbb{N}^*$, et admet donc un minimum. □

On pourrait généraliser les notions de PGCD et de PPCM à plus de deux entiers de manière tout à fait similaire.

On remarquera que, pour tous $a, b \in \mathbb{Z}^*$,

$$1 \leq a \wedge b \leq \min(|a|, |b|), \quad \max(|a|, |b|) \leq a \vee b \leq |ab|,$$

et que

$$a \wedge b = b \wedge a = |a| \wedge |b|, \quad a \vee b = b \vee a = |a| \vee |b|.$$

Exemple 2.5 :
On a

$$21 \wedge 14 = 7, 21 \vee 14 = 42, \qquad 21 \wedge 26 = 1, \quad 21 \vee 26 = 546.$$

◊

Lemme 2.6
Soient $a, b \in \mathbb{Z}^*$ admettant les décompositions suivantes :

$$a = \pm \prod_{i=1}^{r} p_i^{\alpha_i}, \quad b = \pm \prod_{i=1}^{r} p_i^{\beta_i},$$

où les p_i sont des nombres premiers distincts et les α_i, β_i sont des entiers naturels. Alors

$$a | b \iff \forall i \in [\![1, r]\!], \alpha_i \leq \beta_i.$$

Remarquons que tous les entiers a et b non-nuls admettent une telle décomposition, quitte à supposer que quelques exposants α_i ou β_i sont nuls. On n'a évidemment plus unicité.

Démonstration : Posons $c = \dfrac{b}{a} \in \mathbb{R}$. Alors $c = \pm \displaystyle\prod_{i=1}^{r} p_i^{\gamma_i}$ avec $\gamma_i = \beta_i - \alpha_i$. Alors

$$\forall i \in [\![1, r]\!], \alpha_i \leq \beta_i \in \mathbb{N} \iff \forall i \in [\![1, r]\!], \gamma_i \geq 0 \iff c \in \mathbb{Z} \iff a|b.$$

□

Proposition 2.7

Soient $a, b \in \mathbb{Z}^*$ admettant les décompositions suivantes :

$$a = \pm \prod_{i=1}^{r} p_i^{\alpha_i}, \quad b = \pm \prod_{i=1}^{r} p_i^{\beta_i},$$

où les p_i sont des nombres premiers distincts et les α_i, β_i sont des entiers naturels. Alors :

(i) $a \wedge b = \displaystyle\prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)}$.

(ii) $\forall n \in \mathbb{Z}, (n|a \text{ et } n|b) \iff n|a \wedge b$.

(iii) $a \vee b = \displaystyle\prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}$.

(iv) $\forall n \in \mathbb{Z}, (a|n \text{ et } b|n) \iff a \vee b|n$.

Démonstration : $\boxed{(i)}$ Notons $\delta_i = \min(\alpha_i, \beta_i)$ et posons $d = \displaystyle\prod_{i=1}^{r} p_i^{\delta_i}$. Puisque pour tout $i \in [\![1, r]\!], \delta_i \leq \alpha_i$ et $\delta_i \leq \beta_i$ l est un diviseur commun de a et b. Soit $c = \pm \displaystyle\prod_{i=1}^{r} p_i^{\gamma_i}$ un diviseur commun de a et b. Alors pour tout $i \in [\![1, r]\!], \gamma_i \leq \alpha_i$ et $\gamma_i \leq \beta_i$, donc $\gamma_i \leq \delta_i$ et $c|d$ car $d \geq 0$. Donc $c \leq d$ et, par suite, $d = a \wedge b$.

$\boxed{(ii)}$ En reprenant la preuve du point (i), on a montré que tout diviseur commun de a et b divise $d = a \wedge b$. Par transitivité de la divisibilité, la réciproque est évidente.

$\boxed{(iii) \text{ et } (iv)}$ Exercice. □

Définition 2.8 *Nombres premiers entre eux*

Soient $a, b \in \mathbb{Z}$. On dit que a et b sont *premiers entre eux* si $a \wedge b = 1$.

Exemple 2.9 :
2 et 3 sont premiers entre eux. 45 et 24 ne le sont pas, car $24 \wedge 45 = 3$. ◇

Cette notion permet de rendre compte que a et b n'ont aucun diviseurs en commun, et donc aucun facteurs premiers en commun, et sera fondamentale dans la suite. Elle est très intuitive : on l'utilise par exemple lorsque l'on cherche à rendre une fraction irréductible. Voyons un exemple fondamental d'utilisation des nombres premiers entre eux.

Exercice 2.10 :
Montrer que $\sqrt{2}$ est irrationnel.

Réponse

Supposons par l'absurde que $\sqrt{2} \in \mathbb{Q}$. Alors il existe $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $\sqrt{2} = \frac{p}{q}$. On peut supposer sans perte de généralité que p et q premiers entre eux, puisque $\frac{kp}{kq} = \frac{p}{q}$ pour tout $k \in \mathbb{Z}^*$. Alors

$$\frac{p^2}{q^2} = 2, \quad p^2 = 2q^2$$

donc p^2 est pair, et donc p est pair. Autrement dit, il existe $\widetilde{p} \in \mathbb{Z}$ tel que $p = 2\widetilde{p}$. Alors

$$2q^2 = p^2 = 4\widetilde{p}^2, \quad q^2 = 2\widetilde{p}^2.$$

donc q^2 est pair et donc q est pair. Donc 2 est un diviseur commun de p et q, ce qui est impossible car on a supposé $p \wedge q = 1$.

$\diamondsuit$

On peut montrer de la même manière que, pour tout $p \in \mathcal{P}$, $\sqrt{p}$ est irrationnel. On aura juste besoin du lemme d'Euclide, que l'on abordera seulement un peu plus tard.

3. Algorithme d'Euclide

Dans cette section, on souhaite répondre à la question suivante : comment déterminer le PGCD de deux entiers sans avoir accès à leur décomposition en facteurs premiers ? Pour ce faire, on s'appuie sur le lemme suivant.

Lemme 2.11

Soient $a, b, q, r \in \mathbb{Z}$ tels que $a = bq + r$. Alors $a \wedge b = b \wedge r$.

Ce résultat va devenir particulièrement utile lorsque q et r sont respectivement le quotient et le reste dans la division euclidienne de a par b, c'est-à-dire quand $b \in \mathbb{N}^*$ et $r \in [\![0, b-1]\!]$.

Démonstration : Soit n un diviseur de a et b. Alors $a \equiv b \equiv 0 \ [n]$ donc $r \equiv 0 \ [n]$, et n est donc un diviseur de r. Réciproquement, si n est un diviseur de b et r, alors $b \equiv r \equiv 0 \ [n]$ donc $a \equiv 0 \ [n]$, et n est donc un diviseur de a. On en déduit que l'ensemble des diviseurs communs de a et de b est égal à l'ensemble des diviseurs communs de b et de r ; leurs maxima sont donc égaux. $\square$

Théorème 2.12 *Algorithme d'Euclide*

Soient $a, b \in \mathbb{N}^*$.

- On pose $x_0 = a, y_0 = r_{-1} = b$ et q_0 et r_0 le quotient et le reste dans la division euclidienne de a par b.
- Pour tout $n \in \mathbb{N}$, si $r_n = 0$ on s'arrête. Sinon, on pose $x_{n+1} = r_{n-1}, y_{n+1} = r_n$ et q_{n+1} et r_{n+1} le quotient et le reste dans la division euclidienne de x_{n+1} par y_{n+1}.

Alors il existe $p \in \mathbb{N}$ tel que $r_p = 0$ et $a \wedge b = r_{p-1}$.

Pour déterminer le PGCD de deux entiers relatifs $a, b \in \mathbb{Z}^*$, on appliquera simplement l'algorithme d'Euclide à $|a|$ et $|b|$. Le cas $a \wedge b = r_{-1}$ correspond au fait que $r_0 = 0$, c'est-à-dire que $b|a$.

Démonstration : Montrons que l'algorithme prend fin au bout d'un nombre fini d'étapes (au maximum b, en fait). Par définition de la division euclidienne, $r_{n+1} \in [\![0, r_n - 1]\!]$ donc (r_n) est une suite d'entiers strictement décroissante dans $[\![0, b]\!]$. Il existe donc $p \in \mathbb{N}$ tel que $r_p = 0$ et $r_{p-1} \neq 0$.

En appliquant le lemme 2.11 dans une récurrence évidente, il est clair que

$$a \wedge b = r_0 \wedge r_1 = \cdots = r_{p-1} \wedge r_p = r_{p-1} \wedge 0 = r_{p-1}.$$

$\square$

Exemple 2.13 :
Déterminons le PGCD de 231 et 84 par l'algorithme d'Euclide :

$$\begin{aligned} 231 &= 84 \times 2 + 63 \\ 84 &= 63 \times 1 + 21 \\ 63 &= 21 \times 3 + 0. \end{aligned}$$

$\diamondsuit$

Exercice 2.14 :
Déterminer le PGCD de 9945 et 3003.

Réponse

Première méthode, on factorise en produit de facteurs premiers :

$$9945 = 3^2 \times 5 \times 13 \times 17, \quad 3003 = 3 \times 7 \times 11 \times 13.$$

Alors $9945 \wedge 3003 = 3 \times 13 = 39$.

Seconde méthode, on effectue l'algorithme d'Euclide

$$\begin{aligned} 9945 &= 3003 \times 3 + 936 \\ 3003 &= 936 \times 3 + 195 \\ 936 &= 195 \times 4 + 156 \\ 195 &= 156 \times 1 + 39 \\ 156 &= 39 \times 4 + 0. \end{aligned}$$

Le dernier reste non-nul de l'algorithme étant 39, on en déduit que $9945 \wedge 3003 = 39$.

$\diamondsuit$

Cet algorithme d'obtention de $a \wedge b$ est particulièrement utile lorsque l'on souhaite résoudre des exercices théoriques pour lesquels on n'a pas d'expression concrète pour a et b, ou si a et b sont trop grands pour être décomposés rapidement en facteurs premiers.

4. Théorème de Bézout et conséquences

Théorème 2.15 *Théorème de Bézout*
Soient $a, b \in \mathbb{Z}$. Alors on a l'équivalence suivante :

(i) a et b sont premiers entre eux.
(ii) $\exists (u, v) \in \mathbb{Z}^2, au + bv = 1$.

Démonstration : $\boxed{(ii) \Rightarrow (i)}$ Il est clair que $a \wedge b | au + bv$ donc $a \wedge b = 1$.

$\boxed{(i) \Rightarrow (ii)}$ Puisque $a \wedge b = |a| \wedge |b|$, on peut supposer $a, b \in \mathbb{N}$. Reprenons l'algorithme d'Euclide et les suites (q_k) et (r_k) qui y sont définies. Les cas $a = 0$ ou $b = 0$ étant évident, on suppose $(a, b) \in \mathbb{N}^*$. On pose alors

$$\left\{\begin{array}{ll} u_0 & = 1 \\ v_0 & = -q_0 \end{array}\right. \qquad \left\{\begin{array}{ll} u_1 & = -q_1 u_0 \\ v_1 & = 1 - q_1 v_0 \end{array}\right. \qquad \forall k \in \mathbb{N}^*, \left\{\begin{array}{ll} u_{k+1} & = u_{k-1} - q_{k+1} u_k \\ v_{k+1} & = v_{k-1} - q_{k+1} v_k \end{array}\right. .$$

Il est alors aisé de vérifier que $\forall k \in \mathbb{N}, r_k = u_k a + v_k b$. Puisque $a \wedge b = r_{p-1}$, il suffit de choisir $(u, v) = (u_{p-1}, v_{p-1})$. $\square$

Le couple (u, v) n'est pas unique. Plutôt que de retenir par cœur la preuve, il convient de savoir retrouver ce couple (u, v), dont on aura besoin pour le résultat suivant.

Exemple 2.16 :
Comment trouver $u, v \in \mathbb{Z}$ tels que $23u+7v = 1$? Cette méthode s'appelle *la remontée de l'algorithme d'Euclide* :

$$\begin{array}{rl|ll} 23 & = 7 \times 3 + 2 & 1 & = 7 - 2 \times 3 \\ 7 & = 2 \times 3 + 1 & 1 & = 7 - (23 - 7 \times 3) \times 3 = 7 \times 10 - 23 \times 3 \\ 2 & = 1 \times 2 + 0 & & \end{array}$$

On en déduit qu'un couple solution est $(u, v) = (10, -3)$. $\diamondsuit$

Le théorème de Bézout a deux conséquences importantes : le théorème de Gauss et le lemme d'Euclide.

Théorème 2.17 *Théorème de Gauss*
Soient $a, b, c \in \mathbb{Z}$. Alors :

$$\left\{\begin{array}{l} a|bc \\ a \wedge b = 1 \end{array}\right. \Longrightarrow a|c.$$

Démonstration : D'après le théorème de Bézout et par définition de la divisibilité, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$ et $ak = bc$. Alors

$$c = (au + bv)\, c = auc + bvc = a\,(uc + vk)\,,$$

donc $a|c$. $\square$

Lemme 2.18 *Lemme d'Euclide*
Soient $p \in \mathcal{P}$. Alors :

(i) $\forall a, b \in \mathbb{Z}$,

$$p|ab \iff p|a \text{ ou } p|b.$$

(ii) $\forall n \in \mathbb{N}^*, \forall b_1, \ldots, b_n \in \mathbb{Z}$,

$$p | \prod_{i=1}^{n} b_i \iff \exists i \in [\![1, n]\!], p | b_i.$$

Démonstration : $\boxed{(ii)}$ La réciproque est évidente, on se concentre donc sur le sens direct, qu'on va montrer par récurrence simple. Si $n = 1$ et $p|b_1$, alors $p|b_1$. Soit $n \in \mathbb{N}^*$ et supposons que

$$p | \prod_{i=1}^{n} b_i \implies (\exists i \in [\![1, n]\!], p | b_i).$$

Supposons maintenant que $p | \prod_{i=1}^{n+1} b_i$. Si $p | b_{n+1}$, la propriété est vraie au rang $n+1$. Sinon, $p \wedge b_{n+1} = 1$ car les seuls diviseurs positifs de p sont 1 et p. Donc $p | \prod_{i=1}^{n} b_i$ par le théorème de Gauss, et il existe $i \in [\![1, n]\!], p | b_i$. Dans tous les cas, la propriété est vérifiée au rang $n + 1$.

$\boxed{(i)}$ Cas particulier de (ii) (équivalent à l'hérédité). $\square$

Corollaire 2.19

Soient $a \in \mathbb{Z}, n \in \mathbb{N}^*$ et $b_1, \ldots, b_n \in \mathbb{Z}$. Alors

$$\forall i \in [\![1, n]\!], a \wedge b_i = 1 \implies a \wedge \prod_{i=1}^{n} b_i = 1.$$

Démonstration : Notons $b = \prod_{i=1}^{n} b_i$ et supposons, par l'absurde, que $a \wedge b \neq 1$. Alors $a \wedge b$ admet un diviseur premier p et $p|b$. Par le lemme d'Euclide, il existe $i \in [\![1, n]\!]$ tel que $p|b_i$. Puisque $p|a, p \leq a \wedge b_i$ donc $a \wedge b_i \neq 1$: impossible. $\square$

Corollaire 2.20

Soient $a \in \mathbb{Z}, n \in \mathbb{N}^*$ et $b_1, \ldots, b_n \in \mathbb{Z}$. Alors

$$\left\{ \begin{array}{l} \forall i, j \in [\![1, n]\!], i \neq j, b_i \wedge b_j = 1 \\ \forall i \in [\![1, n]\!], b_i | a \end{array} \right. \implies \prod_{i=1}^{n} b_i | a.$$

Démonstration : On va montrer par récurrence simple sur n que

$$\forall n \in \mathbb{N}^*, \quad P(n) : \forall b_1, \ldots, b_n \in \mathbb{Z}, \left\{ \begin{array}{l} \forall i \neq j, b_i \wedge b_j = 1 \\ \forall i, b_i | a \end{array} \right. \implies \prod_{i=1}^{n} b_i | a.$$

Si $n = 1$ et $b_1 \in \mathbb{Z}$ tel que $b_1|a$, alors $b_1|a$. Soit $n \in \mathbb{N}^*$ et supposons que $P(n)$ soit vérifiée. Soient $b_1, \ldots, b_{n+1} \in \mathbb{Z}$ tels que pour tous $i, j \in [\![1, n+1]\!], b_i|a$ et $i \neq j \Rightarrow b_i \wedge b_j = 1$. Les entiers $b_1, \ldots, b_n$ vérifient $P(n)$ donc $b = \prod_{i=1}^{n} b_i | a$, donc il existe $k \in \mathbb{Z}$ tel que $bk = a$. De plus, pour tout $i \in [\![1, n]\!], b_{n+1} \wedge b_i$ donc $b_{n+1} \wedge b = 1$ par le corollaire 2.19. Puisque $b_{n+1}|a = bk$, $b_{n+1}|k$ par le théorème de Gauss. Donc il existe $k' \in \mathbb{Z}$ tel que $b_{n+1}k' = k$, et donc $a = bb_{n+1}k'$. Donc $\prod_{i=1}^{n+1} b_i | a$, et $P(n+1)$ est vérifiée. $\square$

III Applications

1. Equations diophantiennes

Une équation diophantienne est une équation à coefficients entiers dont on cherche des solutions entières. Une application majeure (et historique) de l'algorithme d'Euclide et du théorème de Bézout est la résolution dans $\mathbb{Z}$ des équations diophantiennes de la forme

$$ax + by = c, \quad a, b, c \in \mathbb{Z}.$$

Proposition 3.1

Soient $a, b, c \in \mathbb{Z}$. L'équation diophantienne $ax + by = c$ admet des solutions dans $\mathbb{Z}$ si, et seulement si, $a \wedge b | c$.

Démonstration : On remarquera qu'on peut reformuler la proposition en

$$\exists (u, v) \in \mathbb{Z}, au + bv = c \iff a \wedge b | c.$$

Puisqu'on peut trouver $(u, v) \in \mathbb{Z}$ tel que $au + bv = a \wedge b$ grâce à la remontée de l'algorithme d'Euclide, la preuve est absolument similaire à celle du théorème de Bézout. $\square$

Exercice 3.2 :
Résoudre dans $\mathbb{Z}$ l'équation

$$70x - 21y = 14.$$

Réponse

Puisque $21 \wedge 70 = 7$ et $7|14$, l'équation admet des solutions (une infinité, même). En simplifiant par 7 on a

$$70x - 21y = 14 \iff 10x - 3y = 2$$

On a $10 = 3 \times 3 + 1$ donc $2 = 2 \times 1 = 10 \times 2 + (-3) \times 6$. On a donc trouvé une solution particulière $(x_0, y_0) = (2, 6)$. On va trouver toutes les solutions par analyse/synthèse.

$\boxed{\text{Analyse}}$ Soit $(x, y) \in \mathbb{Z}^2$ une solution de l'équation. Alors on a

$$10x - 3y = 10x_0 - 3y_0, \quad 10(x - x_0) = 3(y - y_0).$$

$3|10(x - x_0)$ et $3 \wedge 10 = 1$ donc $3|x - x_0$, donc d'après le théorème de Gauss, il existe $k \in \mathbb{Z}$ tel que $x = x_0 + 3k$. Donc

$$10(x - x_0) = 3(y - y_0), \quad 30k = 3(y - y_0), \quad y = y_0 + 10k.$$

Donc $(x, y) = (2 + 3k, 6 + 10k)$.

$\boxed{\text{Synthèse}}$ Il est clair que, pour tout $k \in \mathbb{Z}, 10(2 + 3k) - 3(6 + 10k) = 2$. Donc

$$70x - 21y = 14 \iff \exists k \in \mathbb{Z}, (x, y) = (2 + 3k, 6 + 10k).$$

$\diamondsuit$

En général, si la solution particulière n'est pas évidente, on effectuera la remontée de l'algorithme d'Euclide, qui fonctionne tout le temps.

2. Division et congruence

Pour rappel, la relation de congruence se comporte bien avec les lois $+, -, \times$. Nous avons maintenant les outils pour diviser dans une relation de congruence.

Proposition 3.3

Soit $n \in \mathbb{N}^*$. Alors, pour tous $a, b \in \mathbb{Z}, c \in \mathbb{Z}^*$,

$$\left\{\begin{array}{l} ac \equiv bc \ [n] \\ c \wedge n = 1 \end{array}\right. \Longrightarrow a \equiv b \ [n].$$

Démonstration : Il existe $k \in \mathbb{Z}$ tel que $ac = bc + kn$, donc $c|kn$ et $c \wedge n = 1$. D'après le théorème de Gauss, $c|k$ donc il existe $k' \in \mathbb{Z}$ tel que $ck' = k$. D'où $a = b + k'n$. $\square$

3. Décomposition en produit de facteurs premiers

A l'aide du lemme d'Euclide et du théorème de Gauss, on est enfin en mesure de prouver l'unicité de la décomposition en produit de facteurs premiers dans le théorème 1.17.

Démonstration du théorème 1.17 : Existence Montrons par récurrence forte que tout entier $n \geq 2$ admet une décomposition en produit de facteurs premiers. Il est clair que $2 = 2$ admet une telle décomposition. Soit $n \geq 2$ et supposons la propriété vérifiée pour tout $k \in [\![2, n]\!]$. Si $n+1 \in \mathcal{P}$, on a $n+1 = n+1$ et la propriété est vrai au rang $n+1$. On suppose donc dans la suite que $(n+1)$ n'est pas premier, et on pose $p_1 = \min\{p \in \mathcal{P}/p|\,(n+1)\}$ (p_1 existe d'après le lemme 1.13 et $p_1 < n+1$ car $n+1 \notin \mathcal{P}$). Donc il existe $k \in [\![2, n]\!]$, tel que $p_1 k = n+1$. Par l'hypothèse de récurrence, k admet une décomposition en facteurs premiers :

$$k = \prod_{i=1}^{r} p_i^{\alpha_i}, \quad n+1 = p_1^{\alpha_1+1} \prod_{i=2}^{r} p_i^{\alpha_i},$$

la propriété est donc vraie au rang $n+1$.[5]

Unicité Supposons qu'il existe des nombres premiers $p_1 < \cdots < p_r$ et $q_1 < \cdots < q_s$ tels que

$$n = \prod_{i=1}^{r} p_i^{\alpha_i} = \prod_{i=1}^{s} q_i^{\beta_i}.$$

Pour tout $j \in [\![1, r]\!], p_j | n = \prod_{i=1}^{s} q_i^{\beta_i}$ donc, par le lemme d'Euclide, il existe $k \in [\![1, s]\!]$ tel que $p_j | q_k$. Puisque $q_k \in \mathcal{P}, p_j = q_k$ donc $p_j \in \{q_1, \ldots, q_s\}$. Donc $\{p_1, \ldots, p_r\} \subseteq \{q_1, \ldots, q_s\}$. Par raisonnement symétrique, l'inclusion inverse est vraie aussi et donc

$$\{p_1, \ldots, p_r\} = \{q_1, \ldots, q_s\}.$$

5. Notons que α_1 peut éventuellement être nul, ce qui n'empêche pas la décomposition d'exister. On suppose que les α_i sont nuls uniquement pour avoir unicité.

En particulier, $r = s$ et pour tout $i \in [\![1, r]\!], p_i = q_i$ puisqu'on a supposé que les p_i et les q_i sont rangés dans l'ordre croissant. Donc

$$\prod_{i=1}^{r} p_i^{\alpha_i} = \prod_{i=1}^{r} p_i^{\beta_i}.$$

Pour tous $i, j \in [\![1, r]\!]$ tels que $i \neq j$

$$p_i \wedge p_j = 1, \quad p_i^{\alpha_i} \wedge p_j = 1, \quad p_i^{\alpha_i} \wedge p_j^{\beta_j} = 1, \quad p_i^{\alpha_i} \wedge \prod_{j \neq i} p_j^{\beta j} = 1.$$

et $p_i^{\alpha_i} | n = p_i^{\beta_i} \prod_{j \neq i} p_j^{\beta j}$ donc, d'après le théorème de Gauss, $p_i^{\alpha_i} | p_i^{\beta_i}$ donc $\alpha_i \leq \beta_i$. Encore une fois, on peut appliquer le raisonnement symétrique et en conclure que $\alpha_i = \beta_i$. □

4. Sous-groupes de $\mathbb{Z}$

Dans ce chapitre, on donne une caractérisation alternative du PGCD et du PPCM comme générateurs de certains sous-groupes de $\mathbb{Z}$.

Lemme 3.4 *Sous-groupes de* $\mathbb{Z}$

Soit H une partie non-vide de $\mathbb{Z}$. On a alors l'équivalence suivante :

(i) $(H, +)$ est un sous-groupe de $(\mathbb{Z}, +)$.
(ii) $\exists n \in \mathbb{N}, H = n\mathbb{Z}$.

Démonstration : Soit $n \in \mathbb{N}$, montrons que $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. On remarque que $n\mathbb{Z} = \{a \in \mathbb{Z}/a \equiv 0 \ [n]\}$. I est clair que $n\mathbb{Z}$ est non-vide car $0 \in n\mathbb{Z}$. De plus, $\forall a, b \in n\mathbb{Z}$ il est clair que $a - b \equiv 0 \ [n]$ donc $a - b \in n\mathbb{Z}$. Donc $n\mathbb{Z}$ est bien un sous-groupe de $\mathbb{Z}$.

Réciproquement, soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. On suppose donc que $H \neq \{0\}$. Donc $\exists a \in H \setminus \{0\}$, donc $|a| \in H \cap \mathbb{N}^*$. Posons $H_+ = H \cap \mathbb{N}^*$. Alors H_+ est une partie non-vide de $\mathbb{N}^*$, et admet donc un plus petit élément noté n. On va montrer que tout élément de H_+ est un multiple de n ; soit $a \in H$. On effectue la division euclidienne de $|a|$ par n, il existe donc $(q, r) \in \mathbb{Z}^2$ tel que $|a| = qn + r$ et $r \in [\![0, n-1]\!]$. Puisque $|a| \in H, qn \in H$, on a $r \in H$. Puisque $r < n$, on en déduit que $r = 0$ et donc $n|a$. Donc $a \in n\mathbb{Z}$. Donc $H = n\mathbb{Z}$. □

Proposition 3.5

Soient $a, b \in \mathbb{Z}$. Alors :

(i) $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\,\mathbb{Z}$.
(ii) $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\,\mathbb{Z}$.

Démonstration : $\boxed{(ii)}$ On sait que $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ donc il existe $n \in \mathbb{N}$ tel que $n\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$. Montrons que $n = a \vee b$. Tout d'abord, $n \in a\mathbb{Z}$ et $n \in b\mathbb{Z}$ donc n est un multiple commun de a et b. Soit $c \in \mathbb{Z}$ un multiple commun strictement positif de a et b. Alors $c \in a\mathbb{Z} \cap b\mathbb{Z}$ donc $n|c$ donc $n \leq c$. Donc $n = a \vee b$.

$\boxed{(i)}$ On note $a\mathbb{Z} + b\mathbb{Z} = \{au + bv / \, (u, v) \in \mathbb{Z}^2\}$. Il s'agit d'un sous-groupe de $\mathbb{Z}$ car $0 \in a\mathbb{Z} + b\mathbb{Z}$ et, pour tout $x, x' \in a\mathbb{Z} + b\mathbb{Z}$, il existe $u, u', v, v' \in \mathbb{Z}$ tels que

$$x = au + bv, \quad x' = au' + bv', \quad x - x' = a\,(u - u') + b\,(v - v'),$$

et donc $x - x' \in a\mathbb{Z} + b\mathbb{Z}$. Il existe donc $n \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = n\mathbb{Z}$. Montrons que $n = a \wedge b$. Si $a = b = 0$, il est clair que $n = 0$. Supposons donc que $(a, b) \neq (0, 0)$. Puisque $a \in a\mathbb{Z} + b\mathbb{Z} = n\mathbb{Z}, n|a$. De la même manière, $n|b$. Donc n est un diviseur de a et b. Il existe $(u, v) \in \mathbb{Z}$ tel que $au + bv = 1$. Soit $c \in \mathbb{Z}$ un multiple commun de a et b. Alors $\exists k, k' \in \mathbb{Z}$ tels que $a = kc$ et $b = k'c$. Donc

$$n = au + bv = kcu + k'cv = (ku + k'v)\, c$$

donc $c|n$. Donc $c \leq |c| \leq n$. Donc $n = a \wedge b$. $\square$

CHAPITRE 5

ALGÈBRE LINÉAIRE – ESPACES VECTORIELS

CHAPITRE 6

FONCTIONS – LIMITE ET CONTINUITÉ

> C'est Cosinus et Exponentielle qui sortent en boîte. Cosinus boit, fume et a une gueule de bois comme jamais le lendemain. Quand Exponentielle l'interroge sur son comportement, Cosinus répond : "Désolé, vieux, mais j'connais pas mes limites !".
>
> Blague mathématique

Dans ce chapitre, on définit rigoureusement la notion de limite et de continuité pour les fonctions d'une variable réelle. Ces notions seront fondamentales lorsque l'on parlera de dérivabilité plus tard dans l'année. Même si ce chapitre part de zéro en ce qui concerne de nombreuses notions, il est important d'être à l'aise avec la notion de limite déjà définie dans le chapitre de suites numériques.

On rappelle que $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty\} \cup \{+\infty\}$. Dans tout ce chapitre, I désigne une partie de $\mathbb{R}$ possédant au moins deux éléments, et $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Cette année, on ne considèrera que des fonctions d'une variable réelle, à valeurs dans $\mathbb{R}$ ou $\mathbb{C}$, c'est-à-dire les éléments de $\mathcal{F}(I, \mathbb{K})$. En revanche, on ne traitera pas le cas des fonctions d'une variable complexe.

I Rappels sur les fonctions et les applications

Attention à la différence entre "fonction" et "application" :

- Une application f de I dans $\mathbb{K}$ est définie sur tout I, c'est-à-dire

  $$\forall x \in I, \exists! y \in \mathbb{K}, f(x) = y.$$

- Une fonction f de I dans $\mathbb{K}$ n'est pas nécessairement définie sur I tout entier. Il convient alors de déterminer son ensemble de définition

  $$D_f = \{x \in I / f(x) \text{ est bien défini}\}.$$

Pourquoi faire la différence ?

- En théorie (dans le cours), on étudie des applications pour ne pas avoir à se soucier de tous les cas particuliers où telle ou telle fonction n'est pas définie en tel ou tel point.

- En pratique (dans les exercices), on étudie des fonctions. Après avoir déterminé leur ensemble de définition, cela en fait de simples applications auxquelles on peut appliquer la théorie.

Dans la suite, on ne fait plus vraiment la différence, mais il suffit de retenir que dans le cours, on ne traite pas le problème des ensembles de définition.

1. Fonctions de I dans $\mathbb{K}$

Définition/Proposition 1.1 *Graphe*

On note $\mathcal{F}(I,\mathbb{K})$ l'ensemble des applications de I dans $\mathbb{K}$. Soit $f \in \mathcal{F}(I,\mathbb{K})$. On appelle *graphe de* f le sous-ensemble de $\mathbb{R}\times\mathbb{K}$ défini par

$$G_f = \{(x,y) \in \mathbb{R}\times\mathbb{K}/y = f(x)\}.$$

Définition/Proposition 1.2 *Structure d'espace vectoriel et d'anneau*

On munit $\mathcal{F}(I,\mathbb{K})$ de deux lois de composition interne et d'une loi de composition externe : pour tous $f,g \in \mathcal{F}(I,\mathbb{K})$ et $\lambda \in \mathbb{K}$, on définit

$$f+g : x \mapsto f(x)+g(x), \quad f\times g : x \mapsto f(x)\times g(x), \quad \lambda\cdot f : x \mapsto \lambda f(x).$$

Alors $(\mathcal{F}(I,\mathbb{K}),+,\times)$ est un anneau commutatif et $(\mathcal{F}(I,\mathbb{K}),+,\cdot)$ est un $\mathbb{K}$-espace vectoriel.

En fait, on dit que $(\mathcal{F}(I,\mathbb{K}),+,\times,\cdot)$ a une structure de $\mathbb{K}$-algèbre commutative (globalement, "espace vectoriel" + "anneau commutatif").

Définition/Proposition 1.3 *Structure d'ensemble ordonné*

On munit $\mathcal{F}(I,\mathbb{R})$ d'une relation d'ordre : pour tous $f,g \in \mathcal{F}(I,\mathbb{R})$, on définit

$$f \leq g \iff \forall x \in I, \quad f(x) \leq g(x).$$

Alors $(\mathcal{F}(I,\mathbb{R}),\leq)$ est un ensemble partiellement ordonné.

⚠ $(\mathcal{F}(I,\mathbb{R}),\leq)$ n'est pas totalement ordonné. En effet, les fonctions Id et $-$Id ne sont pas comparables. Et $\mathcal{F}(I,\mathbb{C})$ n'est pas ordonné (il n'est pas possible de définir un ordre sur $\mathbb{C}$).

Définition 1.4 *Fonction constante*

Soit $f \in \mathcal{F}(I,\mathbb{K})$. On dit que f est constante si

$$\exists a \in \mathbb{K}, \quad \forall x \in I, \quad f(x) = a.$$

Dans la suite, on note $\widetilde{a}$ la fonction constante égale à a.

Attention, la notation $\widetilde{a}$ n'est pas vraiment standard, et devrait être manipulée avec précaution en dehors du cercle familial.

⚠ Les objets a et $\widetilde{a}$ sont très différents !

Définition 1.5 *Maximum et minimum*

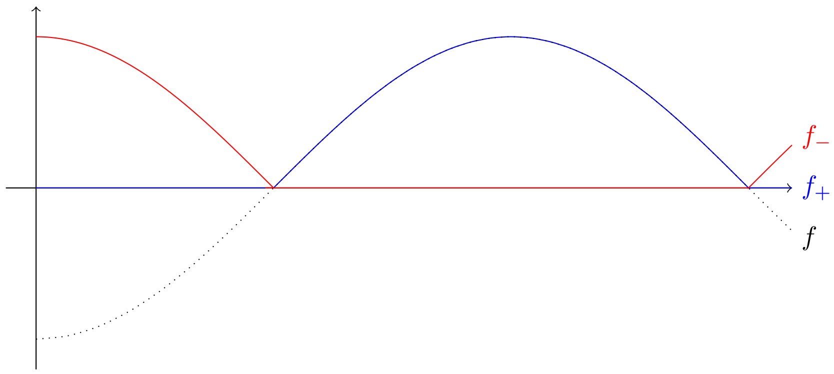
Soient $f, g \in \mathcal{F}(I, \mathbb{R})$. On définit

$$\max(f, g) : x \mapsto \max(f(x), g(x)), \quad \min(f, g) : x \mapsto \min(f(x), g(x)).$$

On note également

$$f_+ = \max\left(f, \widetilde{0}\right), \quad f_- = \max\left(-f, \widetilde{0}\right) = -\min\left(f, \widetilde{0}\right).$$

Pour bien comprendre ces définitions dans le cas des fonctions à valeurs réelles, il est vivement recommandé de faire un dessin.



Définition 1.6 *Module et valeur absolue*

Soit $f \in \mathcal{F}(I, \mathbb{C})$. On appelle *module de f* la fonction à valeurs réelles définie par

$$|f| : x \mapsto \sqrt{f(x)\,\overline{f(x)}}.$$

Lorsque f est à valeurs réelles, le module de f est appelé *valeur absolue de f*. On a alors

$$|f| = \max(f, -f) = f_+ + f_-.$$

2. Fonctions bornées

Définition 1.7 *Fonction bornée*

Soit $f \in \mathcal{F}(I, \mathbb{R})$. On dit que f est *majorée sur I* s'il existe $M \in \mathbb{R}$ tel que

$$\forall x \in I, \quad f(x) \leq M.$$

On dit que f est *minorée sur I* s'il existe $m \in \mathbb{R}$ tel que

$$\forall x \in I, \quad f(x) \geq m.$$

Soit $f \in \mathcal{F}(I, \mathbb{K})$. On dit que f est *bornée sur I* s'il existe $M \in \mathbb{R}$ tel que

$$\forall x \in I, \quad |f(x)| \leq M.$$

Exemple 1.8 :
Les fonctions $x \mapsto e^{ix}$, cos, sin et arctan sont bornées. La fonction $x \mapsto x^2$ est minorée mais pas majorée. $\diamond$

On pourra remarquer que, si f est à valeurs réelles, alors f est bornée si, et seulement si, f est majorée et minorée. En pratique, on utilise plutôt la définition avec la valeur absolue pour avoir un seul paramètre.

On ne parle pas de fonction majorée ou minorée si elle est à valeur dans $\mathbb{C}$, car on n'a pas défini d'ordre sur $\mathbb{C}$.

Proposition 1.9
Soient $f, g \in \mathcal{F}(I, \mathbb{K})$, et soit $\lambda \in \mathbb{K}$. Si f et g sont bornées sur I, alors $f+g$, $f \times g$ et $\lambda \cdot f$ sont bornées sur I.

Définition 1.10 *Borne inférieure et borne supérieure*
Soit $f \in \mathcal{F}(I, \mathbb{R})$. On définit, lorsque ces nombres existent

$$\sup_I (f) = \sup (f(I)), \quad \inf_I (f) = \inf (f(I)).$$

Proposition 1.11
Soit $f \in \mathcal{F}(I, \mathbb{R})$. Alors

(i) f est majorée sur I si, et seulement si, $\sup_I f$ existe.
(ii) f est minorée sur I si, et seulement si, $\inf_I f$ existe.

Démonstration : Aucune difficulté en revenant à la définition. Puisque $I \neq \emptyset$, alors $f(I) \neq \emptyset$. Puisque $f(I)$ est une partie non-vide de $\mathbb{R}$, elle est majorée si, et seulement si, elle admet une borne supérieure. Le point (ii) s'obtient de la même façon, ou en appliquant le point (i) à $-f$. $\square$

Définition 1.12 *Maximum et minimum*
Soit $f \in \mathcal{F}(I, \mathbb{R})$. On définit, lorsque ces nombres existent

$$\max_I (f) = \max (f(I)), \quad \min_I (f) = \min (f(I)).$$

Définition 1.13 *Extremum*
Soit $a \in I$. On dit que f *admet un maximum en* a si $f(a) = \max_I f$. On dit que f *admet un minimum en* a si $f(a) = \min_I f$. On dit que f *admet un extremum en* a si f admet un minimum ou un maximum en a.

Si $\max_I f$ existe, alors il est unique (par définition, c'est le maximum d'un sous ensemble de $\mathbb{R}$). En revanche, les points où le maximum de f est atteint ne sont pas forcément uniques. Par exemple, $\max_{\mathbb{R}} \cos = 1$ et cos admet un maximum en tout point de la forme $2k\pi$ avec $k \in \mathbb{Z}$.

Exemple 1.14 :
Soit $f : x \mapsto \mathrm{e}^{-x^2}$. La fonction f est majorée sur $\mathbb{R}$ et $\sup_{\mathbb{R}} f = 1$. On a également $\max_{\mathbb{R}} f = f(0) = 1 = \sup_{\mathbb{R}} f$. La fonction f est minorée sur $\mathbb{R}$ et $\inf_{\mathbb{R}} f = 0$, mais f n'admet pas de minimum sur $\mathbb{R}$ (f est strictement décroissante sur $\mathbb{R}_+$). ♢

3. Fonctions monotones

Cette section concerne uniquement les fonctions à valeurs réelles, comme tous les résultats faisant intervenir la structure d'ensemble ordonné de $\mathbb{R}$ (majoration, minoration, optimisation, etc.).

Définition 1.15 *Fonction monotone*
Soit $f \in \mathcal{F}(I, \mathbb{R})$. On dit que f est *croissante sur I* (resp. *décroissante sur I*) si, pour tous $x, y \in I$,

$$x \leq y \Rightarrow f(x) \leq f(y) \quad (\text{resp.} x \leq y \Rightarrow f(x) \geq f(y)).$$

On dit que f est *strictement croissante sur I* (resp. *strictement décroissante sur I*) si, pour tous $x, y \in I$,

$$x < y \Rightarrow f(x) < f(y) \quad (\text{resp.} x < y \Rightarrow f(x) > f(y)).$$

On dit que f est *monotone sur I* (resp. *strictement monotone sur I*) si f est croissante ou décroissante sur I (resp. strictement croissante ou strictement décroissante sur I).

Exemple 1.16 :
Les fonctions exp, ln et $x \mapsto \sqrt{x}$ sont croissantes. Attention, la fonction $x \mapsto \dfrac{1}{x}$ n'est pas monotone sur $\mathbb{R}^*$. ♢

En général, la somme ou le produit de fonctions monotones ne sont pas monotones (il faut aussi faire attention au signe des fonctions, et donc étudier au cas par cas). Par contre, la composition de deux fonctions monotone reste monotone.

Exemple 1.17 :
La fonction $\mathrm{Id}_{\mathbb{R}}$ est croissante sur $\mathbb{R}$. En revanche, $\mathrm{Id}_{\mathbb{R}} \times \mathrm{Id}_{\mathbb{R}}$ n'est pas monotone sur $\mathbb{R}$.

De même, les fonctions $x \mapsto -x$ et $x \mapsto x^3$ sont monotones sur $\mathbb{R}$, mais $x \mapsto x^3 - x$ n'est pas monotone sur $\mathbb{R}$. ♢

Proposition 1.18
Une fonction strictement monotone est injective.

Proposition 1.19
Soit $f \in \mathcal{F}(I, \mathbb{R})$. Alors

$$f \text{ est croissante} \iff -f \text{ est décroissante.}$$

4. Fonctions paires, fonctions impaires

Définition 1.20 *Fonction paire et fonction impaire*
Soit $f \in \mathcal{F}(I, \mathbb{K})$. On dit que f est *paire* si

$$\forall x \in I, \quad -x \in I \text{ et } f(-x) = f(x).$$

On dit que f est *impaire* si

$$\forall x \in I, \quad -x \in I \text{ et } f(-x) = -f(x).$$

Exemple 1.21 :
Les fonctions $x \mapsto |x|$, $x \mapsto x^2$, cos et ch sont paires. Les fonctions Id, $x \mapsto x^3$, sin et sh sont impaires. ♢

Le graphe d'une fonction paire est symétrique par rapport à l'axe des ordonnées. Le graphe d'une fonction impaire est symétrique par rapport à l'origine. En pratique, on limitera l'étude d'une fonction paire ou impaire à $I \cap \mathbb{R}_+$.

Proposition 1.22
Soient $f, g \in \mathcal{F}(I, \mathbb{K})$, et soit $\lambda \in \mathbb{K}$. Alors

1. si f et g sont paires, alors $f + g$, $f \times g$ et $\lambda \cdot f$ sont paires sur I.
2. si f et g sont impaires, alors $f + g$ et $\lambda \cdot f$ sont impaires sur I. En revanche, $f \times g$ est paire.

Proposition 1.23
Soit I un sous-ensemble de $\mathbb{R}$ symétrique par rapport à 0 (i.e. $\forall x \in I, -x \in I$). Soit $f \in \mathcal{F}(I, \mathbb{K})$. Alors f se décompose de manière unique comme somme d'une fonction paire φ et d'une fonction impaire ψ. De plus, on a

$$\forall x \in I, \quad \varphi(x) = \frac{f(x) + f(-x)}{2}, \quad \psi(x) = \frac{f(x) - f(-x)}{2}.$$

Démonstration : $\boxed{\text{Analyse}}$ Soit $f \in \mathcal{F}(I, \mathbb{K})$. On suppose qu'il existe $\varphi, \psi \in \mathcal{F}(I, \mathbb{K})$ telles que φ soit paire, ψ soit impaire et $f = \varphi + \psi$. On a alors,

$$\forall x \in I, \quad f(x) = \varphi(x) + \psi(x), \quad f(-x) = \varphi(x) - \psi(x).$$

On en déduit que

$$\forall x \in I, \quad \varphi(x) = \frac{f(x) + f(-x)}{2}, \quad \psi(x) = \frac{f(x) - f(-x)}{2}.$$

$\boxed{\text{Synthèse}}$ Soit $f \in \mathcal{F}(I, \mathbb{K})$. Soient $\varphi, \psi \in \mathcal{F}(I, \mathbb{K})$ les applications définies par

$$\forall x \in I, \quad \varphi(x) = \frac{f(x) + f(-x)}{2}, \quad \psi(x) = \frac{f(x) - f(-x)}{2}.$$

On a alors :

- pour tout $x \in I$, $\varphi(-x) = \dfrac{f(-x) + f(x)}{2} = \varphi(x)$ donc φ est paire.
- pour tout $x \in I$, $\psi(-x) = \dfrac{f(-x) - f(x)}{2} = -\dfrac{f(x) + f(-x)}{2} = -\psi(x)$ donc ψ est impaire.

- pour tout $x \in I$,
$$\varphi(x) + \psi(x) = \frac{f(x) + f(-x)}{2} + \frac{f(x) - f(-x)}{2} = \frac{2f(x)}{2} = f(x),$$
donc $f = \varphi + \psi$.

On a donc montré que f se décompose comme somme d'une fonction paire et d'une fonction impaire. L'unicité découle de l'analyse. □

En termes d'algèbre linéaire, les deux propositions précédentes se traduisent par "l'ensemble des fonctions paires et l'ensemble des fonctions impaires sur I sont deux sous-espaces vectoriels supplémentaires de $\mathcal{F}(I, \mathbb{K})$.

Exemple 1.24 :
Pour tout $x \in \mathbb{R}$, on a
$$\mathrm{e}^{ix} = \cos x + i \sin x, \quad \mathrm{e}^{x} = \operatorname{ch} x + \operatorname{sh} x.$$
♢

5. Fonctions périodiques

Définition 1.25 *Fonction périodique*
Soit $f \in \mathcal{F}(I, \mathbb{K})$ et soit $T > 0$. On dit que f est *T-périodique* si
$$\forall x \in I, \quad x + T \in I \text{ et } f(x+T) = -f(x).$$
On dit alors que T est *une période de f*.

En pratique, on limitera l'étude d'une fonction T-périodique à un intervalle de longueur T.

Exemple 1.26 :
Les fonctions cos et sin sont 2π périodiques. La fonction tan est π-périodique. ♢

Proposition 1.27
Soit $f \in \mathcal{F}(I, \mathbb{K})$ une fonction T-périodique. Alors, pour tout $n \in \mathbb{N}$ et pour tout $x \in I$,
$$x + nT \in I, \quad f(x+nT) = f(x).$$

Cette propriété peut s'interpréter comme "si T est une période de f, alors nT est aussi une période de f pour tout $n \in \mathbb{N}^*$". En particulier, une période d'une fonction périodique n'est pas unique.

Démonstration : Soit $x \in I$. Montrons par récurrence sur $n \in \mathbb{N}$ que
$$x + nT \in I, \quad f(x+nT) = f(x).$$

Initialisation : Évident.

Hérédité : Soit $n \in \mathbb{N}$, et supposons que
$$x + nT \in I, \quad f(x+nT) = f(x).$$
D'abord, $x + nT + T \in I$ par périodicité de f. De plus, on a
$$f(x + (n+1)T) = f(x+nT) = f(x),$$
ce qui achève la récurrence et la preuve. □

Exercice 1.28 :
Montrer qu'une fonction périodique et monotone est constante.

Réponse

Notons I le domaine de définition de f. Soit $T > 0$ une période de f. Quitte à considérer $-f$, on peut supposer que f est croissante. Soient $x, y \in I$ tels que $x < y$. Posons $n = E\left(\frac{y-x}{T}\right) + 1$. Alors $n \geq 1$ et

$$n > \frac{y-x}{T}, \quad x + nT > y.$$

Or, par croissance et périodicité de f,

$$f(x) = f(x+nT) \geq f(y) \geq f(x).$$

Ces inégalités sont donc des égalités, et donc $f(x) = f(y)$. On en déduit que f est constante sur I.

◊

Proposition 1.29

Soient $f, g \in \mathcal{F}(I, \mathbb{K})$, $\lambda \in \mathbb{K}$ et $T > 0$. Si f et g sont T-périodiques, alors $f+g$, $f \times g$ et $\lambda \cdot f$ sont T-périodiques.

6. Fonctions lipschitziennes

Définition 1.30 *Fonction lipschitzienne*[1]

Soit $f \in \mathcal{F}(I, \mathbb{K})$. On dit que f est *lipschitzienne sur I* si

$$\exists K \geq 0, \quad \forall x, y \in I, \quad |f(x) - f(y)| \leq K|x-y|.$$

On dit alors que f est *K-lipschitzienne*.

On dit que f est *contractante sur I* si f est K-lipschitzienne avec $K < 1$.

Exemple 1.31 :
Soient $a, b \in \mathbb{K}$. Alors l'application $f : x \mapsto ax + b$ est $|a|$-lipschitzienne sur $\mathbb{R}$. En effet, pour tous $x, y \in \mathbb{R}$,

$$f(x) - f(y) = ax + b - (ay + b) = a(x-y), \quad |f(x) - f(y)| = |a| \times |x-y|.$$

◊

Proposition 1.32

Soit $f \in \mathcal{F}(I, \mathbb{K})$, et soit $K \geq 0$. Si f est K-lipschitzienne, alors f est K'-lipschitzienne pour tout $K' \geq K$.

Proposition 1.33

Soient $f, g \in \mathcal{F}(I, \mathbb{K})$, et soit $\lambda \in \mathbb{K}$. Si f et g sont lipschitziennes, alors $f + g$ et $\lambda \cdot f$ sont lipschitziennes.

1. Rudolf Lipschitz (1832-1903) : Mathématicien allemand. Grosse moustache.

Le produit de deux fonctions lipschitziennes n'est pas lipschitzien en général.

Exercice 1.34 :
Soit $A > 0$. Montrer que la fonction $f : x \mapsto x^2$ est lipschitzienne sur $[-A, A]$, mais que f n'est pas lipschitzienne sur $\mathbb{R}$.

Réponse

Soient $x, y \in [-A, A]$. On a alors

$$|f(x) - f(y)| = |x^2 - y^2| = |x + y|.|x - y| \leq 2A|x - y|.$$

f est donc $2A$-lipschitzienne sur $[-A, A]$.

Supposons par l'absurde que f soit K-lipschitzienne sur $\mathbb{R}$. Alors, pour tous $x, y \in \mathbb{R}_+, y > x$,

$$y^2 - x^2 \leq K(y - x), \quad y + x \leq K.$$

Ceci est absurde si $x = K$ et $y = K + 1$. On en déduit que f n'est pas lipschitzienne sur $\mathbb{R}$.

$\diamondsuit$

Exercice 1.35 :
Soit $f \in \mathcal{F}(I, \mathbb{K})$. Alors f est 0-lipschitzienne si, et seulement si, f est constante.

Réponse

Si f est constante, alors il existe $\lambda \in \mathbb{K}$ tel que $f = \widetilde{\lambda}$. Alors, pour tous $x, y \in I$,

$$|f(x) - f(y)| = |\lambda - \lambda| = 0 \leq 0|x - y|,$$

donc f est 0-lipschitzienne. Réciproquement, supposons que f soit 0-lipschitzienne. Soit $x_0 \in I$. Alors, pour tout $x \in I$,

$$|f(x) - f(x_0)| \leq 0|x - x_0|, \quad f(x) = f(x_0),$$

donc $f = \widetilde{f(x_0)}$, et donc f est constante sur I.

$\diamondsuit$

Exercice 1.36 :
Montrer que cos est 1-lipschitzienne sur $\mathbb{R}$.

Réponse

Soient $x, y \in \mathbb{R}$.

$\boxed{\text{Méthode 1}}$ D'après les formules usuelles de trigonométrie, on sait que

$$\cos x - \cos y = -2\sin\left(\frac{x+y}{2}\right)\sin\left(\frac{x-y}{2}\right).$$

On sait également que, pour tout $t \in \mathbb{R}$, $|\sin t| \leq |t|$. On en déduit que

$$|\cos x - \cos y| = 2\left|\sin\left(\frac{x+y}{2}\right)\right|\left|\sin\left(\frac{x-y}{2}\right)\right| \leq 2\left|\sin\left(\frac{x-y}{2}\right)\right| \leq 2\left|\frac{x-y}{2}\right| = |x-y|.$$

Donc cos est 1-lipschitzienne sur $\mathbb{R}$.

$\boxed{\text{Méthode 2}}$ Cette méthode n'est pas vraiment d'actualité, puisqu'elle fait intervenir des résultats d'intégration (théorème fondamental de l'analyse, inégalité triangulaire, etc.) qui ne seront vus que plus tard. Par contre, elle s'applique à toutes les fonctions de classe $\mathcal{C}^1$ dont la dérivée est bornée. Bref, en supposant que $y > x$, on a

$$|\cos x - \cos y| = \left| \int_x^y (-\sin t)\, dt \right| \leq \int_x^y |-\sin t| dt \leq \int_x^y 1 dt = y - x = |y - x|.$$

Donc cos est 1-lipschitzienne sur $\mathbb{R}$.

$\diamondsuit$

Exemple 1.37 :
Montrer que la composition de deux fonctions lipschitziennes est encore lipschitzienne.

Réponse

Soient $f : I \to J, g : J \to \mathbb{K}$ avec I, J deux intervalles de $\mathbb{R}$. On suppose que f est K-lipschitzienne et que g est K'-lipschitzienne. Alors, pour tous $x, y \in D_g$,

$$|g \circ f(x) - g \circ f(y)| \leq K'|f(x) - f(y)| \leq KK'|x - y|.$$

Donc $g \circ f$ est KK'-lipschitzienne.

$\diamondsuit$

Exemple 1.38 :
Montrer que $x \mapsto \sqrt{x}$ n'est pas lipschitzienne sur $[0, 1]$.

Réponse

On a, pour tous $x, y \in]0, 1]$,

$$|\sqrt{x} - \sqrt{y}| = \left| \frac{x - y}{\sqrt{x} + \sqrt{y}} \right| = \frac{1}{|\sqrt{x} + \sqrt{y}|} |x - y|.$$

Or, pour tout $K > 0$, si $x, y < \dfrac{1}{4K^2}$ alors

$$\frac{1}{|\sqrt{x} + \sqrt{y}|} > \frac{1}{\frac{1}{2K} + \frac{1}{2K}} = K, \quad |\sqrt{x} - \sqrt{y}| > K|x - y|.$$

$\diamondsuit$

II Limite

A partir de maintenant, on va vouloir passer à la limite (en généralisant la démarche du cours de suites), et pour cela faire tendre une variable vers un point fixé x_0 de l'ensemble de définition. En particulier, on ne veut pas de "trou" dans cet ensemble de définition. [2] Cela signifie qu'on considèrera des applications définies sur des intervalles de $\mathbb{R}$.

2. Du moins, pas de trou autour du point d'intérêt x_0.

Dans la suite du chapitre, I donc est un intervalle non-trivial de $\mathbb{R}$ (c'est-à-dire possédant au moins deux éléments distincts). En pratique, on étudiera des applications définies sur un intervalle ou une réunion d'intervalles.

Les notions de limite et de continuité (comme celle de dérivabilité) sont des notions *locales*. Par exemple, pour étudier la continuité d'une fonction f en un point x_0, il suffit d'avoir des informations sur $f(x)$ lorsque x est proche de x_0. C'est cette notion de proximité que l'on définit avec les voisinages.

1. Voisinage

Cette première partie est optionnelle en première lecture. Elle sert à unifier toutes les définitions de limite sans avoir à différencier tous les cas (limite finie ou infinie en un point fini ou infini). Cette notion a un intérêt théorique, et permet de comprendre les choses, mais est trop compliquée à utiliser en pratique.

Définition 2.1 *Adhérence et intérieur*

Soit I un intervalle non-vide de $\mathbb{R}$. On note $a = \inf I$ et $b = \sup I$ lorsqu'ils existent. On appelle *adhérence de I* l'intervalle fermé $\overline{I} = [a, b]$. On appelle *intérieur de I* l'intervalle ouvert $\mathring{I} =]a, b[$.

Si $I =]-\infty, a]$ ou $]-\infty, a[$ avec $a \in \mathbb{R}$, on pose

$$\overline{I} = [-\infty, a] \subseteq \overline{\mathbb{R}}, \quad \mathring{I} =]-\infty, a[\subseteq \mathbb{R}.$$

Si $I = [a, +\infty[$ ou $]a, +\infty[$ avec $a \in \mathbb{R}$, on pose

$$\overline{I} = [a, +\infty] \subseteq \overline{\mathbb{R}}, \quad \mathring{I} =]a, +\infty[\subseteq \mathbb{R}.$$

On dira qu'un intervalle I est *non-trivial* si $\mathring{I} \neq \emptyset$.

Remarquons qu'un intervalle est non-trivial si, et seulement si, il possède au moins deux éléments distincts. Ces notations sont donc cohérentes avec la notation $\overline{\mathbb{R}}$.

Définition 2.2 *Boule ouverte et boule fermée dans le cas réel*

Soient $x \in \mathbb{R}$ et $\alpha > 0$. On appelle *boule fermée de centre x et de rayon α* l'intervalle

$$B_f(x, \alpha) = \overline{B}(x, \alpha) = [x - \alpha, x + \alpha].$$

On appelle *boule ouverte de centre x et de rayon α* l'intervalle

$$B(x, \alpha) = \mathring{B}(x, \alpha) =]x - \alpha, x + \alpha[.$$

Définition 2.3 *Boule ouverte et boule fermée dans le cas complexe*

Soient $z \in \mathbb{C}$ et $\alpha \geq 0$. On appelle *boule fermée de centre z et de rayon α* l'ensemble

$$B_f(z, \alpha) = \overline{B}(z, \alpha) = \{z' \in \mathbb{C} / |z - z'| \leq \alpha\}.$$

On appelle *boule ouverte de centre z et de rayon α* l'ensemble

$$B(z, \alpha) = \mathring{B}(z, \alpha) = \{z' \in \mathbb{C} / |z - z'| < \alpha\}.$$

Les notations des boules ouvertes et fermées sont consistantes avec celles de l'adhérence et de l'intérieur définies plus haut. On remarque que le cas complexe généralise le cas réel et donne son vrai sens au mot boule (une boule est ici un disque).

Définition 2.4 *Voisinage*

Soit $x \in \mathbb{K}$. On appelle *voisinage ouvert (resp. fermé) de* x toute boule ouverte (resp. fermée) de centre x et de rayon strictement positif.

On appelle *voisinage ouvert (resp. fermé) de* $-\infty$ tout intervalle de la forme $]-\infty, A[$ (resp. $]-\infty, A]$) avec $A \in \mathbb{R}$.

On appelle *voisinage ouvert (resp. fermé) de* $+\infty$ tout intervalle de la forme $]A, +\infty[$ (resp. $[A, +\infty[$) avec $A \in \mathbb{R}$.

Soit $x \in \overline{\mathbb{R}} \cup \mathbb{C}$. On note $\mathcal{V}_x$ l'ensemble des voisinages fermés de x.

Autrement dit, si $x \in \mathbb{R}$, $\mathcal{V}_x = \{[x-\alpha, x+\alpha] \subseteq \mathbb{R} / \alpha > 0\}$. On notera que x appartient à tous ses voisinages.

Tout ce qu'on dira dans la suite pour des voisinages fermés reste vrai pour des voisinages ouverts. Il suffit donc de choisir au début si l'on veut travailler avec des boules ouvertes (et des inégalités strictes) ou des boules fermées (et des inégalités larges, en général plus faciles à manier si l'on ne veut pas avoir à réfléchir).

Définition 2.5 *Propriété au voisinage d'un point*

Soient $f \in \mathcal{F}(I, \mathbb{R})$ et soit $x \in I$. On dit que f vérifie une propriété *au voisinage de* x s'il existe $V \in \mathcal{V}_x$ tel que f vérifie cette propriété sur $I \cap V$.

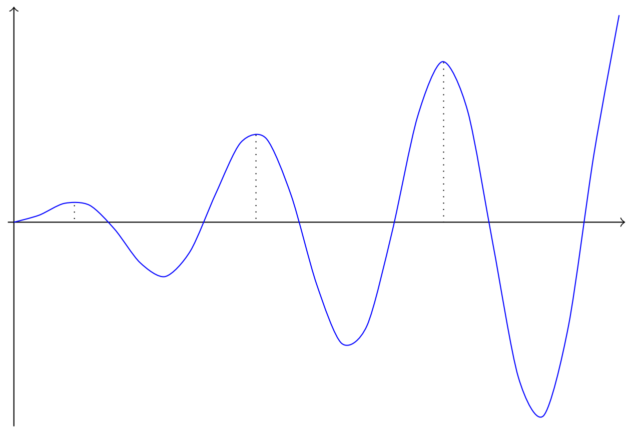
Exemple 2.6 :
La fonction $x \mapsto x^2$ est croissante au voisinage de 1. En effet, la fonction $x \mapsto x^2$ est croissante sur $[0, 2]$. Attention, cette fonction n'est pas croissante sur $\mathbb{R}$. $\diamondsuit$

Exemple 2.7 :
La fonction cos ne s'annule pas au voisinage de 0. En effet, cos ne s'annule pas sur $[-1, 1]$. Par contre, cos s'annule évidemment sur $\mathbb{R}$. $\diamondsuit$

En fait, les propriétés qui nous intéresseront dans la suite sont celles qui sont vraies sur un voisinage de x *et pour tout voisinage plus petit*, comme dans les exemples précédents.

Définition 2.8 *Extremum local*

Soit $a \in I$. On dit que f *admet un maximum local en* a s'il existe $V \in \mathcal{V}_a$, tel que $f(a) = \max\limits_V f$. On dit que f *admet un minimum local en* a s'il existe $V \in \mathcal{V}_a$, tel que $f(a) = \min\limits_V f$. On dit que f *admet un extremum local en* a si f admet un minimum local ou un maximum local en a.



2. Limite d'une fonction

Définition 2.9 *Limite d'une fonction à valeurs réelles*

Soit $f \in \mathcal{F}(I, \mathbb{R})$ et soit $x_0 \in \overline{I}$. On dit que f *admet une limite en* x_0 si

$$\exists \ell \in \overline{\mathbb{R}}, \quad \forall U \in \mathcal{V}_\ell, \quad \exists V \in \mathcal{V}_{x_0}, \quad \forall x \in I \cap V, \quad f(x) \in U.$$

Dans ce cas, on dit que f *admet* ℓ *pour limite en* x_0 ou que f *tend vers* ℓ *en* x_0. On note alors $\lim\limits_{x_0} f = \ell$ ou $\lim\limits_{x \to x_0} f(x) = \ell$ ou $f(x) \xrightarrow[x \to x_0]{} \ell$.

Définition 2.10 *Limite d'une fonction à valeurs complexes*

Soit $f \in \mathcal{F}(I, \mathbb{C})$ et soit $x_0 \in \overline{I}$. On dit que f *admet une limite en* x_0 si

$$\exists \ell \in \mathbb{C}, \quad \forall U \in \mathcal{V}_\ell, \quad \exists V \in \mathcal{V}_{x_0}, \quad \forall x \in I \cap V, \quad f(x) \in U.$$

Dans ce cas, on dit que f *admet* ℓ *pour limite en* x_0 ou que f *tend vers* ℓ *en* x_0. On note alors $\lim\limits_{x_0} f = \ell$ ou $\lim\limits_{x \to x_0} f(x) = \ell$ ou $f(x) \xrightarrow[x \to x_0]{} \ell$.

La seule différence entre le cas réel et le cas complexe est qu'une fonction à valeurs complexes ne peut pas "tendre vers l'infini" (la notion d'infini n'étant pas bien définie quand on parle de complexes).

Ces définitions sont abstraites, et pas vraiment maniables en pratique. Réécrivons-les pour quelques cas particuliers :

- Si $x_0 \in \mathbb{R}$ et $\ell \in \mathbb{K}$ alors
$$\lim_{x_0} f = \ell \iff \forall \varepsilon > 0, \quad \exists \alpha > 0, \quad \forall x \in I, \quad |x - x_0| \leq \alpha \Rightarrow |f(x) - \ell| \leq \varepsilon.$$
- Si $x_0 \in \mathbb{R}$ et $\ell = +\infty$ (cas $\mathbb{K} = \mathbb{R}$) alors
$$\lim_{x_0} f = \ell \iff \forall M \in \mathbb{R}, \quad \exists \alpha > 0, \quad \forall x \in I, \quad |x - x_0| \leq \alpha \Rightarrow f(x) \geq M.$$
- Si $x_0 = -\infty$ et $\ell \in \mathbb{K}$ alors
$$\lim_{-\infty} f = \ell \iff \forall \varepsilon > 0, \quad \exists A \in \mathbb{R}, \quad \forall x \in I, \quad x \leq A \Rightarrow |f(x) - \ell| \leq \varepsilon.$$
- Si $x_0 = +\infty$ et $\ell = -\infty$ (cas $\mathbb{K} = \mathbb{R}$) alors
$$\lim_{-\infty} f = \ell \iff \forall M \in \mathbb{R}, \quad \exists A \in \mathbb{R}, \quad \forall x \in I, \quad x \geq A \Rightarrow f(x) \leq M.$$

Proposition 2.11 *Unicité de la limite*
Soit $f \in \mathcal{F}(I, \mathbb{K})$ et soit $x_0 \in \overline{I}$. Si f admet une limite en x_0 alors celle-ci est unique.

Démonstration : Pour simplifier, on traite le cas $x_0 \in \mathbb{R}$ et $\mathbb{K} = \mathbb{R}$. Soient $\ell_1, \ell_2 \in \overline{\mathbb{R}}$ tels que

$$\lim_{x_0} f = \ell_1, \quad \lim_{x_0} f = \ell_2.$$

Premier cas : $\ell_1, \ell_2 \in \mathbb{R}$ Supposons, par l'absurde, que $\ell_1 \neq \ell_2$, et posons $\varepsilon = \dfrac{|\ell_1 - \ell_2|}{4} \in \mathbb{R}_+^*$. Par définition, il existe $\alpha_1, \alpha_2 > 0$ tels que

$$\forall x \in I, \quad \begin{cases} |x - x_0| \leq \alpha_1 \Rightarrow |f(x) - \ell_1| \leq \varepsilon \\ |x - x_0| \leq \alpha_2 \Rightarrow |f(x) - \ell_2| \leq \varepsilon \end{cases}.$$

Notons $\alpha = \min(\alpha_1, \alpha_2)$. Soit $x \in I \cap [x_0 - \alpha, x_0 + \alpha]$. On a alors, par inégalité triangulaire,

$$|\ell_1 - \ell_2| \leq |\ell_1 - f(x)| + |f(x) - \ell_2| \leq \varepsilon + \varepsilon = \frac{|\ell_1 - \ell_2|}{2},$$

ce qui est impossible. On en déduit que $\ell_1 = \ell_2$.

Second cas : $\ell_1 = +\infty, \ell_2 \in \mathbb{R}$ On va montrer que ce cas est absurde. En effet, dans les définitions de limites, on prend $M = \ell_2 + 2$ et $\varepsilon = 1$. Alors il existe $\alpha_1, \alpha_2 > 0$ tels que

$$\forall x \in I, \quad \begin{cases} |x - x_0| \leq \alpha_1 \Rightarrow f(x) \geq \ell_2 + 2 \\ |x - x_0| \leq \alpha_2 \Rightarrow |f(x) - \ell_2| \leq 1 \end{cases}.$$

Donc pour $x \in I \cap [x_0 - \alpha, x_0 + \alpha]$ avec $\alpha = \min(\alpha_1, \alpha_2)$, on a

$$f(x) \leq \ell_2 + 1, \quad f(x) \geq \ell_2 + 2,$$

ce qui est absurde.

Les cas $\ell_1 = -\infty, \ell_2 \in \mathbb{R}$ et $\ell_1 = -\infty, \ell_2 = +\infty$ sont absurdes aussi, donc dans tous les cas, $\ell_1 = \ell_2$. □

Exemple 2.12 :
A l'aide de la définition formelle, montrons que $\lim\limits_{x \to +\infty} \mathrm{e}^x = +\infty$ et $\lim\limits_{x \to -\infty} \mathrm{e}^x = 0$.

- Soit $M > 0$. Alors, pour tout $x \geq \ln M$, on a, par croissance de l'exponentielle,

  $$\mathrm{e}^x \geq \mathrm{e}^{\ln M} = M.$$

  On pose donc $A = \ln M$. On a donc bien montré que

  $$\forall M > 0, \quad \exists A \in \mathbb{R}, \quad \forall x \in [A, +\infty[, \quad \mathrm{e}^x \geq M.$$

  On en déduit que $\lim\limits_{+\infty} \exp = +\infty$.
- Soit $\varepsilon > 0$. Alors, pour tout $x \leq \ln \varepsilon$, on a, par croissance et positivité de l'exponentielle,

  $$0 \leq \mathrm{e}^x \leq \mathrm{e}^{\ln \varepsilon} = \varepsilon, \quad |\,\mathrm{e}^x\,| \leq \varepsilon.$$

  On pose donc $A = \ln \varepsilon$. On a donc bien montré que

  $$\forall \varepsilon > 0, \quad \exists A \in \mathbb{R}, \quad \forall x \in]-\infty, A], \quad |\,\mathrm{e}^x - 0| \leq \varepsilon.$$

  On en déduit que $\lim\limits_{-\infty} \exp = 0$.

$\diamondsuit$

Dans cet exemple, il nous suffit de considérer ε *petit* et M *grand* (ici, on a même pris $M > 0$).

Proposition 2.13

Soit $f \in \mathcal{F}(I, \mathbb{K})$ et soit $x_0 \in \overline{I}$. Alors

(i) Si f admet une limite finie en x_0 alors f est bornée au voisinage de x_0.
(ii) Si $\mathbb{K} = \mathbb{R}$, et $\lim\limits_{x \to x_0} f(x) = \pm\infty$, alors f n'est pas bornée.

Que peut-on dire des réciproques ?

Démonstration : (i) Supposons que $\lim\limits_{x_0} f = \ell \in \mathbb{K}$. Posons $\varepsilon = 1$. Alors

$$\exists V \in \mathcal{V}_{x_0}, \quad \forall x \in V \cap I, \quad |f(x) - \ell| \leq 1, \quad |f(x)| \leq |f(x) - \ell| + |\ell| \leq |\ell| + 1.$$

Donc f est bornée sur V.

(ii) Supposons que $\mathbb{K} = \mathbb{R}$, et que $\lim\limits_{x \to x_0} f(x) = \pm\infty$. Alors,

$$\forall M > 0, \quad \exists V \in \mathcal{V}_{x_0}, \quad \forall x \in I \cap V, \quad |f(x)| \geq M,$$

donc f n'est pas bornée.

$\square$

Exercice 2.14 :

Soit $f : \begin{array}{ccc}]0, +\infty[& \to & \mathbb{R} \\ x & \mapsto & \sin(1/x) \end{array}$. f admet-elle une limite en 0 ?

Réponse

On va montrer que f n'admet pas de limite en 0. Tout d'abord, f est bornée donc il est impossible que $\lim\limits_{0} f = +\infty$ ou $\lim\limits_{0} f = -\infty$. Soit $\ell \in \mathbb{R}$, posons $\varepsilon = \dfrac{1}{2}$. Supposons que $\ell \geq 0$. Alors, pour tout $\alpha > 0$, posons

$$n = E\left(\frac{1}{2\pi}\left(\frac{1}{\alpha} + \frac{\pi}{2}\right)\right) + 1, \quad x = \frac{1}{2n\pi - \frac{\pi}{2}}.$$

Alors

$$n \geq \frac{1}{2\pi}\left(\frac{1}{\alpha} + \frac{\pi}{2}\right), \quad \frac{1}{x} \geq \frac{1}{\alpha}, \quad 0 < x \leq \alpha$$

et $f(x) = -1$, donc $f(x) < 0 - \dfrac{1}{2} \leq \ell - \dfrac{1}{2}$. On a donc montré que

$$\forall l \geq 0, \quad \exists \varepsilon > 0, \quad \forall \alpha > 0, \quad \exists x \in \mathbb{R}_+^* \cap [-\alpha, \alpha], \quad |f(x) - \ell| > \varepsilon.$$

On raisonne de la même manière si $\ell \leq 0$, ce qui prouve que f n'admet pas de limite en 0.

$\diamondsuit$

Proposition 2.15 *Reformulation de la limite*

Soit $f \in \mathcal{F}(I, \mathbb{K})$ et soit $x_0 \in \overline{I}$. Alors

(i) Si $\ell = 0$,
$$\lim_{x \to x_0} f(x) = 0 \iff \lim_{x \to x_0} |f(x)| = 0.$$

(ii) Si $\ell \in \mathbb{K}$,
$$\lim_{x \to x_0} f(x) = \ell \iff \lim_{x \to x_0} (f(x) - \ell) = 0 \iff \lim_{x \to x_0} |f(x) - \ell| = 0.$$

(iii) Si $x_0 \in \mathbb{R}$,
$$\lim_{x \to x_0} f(x) = \ell \iff \lim_{h \to 0} f(x_0 + h) = \ell.$$

Il s'agit simplement de réécrire les définitions. Aucune difficulté, mais c'est un bon exercice pour s'assurer que l'on a compris.

$\lim_{x_0} f = \ell \Rightarrow \lim_{x_0} |f| = |\ell|$ mais la réciproque n'est pas vraie.

3. Caractérisation séquentielle de la limite

Le théorème suivant peut être très utile en pratique, car il ramène des calculs fastidieux avec des ε à des calculs de limites de suites que l'on sait déjà étudier.

Théorème 2.16 *Caractérisation séquentielle de la limite*

Soient $f \in \mathcal{F}(I, \mathbb{K})$ et $x_0 \in \overline{I}$. Soit $\ell \in \overline{\mathbb{R}}$ (si $\mathbb{K} = \mathbb{R}$) ou $\ell \in \mathbb{C}$ (si $\mathbb{K} = \mathbb{C}$). Alors
$$\lim_{x_0} f = \ell \iff \forall (u_n) \in I^{\mathbb{N}}, \quad \left(\lim_{n \to +\infty} u_n = x_0 \Rightarrow \lim_{n \to +\infty} f(u_n) = \ell \right).$$

Démonstration : On fait la preuve dans le cas $x_0 \in \mathbb{R}$ et $\ell \in \mathbb{K}$ (les cas "infinis" se traitant de manière similaire).

$\boxed{\Rightarrow}$ Supposons que $\lim_{x_0} f = \ell$. Soit $(u_n) \in I^{\mathbb{N}}$ telle que $\lim (u_n) = x_0$. Alors
$$\forall \varepsilon > 0, \exists \alpha > 0, \forall x \in I \cap [x_0 - \alpha, x_0 + \alpha], |f(x) - \ell| \leq \varepsilon.$$

De plus,
$$\exists N \in \mathbb{N}, \forall n \geq N, |u_n - x_0| \leq \alpha.$$

On en déduit que
$$\forall n \geq N, \quad |f(u_n) - \ell| \leq \varepsilon,$$

ce qui achève la preuve de l'implication.

$\boxed{\Leftarrow}$ On va montrer la contraposée. Supposons donc que
$$\exists \varepsilon > 0, \quad \forall \alpha > 0, \quad \exists x \in I \cap [x_0 - \alpha, x_0 + \alpha], \quad |f(x) - \ell| > \varepsilon.$$

En particulier, notons pour $n \in \mathbb{N}^*$, $\alpha_n = \dfrac{1}{n}$. Alors il existe $x_n \in I \cap \left[x_0 - \dfrac{1}{n}, x_0 + \dfrac{1}{n}\right]$, tel que $|f(x_n) - \ell| > \varepsilon$. On vient donc de construire une suite (x_n) qui converge vers x_0 mais telle que $(f(x_n))$ n'admet pas ℓ pour limite, ce qui achève la preuve de ce théorème. □

En fait, ce théorème est très pratique pour trouver des contre-exemples.

Exemple 2.17 :
Montrer que la fonction cos n'admet pas de limite en $+\infty$.

Réponse

Pour $n \in \mathbb{N}$, on note

$$u_n = 2\pi n, \quad v_n = 2\pi n + \frac{\pi}{2}.$$

Alors les suites (u_n) et (v_n) vérifient $\lim(u_n) = \lim(v_n) = +\infty$ et

$$\lim_{n\to+\infty} \cos(u_n) = 1, \quad \lim_{n\to+\infty} \cos(v_n) = 0.$$

Par la caractérisation séquentielle de la limite, il est donc impossible que cos admette une limite en $+\infty$.

♢

4. Limites à gauche et à droite

Définition 2.18 *Limite à gauche et à droite*

Soit $f \in \mathcal{F}(I, \mathbb{K})$ et soit $x_0 \in \overline{I} \cap \mathbb{R}$. Si $x_0 \neq \inf I$, on définit la *limite à gauche de f en x_0* (si elle existe) :

$$\lim_{x_0^-} f = \lim_{x\to x_0^-} f(x) = \lim_{\substack{x\to x_0 \\ x<x_0}} f(x) = \lim_{x_0} \left(f_{|I\cap]-\infty,x_0[}\right).$$

Si $x_0 \neq \sup I$, on définit la *limite à droite de f en x_0* (si elle existe) :

$$\lim_{x_0^+} f = \lim_{x\to x_0^+} f(x) = \lim_{\substack{x\to x_0 \\ x>x_0}} f(x) = \lim_{x_0} \left(f_{|I\cap]x_0,+\infty[}\right).$$

Par définition, la limite en $+\infty$ est toujours une limite à gauche, et la limite en $-\infty$ est toujours une limite à droite.

On définit de la même manière la *limite épointée de f en x_0* $\in \mathring{I}$:

$$\lim_{\substack{x\to x_0 \\ x\neq x_0}} f(x) = \lim_{x_0} \left(f_{|I\setminus\{x_0\}}\right)$$

Définition 2.19 *Limite ℓ^- et ℓ^+*

Soit $f \in \mathcal{F}(I, \mathbb{R})$ et soit $x_0 \in \overline{I}$. Soit $\ell \in \mathbb{R}$. On note

$$\lim_{x_0} f = \ell^- \iff \begin{cases} \lim_{x_0} f = \ell \\ f \leq \ell \text{ au voisinage de } x_0 \end{cases} , \quad \lim_{x_0} f = \ell^+ \iff \begin{cases} \lim_{x_0} f = \ell \\ f \geq \ell \text{ au voisinage de } x_0 \end{cases}$$

Exercice 2.20 :
Étudier la limite, la limite épointée, la limite à gauche et la limite à droite de la fonction partie entière E en 0. ♢

5. Manipulation de limites

Avant de manipuler des limites, on doit toujours justifier qu'elles existent.

Proposition 2.21 *Opérations sur les limites finies*
Soient $f, g \in \mathcal{F}(I, \mathbb{K})$ et $x_0 \in \overline{I}$. Supposons que $\lim\limits_{x_0} f = \ell \in \mathbb{K}$ et $\lim\limits_{x_0} g = \ell' \in \mathbb{K}$. Alors :

(i) $f + g$ admet une limite en x_0 et

$$\lim_{x_0} (f + g) = \ell + \ell'.$$

(ii) $f \times g$ admet une limite en x_0 et

$$\lim_{x_0} (f \times g) = \ell\ell'.$$

(iii) Pour tout $\lambda \in \mathbb{K}$, λf admet une limite en x_0 et

$$\lim_{x_0} (\lambda f) = \lambda\ell.$$

(iv) Si $\ell' \neq 0$ alors $\dfrac{f}{g}$ admet une limite en x_0 et

$$\lim_{x_0} \frac{f}{g} = \frac{\ell}{\ell'}.$$

Démonstration : Puisqu'on a déjà démontré ce genre de propriétés pour les suites, on va le réutiliser grâce à la caractérisation séquentielle de la limite. Soit $(u_n) \in I^{\mathbb{N}}$ vérifiant $\lim (u_n) = x_0$. Alors $\lim (f(u_n)) = \ell$ et $\lim (g(u_n)) = \ell'$. Classiquement, on a donc, pour tout $\lambda \in \mathbb{K}$,

$$\lim_{n\to+\infty} f(u_n) + g(u_n) = \ell + \ell', \quad \lim_{n\to+\infty} f(u_n) \times g(u_n) = \ell\ell', \quad \lim_{n\to+\infty} \lambda f(u_n) = \lambda\ell, \quad \lim_{x_0} \frac{f(u_n)}{g(u_n)} = \frac{\ell}{\ell'}.$$

Toujours d'après la caractérisation séquentielle de la limite, on a donc

$$\lim_{x_0} (f + g) = \ell + \ell', \quad \lim_{x_0} (f \times g) = \ell\ell', \quad \lim_{x_0} (\lambda f) = \lambda\ell, \quad \lim_{x_0} \frac{f}{g} = \frac{\ell}{\ell'}.$$

□

Exercice 2.22 :
Redémontrer ces résultats en revenant à la définition de limite. ♢

De la même manière, on a des formulaires concernant la somme, le produit et le quotient de fonctions, qui suivent les règles de calcul dans $\overline{\mathbb{R}}$.

Proposition 2.23 *Limite de la somme*

On a le formulaire suivant pour la limite de la somme dans $\overline{\mathbb{R}}$. Soient $f, g \in \mathcal{F}(I, \mathbb{R})$, $x_0 \in \overline{I}$. Supposons que $\lim\limits_{x_0} f = \ell$ et $\lim\limits_{x_0} g = \ell'$. Alors

$\lim\limits_{x_0}(f+g)$	$\ell' \in \mathbb{R}$	$\ell' = +\infty$	$\ell' = -\infty$
$\ell \in \mathbb{R}$	$\ell + \ell'$	$+\infty$	$-\infty$
$\ell = +\infty$	$+\infty$	$+\infty$	??
$\ell = -\infty$	$-\infty$	??	$-\infty$

Attention à la forme indéterminée $(+\infty) + (-\infty)$.

Exemple 2.24 :
Soit $f : x \mapsto x + \cos x$ et $g : x \mapsto -x$. Alors f et g admettent une limite en $+\infty$, mais $f + g$ n'admet pas de limite en $+\infty$. $\diamondsuit$

Proposition 2.25 *Limite du produit*

On a le formulaire suivant pour la limite du produit dans $\overline{\mathbb{R}}$. Soient $f, g \in \mathcal{F}(I, \mathbb{R})$, $x_0 \in \overline{I}$. Supposons que $\lim\limits_{x_0} f = \ell$ et $\lim\limits_{x_0} g = \ell'$. Alors

$\lim\limits_{x_0}(f \times g)$	$\ell' > 0$	$\ell' < 0$	$\ell' = 0$	$\ell' = +\infty$	$\ell' = -\infty$
$\ell > 0$	$\ell \times \ell'$	$\ell \times \ell'$	0	$+\infty$	$-\infty$
$\ell < 0$	$\ell \times \ell'$	$\ell \times \ell'$	0	$-\infty$	$+\infty$
$\ell = 0$	0	0	0	??	??
$\ell = +\infty$	$+\infty$	$-\infty$	??	$+\infty$	$-\infty$
$\ell = -\infty$	$-\infty$	$+\infty$	??	$-\infty$	$+\infty$

Attention à la forme indéterminée $(\pm\infty) \times 0$.

Proposition 2.26 *Limite du quotient*

On a le formulaire suivant pour la limite du quotient dans $\overline{\mathbb{R}}$. Soient $f, g \in \mathcal{F}(I, \mathbb{R})$, $x_0 \in \overline{I}$. Supposons que $\lim\limits_{x_0} f = \ell$ et $\lim\limits_{x_0} g = \ell'$. Alors

$\lim\limits_{x_0} \frac{f}{g}$	$\ell' > 0$	$\ell' < 0$	$\ell' = 0^+$	$\ell' = 0^-$	$\ell' = +\infty$	$\ell' = -\infty$
$\ell > 0$	ℓ/ℓ'	ℓ/ℓ'	$+\infty$	$-\infty$	0^+	0^-
$\ell < 0$	ℓ/ℓ'	ℓ/ℓ'	$-\infty$	$+\infty$	0^-	0^+
$\ell = 0^+$	0^+	0^-	??	??	0^+	0^-
$\ell = 0^-$	0^-	0^+	??	??	0^-	0^+
$\ell = +\infty$	$+\infty$	$-\infty$	$+\infty$	$-\infty$	??	??
$\ell = -\infty$	$-\infty$	$+\infty$	$-\infty$	$+\infty$	??	??

Attention aux formes indéterminées $\dfrac{\pm\infty}{\pm\infty}$ et $\dfrac{0^{\pm}}{0^{\pm}}$ (formes indéterminées héritées du produit).

Exemple 2.27 :

$\lim\limits_{+\infty} \dfrac{x^2}{x} = +\infty$ et $\lim\limits_{+\infty} \dfrac{x}{x^2} = 0$.

◊

Proposition 2.28

Soient $f, g \in \mathcal{F}(I, \mathbb{K})$ et $x_0 \in \overline{I}$. Si $\lim\limits_{x_0} f = 0$ et si g est bornée au voisinage de x_0, alors $\lim\limits_{x_0} (f \times g) = 0$.

Démonstration : Soit $\varepsilon > 0$. Alors il existe $\alpha_1 > 0$ tel que

$$\exists M > 0, \forall x \in I \cap [x_0 - \alpha_1, x_0 + \alpha_1], \quad |g(x) \leq M.$$

Alors, il existe $\alpha_2 > 0$ (et on peut supposer $\alpha_2 \leq \alpha_1$), tel que

$$\forall x \in I \cap [x_0 - \alpha_2, x_0 + \alpha_2], \quad |f(x)| \leq \frac{\varepsilon}{M}.$$

Alors

$$\forall x \in I \cap [x_0 - \alpha_2, x_0 + \alpha_2], \quad |f(x) g(x)| = |f(x)|.|g(x)| \leq M \frac{\varepsilon}{M} = \varepsilon.$$

Donc $\lim\limits_{x_0} (fg) = 0$. Encore une fois, la caractérisation séquentielle aurait pu nous permettre de conclure directement. □

Proposition 2.29

Soient I et J deux intervalles de $\mathbb{R}$. Soit $f \in \mathcal{F}(I, J)$ et $g \in \mathcal{F}(J, \mathbb{K})$. Soient $x_0 \in \overline{I}$ et $y_0 \in \overline{J}$. Si

$$\lim_{x \to x_0} f(x) = y_0, \quad \lim_{y \to y_0} g(y) = \ell,$$

alors $\lim\limits_{x_0} (g \circ f) = \ell$.

Démonstration : Supposons que $\lim\limits_{x_0} f = y_0$ et $\lim\limits_{y_0} g = \ell$. Pour simplifier, on suppose que $y_0 \in \mathbb{R}$. Soit $\varepsilon > 0$. Alors

$$\exists \beta > 0, \quad \forall y \in J, \quad |y - y_0| \leq \beta \Rightarrow |g(y) - \ell| \leq \varepsilon.$$

De plus,

$$\exists \alpha > 0, \quad \forall x \in I, \quad |x - x_0| \leq \alpha \Rightarrow |f(x) - y_0| \leq \beta \Rightarrow |g \circ f(x) - \ell| \leq \varepsilon.$$

On en déduit que $\lim\limits_{x_0} (g \circ f) = \ell$. □

Exemple 2.30 :
On a $\lim\limits_{x \to -\infty} \exp\left(-x^2\right) = 0^+$ et $\lim\limits_{x \to +\infty} \exp\left(-x^2\right) = 0^+$. En effet,

$$\lim_{x \to -\infty} -x^2 = -\infty, \quad \lim_{y \to -\infty} e^y = 0^+, \quad \lim_{x \to -\infty} \mathrm{e}^{-x^2} = 0^+.$$

De même,

$$\lim_{x \to +\infty} -x^2 = -\infty, \quad \lim_{y \to -\infty} e^y = 0^+, \quad \lim_{x \to +\infty} \mathrm{e}^{-x^2} = 0^+.$$

◊

6. Limite et relation d'ordre

Évidemment, on considère uniquement des fonctions à valeurs réelles dans cette partie.

Proposition 2.31

Soit $f \in \mathcal{F}(I, \mathbb{R})$ et soit $x_0 \in I$. Supposons qu'il existe $\ell \in]0, +\infty]$ tel que $\lim_{x_0} f = \ell$. Alors f est strictement positive au voisinage de x_0.

Démonstration : Si $\ell = +\infty$, le résultat est vrai par définition (prendre $M = 1$). Sinon, posons $\varepsilon = \dfrac{\ell}{2}$. Alors

$$\exists V \in \mathcal{V}_{x_0}, \quad \forall x \in I \cap V, \quad \ell - \varepsilon \leq f(x) \leq \ell + \varepsilon, \quad 0 < \frac{\ell}{2} \leq f(x),$$

donc f est strictement positive sur $V \cap I$. $\square$

Proposition 2.32

Soient $f, g \in \mathcal{F}(I, \mathbb{R})$, $x_0 \in \overline{I}$ et $M \in \mathbb{R}$. Alors

(i) Si f et g admettent des limites en x_0 et si $f \leq g$ au voisinage de x_0 alors

$$\lim_{x_0} f \leq \lim_{x_0} g.$$

(ii) Si f admet une limite en x_0 et si $f \leq M$ au voisinage de x_0 alors

$$\lim_{x_0} f \leq M.$$

(iii) Si $f \leq g$ au voisinage de x_0 et si $\lim_{x_0} f = +\infty$, alors g admet une limite en x_0 et

$$\lim_{x_0} g = +\infty.$$

Cette proposition englobe aussi les cas ou les limites sont infinies (autrement dit, les inégalités ont lieu dans $\overline{\mathbb{R}}$). On pourra évidemment appliquer (ii) avec l'inégalité inverse et (iii) avec l'inégalité inverse quand $\lim f = -\infty$.

Démonstration : $\boxed{(i)}$ On suppose que $x_0 \in \mathbb{R}$ pour simplifier l'écriture de la preuve. On suppose donc que f et g admettent des limites en x_0, notées respectivement ℓ et ℓ', et que $f \leq g$ au voisinage de x_0. Les cas infinis sont évidents, et le cas $\ell = +\infty$ et $\ell' = -\infty$ est absurde (à faire !). On suppose donc que $\ell, \ell' \in \mathbb{R}$. Soit $\varepsilon > 0$. Alors

$$\exists \alpha > 0, \forall x \in I, |x - x_0| \leq \alpha \Rightarrow |f(x) - \ell| \leq \varepsilon, \quad \exists \alpha' > 0, \forall x \in I, |x - x_0| \leq \alpha' \Rightarrow |g(x) - \ell'| \leq \varepsilon.$$

Il existe aussi $\alpha'' > 0$ tel que

$$\forall x \in [x_0 - \alpha'', x_0 + \alpha''] \cap I, \quad f(x) \leq g(x).$$

En particulier, pour en notant $\beta = \min(\alpha, \alpha', \alpha'')$, pour tout $x \in I \cap [x_0 - \beta, x_0 + \beta]$,

$$\ell \leq f(x) + \varepsilon \leq g(x) + \varepsilon \leq \ell' + \varepsilon + \varepsilon, \quad \ell \leq \ell' + 2\varepsilon.$$

Cette inégalité étant vraie pour tout $\varepsilon > 0$, on a $\ell \leq \ell'$.

$\boxed{(ii)}$ Conséquence directe de (i) lorsque $g = \widetilde{M}$.

$\boxed{(iii)}$ Soit $M > 0$. Il existe $\alpha, \alpha' > 0$ tel que, pour tout $x \in I$,

$$|x - x_0| \leq \alpha \Rightarrow f(x) \geq M, \quad |x - x_0| \leq \alpha' \Rightarrow g(x) \geq f(x).$$

En notant $\alpha'' = \min(\alpha, \alpha')$, pour tout $x \in I \cap [x_0 - \alpha'', x_0 + \alpha'']$, $g(x) \geq f(x) \geq M$ donc $\lim_{x_0} g = +\infty$. □

⚠ Les inégalités strictes <u>ne sont pas conservées</u> par passage à la limite. Si $f > M$ sur I alors $\lim_{x_0} f \geq M$ (si elle existe). En effet,

$$\forall x \in \mathbb{R}_+^*, \quad \frac{1}{x} > 0, \quad \lim_{x \to +\infty} \frac{1}{x} = 0.$$

Théorème 2.33 *Théorème des gendarmes*

Soient $f, g, h \in \mathcal{F}(I, \mathbb{R})$ et soit $x_0 \in \overline{I}$. Supposons qu'il existe $\ell \in \overline{\mathbb{R}}$ tel que $\lim_{x_0} g = \lim_{x_0} h = \ell$ et que $g \leq f \leq h$ au voisinage de x_0. Alors f admet une limite en x_0 et $\lim_{x_0} f = \ell$.

Démonstration : Soit $(u_n) \in I^{\mathbb{N}}$ convergeant vers x_0. Alors, par caractérisation séquentielle de la limite,

$$\lim(h(u_n)) = \lim(g(u_n)) = \ell,$$

De plus, puisque $g \leq f \leq h$ au voisinage de x_0, il existe $n_0 \in \mathbb{N}$ tel que, pour tout $n \geq n_0$,

$$g(u_n) \leq f(u_n) \leq h(u_n).$$

Par le théorème des gendarmes pour les suites, on en déduit que $\lim(f(u_n)) = \ell$. Donc, par caractérisation séquentielle, f admet une limite en x_0 et $\lim_{x_0} f = \ell$. □

Théorème 2.34 *Théorème de la limite monotone*

Soit $f \in \mathcal{F}(I, \mathbb{R})$ et soit $x_0 \in \overline{I}$. On suppose que f est croissante sur I. Alors

(i) Si $x_0 = \sup I$ (ou $x_0 = +\infty$ si I n'est pas majoré), alors f admet une limite à gauche en x_0, qui est finie si, et seulement si, f est majorée.

(ii) Si $x_0 = \inf I$ (ou $x_0 = -\infty$ si I n'est pas minoré), alors f admet une limite à droite en x_0, qui est finie si, et seulement si, f est minorée.

(iii) Si $x_0 \in \mathring{I}$, alors f admet des limites à gauche et à droite finies en x_0 qui vérifient

$$\lim_{x_0^-} f \leq f(x_0) \leq \lim_{x_0^+} f.$$

Remarque 2.35 : Ce théorème reste bien évidemment valable pour une fonction décroissante. Il suffit de renverser le sens de toutes les inégalités et d'échanger "minoré" et "majoré". ◇

Démonstration : Comme d'habitude, on suppose pour simplifier que $x_0 \in \mathbb{R}$. Les trois cas se démontrent de manière très similaire, on va donc juste montrer le point (i).

Si f n'est pas majorée sur I alors f n'est pas majorée sur $I \setminus \{x_0\}$ (évident si $x_0 \notin I$, presque évident par l'absurde sinon). Alors, pour tout $M > 0$, il existe $x \in I \setminus \{x_0\}$ tel que $f(x) \geq M$. On pose alors $\alpha = x_0 - x > 0$. Puisque f est croissante alors, pour tout $x \in [x_0 - \alpha, x_0[$, $f(x) \geq M$. On en déduit que $\lim_{x_0^-} f = +\infty$.

Si f est majorée, notons $\ell = \sup f_{|I\setminus\{x_0\}}$. Soit $\varepsilon > 0$. Par définition de la borne supérieure, il existe $x \in I \setminus \{x_0\}$ tel que

$$\ell - \varepsilon \leq f(x) \leq \ell.$$

Notons $\alpha = x_0 - x$. Alors, par croissance de f et par définition de ℓ, pour tout $x \in [x_0 - \alpha, x_0[$,

$$\ell - \varepsilon \leq f(x) \leq \ell.$$

On en déduit que $\lim\limits_{x_0^-} f = \ell$. □

On déduit de ces résultats un théorème fondamental en pratique.

Théorème 2.36 *Théorème des croissances comparées*

Soit $a > 0$. Alors

$$\lim_{x\to+\infty} \frac{\mathrm{e}^x}{x^a} = +\infty, \qquad \lim_{x\to-\infty} |x|^a \,\mathrm{e}^x = 0, \qquad \lim_{x\to+\infty} \frac{\ln x}{x^a} = 0, \qquad \lim_{x\to 0^+} x^a \ln x = 0.$$

Démonstration : Soit $a > 0$.

- La fonction $t \mapsto \mathrm{e}^t - t$ est positive sur $\mathbb{R}_+$ (par convexité ou simple étude de fonction). On en déduit que, pour tout $x \geq 0$
$$\exp\left(\frac{x}{a+1}\right) \geq \frac{x}{a+1}, \qquad \mathrm{e}^x \geq \frac{x^{a+1}}{(a+1)^{a+1}}, \qquad \frac{\mathrm{e}^x}{x^a} \geq \frac{x}{(a+1)^{a+1}} \xrightarrow[x\to+\infty]{} +\infty.$$
Donc $\lim\limits_{x\to+\infty} \frac{\mathrm{e}^x}{x^a} = +\infty$.
- Soit $x < 0$. En posant $t = -x$, on a
$$\lim_{x\to-\infty} |x|^a \,\mathrm{e}^x = \lim_{t\to+\infty} \frac{t^a}{\mathrm{e}^t} = 0.$$
- Soit $x > 0$. En posant $t = \ln x$, on a
$$\lim_{x\to+\infty} \frac{\ln x}{x^a} = \lim_{t\to+\infty} \frac{\mathrm{e}^{at}}{t} = +\infty.$$
- Soit $x > 0$. En posant $t = \ln x$, on a
$$\lim_{x\to 0^+} x^a \ln x = \lim_{t\to-\infty} t\,\mathrm{e}^{at} = 0.$$

□

III Relations de comparaison

Comme pour les suites, les relations de comparaison vont s'avérer cruciales pour déterminer le comportement local (ou asymptotique) de fonctions compliquées : on va les comparer à des fonctions connues.

Dans la suite, on introduit les notations de Landau [3] : $o, \mathcal{O}, \sim$.

1. Fonctions négligeables, fonctions dominées

3. Edmund Landau (1877-1938) : Mathématicien allemand. Grosse moustache.

Définition 3.1 *Fonction négligeable*

Soient $f, g \in \mathcal{F}(I, \mathbb{K})$ et soit $x_0 \in \overline{I}$. On dit que f ***est négligeable devant*** g ***au voisinage de*** x_0, si

$$\forall \varepsilon > 0, \quad \exists V \in \mathcal{V}_{x_0}, \quad \forall x \in I \cap V, \quad |f(x)| \leq \varepsilon |g(x)|.$$

On note alors $f \underset{x_0}{=} o(g)$ ou $f(x) \underset{x \to x_0}{=} o(g(x))$

On remarquera que, si $x_0 \in I$ alors

$$f \underset{x_0}{=} o(g) \Rightarrow f(x_0) = 0.$$

Proposition 3.2

Soient $f, g \in \mathcal{F}(I, \mathbb{K})$ et soit $x_0 \in \overline{I}$. Alors

$$f \underset{x_0}{=} o(g) \iff \exists V \in \mathcal{V}_{x_0}, \exists h \in \mathcal{F}(I \cap V, \mathbb{K}), \quad \begin{cases} f = gh \\ \lim_{x_0} h = 0 \end{cases}.$$

Démonstration : $\boxed{\Leftarrow}$ C'est la définition de limite :

$$\forall \varepsilon > 0, \exists V \in \mathcal{V}_{x_0}, \forall x \in I \cap V, \quad |h(x)| \leq \varepsilon, \quad |f(x)| \leq \varepsilon |g(x)|.$$

$\boxed{\Rightarrow}$ Posons

$$\forall x \in I, \quad h(x) = \begin{cases} \frac{f(x)}{g(x)} & \text{si } g(x) \neq 0 \\ 0 & \text{si } g(x) = 0 \end{cases}.$$

Alors, puisque $f \underset{x_0}{=} o(g)$ par hypothèse,

$$\forall \varepsilon > 0, \exists V \in \mathcal{V}_{x_0}, \forall x \in I \cap V, \quad |f(x)| \leq \varepsilon |g(x)|.$$

Si $g(x) = 0$ alors $|h(x)| = 0 \leq \varepsilon$. Si $g(x) \neq 0$, alors $|h(x)| = \dfrac{|f(x)|}{|g(x)|} \leq \varepsilon$. Dans tous les cas, $|h(x)| \leq \varepsilon$ donc $\lim\limits_{x_0} h = 0$. □

Remarque 3.3 : En pratique,[4] on applique le résultat suivant :

$$f \underset{x_0}{=} o(g) \iff \lim_{x \to x_0} \frac{f(x)}{g(x)} = 0.$$

♢

Exemple 3.4 :
Montrons que

$$x^3 \underset{x \to 0}{=} o\left(\sqrt{x}\right), \quad \sqrt{x} \underset{x \to +\infty}{=} o\left(x^3\right).$$

- Soit x au voisinage de 0^+. Alors

  $$\frac{x^3}{\sqrt{x}} = x^{5/2} \xrightarrow[x \to 0^+]{} 0, \quad x^3 \underset{x \to 0}{=} o\left(\sqrt{x}\right).$$

  On comprend ce résultat comme "La fonction cube converge vers 0 plus vite que la fonction racine".

4. Quitte à passer sous silence quelques conditions techniques liées à l'annulation potentielle de f et g en x_0.

- Soit x au voisinage de $+\infty$. Alors
$$\frac{\sqrt{x}}{x^3} = x^{-5/2} \xrightarrow[x\to+\infty]{} 0^+, \quad \sqrt{x} \underset{x\to+\infty}{=} o\left(x^3\right).$$
On comprend ce résultat comme "La fonction cube diverge vers $+\infty$ plus vite que la fonction racine".

$\diamondsuit$

Il faut préciser x_0 quand on écrit $f \underset{x_0}{=} o(g)$. En effet, contrairement aux suites (où on regarde forcément $n \to +\infty$), on peut faire des limites en n'importe quel point de $\overline{I}$.

Si $f(x) \underset{x\to x_0}{=} o(0)$ alors f est nulle au voisinage de x_0. En effet, pour $\varepsilon = 1$,
$$\exists V \in \mathcal{V}_{x_0}, \quad \forall x \in V, \quad |f(x)| \leq 1 \times 0 = 0.$$
La réciproque est évidente.

On ne peut pas définir une fonction avec une phrase du type : "soit $f(x) = o\left(x^2\right)$".

Définition 3.5 *Fonction dominée*

Soient $f, g \in \mathcal{F}(I, \mathbb{K})$ et soit $x_0 \in \overline{I}$. On dit que f *est dominée par g au voisinage de x_0*, si
$$\exists M > 0, \quad \exists V \in \mathcal{V}_{x_0}, \quad \forall x \in I \cap V, \quad |f(x)| \leq M|g(x)|.$$
On note alors $f \underset{x_0}{=} \mathcal{O}(g)$ ou $f(x) \underset{x\to x_0}{=} \mathcal{O}(g(x))$

Lorsque l'on sait manipuler des o, on sait manipuler des $\mathcal{O}$. En effet, il suffit de changer $\forall\varepsilon > 0$ en $\exists M > 0$ (c'est donc en général plus facile).

Proposition 3.6

Soient $f, g \in \mathcal{F}(I, \mathbb{K})$ et soit $x_0 \in \overline{I}$. Alors
$$f \underset{x_0}{=} \mathcal{O}(g) \iff \exists V \in \mathcal{V}_{x_0}, \exists h \in \mathcal{F}(I \cap V, \mathbb{K}), \quad \begin{cases} f = gh \\ h \text{ est bornée au voisinage de } x_0 \end{cases}.$$

Démonstration : $\boxed{(i) \Leftarrow}$ Par définition,
$$\exists M > 0, \exists V \in \mathcal{V}_{x_0}, \forall x \in I \cap V, \quad |h(x)| \leq M, \quad |f(x)| \leq M|g(x)|.$$

$\boxed{(i) \Rightarrow}$ Posons
$$\forall x \in I, \quad h(x) = \begin{cases} \frac{f(x)}{g(x)} & \text{si } g(x) \neq 0 \\ 0 & \text{si } g(x) = 0 \end{cases}.$$
Alors, puisque $f \underset{x_0}{=} \mathcal{O}(g)$ par hypothèse,
$$\exists M > 0, \exists V \in \mathcal{V}_{x_0}, \forall x \in I \cap V, \quad |f(x)| \leq M|g(x)|.$$

Si $g(x) = 0$ alors $|h(x)| = 0 \leq M$. Si $g(x) \neq 0$, alors $|h(x)| = \dfrac{|f(x)|}{|g(x)|} \leq M$. Dans tous les cas, $|h(x)| \leq M$ donc h est bornée au voisinage de x_0. □

Remarque 3.7 : En pratique, on applique le résultat suivant :

$$f \underset{x_0}{=} \mathcal{O}(g) \iff \frac{f}{g} \text{ est bornée au voisinage de } x_0.$$

♢

Remarque 3.8 : On remarquera donc que :

- $f \underset{x_0}{=} o(1)$ si, et seulement si, $\lim\limits_{x_0} f = 0$.
- $f \underset{x_0}{=} \mathcal{O}(1)$ si, et seulement si, f est bornée au voisinage de x_0.

♢

Proposition 3.9 *Manipulation de o et $\mathcal{O}$*

Soient $f, g, \varphi, \psi \in \mathcal{F}(I, \mathbb{K})$, soit $\lambda \in \mathbb{K}$, et soit $x_0 \in \overline{I}$. Alors

(i) Si $f \underset{x_0}{=} o(\varphi)$ alors $f \underset{x_0}{=} \mathcal{O}(\varphi)$.
(ii) Si $f \underset{x_0}{=} o(\varphi)$ et $g \underset{x_0}{=} o(\varphi)$ alors $\lambda f + g \underset{x_0}{=} o(\varphi)$.
(iii) Si $f \underset{x_0}{=} \mathcal{O}(\varphi)$ et $g \underset{x_0}{=} \mathcal{O}(\varphi)$ alors $\lambda f + g \underset{x_0}{=} \mathcal{O}(\varphi)$.
(iv) Si $f \underset{x_0}{=} o(\varphi)$ et $g \underset{x_0}{=} o(\psi)$ alors $fg \underset{x_0}{=} o(\varphi\psi)$.
(v) Si $f \underset{x_0}{=} o(\varphi)$ et $g \underset{x_0}{=} \mathcal{O}(\psi)$ alors $fg \underset{x_0}{=} o(\varphi\psi)$.
(vi) Si $f \underset{x_0}{=} \mathcal{O}(\varphi)$ et $g \underset{x_0}{=} \mathcal{O}(\psi)$ alors $fg \underset{x_0}{=} \mathcal{O}(\varphi\psi)$.
(vii) Si $f \underset{x_0}{=} \mathcal{O}(\varphi)$ et $\varphi \underset{x_0}{=} o(\psi)$ alors $f \underset{x_0}{=} o(\psi)$.
(viii) Si $f \underset{x_0}{=} o(\varphi)$ et $\varphi \underset{x_0}{=} \mathcal{O}(\psi)$ alors $f \underset{x_0}{=} o(\psi)$.

Démonstration : (i) Une fonction tendant vers 0 est bornée.
(ii) La combinaison linéaire de fonctions tendant vers 0 tend vers 0.
(iii) La combinaison linéaire de fonctions bornées est bornée.
(iv) Le produit de fonctions tendant vers 0 tend vers 0.
(v) Le produit d'une fonction tendant vers 0 avec une fonction bornée tend vers 0 (idem pour (*vii*) et (*viii*)).
(vi) Le produit de fonctions bornées est borné.

□

2. Fonctions équivalentes

Définition 3.10 *Fonctions équivalentes*

Soient $f, g \in \mathcal{F}(I, \mathbb{K})$ et soit $x_0 \in \overline{I}$. On dit que f ***est équivalente à*** g ***au voisinage de*** x_0, si

$$f \underset{x_0}{=} g + o(g).$$

On note alors $f \underset{x_0}{\sim} g$ ou $f(x) \underset{x \to x_0}{\sim} g(x)$.

Proposition 3.11

Soient $f, g \in \mathcal{F}(I, \mathbb{K})$ et soit $x_0 \in \overline{I}$. Alors

$$f \underset{x_0}{\sim} g \iff \exists V \in \mathcal{V}_{x_0}, \exists h \in \mathcal{F}(I \cap V, \mathbb{K}), \quad \begin{cases} f = gh \\ \lim_{x_0} h = 1 \end{cases}.$$

La preuve est similaire à tout ce que l'on a fait auparavant.

Remarque 3.12 : En pratique, on applique le résultat suivant :

$$f \underset{x_0}{\sim} g \iff \lim_{x \to x_0} \frac{f(x)}{g(x)} = 1.$$

◊

Proposition 3.13

Soit $x_0 \in \overline{I}$. La relation $\underset{x_0}{\sim}$ est une relation d'équivalence sur $\mathcal{F}(I, \mathbb{K})$.

Démonstration : Soient $f, g, h \in \mathcal{F}(I, \mathbb{K})$.

- $f - f = 0 = o(f)$ donc $\underset{x_0}{\sim} f$, donc $\underset{x_0}{\sim}$ est réflexive.
- Supposons que $f \underset{x_0}{\sim} g$. Alors il existe $\varphi \in \mathcal{F}(V, \mathbb{K})$ avec $V \in \mathcal{V}_{x_0}$ telle que $f = \varphi g$ et $\lim_{x_0} \varphi = 1$. En particulier, φ est non-nulle sur un voisinage $V' \in \mathcal{V}_{x_0}$. Quitte à considérer $V' \cap V$, on peut supposer que $V' \subseteq V$. On définit alors

$$\forall x \in I \cap V', \quad \widetilde{\varphi}(x) = \frac{1}{\varphi(x)}.$$

  Alors $\lim_{x_0} \widetilde{\varphi} = 1$ et $g = f\widetilde{\varphi}$. Donc $g \underset{x_0}{\sim} f$ donc $\underset{x_0}{\sim}$ est symétrique.
- Supposons que $f \underset{x_0}{\sim} g$ et $g \underset{x_0}{\sim} h$. Alors il existe $\varphi, \widetilde{\varphi}$ vérifiant $f = \varphi g, g = \varphi h$ et $\lim_{x_0} \varphi = \lim_{x_0} \widetilde{\varphi} = 1$. Donc $f = h\varphi\widetilde{\varphi}$ et $\lim_{x_0} \varphi\widetilde{\varphi} = 1$. Donc $f \underset{x_0}{\sim} h$ et donc $\underset{x_0}{\sim}$ est transitive.

On a donc montré que $\underset{x_0}{\sim}$ est une relation d'équivalence. □

Proposition 3.14

Soient $f, g \in \mathcal{F}(I, \mathbb{R})$ et soit $x_0 \in \overline{I}$. Si $f \underset{x_0}{\sim} g$ alors f et g sont strictement de même signe au voisinage de x_0, c'est-à-dire

$$\exists V \in \mathcal{V}_{x_0}, \quad \forall x \in I \cap V, \quad \begin{cases} f(x) = 0 \iff g(x) = 0 \\ f(x) > 0 \iff g(x) > 0 \\ f(x) < 0 \iff g(x) < 0 \end{cases}.$$

Démonstration : Par définition, il existe $V \in \mathcal{V}_{x_0}$ et $h \in \mathcal{F}(V, \mathbb{K})$ telle que $f = gh$ et $\lim\limits_{x_0} h = 1$. En particulier, h est strictement positive sur un voisinage $V' \in \mathcal{V}_{x_0}$. On peut supposer $V' \subseteq V$, et alors

$$\forall x \in V', \quad \begin{cases} f(x) = 0 \iff g(x) = 0 \\ f(x) > 0 \iff g(x) > 0 \\ f(x) < 0 \iff g(x) < 0 \end{cases}.$$

□

Proposition 3.15

Soit $f \in \mathcal{F}(I, \mathbb{K})$ et soit $x_0 \in \overline{I}$. Soit $\ell \in \mathbb{K}^*$. Alors

(i) $f(x) \underset{x \to x_0}{\sim} \ell$ si, et seulement si, $\lim\limits_{x \to x_0} f(x) = \ell$.

(ii) $f(x) \underset{x \to x_0}{\sim} 0$ si, et seulement si, f est nulle au voisinage de x_0.

Proposition 3.16 *Manipulation d'équivalents*

Soient $f, g, \varphi, \psi \in \mathcal{F}(I, \mathbb{R})$ et soit $x_0 \in \overline{I}$. Supposons que $f \underset{x_0}{\sim} \varphi$ et $g \underset{x_0}{\sim} \psi$. Alors

$$\forall \lambda \in \mathbb{K}, \quad \lambda f \underset{x_0}{\sim} \lambda\varphi, \quad fg \underset{x_0}{\sim} \varphi\psi.$$

De plus, si g et ψ ne s'annulent pas au voisinage de x_0 (sauf peut-être en x_0) alors

$$\frac{f}{g} \underset{x_0}{\sim} \frac{\varphi}{\psi}.$$

Démonstration : Par définition, il existe $V \in \mathcal{V}_{x_0}$ et $h, \kappa \in \mathcal{F}(V, \mathbb{K})$ telle que $f = gh$, $\varphi = \psi\kappa$ et $\lim\limits_{x_0} h = \lim\limits_{x_0} \kappa = 1$. Quitte à considérer un voisinage plus petit, on peut supposer que h et κ sont strictement positives sur V. Alors

$$fg = \varphi\psi \times h\kappa, \quad \lim_{x_0} h\kappa = 1.$$

De plus, si g et ψ ne s'annulent pas au voisinage de x_0 (sauf peut-être en x_0) alors

$$\frac{f}{g} = \frac{\varphi}{\psi} \times \frac{h}{\kappa}, \quad \lim_{x_0} \frac{h}{\kappa} = 1.$$

□

Les équivalents se comportent bien avec la multiplication et la division. Et c'est tout ! En règle générale, on préférera des égalités avec des o pour traiter les expressions compliquées.

On ne peut pas additionner des équivalents !

Exemple 3.17 :
Notons $f : x \mapsto x^2 + x$ et $g : x \mapsto -x^2$. Alors

$$\lim_{x \to +\infty} \frac{f(x)}{x^2} = \lim_{x \to +\infty} \left(1 + \frac{1}{x}\right) = 1, \quad f(x) \underset{x \to +\infty}{\sim} x^2.$$

On notera que, évidemment, $f + g$ n'est pas équivalent à 0. ◇

On ne peut pas composer des équivalents !

Exemple 3.18 :
Soient $f : x \mapsto x^2 + x$ et $g : x \mapsto x^2$. On a vu que $f \underset{+\infty}{\sim} g$. Cependant, pour x au voisinage de $+\infty$,

$$\frac{e^{f(x)}}{e^{g(x)}} = \frac{e^{x^2+x}}{e^{x^2}} = \frac{e^{x^2} e^{x}}{e^{x^2}} = e^x \xrightarrow[x\to+\infty]{} +\infty,$$

donc e^f et e^g ne sont pas équivalents en $+\infty$.. ◇

La proposition suivante est cruciale pour justifier l'intérêt des équivalents : ils servent à calculer des limites de termes compliqués en les remplaçant par des équivalents plus simples.

Proposition 3.19

Soient $f, g \in \mathcal{F}(I, \mathbb{K})$, et soit $x_0 \in \overline{I}$. Supposons que $f \underset{x_0}{\sim} g$. Alors f admet une limite en x_0 si, et seulement si, g admet une limite en x_0. De plus, si ces fonctions admettent une limite, alors $\lim\limits_{x_0} f = \lim\limits_{x_0} g$.

Démonstration : Supposons que f admette une limite ℓ en x_0. On sait qu'il existe une fonction h vérifiant

$$g = fh, \quad \lim_{x_0} h = 1.$$

Donc $\lim\limits_{x_0} g = \lim\limits_{x_0} fh = \lim\limits_{x_0} f$.

La réciproque est évidente car $\sim$ est symétrique. □

Exemple 3.20 :
Montrer que la fonction $x \mapsto \dfrac{1}{x} + \dfrac{7\cos x}{x^2}$ est strictement positive au voisinage de $+\infty$.

Réponse

Pour x au voisinage de $+\infty$, on a

$$\frac{7\cos x}{x^2} = \frac{\mathcal{O}(1)}{x^2} = \mathcal{O}\left(\frac{1}{x^2}\right) = o\left(\frac{1}{x}\right), \quad \frac{1}{x} + \frac{7\cos x}{x^2} \underset{x\to+\infty}{\sim} \frac{1}{x}.$$

Or la fonction $x \mapsto \dfrac{1}{x}$ est strictement positive au voisinage de $+\infty$, donc $x \mapsto \dfrac{1}{x} + \dfrac{7\cos x}{x^2}$ l'est aussi.

◇

3. Comparaison de fonctions de référence

Proposition 3.21

Soient $a, b \in \mathbb{R}, a < b$. Alors

$$x^a \underset{x\to+\infty}{=} o\left(x^b\right), \quad x^b \underset{x\to 0^+}{=} o\left(x^a\right).$$

Proposition 3.22

Soit $a > 0$. Alors

$$x^a \underset{x\to+\infty}{=} o\left(e^x\right), \quad e^{-x} \underset{x\to+\infty}{=} o\left(\frac{1}{x^a}\right), \quad \ln x \underset{x\to+\infty}{=} o\left(x^a\right), \quad \ln x \underset{x\to0^+}{=} o\left(\frac{1}{x^a}\right).$$

On peut interpréter tous ces résultats en terme de "vitesse de convergence vers 0" ou de "vitesse d'explosion vers $+\infty$" [5]

Proposition 3.23

Soit $\alpha \in \mathbb{R}$. On a les équivalents suivants :

$\sin x \underset{x\to0}{\sim} x$	$\cos x - 1 \underset{x\to0}{\sim} -\frac{x^2}{2}$	$\tan x \underset{x\to0}{\sim} x$	$\arcsin x \underset{x\to0}{\sim} x$	$\arctan x \underset{x\to0}{\sim} x$
$\operatorname{sh} x \underset{x\to0}{\sim} x$	$\operatorname{ch} x - 1 \underset{x\to0}{\sim} \frac{x^2}{2}$	$\operatorname{th} x \underset{x\to0}{\sim} x$	$\operatorname{argsh} x \underset{x\to0}{\sim} x$	$\operatorname{argth} x \underset{x\to0}{\sim} x$
$e^x - 1 \underset{x\to0}{\sim} x$	$\ln(1+x) \underset{x\to0}{\sim} x$	$(1+x)^\alpha - 1 \underset{x\to0}{\sim} \alpha x$		

Par résultats sur la composition de limite, on a le droit de changer de variable dans les équivalents, c'est-à-dire :

$$\begin{cases} \lim\limits_{x\to x_0} u(x) = u_0 \\ f(u) \underset{u\to u_0}{\sim} g(u) \end{cases} \Rightarrow f(u(x)) \underset{x\to x_0}{\sim} g(u(x)).$$

Autrement dit, on peut composer *à droite.*

Proposition 3.24

Soient $f, g \in \mathcal{F}(I, \mathbb{R})$, et soit $x_0 \in \overline{I}$. Si $f > 0$ au voisinage de a (sauf peut-être en a) alors

$$\forall \alpha \in \mathbb{R}, \quad f \underset{x_0}{\sim} g \Longrightarrow f^\alpha \underset{x_0}{\sim} g^\alpha$$

On a le droit de composer des équivalents par la fonction $x \mapsto x^\alpha$ si ceux-ci sont strictement positifs (localement).

Exercice 3.25 :
Déterminer un équivalent simple de la fonction partie entière lorsque $x \to +\infty$.

Réponse

Soit x au voisinage de $+\infty$. Alors on a par définition

$$x - 1 < E(x) \leq x, \quad 1 - \frac{1}{x} < \frac{E(x)}{x} \leq 1.$$

Alors d'après le théorème des gendarmes, $\lim\limits_{x\to+\infty} \frac{E(x)}{x} = 1$, donc $E(x) \underset{x\to+\infty}{\sim} x$.

5. Par exemple, $x \mapsto e^{-x}$ converge vers 0 plus vite que $x \mapsto \frac{1}{x^a}$.

$\diamondsuit$

Exercice 3.26 :
Chercher un équivalent de $e^{2x} - 3e^{x^2} + 2\ln x$ lorsque $x \to +\infty$, lorsque $x \to 0$ et lorsque $x \to 1$.

Réponse

- Soit x au voisinage de $+\infty$. On a, par croissances comparées,

$$\ln(x) = o\left(e^{2x}\right), \quad \frac{e^{2x}}{e^{x^2}} = e^{2x-x^2} \xrightarrow[x\to+\infty]{} 0, \quad e^{2x} = o\left(e^{x^2}\right).$$

  On en déduit que $e^{2x} - 3e^{x^2} + 2\ln x \underset{x\to+\infty}{\sim} -3e^{x^2}$.
- Soit x au voisinage de 0. Alors

$$\lim_{x\to0^+} e^{2x} - 3e^{x^2} = -4, \quad e^{2x} - 3e^{x^2} = o(\ln x).$$

  On en déduit que $e^{2x} - 3e^{x^2} + 2\ln x \underset{x\to0^+}{\sim} 2\ln x$.
- Soit x au voisinage de 1. Alors

$$\lim_{x\to1} e^{2x} - 3e^{x^2} + 2\ln x = e^2 - 3e.$$

  On en déduit que $e^{2x} - 3e^{x^2} + 2\ln x \underset{x\to1}{\sim} e^2 - 3e$.

$\diamondsuit$

Exercice 3.27 :
Déterminer un équivalent de arcos au voisinage de 1.

Réponse

Pour x au voisinage de 0, on a

$$\cos x - 1 \sim -\frac{x^2}{2}, \quad 2(1-\cos x) \sim x^2, \quad x \underset{x\to0}{\sim} \sqrt{2(1-\cos x)}.$$

De plus $\arccos t \xrightarrow[t\to1]{} 0$ et $\cos \circ \arccos = \mathrm{Id}$ donc

$$\arccos t \underset{t\to1}{\sim} \sqrt{2(1-\cos(\arccos t))} = \sqrt{2(1-t)}$$

$\diamondsuit$

IV Continuité locale

La notion de continuité est intimement liée à la notion de limite. C'est aussi une notion fondamentalement locale.

1. Notion de continuité

Au contraire des limites, on parle de continuité en un point où la fonction est définie (et pas lorsque la variable tend vers une borne de l'intervalle de définition). Concrètement, cela signifie qu'on prendra $x_0 \in I$.

Définition 4.1 *Fonction continue*

Soit $f \in \mathcal{F}(I, \mathbb{K})$ et soit $x_0 \in I$. On dit que f *est continue en* x_0 si f admet une limite (finie) en x_0.

On dit que f *est continue sur* I [6] si f est continue en tout point de I. On note $\mathcal{C}^0(I, \mathbb{K})$ ou $\mathcal{C}^0(I)$ (lorsqu'il n'y a pas d'ambiguïté) l'ensemble des fonctions continues sur I.

Cette limite est nécessairement finie car f est définie en x_0. En effet, supposons par l'absurde que f admette $+\infty$ pour limite en x_0 (ici $\mathbb{K} = \mathbb{R}$ car les limites dans $\mathbb{C}$ sont toujours finies). Alors, pour $M = f(x_0) + 1$,

$$\exists \alpha > 0, \forall x \in I, |x - x_0| \leq \alpha \Rightarrow f(x) \geq M,$$

ce qui est impossible car x_0 vérifie bien $|x_0 - x_0| \leq \alpha$. Le cas $\lim\limits_{x_0} f = -\infty$ est tout aussi absurde.

Remarque 4.2 : Tracer la courbe représentative d'une fonction continue correspond moralement à ne pas lever le crayon, c'est-à-dire qu'il n'y a pas de "trou" dans la courbe. Lorsqu'on étend cette définition aux fonctions définies sur un sous-ensemble A de $\mathbb{R}$ qui n'est pas un intervalle, il peut par contre y avoir des "trous" (dûs aux "trous" dans l'ensemble A). $\diamondsuit$

Exemple 4.3 :
Les fonctions polynomiales, $\sin, \cos, \exp$ sont continues sur $\mathbb{R}$. La fonction $\ln$ est continue sur $\mathbb{R}_+^*$. La fonction $x \mapsto \sqrt{x}$ est continue sur $\mathbb{R}_+$. La fonction $x \mapsto \dfrac{1}{x}$ est continue sur $\mathbb{R}^*$ (plus précisément, sur $\mathbb{R}_+^*$ et sur $\mathbb{R}_-^*$). $\diamondsuit$

Proposition 4.4

Soit $f \in \mathcal{F}(I, \mathbb{K})$ et soit $x_0 \in I$. Alors

$$f \text{ est continue en } x_0 \iff \lim_{\substack{x \to x_0 \\ x \neq x_0}} f(x) = f(x_0).$$

De plus, si $x_0 \in \mathring{I}$, alors

$$f \text{ est continue en } x_0 \iff \lim_{x \to x_0^-} f(x) = \lim_{x \to x_0^+} f(x) = f(x_0).$$

En pratique, c'est cette proposition qu'on utilise étudier la continuité de la plupart des fonctions.

Démonstration : Il ne s'agit ni plus ni moins que de montrer

$$f \text{ est continue en } x_0 \iff \lim_{x_0} f = f(x_0),$$

dans différents cas de figure. La réciproque étant évidente, on s'intéresse au sens direct. Supposons que f soit continue en x_0. Alors f admet une limite finie $\ell \in \mathbb{K}$ en x_0. Alors

$$\forall \varepsilon > 0, \exists \alpha > 0, \forall x \in I \cap [x_0 - \alpha, x_0 + \alpha], |f(x) - \ell| \leq \varepsilon, \quad |f(x_0) - \ell| \leq \varepsilon.$$

Ceci étant vrai pour tout $\varepsilon > 0$, on en déduit que $\ell = f(x_0)$. $\square$

Définition 4.5 *Continuité à gauche ou à droite*

Soient $f \in \mathcal{F}(I, \mathbb{K})$ et $x_0 \in I$. On dit que f *est continue à gauche en* x_0 si $\lim\limits_{x_0^-} f = f(x_0)$. On dit que f *est*

6. On peut étendre cette définition à des unions d'intervalles, c'est ce dont on aura besoin en pratique.

continue à droite en x_0 si $\lim\limits_{x_0^+} f = f(x_0)$.

Les propositions suivantes découlent directement des propriétés sur les limites.

Proposition 4.6

Soit $f \in \mathcal{F}(I, \mathbb{R})$ et soit $x_0 \in I$. Si f est continue en x_0 et $f(x_0) > 0$ alors f est strictement positive au voisinage de x_0.

Démonstration : Evident, puisque $\lim\limits_{x_0} f > 0$. □

Proposition 4.7

Soient $f, g \in \mathcal{F}(I, \mathbb{K})$, $\lambda \in \mathbb{K}$ et $x_0 \in I$. Si f et g sont continues en x_0 alors les fonctions $f + g$, $f \times g$, λf.

Si de plus $g(x_0) \neq 0$ alors $\dfrac{f}{g}$ est continue en x_0.

Cette proposition implique en particulier que l'ensemble $\mathcal{C}^0(I, \mathbb{K})$ est un sous-anneau et un sous-espace vectoriel de $\mathcal{F}(I, \mathbb{K})$.

Exercice 4.8 :
Soient $f, g \in \mathcal{F}(I, \mathbb{R})$.

1. On note $h = \max(f, g)$. Montrer que si f et g sont continues en x_0 alors h est continue en x_0.
2. Montrer que si f et g sont continues en x_0 alors $\min(f, g)$ est continue en x_0.
3. Montrer que si f est continue alors $|f|$ est continue.

Réponse

1. Plusieurs cas se présentent :
   - si $f(x_0) = g(x_0)$, alors on fixe $\varepsilon > 0$. Il existe $\alpha_1, \alpha_2 > 0$ tels que, pour tout $x \in I$,

     $$|x - x_0| \leq \alpha_1 \Rightarrow |f(x) - f(x_0)| \leq \varepsilon, \quad |x - x_0| \leq \alpha_2 \Rightarrow |g(x) - g(x_0)| \leq \varepsilon.$$

     On pose donc $\alpha = \min(\alpha_1, \alpha_2)$. Alors, pour tout $x \in I \cap [x_0 - \alpha, x_0 + \alpha]$, $f(x_0) = g(x_0) = h(x_0)$ donc

     $$h(x_0) - \varepsilon \leq f(x) \leq h(x_0) + \varepsilon, \quad h(x_0) - \varepsilon \leq g(x) \leq h(x_0) + \varepsilon.$$

     En particulier, $h(x_0) - \varepsilon \leq \max(f(x), g(x)) \leq h(x_0) + \varepsilon$. Autrement dit, $\lim\limits_{x_0} h = h(x_0)$. On a donc montré que h est continue en x_0.
   - si $f(x_0) > g(x_0)$, alors d'après la proposition4.6, il existe $\alpha_1 > 0$ tel que, pour tout $x \in [x_0 - \alpha, x_0 + \alpha]$, $f(x) - g(x) > 0$. En particulier $h = f$ au voisinage de x_0, et donc h est continue en x_0.
   - si $f(x_0) < g(x_0)$, le raisonnement précédent s'applique en échangeant les rôles de f et g.
2. On a $\min(f, g) = -\max(-f, -g)$. Le résultat est clair d'après la question 1.
3. On a $|f| = \max(f_+, f_-)$ si $\mathbb{K} = \mathbb{R}$. Le résultat est alors clair d'après la question 1. Si $\mathbb{K} = \mathbb{C}$, il faut pouvoir composer des fonctions continues (voir proposition suivante).

♢

Proposition 4.9

Soient I et J deux intervalles de $\mathbb{R}$. Soit $f \in \mathcal{F}(I, J)$ et $g \in \mathcal{F}(J, \mathbb{K})$. Soient $x_0 \in I$ et $y_0 \in J$. Si f est continue en x_0 et g est continue en $f(x_0)$ alors $g \circ f$ est continue en x_0.

Toutes les propriétés des limites sont transmises aux fonctions continues.

Exercice 4.10 :

Soit $a \in \mathbb{R}$ et soit $f \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ définie par

$$\forall x \in \mathbb{R}, \quad f(x) = \begin{cases} \frac{\sin x}{x} & \text{si } x \neq 0 \\ a & \text{si } x = 0 \end{cases}.$$

Pour quelles valeurs de a la fonction f est-elle continue sur $\mathbb{R}$?

Réponse

On a

$$\sin x \underset{x \to 0}{\sim} x, \quad \lim_{\substack{x \to 0 \\ x \neq 0}} \frac{\sin x}{x} = 1, \quad f(0) = a.$$

On en déduit que f est continue en 0 si, et seulement si $a = 1$. Dans la suite, on suppose donc que $a = 1$. Alors, pour tout $x_0 \in \mathbb{R}^*$, les fonctions sin et $x \mapsto x$ sont continues en x_0 et $x_0 \neq 0$ donc f est continue en x_0. Donc f est continue sur $\mathbb{R}$ si, et seulement si $a = 1$.

♢

Théorème 4.11 *Caractérisation séquentielle de la continuité*

Soient $f \in \mathcal{F}(I, \mathbb{K})$ et $x_0 \in I$. Alors

$$f \text{ est continue en } x_0 \iff \forall (u_n) \in I^{\mathbb{N}}, \quad \left(\lim_{n \to +\infty} u_n = x_0 \Rightarrow \lim_{n \to +\infty} f(u_n) = f(x_0) \right).$$

Démonstration : C'est une application directe de la caractérisation séquentielle de la limite. □

Proposition 4.12

Soit $f \in \mathcal{F}(I, \mathbb{C})$ et soit $x_0 \in I$. Alors f est continue en x_0 si, et seulement si, $\mathfrak{Re}(f)$ et $\mathfrak{Im}(f)$ sont continues en x_0

Démonstration : La réciproque est évidente, car $f = \mathfrak{Re}(f) + i\mathfrak{Im}(f)$. Supposons donc que f soit continue en x_0. Soit $(u_n) \in I^{\mathbb{N}}$ convergeant vers x_0. Alors, par les résultats de convergence des suites complexes,

$$\lim_{n \to +\infty} f(u_n) = f(x_0), \quad \begin{cases} \lim_{n \to +\infty} \mathfrak{Re}(f(u_n)) = \mathfrak{Re}(f(x_0)) \\ \lim_{n \to +\infty} \mathfrak{Im}(f(u_n)) = \mathfrak{Im}(f(x_0)) \end{cases}.$$

On en déduit que les fonctions $\mathfrak{Re}(f)$ et $\mathfrak{Im}(f)$ sont continues, par caractérisation séquentielle de la continuité.

□

Proposition 4.13

Soit $f \in \mathcal{F}(I, \mathbb{K})$ une fonction lipschitzienne sur I. Alors f est continue sur I.

Démonstration : Il existe $K \geq 0$ tel que, pour tous $x, y \in I$, $|f(x) - f(x_0)| \leq K|x - x_0|$. On sait que $\lim\limits_{x \to x_0} K|x - x_0| = 0$ donc $\lim\limits_{x \to x_0} |f(x) - f(x_0)| = 0$, autrement dit $\lim\limits_{x \to x_0} f(x) = f(x_0)$. Donc f est continue en x_0. Donc f est continue sur I. □

2. Prolongement par continuité

Voyons comment on peut construire une fonction continue à partir d'une fonction qui n'est pas continue *a priori*.

Théorème 4.14 *Prolongement par continuité*

Soient $x_0 \in I$ et soit $f \in \mathcal{C}^0(I \setminus \{x_0\})$. Si $\lim\limits_{x \to x_0} f(x) = \ell \in \mathbb{K}$, alors la fonction $\widetilde{f} : I \to \mathbb{K}$ définie par

$$\forall x \in I, \quad \widetilde{f}(x) = \begin{cases} f(x) & \text{si } x \neq x_0 \\ \ell & \text{si } x = x_0 \end{cases}$$

est continue sur I. C'est l'unique prolongement continu de f sur I.

$\widetilde{f}$ est appelé *prolongement par continuité* de f en x_0. On fera naturellement le lien entre ce théorème et l'exercice 4.10.

Démonstration : Tout d'abord, on remarque que $\widetilde{f}$ est bien un prolongement de f sur $I \cup \{x_0\}$, c'est-à-dire que $\widetilde{f} = f$ sur I. Soit g un prolongement de f sur $I \cup \{x_0\}$. Puisque f et g coïncident sur I, alors $g \in \mathcal{C}^0(I)$. On a également

$$\lim_{\substack{x \to x_0 \\ x \neq x_0}} g(x) = \lim_{\substack{x \to x_0 \\ x \neq x_0}} f(x) = \ell.$$

On en déduit que

$$g \in \mathcal{C}^0(I \cup \{x_0\}) \iff g \text{ est continue en } x_0 \iff g(x_0) = \lim_{\substack{x \to x_0 \\ x \neq x_0}} g(x) \iff g(x_0) = \ell.$$

On en déduit que $\widetilde{f}$ est continue, et que c'est l'unique prolongement continu de f sur $I \cup \{x_0\}$. □

Exemple 4.15 :

On pose $f : \begin{array}{ccc} \mathbb{R}^* & \to & \mathbb{R} \\ x & \mapsto & x \sin\left(\dfrac{1}{x}\right) \dfrac{\left(\mathrm{e}^{4x} - 1\right)(1 - \cos x)}{x^2} \end{array}$. La fonction f est clairement continue sur $\mathbb{R}^*$ comme composée de fonctions continues. Par équivalents classiques, on a

$$f(x) \underset{x \to 0}{\sim} \sin\left(\frac{1}{x}\right) \frac{4x \frac{x^2}{2}}{x^2} \underset{x \to 0}{\sim} \sin\left(\frac{1}{x}\right) 2x.$$

Comme produit d'une fonction bornée par une fonction tendant vers 0, on a donc $\lim\limits_{x \to 0} f(x) = 0$. f admet donc un unique prolongement par continuité $\widetilde{f}$ sur $\mathbb{R}$ défini par

$$\forall x \in \mathbb{R}, \quad \widetilde{f}(x) = \begin{cases} x \sin\left(\frac{1}{x}\right) & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases}.$$

◇

V Continuité globale

Dans cette dernière section, on s'intéresse à l'image de fonctions réelles continues sur un intervalle. A partir de maintenant, les fonctions considérées sont à valeurs dans $\mathbb{R}$ et donc $\mathbb{K} = \mathbb{R}$.

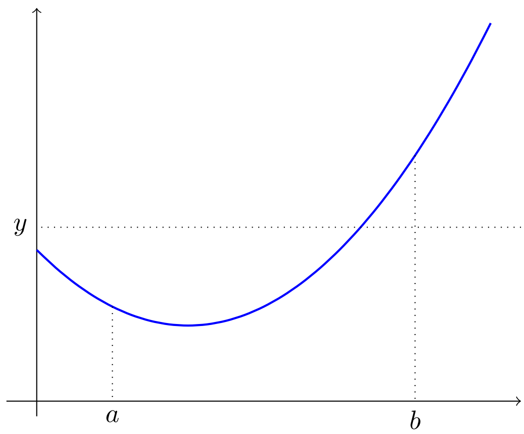
1. Continuité sur un intervalle

On rappelle que I est un intervalle non-trivial de $\mathbb{R}$.

Théorème 5.1 *Théorème des valeurs intermédiaires*

Soient $a, b \in \mathbb{R}$ tels que $a < b$ et $f \in \mathcal{F}([a,b], \mathbb{R})$. Si f est continue sur $[a,b]$ alors

$$\forall y \in [f(a), f(b)] \cup [f(b), f(a)], \quad \exists c \in [a,b], \quad f(c) = y.$$



Démonstration : Supposons que $f \in \mathcal{C}^0([a,b])$ avec $a < b$. Pour simplifier, supposons que $f(a) < f(b)$, et considérons $y \in [f(a), f(b)]$. Si $y = f(a)$ ou $y = f(b)$, il est clair que le théorème est vrai (prendre $c = a$ ou $c = b$). On considère donc le cas $f(a) < y < f(b)$. Posons $E = \{x \in [a,b] / f(x) \leq y\}$. E est une partie de $\mathbb{R}$ non-vide (car $a \in E$) et majorée (par b), donc possède une borne supérieure $c = \sup E$. Par caractérisation séquentielle de la borne supérieure, il existe $(x_n) \in E^{\mathbb{N}}$ telle que $\lim\limits_{n \to +\infty} x_n = c$. Par continuité de f, $\lim\limits_{n \to +\infty} f(x_n) = f(c)$ et donc

$$\forall n \in \mathbb{N}, \quad f(x_n) \leq y, \quad f(c) \leq y.$$

D'autre part, $c < b$ donc, pour $n \in \mathbb{N}$ suffisamment grand, $c_n = c + \dfrac{1}{n} \in]c, b]$. Donc $c_n \notin E$ et $\lim\limits_{n \to +\infty} c_n = c$ donc, par continuité de f,

$$f\left(c + \frac{1}{n}\right) > y, \quad f(c) = \lim_{n \to +\infty} f(c_n) \geq y.$$

Donc $f(c) = y$. □

Remarque 5.2 (*Preuve par dichotomie*) : Une autre méthode pour démontrer ce théorème est par dichotomie (c'est-à-dire "couper en deux"). On pose $u_0 = a$ et $v_0 = b$.

- Si $f\left(\dfrac{u_0 + v_0}{2}\right) \leq y$, on pose $u_1 = \dfrac{u_0 + v_0}{2}$ et $v_1 = v_0$.

- Si $f\left(\dfrac{u_0+v_0}{2}\right) > y$, on pose $u_1 u_0$ et $v_1 = \dfrac{u_0+v_0}{2}$.

On procède alors de même pour définir par récurrence des suites (u_n) et (v_n). On vérifie alors que les suites (u_n) et (v_n) sont adjacentes, et par continuité de f, leur limite commune ℓ vérifie $f(\ell) = y$. Cette méthode permet d'approcher numériquement une solution de l'équation $f(x) = y$. ♢

Remarque 5.3 : Attention, il n'y a pas forcément unicité de la solution à l'équation $f(x) = y$. En effet, si on prend $f = \sin, a = -\pi, b = \pi$ alors l'équation $f(x) = 0$ possède trois solutions sur $[-\pi, \pi]$: $-\pi, 0$ et π. ♢

Remarque 5.4 : Le théorème des valeurs intermédiaires est faux pour une fonction discontinue ou pour une fonction à valeurs complexes :

- Si $f : x \mapsto (-1)^{E(x)}$, alors $f(0) = 1, f(\pi) = -1$ et pourtant l'équation $f(x) = 0$ n'admet pas de solution.
- Si $f : x \mapsto \mathrm{e}^{ix}$, alors $f(0) = 1, f(\pi) = -1$ et pourtant l'équation $f(x) = 0$ n'admet pas de solution. Au fait, pourquoi f est-elle continue ?

En effet, la courbe représentative peut "sauter 0" (si la fonction est discontinue) ou "contourner 0" (dans $\mathbb{C}$). ♢

Corollaire 5.5

Soit $f \in \mathcal{C}^0(I, \mathbb{R})$. Alors $f(I)$ est un intervalle.

Démonstration : Soient $y_1, y_2 \in f(I)$ tels que $y_1 < y_2$. Alors il existe $x_1, x_2 \in I$ tels que $f(x_1) = y_1$ et $f(x_2) = y_2$. Puisque f est continue sur I, f est continue sur $[x_1, x_2] \cup [x_2, x_1]$. D'après le théorème des valeurs intermédiaires, pour tout $y \in [y_1, y_2]$, il existe $c \in I$ tel que $f(c) = y$, et donc $y \in f(I)$. Donc $f(I)$ est un intervalle. □

Si $I = [a, b]$, on n'a pas forcément $f(I) = [f(a), f(b)]$ ou $f(I) = [f(b), f(a)]$. Par exemple

$\sin([0, 2\pi]) = [-1, 1]$.

Corollaire 5.6

Soit $f \in \mathcal{F}(I, \mathbb{R})$. Si f est continue sur I et ne s'annule pas, alors f garde un signe constant sur I.

Démonstration : C'est clair par l'absurde. S'il existe $a, b \in I$ tels que $f(a) < 0, f(b) > 0$, alors d'après le théorème des valeurs intermédiaires, il existe $c \in [a, b] \cup [b, a]$ tel que $f(c) = 0$, ce qui est impossible par hypothèse. □

Exercice 5.7 :
Montrer que tout polynôme de degré impair possède au moins une racine réelle.

Réponse

Soient $d \in \mathbb{N}$ un entier impair, $(a_0, \dots, a_d) \in \mathbb{R}^d$ et $f : x \mapsto \displaystyle\sum_{k=0}^{d} a_k x^k$ avec $a_d \neq 0$. f est une fonction polynomiale donc continue sur $\mathbb{R}$. Quitte à considérer $-f$, on suppose que $a_d > 0$. Alors

$$f(x) \underset{x \to -\infty}{\sim} a_d x^d, \quad \lim_{x \to -\infty} f(x) = -\infty, \quad f(x) \underset{x \to +\infty}{\sim} a_d x^d, \quad \lim_{x \to -\infty} f(x) = +\infty.$$

Par définition, il existe $a, b \in \mathbb{R}$ tel que

$$\forall x \leq a, \quad f(x) \leq -1, \quad \forall x \geq b, \quad f(x) \geq 1.$$

En particulier, $f(a) \leq -1$ donc $a < b$. Puisque $f(a) \leq -1$, $f(b) \geq 1$ et f est continue sur $[a, b]$, alors il existe $c \in [a, b]$ vérifiant $f(c) = 0$.

♢

Exercice 5.8 :
Soient $a, b \in \mathbb{R}$ tels que $a < b$. Soit $f : [a, b] \to [a, b]$. On suppose que f est K-lipschitzienne avec $K \in [0, 1[$. On dit que f *est contractante.*

1. Montrer que f possède un unique point fixe $\ell \in [a, b]$.
2. Soit $(u_n) \in [a, b]^{\mathbb{N}}$ définie par

$$u_0 \in [a, b], \quad \forall n \in \mathbb{N}, \quad u_{n+1} = f(u_n).$$

Montrer que (u_n) converge vers ℓ.

Réponse

1. $\boxed{\text{Existence}}$ On considère $g : x \mapsto f(x) - x$. Alors g est continue (en effet, f est continue car lipschitzienne). D'autre part, $g(a) = f(a) - a \geq 0$ et $g(b) = f(b) - b \leq 0$. D'après le théorème des valeurs intermédiaires, il existe $\ell \in [a, b]$ tel que $g(\ell) = 0$, et donc $f(\ell) = \ell$.
$\boxed{\text{Unicité}}$ Soient $\ell_1, \ell_2 \in [a, b]$ tels que $f(\ell_1) = \ell_1$ et $f(\ell_2) = \ell_2$. On a alors

$$|\ell_1 - \ell_2| = |f(\ell_1) - f(\ell_2)| \leq K|\ell_1 - \ell_2|,$$

donc $|\ell_1 - \ell_2| = 0$ car $K < 1$. On en déduit que $\ell_1 = \ell_2$.
2. Pour tout $n \in \mathbb{N}$, on a

$$|u_{n+1} - \ell| = f(u_n) - f(\ell)| \leq K|u_n - \ell|.$$

Par une récurrence directe, on a donc

$$\forall n \in \mathbb{N}, \quad |u_n - \ell| \leq K^n |u_0 - \ell|.$$

Puisque $|K| < 1$, on en déduit que $\lim_{n \to +\infty} |u_n - \ell| = 0$, donc $\lim(u_n) = \ell$.

♢

2. Continuité sur un segment

Dans toute cette partie, on considère $a, b \in \mathbb{R}$ vérifiant $a < b$.

Théorème 5.9
Soit $f \in \mathcal{F}([a, b], \mathbb{R})$. Si f est continue sur $[a, b]$, alors

$$\exists c, d \in [a, b], \quad f(c) = \min_{[a,b]} f, \quad f(d) = \max_{[a,b]} f.$$

On dit qu'une fonction continue sur un segment est bornée et atteint ses bornes.

Démonstration : On va montrer l'existence d'un maximum, et le raisonnement est similaire pour le minimum.

- Si f est majorée, alors $f([a,b])$ est une partie non-vide et majorée de $\mathbb{R}$ qui admet donc une borne supérieure $M = \sup f([a,b])$. Par caractérisation séquentielle, il existe $(y_n) \in f([a,b])^{\mathbb{N}}$ telle que $\lim (y_n) = M$.
- Si f n'est pas majorée, alors on note $M = +\infty$. Par définition, pour tout $n \in \mathbb{N}$, il existe $y_n \in f([a,b])$ tel que $y_n \geq n$.

Dans tous les cas, il existe $(x_n) \in [a,b]^{\mathbb{N}}$ vérifiant

$$\forall n \in \mathbb{N}, f(x_n) = y_n, \quad \lim_{n\to+\infty} f(x_n) = M.$$

La suite (x_n) est bornée, donc d'après le théorème de Bolzano-Weierstrass, on peut en extraire une suite $\left(x_{\varphi(n)}\right)$ qui converge vers $d \in \mathbb{R}$. Alors, en passant à la limite,

$$\forall n \in \mathbb{N}, \quad a \leq x_{\varphi(n)} \leq b, \quad a \leq d \leq b.$$

De plus, $\left(y_{\varphi(n)}\right)$ est une suite extraite de (y_n) donc elle admet M pour limite et, par continuité de f, on a

$$f(d) = \lim_{n\to+\infty} f\left(x_{\varphi(n)}\right) = \lim_{n\to+\infty} y_{\varphi(n)} = M.$$

Donc M est fini (autrement dit, supposer $M = +\infty$ était absurde) et on a

$$f(d) = M = \sup_{[a,b]} f = \max_{[a,b]} f.$$

$\square$

Corollaire 5.10

Soit $f \in \mathcal{C}^0([a,b],\mathbb{R})$. Alors $f([a,b])$ est un segment.

Démonstration : D'après le théorème précédent, il existe $c, d \in [a,b]$ tels que $f(c) = \min_{[a,b]} f$ et $f(d) = \max_{[a,b]} f$. On a donc

$$f([a,b]) \subseteq [f(c), f(d)].$$

D'autre part, on sait que $f([a,b])$ est un intervalle et $f(c), f(d) \in f([a,b])$ donc $f([a,b]) = [f(c), f(d)]$. $\square$

Exemple 5.11 :
Soient $f, g \in \mathcal{C}^0([a,b])$ vérifiant

$$\forall x \in [a,b], \quad f(x) > g(x).$$

Montrer qu'il existe $\delta > 0$ tel que $f \geq g + \widetilde{\delta}$ sur $[a,b]$.

Réponse

La fonction $f - g$ est continue sur $[a,b]$ donc il existe $c \in [a,b]$ tel que $(f-g)(c) = \min_{[a,b]} (f-g)$. Notons $\delta = f(c) - g(c)$. Puisque $c \in [a,b]$, par hypothèse on a $f(c) > g(c)$ donc $\delta > 0$ et

$$\forall x \in [a,b], \quad f(x) - g(x) \geq f(c) - g(c) = \delta > 0, \quad f(x) \geq g(x) + \delta = g(x) + \widetilde{\delta}(x),$$

donc $f \geq g + \widetilde{\delta}$ sur $[a,b]$.

$\diamondsuit$

3. Théorème de la bijection

Proposition 5.12

Soit $f \in \mathcal{C}^0(I, \mathbb{R})$. Alors f est strictement monotone sur I si, et seulement si, f est injective.

On verra la preuve en exercice. Il est important de noter que l'implication directe est vraie même si f est discontinue, et beaucoup plus facile à montrer.

Théorème 5.13 *Théorème de la bijection (sur un segment)*

Soient $a, b \in \mathbb{R}$ tels que $a < b$ et $f \in \mathcal{F}([a,b], \mathbb{R})$. Si f est continue et strictement croissante sur $[a,b]$, alors

(i) f réalise une bijection entre $[a,b]$ et $[f(a), f(b)]$.
(ii) La bijection réciproque f^{-1} est continue et strictement croissante sur $[f(a), f(b)]$.

Démonstration : f étant continue, on sait que $f([a,b])$ est un segment. Par croissance de f, on sait que

$$\forall x \in [a,b], \quad f(a) \leq f(x) \leq f(b), \quad f([a,b]) = [f(a), f(b)].$$

Puisque f est strictement croissante, alors elle est injective. On en déduit que f réalise une bijection de $[a,b]$ sur $f([a,b]) = [f(a), f(b)]$. Cela définit donc une bijection réciproque $f^{-1} \in \mathcal{F}([f(a), f(b)], [a,b])$. Il est clair que f^{-1} est strictement croissante (évident par l'absurde). Soit $y_0 \in [f(a), f(b)]$. Pour simplifier, on suppose que $y_0 \neq f(a)$ et $y_0 \neq f(b)$. Pour $y \in I$, on pose $x = f^{-1}(y)$ et $x_0 = f^{-1}(y_0)$. Soit $\varepsilon > 0$ tel que $[x_0 - \varepsilon, x_0 + \varepsilon] \subseteq [a,b]$. Alors

$$|f^{-1}(y) - f^{-1}(y_0)| \leq \varepsilon \iff |x - x_0| \leq \varepsilon \iff x_0 - \varepsilon \leq x \leq x_0 + \varepsilon \iff f(x_0 - \varepsilon) \leq y \leq f(x_0 + \varepsilon).$$

Par stricte croissance de f, on sait que

$$f(x_0 - \varepsilon) < y_0 < f(x_0 + \varepsilon),$$

on pose donc $\alpha = \min(y_0 - f(x_0 - \varepsilon), f(x_0 + \varepsilon) - y_0)$. Alors

$$y \in [y_0 - \alpha, y_0 + \alpha] \Rightarrow y \in [f(x_0 - \varepsilon), f(x_0 + \varepsilon)] \Rightarrow |f^{-1}(y) - f^{-1}(y_0)|.$$

On a donc montré que $\lim\limits_{y_0} f^{-1} = f(y_0)$, donc f^{-1} est continue en y_0. Le raisonnement si y_0 est une borne du segment image est plus simple, puisqu'on a juste une inégalité à considérer (c'est-à-dire une limite à gauche ou une limite à droite). $\square$

Le théorème de la bijection se généralise aux intervalles ouverts ou semi-ouverts sans difficulté, mais les cas sont beaucoup plus nombreux.

Théorème 5.14 *Théorème de la bijection (sur un intervalle)*

Soit $f \in \mathcal{F}(I, \mathbb{R})$. Si f est continue et strictement monotone sur I, alors

(i) f réalise une bijection entre I et $f(I)$.
(ii) La bijection réciproque f^{-1} est continue et strictement monotone (de même sens de variation que f) sur $f(I)$.
(iii) En notant $a = \inf I$ (ou $a = -\infty$ si I n'est pas minoré) et $b = \sup I$ (ou $b = +\infty$ si I n'est pas majoré),

on obtient $f(I)$ à l'aide du tableau suivant :

	$I=[a,b]$	$I=]a,b]$	$I=[a,b[$	$I=]a,b[$
f croissante	$[f(a), f(b)]$	$\left]\lim\limits_{a^+} f, f(b)\right]$	$\left[f(a), \lim\limits_{b^-} f\right]$	$\left]\lim\limits_{a^+} f, \lim\limits_{b^-} f\right]$
f décroissante	$[f(b), f(a)]$	$\left[f(b), \lim\limits_{a^+} f\right[$	$\left]\lim\limits_{b^-} f, f(a)\right]$	$\left]\lim\limits_{b^-} f, \lim\limits_{a^+} f\right]$

On peut créer des bijections discontinues qui ne sont pas monotones, mais une bijection continue sera forcément strictement monotone.

Exemple 5.15 :
Soit $f: \begin{array}{ccc} \mathbb{R}_+^* & \to & \mathbb{R} \\ x & \mapsto & x+\ln x \end{array}$. Les fonctions Id et ln sont continues sur $\mathbb{R}_+^*$ donc $f \in \mathcal{C}^0\left(\mathbb{R}_+^*\right)$. Soient $x, x' \in \mathbb{R}_+^*$ vérifiant $x < x'$. Alors

$$f(x') - f(x) = x' - x + \ln x' - \ln x \geq \ln \frac{x'}{x} > 0,$$

car $\frac{x'}{x} > 1$. Donc f est strictement croissante sur $\mathbb{R}_+^*$. Enfin, on calcule

$$\lim_{x\to 0^+} x + \ln x = -\infty, \qquad \lim_{x\to+\infty} x+\ln x = +\infty.$$

D'après le théorème de la bijection, f réalise donc une bijection de $\mathbb{R}_+^*$ sur $\mathbb{R}$. ♢

Exercice 5.16 :
Soit $f \in \mathcal{C}^0([0,1[, [0,1])$.

1. Est-il possible que f soit injective ?
2. Est-il possible que f soit surjective ?
3. Est-il possible que f soit bijective ?

Réponse

1. $x \mapsto x$ vérifie ces conditions.
2. $x \mapsto \sin(\pi x)$ vérifie ces conditions.
3. Supposons par l'absurde que f soit bijective. Alors f est strictement monotone donc, par le théorème de la bijection,

$$f([0,1[) = [f(0), \lim_1 f[\cup] \lim_1 f, f(0)].$$

Autrement dit, $f([0,1[)$ est semi-ouvert, ce qui est impossible si $f([0,1[) = [0,1]$.

♢

4. Continuité uniforme

Définition 5.17
Soit $f \in \mathcal{F}(I, \mathbb{K})$. On dit que f *est uniformément continue sur* I si

$$\forall \varepsilon > 0, \quad \exists \alpha > 0, \quad \forall x, y \in I, \quad |x - y| \leq \alpha \Rightarrow |f(x) - f(y)| \leq \varepsilon.$$

Ici, α ne dépend pas du point où l'on regarde la continuité. En particulier, une fonction uniformément continue est continue.

Contrairement à la continuité, la continuité uniforme est une notion globale. Cela n'a aucun sens de dire que "f est continue uniformément en $x_0 \in I$".

Théorème 5.18 *Caractérisation séquentielle de la continuité uniforme*
Soient $f \in \mathcal{F}(I, \mathbb{K})$. Alors

$$f \text{ est uniformément continue sur } I$$
$$\Longleftrightarrow \forall (u_n), (v_n) \in I^{\mathbb{N}}, \quad \left(\lim_{n \to +\infty} (u_n - v_n) = 0 \Rightarrow \lim_{n \to +\infty} (f(u_n) - f(v_n)) = 0 \right)$$

Démonstration : $\boxed{\Rightarrow}$ Soient $(u_n), (v_n) \in I^{\mathbb{N}}$ telle que $\lim (u_n - v_n) = 0$. Soit $eps > 0$, il existe $\alpha > 0$ tel que

$$\forall x, y \in I, |x - y| \leq \alpha \Rightarrow |f(x) - f(y)| \leq \varepsilon.$$

De plus, il existe $N \in \mathbb{N}$ tel que

$$\forall n \geq N, |u_n - v_n| \leq \alpha.$$

On en déduit que

$$\forall n \geq N, \quad |f(u_n) - f(v_n)| \leq \varepsilon,$$

ce qui achève la preuve de l'implication.

$\boxed{\Leftarrow}$ On va montrer la contraposée. Supposons donc qu'il existe $\varepsilon > 0$ tel que pour tout $\alpha > 0$, il existe $u, v \in I$ vérifiant $|u - v| \leq \alpha$ et $|f(u) - f(v)| > \varepsilon$. En particulier, notons pour $n \in \mathbb{N}^*$, $\alpha_n = \dfrac{1}{n}$. Alors il existe $u_n, v_n \in I$ tels que $|u_n - v_n| \leq \alpha$ et $|f(u_n) - f(v_n)| > \varepsilon$. On vient donc de construire deux suites (u_n) et (v_n) dont la différence tend vers 0 mais telles que $(f(u_n) - f(v_n))$ n'admet pas 0 pour limite, ce qui achève la preuve de ce théorème. $\square$

Exemple 5.19 :
Montrons que exp n'est pas uniformément continue sur $\mathbb{R}$. On pose

$$\forall n \in \mathbb{N}^*, \quad x_n = n + \frac{1}{n}, \quad y_n = n.$$

Il est clair que $\lim_{n \to +\infty} (x_n - y_n) = 0$. En revanche,

$$\mathrm{e}^{x_n} - e^{y_n} = \mathrm{e}^n \left(\mathrm{e}^{1/n} - 1 \right) \underset{n \to +\infty}{\sim} \frac{\mathrm{e}^n}{n} \xrightarrow[n \to +\infty]{} +\infty.$$

$\diamondsuit$

Théorème 5.20 *Théorème de Heine*[7]
Toute fonction continue sur un segment est uniformément continue.

Démonstration : Soient $a, b \in \mathbb{R}$ tels que $a < b$ et soit $f \in \mathcal{C}^0([a, b])$. Supposons, par l'absurde, que f ne soit pas uniformément continue. Alors

$$\exists \varepsilon > 0, \forall \alpha > 0, \exists (x, y) \in [a, b]^2, (|x - y| \leq \alpha \text{ et } |f(x) - f(y)| > \varepsilon).$$

Soit un tel $\varepsilon > 0$. Alors, pour tout $n \in \mathbb{N}^*$, il existe $(x_n, y_n) \in [a, b]$ vérifiant $|x_n - y_n| \leq \dfrac{1}{n}$ et $|f(x_n) - f(y_n)| > \varepsilon$. D'après le théorème de Bolzano-Weierstrass, on peut extraire une suite $\left(x_{\varphi(n)}\right)$ convergeant vers $x \in [a, b]$ puis une suite $\left(y_{\varphi \circ \psi(n)}\right)$ convergeant vers $y \in [a, b]$. Alors la suite $\left(x_{\varphi \circ \psi(n)}\right)$ converge aussi vers x et, en passant à la limite,

$$\forall n \in \mathbb{N}, \quad |x_n - y_n| \leq \frac{1}{n}, \quad |x - y| \leq 0, \quad x = y.$$

D'autre part, par continuité de f, on a

$$\lim_{n \to +\infty} f(x_n) = f(x), \quad \lim_{n \to +\infty} f(y_n) = f(y) = f(x).$$

En passant une nouvelle fois à la limite, on a

$$\forall n \in \mathbb{N}, \quad |f(x_n) - f(y_n)| > \varepsilon, \quad 0 = |f(x) - f(y)| \geq \varepsilon,$$

ce qui est impossible. □

Exercice 5.21 :
Montrer que toute fonction lipschitzienne est uniformément continue, et que toute fonction uniformément continue est continue. Que peut-on dire des réciproques ?

Réponse

- Soit f une fonction K-lipschitzienne sur I. Alors, pour tout $\varepsilon > 0$, posons $\alpha = \dfrac{\varepsilon}{K}$. On a, pour tous $x, y \in I$,

$$|x - y| \leq \alpha \Rightarrow |f(x) - f(y)| \leq K|x - y| \leq K\frac{\varepsilon}{K} = \varepsilon,$$

  donc f est uniformément continue. La réciproque est fausse car $x \mapsto \sqrt{x}$ est uniformément continue sur le segment $[0, 1]$ (d'après le théorème de Heine) mais pas lipschitzienne.
- Par définition, uniforme continuité implique continuité. De plus, la fonction exp est continue mais pas uniformément continue sur $\mathbb{R}$.

◇

7. Eduard Heine (1821-1881) : Mathématicien allemand.

À connaître à la fin du chapitre

Limites

- Manipulation et calcul de limites pour des fonctions : en pratique, et en revenant à la définition.
- Calcul effectif de fonctions équivalentes et de fonctions négligeables.
- Connaître les résultats vrais pour les fonctions à valeurs réelles et ceux pour les fonctions à valeurs complexes.

Continuité

- Être à l'aise avec les notions de comportement local.
- Comprendre les notions de continuité et de discontinuité.
- Connaître et savoir appliquer le théorème des valeurs intermédiaires.
- Image d'un segment ou d'un intervalle par une fonction continue (fonctions à valeurs réelles uniquement).

Pour aller plus loin

- Fonctions localement lipschitziennes
- Autres notations de Landau : Θ, Ω, ω.

CHAPITRE 7

POLYNÔMES ET FRACTIONS RATIONNELLES

Heureusement qu'on la connaissait cette racine,
sinon on était dans la m****.

Gad Elmaleh

Quel est le lien entre la trajectoire d'un boulet de canon, l'équation différentielle $y'' - 2y' + y = 0$, la suite $\left(4^{n+2} + 2 \times 3^n\right)_{n \geq 0}$ et un développement limité ? Réponse : les polynômes ! Plus qu'une simple fonction réelle, un polynôme est aussi un objet algébrique dont l'étude est liée à de nombreux domaines des mathématiques. Dans ce chapitre, on s'intéresse à la construction des polynômes, à leurs liens avec les fonctions et évidemment à leurs racines. On parlera également d'arithmétique sur les polynômes, qui fonctionne globalement comme l'arithmétique sur les entiers. On conclura le chapitre avec les fractions rationnelles, à des fins pratiques, comme par exemple pour intégrer des fractions compliquées.

Dans tout ce chapitre, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. [1]

I Ensemble des polynômes

1. Structure de $\mathbb{K}[X]$

Définition 1.1 *Polynôme*

On appelle *polynôme à coefficients dans* $\mathbb{K}$ toute suite $(a_n)_{n \in \mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ nulle à partir d'un certain rang. On note l'ensemble de ces polynômes :

$$\mathbb{K}[X] = \left\{(a_n)_{n \in \mathbb{N}} \in \mathbb{K}^{\mathbb{N}} / \exists n_0 \in \mathbb{N}, \forall n \geq n_0, a_n = 0\right\}$$

Il convient évidemment de penser à un polynôme comme à un élément de la forme $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots$ pour $x \in \mathbb{K}$. Nous verrons un peu plus loin le rapport entre ces deux approches. En gardant cette interprétation en tête, on peut définir des opérations sur les polynômes.

1. En règle générale, on peut faire des polynômes sur un corps commutatif , voire sur un anneau commutatif intègre.

Définition 1.2 *Opérations sur les polynômes*

Soient deux polynômes $P = (a_n) \in \mathbb{K}[X]$ et $Q = (b_n) \in \mathbb{K}[X]$, et soit $\lambda \in \mathbb{K}$. On définit :

- $P + Q \in \mathbb{K}[X]$ tel que $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$.
- $P \times Q \in \mathbb{K}[X]$ tel que $P \times Q = \left(\sum_{k=0}^{n} a_k b_{n-k}\right)_{n\in\mathbb{N}}$.
- $\lambda \cdot P \in \mathbb{K}[X]$ tel que $\lambda \cdot P = (\lambda a_n)_{n\in\mathbb{N}}$.

La multiplication sur les polynômes est évidemment définie de cette manière pour qu'on ait l'égalité suivante, pour tout $x \in \mathbb{K}$:

$$\left(\sum_{n=0}^{p} a_n x^n\right)\left(\sum_{n=0}^{q} b_n x^n\right) = \sum_{n=0}^{pq}\left(\sum_{k=0}^{n} a_k b_{n-k}\right) x^n.$$

On remarquera que, dans la suite, on pourra omettre d'écrire $\cdot$ ou $\times$ puisque

$$P \times Q = Q \times P, \quad \lambda \cdot (P \times Q) = (\lambda \cdot P) \times Q = P \times (\lambda \cdot Q).$$

Proposition 1.3 *Structure de l'ensemble des polynômes - Admis*

(i) L'ensemble $(\mathbb{K}[X], +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.
(ii) L'ensemble $(\mathbb{K}[X], +, \times)$ est un anneau commutatif.

On dit que l'ensemble $\mathbb{K}[X]$ est une $\mathbb{K}$-algèbre commutative. [2] Pour la suite, rappelons le symbole de Kronecker :

$$\forall k, n \in \mathbb{Z}, \quad \delta_{k,n} = \begin{cases} 1 \text{ si } k = n \\ 0 \text{ sinon} \end{cases}.$$

On remarquera que

- Deux polynômes $P = (a_n)$ et $Q = (b_n)$ sont égaux, si et seulement si, $\forall n \in \mathbb{N}, a_n = b_n$.
- La suite nulle $(0, 0, \dots)$ est un polynôme : on l'appelle polynôme nul. Puisqu'elle est l'élément neutre pour $+$, on la note naturellement 0.
- La suite $(\delta_{0,n})_{n\in\mathbb{N}} = (1, 0, 0, \dots)$ est un polynôme. De plus, elle est l'élément neutre pour $\times$, on la note donc naturellement 1.

Définition 1.4 *Indéterminée*

On note $X = (\delta_{1,n})_{n\in\mathbb{N}} = (0, 1, 0, 0, \dots)$ le polynôme dont le seul terme non-nul est le second. On l'appelle *indéterminée.*

Proposition 1.5

On a, pour tous $p, q \in \mathbb{N}^*$, $X^p = (\delta_{p,n})_{n\in\mathbb{N}}$ et $X^{p+q} = X^p \times X^q$.

2. C'est-à-dire que $\mathbb{K}[X]$ est à la fois un $\mathbb{K}$-ev et un anneau commutatif, et que $\lambda \cdot (P \times Q) = (\lambda \cdot P) \times Q = P \times (\lambda \cdot Q)$.

Par convention, on notera évidemment $X^0 = 1 = (\delta_{0,n})_{n\in\mathbb{N}}$.

Démonstration : On montre par récurrence sur p que $X^p = (\delta_{p,n})_{n\in\mathbb{N}}$.

$\boxed{\text{Initialisation}}$ $X = (\delta_{1,n})_{n\in\mathbb{N}}$, c'est évident.

$\boxed{\text{Hérédité}}$ Soient $p, q \in \mathbb{N}^*$ et supposons que $X^p = (\delta_{p,n})_{n\in\mathbb{N}}$. Alors,

$$X^{p+1} = X^p \times X = \left(\sum_{k=0}^{n} \delta_{p,n-k}\delta_{1,k}\right)_{n\in\mathbb{N}} = (\delta_{p,n-1})_{n\in\mathbb{N}} = (\delta_{p+1,n})_{n\in\mathbb{N}}.$$

Donc la propriété est vraie au rang $p+1$ et donc pour tout $p \in \mathbb{N}$. Il ne reste plus qu'à vérifier que

$$X^pX^q = X^p \times X^q = \left(\sum_{k=0}^{n} \delta_{p,n-k}\delta_{q,k}\right)_{n\in\mathbb{N}} = (\delta_{p,n-q})_{n\in\mathbb{N}} = (\delta_{p+q,n})_{n\in\mathbb{N}} = X^{p+q}.$$

□

On remarquera qu'on peut exprimer tout polynôme comme combinaison linéaire des polynômes $1, X, X^2, \ldots$ En effet, pour tout $P = (a_n) \in \mathbb{K}[X]$, il existe $n_0 \in \mathbb{N}$ tel que, pour tout $n > n_0, a_n = 0$. Alors

$$P = (a_0, a_1, \ldots, a_{n_0}, 0, 0, \ldots) = \sum_{k=0}^{n_0} a_k (\delta_{k,n}) = \sum_{k=0}^{n_0} a_k X^k.$$

A partir de maintenant, on écrira donc

$$P = \sum_{k=0}^{n_0} a_k X^k = \sum_{k=0}^{\infty} a_k X^k.$$

Il est sous-entendu dans cette dernière écriture que la suite (a_n) est nulle à partir d'un certain rang.

X est un symbole, et pas une variable (réelle ou complexe).

Exercice 1.6 :
Calculer $\left(X^2 + 3X + 2\right) \times \left(X^3 + X - 1\right)$ avec les deux écritures possibles pour les polynômes. ◊

2. Degré d'un polynôme

Définition 1.7 *Monôme*

- On appelle *monôme* tout polynôme de la forme $a_k X^k$ pour $k \in \mathbb{N}$.
- Soit $P = \sum_{k=0}^{\infty} a_k X^k \in \mathbb{K}[X]$. On appelle *coefficient* de X^k le scalaire a_k. On appelle *terme de degré k de P* le monôme $a_k X^k$.

Définition 1.8 *Degré*

Soit $P = \sum_{k=0}^{\infty} a_k X^k \in \mathbb{K}[X]$. On définit le *degré de P* par :

$$\deg(P) = \begin{cases} \max\{k \in \mathbb{N} / a_k \neq 0\} & \text{si } P \neq 0 \\ -\infty & \text{si } P = 0 \end{cases}.$$

Il est clair que le degré est bien défini car la suite (a_n) est nulle à partir d'un certain rang. On note parfois $d^\circ = \deg$.

De manière équivalente, si $P = \sum_{k=0}^{\infty} a_k X^k \in \mathbb{K}[X] \setminus \{0\}$ alors

$$\deg P = d \iff \begin{cases} a_d \neq 0 \\ \forall k > d, \quad a_k = 0 \end{cases}.$$

Attention à l'erreur ultra-classique :

$$P = \sum_{k=0}^{d} a_k X^k \Rightarrow \deg P = d.$$

Définition 1.9 *Polynôme unitaire*

Soit $P = \sum_{k=0}^{p} a_k X^k \in \mathbb{K}[X] \setminus \{0\}$ un polynôme de degré $p \in \mathbb{N}$ (c'est-à-dire que $a_p \neq 0$). On appelle *terme dominant de P* le monôme $a_p X^p$. On appelle *coefficient dominant de P*, et on note, $\operatorname{dom}(P) = a_p$. Un polynôme dont le coefficient dominant vaut 1 est dit *unitaire* .

Par convention, on pose

- $\deg(0) = -\infty$
- $\operatorname{dom}(0) = 0$.

On dira parfois qu'on normalise $P = a_p X^P + a_{p-1} X^{p-1} + \cdots + a_1 X + a_0$ en le divisant par son terme dominant :

$$X^P + \frac{a_{p-1}}{a_p} X^{p-1} + \cdots + \frac{a_1}{a_p} X + \frac{a_0}{a_p}.$$

On emploie donc parfois le terme *normalisé* au lieu d'unitaire. On notera aussi que

$$\deg P = -\infty \iff P = 0, \quad \deg P = 0 \iff P \in \mathbb{K}^*.$$

Proposition 1.10

Pour tous $P, Q \in \mathbb{K}[X] \setminus \{0\}, \lambda \in \mathbb{K}^*$, on a

(i) $\deg(PQ) = \deg(P) + \deg(Q)$ et $\operatorname{dom}(PQ) = \operatorname{dom}(P)\operatorname{dom}(Q)$.

(ii) $\deg(P+Q) \leq \max(\deg P, \deg Q)$. De plus,

$$\deg(P+Q) < \max(\deg P, \deg Q) \iff \begin{cases} \deg P = \deg Q \\ \operatorname{dom} P = -\operatorname{dom} Q \end{cases}.$$

(iii) $\deg(\lambda P) = \deg(P)$ et $\mathrm{dom}(\lambda P) = \lambda \,\mathrm{dom}\, P$.

Avec cette proposition, on comprend mieux les conventions $\deg 0 = -\infty$ et $\mathrm{dom}\, 0 = 0$, qui permet de généraliser au polynôme nul les formules précédentes.

Démonstration : Soient $P, Q \in \mathbb{R}[X] \setminus \{0\}$. Posons $P = \sum_{k=0}^{p} a_k X^k$ et $Q = \sum_{k=0}^{q} b_k X^k$ avec $\deg P = p, \deg Q = q$ (autrement dit, $a_p \neq 0$ et $a_q \neq 0$.

(i) On rappelle que $PQ = \sum_{k=0}^{\infty} c_k X^k$ avec $c_k = \sum_{i=0}^{k} a_i b_{k-i}$. Puisque $a_i = 0$ si $i > p$ et $b_j = 0$ si $j > q$, il est clair que $c_{p+q} = a_p b_q \neq 0$ et, pour tout $k > p+q$, $c_k = 0$. Donc $\deg PQ = p+q$ et $\mathrm{dom}(PQ) = a_p b_q$.

(ii) On a $P + Q = \sum_{k=1}^{\infty} (a_k + b_k) X^k$. Puisque pour tout $k > \max(p,q)$, $a_k + b_k = 0$, $\deg(P+Q) \leq \max(p,q)$. On peut supposer que $p \geq q$. Alors

$$\deg(P+Q) < \max(p,q) \iff a_p + b_p = 0 \iff \begin{cases} b_p = -a_p \\ b_p \neq 0 \end{cases} \iff \begin{cases} a_p = -b_q \\ p = q \end{cases}.$$

(iii) Evident.

□

Exemple 1.11 :
Posons $P = 2X^2 - 3X - 1$ et $Q = (X-1)(X-3)(X+1)$. Par définition, on a $\deg P = 2$. De plus, Q est un polynôme (comme produit de trois polynômes) et son degré vaut $\deg Q = 1+1+1 = 3$. On en déduit sans calculs que

$$\deg(PQ) = 5, \quad \mathrm{dom}(PQ) = 2, \quad \deg(P+Q) = 3, \quad \mathrm{dom}(P+Q) = 1.$$

♢

On retiendra de la propriété précédente qu'il faut faire attention au degré de la somme de deux polynômes. On en tire également des conséquences fondamentales relatives à l'anneau $\mathbb{K}[X]$.

Corollaire 1.12

(i) L'anneau $\mathbb{K}[X]$ est intègre.
(ii) Les éléments inversibles de $\mathbb{K}[X]$ sont les polynômes de degré 0, c'est-à-dire les polynômes constants non-nuls.

On rappelle qu'un anneau est intègre si :

$$\forall P, Q \in \mathbb{K}[X], \quad PQ = 0 \iff P = 0 \text{ ou } Q = 0.$$

Démonstration : (i) Soient $P, Q \in \mathbb{R}[X]$. Alors, par contraposée

$$\begin{cases} P \neq 0 \\ Q \neq 0 \end{cases} \Rightarrow \begin{cases} \deg P \geq 0 \\ \deg Q \geq 0 \end{cases} \Rightarrow \deg P + \deg Q \geq 0 \Rightarrow PQ \neq 0.$$

(ii) Il est clair que les polynômes de degré 0 sont inversibles, car ce sont les éléments de $\mathbb{K}^*$. Montrons l'inclusion réciproque en prenant $P \in \mathbb{K}[X]$ inversible. En particulier, $P \neq 0$. Il existe $Q \in \mathbb{R}[X] \setminus \{0\}$ tel que $PQ = 1$. Donc $\deg(P) + \deg(Q) = 0$ et $\deg(P), \deg(Q) \in \mathbb{N}$ donc $\deg(P) = 0$.

□

Définition/Proposition 1.13

Pour tout $n \in \mathbb{N}$, on définit l'ensemble des polynômes de degré inférieur à n

$$\mathbb{K}_n[X] = \{P \in \mathbb{K}[X] / \deg P \leq n\}.$$

Alors $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$.

Exemple 1.14 :
$\mathbb{K}_0[X] = \{\lambda / \lambda \in \mathbb{K}\} = \mathbb{K}$ et $\mathbb{K}_1[X] = \{aX + b / (a, b) \in \mathbb{K}^2\}$. ♢

Démonstration : Il est clair que $\mathbb{K}_n[X] \subseteq \mathbb{K}[X]$ (qui est un espace vectoriel) et que $0 \in \mathbb{K}_n[X]$. Soient $P, Q \in \mathbb{K}_n[X]$ et $\lambda, \mu \in \mathbb{K}$. Alors

$$\deg(\lambda P + \mu Q) \leq \max(\deg(\lambda P), \deg(\mu Q)) \leq \max(\deg P, \deg Q) \leq n.$$

Donc $\lambda P + \mu Q \in \mathbb{K}_n[X]$. Donc $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$. □

Exercice 1.15 :
$\mathbb{K}_n[X]$ est-il un sous-anneau de $\mathbb{K}[X]$?

Réponse

Si $n \geq 1, \mathbb{K}_n[X]$ n'est évidemment pas un sous-anneau de $\mathbb{K}[X]$. En effet, il n'est pas stable par produit : $X^n \times X^n = X^{2n} \notin \mathbb{K}_n[X]$. En revanche, $\mathbb{K}_0[X] = \mathbb{K}$ est bien un sous-anneau de $\mathbb{K}[X]$.

♢

3. Polynôme dérivé

S'il convient de différencier "polynôme" et "fonction polynomiale", il est évident que les deux notions possèdent d'importantes connexions. C'est pourquoi on définit sur l'ensemble des polynômes des applications similaires à celles définies sur les fonctions : la dérivation et la composition.

Définition 1.16 *Dérivation*

On définit l'application "*Dérivation*" sur $\mathbb{K}[X]$:

$$D : \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K}[X] \\ \displaystyle\sum_{k=0}^{\infty} a_k X^k & \mapsto & \displaystyle\sum_{k=0}^{\infty} (k+1) a_{k+1} X^k \end{array}$$

Le polynôme $D(P)$ est appelé *polynôme dérivé de* P, on le note aussi P'.

⚠ Il s'agit d'une définition. En particulier, on ne parle pas ici de dérivabilité : l'application D est bien définie sur tout $\mathbb{K}[X]$. Il ne faut pas confondre polynôme et fonction polynomiale (nous reviendrons là-dessus plus tard).

Pour ce qui est des calculs, on dérive exactement comme on en a l'habitude :

$$\forall n \in \mathbb{N}^*, \quad D(X^n) = nX^{n-1}, \quad D\left(\sum_{k=0}^{\infty} a_k X^k\right) = \sum_{k=0}^{\infty} (k+1) a_{k+1} X^k = \sum_{k=1}^{\infty} k a_k X^{k-1}.$$

On définira avec les notations usuelles,

$$P^{(0)} = P, \quad \forall n \in \mathbb{N}, \quad P^{(n+1)} = D\left(P^{(n)}\right).$$

Exemple 1.17 :
Si $P = 2X^2 - 3X + 6$, alors $P' = 4X - 3$. ♢

Proposition 1.18

(i) $D \in \mathcal{L}(\mathbb{K}[X])$.
(ii) L'application D vérifie

$$\forall P, Q \in \mathbb{R}[X], \quad (PQ)' = PQ' + P'Q.$$

(iii) Pour tout $P \in \mathbb{R}[X]$,

$$\deg(P') = \begin{cases} \deg(P) - 1 & \text{si } \deg P \geq 1 \\ -\infty & \text{si } \deg P \leq 0 \end{cases}.$$

Démonstration : Soient $P = \sum_{k=0}^{\infty} a_k X^k, Q = \sum_{k=0}^{\infty} b_k X^k$ deux polynômes.

(i) Soient $\lambda, \mu \in \mathbb{K}$. On a

$$\begin{aligned} D(\lambda P + \mu Q) &= D\left(\sum_{k=0}^{\infty} (\lambda a_k + \mu b_k) X^k\right) = \sum_{k=0}^{\infty} (\lambda (k+1) a_{k+1} + \mu (k+1) b_{k+1}) X^k \\ &= \lambda \sum_{k=0}^{\infty} (k+1) a_{k+1} X^k + \mu \sum_{k=0}^{\infty} (k+1) b_{k+1} X^k = \lambda D(P) + \mu D(Q). \end{aligned}$$

Donc D est une application linéaire.

(ii) Pour tout $p, q \in \mathbb{N}^*$, on a

$$D(X^p X^q) = (p+q) X^{p+q-1} = pX^{p-1}X^q + qX^{q-1}X^p = QD(P) + PD(Q).$$

La formule précédente reste vraie pour $p = 0$ ou $q = 0$ puisque $X^0 = 1$ et $D\left(X^0\right) = 0$. Alors,

$$\begin{aligned} D(X^p Q) &= D\left(\sum_{k=0}^{\infty} b_k X^k X^p\right) = \sum_{k=0}^{\infty} b_k D\left(X^k X^p\right) = \sum_{k=0}^{\infty} b_k X^k D(X^p) + \sum_{k=1}^{\infty} b_k (k) X^{k-1} X^p \\ &= X^p D(Q) + QD(X^p) \\ D(PQ) &= D\left(\sum_{k=0}^{\infty} a_k X^k Q\right) = \sum_{k=0}^{\infty} a_k D\left(X^k Q\right) = \sum_{k=0}^{\infty} a_k X^k D(Q) + \sum_{k=1}^{\infty} a_k (k) X^{k-1} Q \\ &= PD(Q) + QD(P) \end{aligned}$$

(iii) Il est clair que si $P \in \mathbb{K}$ alors $D(P) = \lambda D\left(X^0\right) = 0$. D'autre part, si $\deg P = p \in \mathbb{N}^*$, alors $a_p \neq 0$ et $\forall k > p, a_k = 0$. Puisque $D(P) = \sum_{k=0}^{\infty} (k+1) a_{k+1} X^k, \deg(D(P)) = p - 1$ par définition.

□

Exercice 1.19 :
Déterminer $\ker D$ et $\operatorname{Im} D$.

Réponse

1. D'après le point (*iii*), on a montré que, pour tout $P \in \mathbb{K}[X]$,
$$P \in \ker D \iff P' = 0 \iff \deg P' = -\infty \iff P \in \mathbb{K}_0[X],$$
donc $\ker D = \mathbb{K}_0[X]$.
2. On va montrer que D est surjective en un cherchant un polynôme "primitive" avec les outils usuels. Soit $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$. On pose alors
$$Q = \sum_{k=0}^{+\infty} \frac{a_k}{k+1} X^{k+1} = \sum_{k=1}^{+\infty} \frac{a_{k-1}}{k} X^k.$$
Alors $D(Q) = P$ et donc $\operatorname{Im} D = \mathbb{K}[X]$.

♢

4. Composition de polynômes

Définition 1.20 *Composition de deux polynômes*

Soient $P, Q \in \mathbb{K}[X]$, on note $P = \sum_{k=0}^{p} a_k X^k$ avec $p \in \mathbb{N}$. On définit le *polynôme composé* :
$$P \circ Q = \sum_{k=0}^{p} a_k Q^k.$$
On note aussi $P \circ Q = P(Q)$.

Cette formule fonctionne, encore une fois, comme la composition de deux fonctions. En particulier, par définition, $P(X) = P$.[3] On notera également que $\circ$ n'est pas commutative :
$$0 \circ 1 = 0, \quad 1 \circ 0 = 1.$$

Exemple 1.21 :
Si $Q = 1 + X$, on a
$$P(Q) = \sum_{k=0}^{p} a_k (X+1)^k = \sum_{k=0}^{p} a_k \left(\sum_{i=0}^{k} \binom{k}{i} X^i \right) = \sum_{k=0}^{p} \sum_{i=0}^{k} a_k \binom{k}{i} X^i = \sum_{i=0}^{p} \left(\sum_{k=i}^{p} a_k \binom{k}{i} \right) X^i$$

♢

Exercice 1.22 :
Soit $P \in \mathbb{R}[X]$ tel que $P = P \circ (-X)$. Montrer qu'il existe $Q \in \mathbb{R}[X]$ tel que $P = Q \circ X^2$.

3. Attention, si $f : E \to F$ alors $f(x) \neq f$! Par contre on a bien $f \circ \mathrm{Id}_E = f$.

Réponse

Notons $P = \sum_{k=0}^{p} a_k X^k$. On a

$$P(-X) = \sum_{k=0}^{\infty} a_k (-X)^k = \sum_{k=0}^{\infty} (-1)^k a_k X^k = \sum_{k=0}^{\infty} a_k X^k.$$

Donc pour tout $k \in \mathbb{N}, a_k = (-1)^k a_k$. Donc $k \equiv 1 \ [2] \Rightarrow a_k = 0$. On en déduit que

$$P = a_0 + a_2 X^2 + a_4 X^4 + \cdots = \sum_{k=0}^{\infty} a_{2k} X^{2k}.$$

En posant $Q = \sum_{k=0}^{\infty} a_{2k}$, on a $P = Q\left(X^2\right)$.

♢

Exercice 1.23 :
Soient $P, Q \in \mathbb{R}[X]$. Déterminer $\deg(P \circ Q)$.

Réponse

Notons $P = \sum_{k=0}^{p} a_k X^k$. Supposons que $\deg P = p, \deg Q = q$ avec $p, q \in \mathbb{N} \cup \{-\infty\}$.

- Si $p = -\infty$ alors $P = P \circ Q = 0$.
- Si $p = 0$ alors $P \circ Q = P$ et $\deg P \circ Q = 0 = pq$.
- Si $p \geq 1$, alors

$$P \circ Q = \sum_{k=0}^{p} a_k Q^k = a_p Q^p + \sum_{k=0}^{p-1} a_k Q^k.$$

  D'une part, $a_p \neq 0$ et $\deg(Q^p) = p \deg Q = pq$ donc $\deg(a_p Q^p) = pq$. D'autre part,

$$\deg\left(\sum_{k=0}^{p-1} a_k Q^k\right) \leq (p-1)\, q.$$

  - Si $q \geq 1$ alors $(p-1)\, q < pq$ et $\deg(P \circ Q) = pq$.
  - Si $q \leq 0$, alors il existe $\lambda \in \mathbb{K}$ tel que $Q = \lambda$. Alors $\deg(P \circ Q) \leq 0$ et

$$\deg(P \circ Q) = -\infty \iff P(\lambda) = 0 \iff \lambda \text{ est une racine de } P,$$

    où l'on définira les racines plus tard dans le cours.

Il convient de remarquer qu'en général, la relation $\deg(P \circ Q) = \deg P \deg Q$ est fausse.

♢

II Arithmétique des polynômes

Dans cette section, on va voir que l'arithmétique sur $\mathbb{K}[X]$ permet de définir toute la structure de l'ensemble des polynômes, et fonctionne exactement comme l'arithmétique sur $\mathbb{Z}$. Cette section suit donc exactement le même plan que le chapitre d'arithmétique.

1. Divisibilité

Définition 2.1 *Multiple et diviseur*

Soient $A, B \in \mathbb{K}[X]$. On dit que A *divise* B si

$$\exists P \in \mathbb{K}[X], \quad AP = B.$$

Dans ce cas, on note $A|B$ et on dit que B est un *multiple* de A, ou que A est un *diviseur* de B. On note l'ensemble des multiples de A

$$A\mathbb{K}[X] = \{P \in \mathbb{K}[X]/A|P\} = \{PA \in \mathbb{K}[X]/P \in \mathbb{K}[X]\}.$$

Même si $A|B$, on n'écrira jamais $\frac{B}{A}$ en travaillant avec des polynômes.[4]

Proposition 2.2

(i) La relation $|$ est réflexive et transitive sur $\mathbb{K}[X]$.

(ii) $\forall A, B \in \mathbb{K}[X]$,

$$A|B \iff \forall \lambda \in \mathbb{K}^*, A|(\lambda B) \iff \forall \lambda \in \mathbb{K}^*, (\lambda A)|B.$$

(iii) $\forall A \in \mathbb{K}[X], 1|A, A|A, A|0$.

(iv) $\forall A \in \mathbb{K}[X], 0|A \iff A = 0$.

(v) $\forall A, B, P \in \mathbb{K}[X]$,

$$(P|A \text{ et } P|B) \iff (\forall U, V \in \mathbb{K}[X], P|(AU + BV)).$$

(vi) $\forall A, B \in \mathbb{K}[X]$,

$$(A|B \text{ et } B|A) \iff \exists \lambda \in \mathbb{K}^*, A = \lambda B.$$

(vii) $\forall A, B \in \mathbb{K}[X]$,

$$(A|B \text{ et } B \neq 0) \implies \deg A \leq \deg B.$$

D'après le point (ii), on remarquera que multiplier par $\lambda \in \mathbb{K}^*$ ne change rien à la relation de divisibilité, tout comme la divisibilité ne dépend pas du signe dans $\mathbb{Z}$. Autrement dit, $\mathbb{K}^*$ joue le rôle de $\{-1, 1\}$: il s'agit de l'ensemble des éléments inversibles. Dans la suite, on s'intéressera donc souvent seulement aux polynômes unitaires.

Démonstration : $\boxed{(i) \sim (v)}$ Aucun problème.

$\boxed{(vi)}$ La réciproque étant évidente, on montrera simplement l'implication. Soient $A, B \in \mathbb{K}[X]$ tels que $A|B$ et $B|A$. Alors il existe $P, Q \in \mathbb{K}[X]$ tels que $AP = B$ et $BQ = A$. Donc $APQ = A$ et $A(PQ - 1) = 0$. Puisque

4. Cela s'appelle une fraction rationnelle, et c'est l'objet de la dernière partie de ce chapitre.

l'anneau $\mathbb{K}[X]$ est intègre, $A = 0$ ou $PQ = 1$. Si $A = 0$, alors $0|B$ donc $B = 0$, donc $A = B$. Si $PQ = 1$, alors Q est inversible et on a trouvé $Q \in \mathbb{K}^*$ tel que $A = QB$.

$\boxed{(vii)}$ Soient $A, B \in \mathbb{K}[X]$ tels que $A|B$ et $B \neq 0$. Alors il existe $P \in \mathbb{K}[X]$ tel que $AP = B$ et $P \neq 0$. Donc $\deg B = \deg A + \deg P \geq \deg A$. □

Définition 2.3 *Polynômes associés*

Soient $A, B \in \mathbb{K}[X]$. On dit que A et B sont ***associés*** s'il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$.

Exercice 2.4 :
Montrer que la relation

$$A \sim B \iff A \text{ est associé à } B$$

est une relation déquivalence sur $\mathbb{K}[X]$. ♢

Définition 2.5 *Polynôme irréductible*

Soit $A \in \mathbb{K}[X]$. On dit que A est ***irréductible*** dans $\mathbb{K}[X]$ si $\deg A \geq 1$ et si les seuls diviseurs de A sont les polynômes associés à A et les polynômes inversibles.

Les polynômes irréductibles dans $\mathbb{K}[X]$ sont l'équivalent des nombres premiers dans $\mathbb{Z}$. De façon équivalente, A est irréductible si, pour tout $P, Q \in \mathbb{K}[X]$,

$$A = PQ \Rightarrow P \in \mathbb{K}^* \text{ ou } Q \in \mathbb{K}^*.$$

Exemple 2.6 :
Le polynôme $X^3 - X^2 + X - 1$ n'est pas irréductible car

$$X^3 - X^2 + X - 1 = (X - 1)\left(X^2 + 1\right).$$

- $X - 1$ est irréductible (dans $\mathbb{R}[X]$ ou $\mathbb{C}[X]$) car, pour tous $P, Q \in \mathbb{K}[X]$ tels que $X - 1 = PQ$, alors $\deg P + \deg Q = 1$ et donc $\deg Q = 0$ ou $\deg P = 0$.
- $X^2 + 1$ n'est pas irréductible dans $\mathbb{C}[X]$, car $X^2 + 1 = (X - i)(X + i)$.
- Soit $P \in \mathbb{R}[X]$ un diviseur de $X^2 + 1$ (dans $\mathbb{R}[X]$). On peut supposer que P est unitaire. Alors il existe $Q \in \mathbb{R}[X]$ tel que $PQ = X^2 + 1$. Supposons par l'absurde que P ne soit pas un diviseur trivial de $X^2 + 1$, c'est-à-dire que $\deg P = 1$. Il existe $a, b, c \in \mathbb{R}$ tels que

  $$P = a + X, \quad Q = b + cX, \quad c \neq 0, \quad X^2 + 1 = cX^2 + (ac + b)X + ab.$$

  Par identification des coefficients, on a donc $c = 1, b = -a$ et donc $-a^2 = 1$, ce qui est impossible car $a \in \mathbb{R}$. Donc $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$.

♢

On fera attention de toujours préciser si un polynôme est irréductible dans $\mathbb{R}[X]$ ou dans $\mathbb{C}[X]$ si le contexte n'est pas évident.

Remarque 2.7 : En prenant un peu d'avance sur la suite du cours, on remarque qu'on peut factoriser un polynôme en trouvant ses racines. Cependant, un polynôme qui n'a pas de racines réelles peut parfois se factoriser dans $\mathbb{R}[X]$:

$$X^4 + 1 = \left(X^2 + 1 + \sqrt{2}X\right)\left(X^2 + 1 - \sqrt{2}X\right).$$

Le but de la suite du cours est donc de déterminer quels sont les polynômes irréductibles de $\mathbb{R}[X]$ et de $\mathbb{C}[X]$. ♢

Proposition 2.8
Les polynômes de degré 1 sont irréductibles dans $\mathbb{K}[X]$.

Théorème 2.9 *Décomposition en produit de facteurs irréductibles - Admis*
Soit $A \in \mathbb{K}[X]$ tel que $\deg A \geq 1$. Alors il existe $\lambda \in \mathbb{K}^*, r \in \mathbb{N}^*, (P_1, \dots P_r) \in \mathbb{K}[X]^r$ distincts, irréductibles dans $\mathbb{K}[X]$ et unitaires, et $(\alpha_1, \dots \alpha_r) \in (\mathbb{N}^*)^r$ tels que

$$A = \lambda \prod_{i=1}^{r} P_i^{\alpha_i}.$$

De plus, cette décomposition est unique (à l'ordre près des facteurs P_i).

Cette décomposition est unique lorsque $\mathbb{K}$ est fixé. En effet, on peut avoir deux décompositions différentes dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$. Par exemple,

$$X^2 + 1 = X^2 + 1 = (X - i)(X + i).$$

Démonstration : La preuve se fait exactement comme dans $\mathbb{Z}$, et nécessite donc l'utilisation du théorème de Gauss ou du lemme d'Euclide. Elle est laissée en exercice pour les plus motivés. $\square$

On en déduit un critère pratique pour déterminer si un polynôme en divise un autre.

Lemme 2.10 *Admis*
Soient $A, B \in \mathbb{K}[X], A \neq 0, B \neq 0$. Il existe $r \in \mathbb{N}^*, P_1, \dots, P_r \in \mathbb{K}[X]$ irréductibles et unitaires, et il existe $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_r \in \mathbb{N}$ et $\lambda, \mu \in \mathbb{K}^*$ tels que

$$A = \lambda \prod_{k=1}^{r} P_k^{\alpha_k}, \quad B = \mu \prod_{k=1}^{r} P_k^{\beta_k}.$$

De plus,

$$A | B \iff \forall k \in [\![1, r]\!], \alpha_k \leq \beta_k.$$

De cette partie préliminaire sur l'arithmétique des polynômes, on peut déduire la correspondance suivante :

$\mathbb{K}[X]$	$\mathbb{Z}$
$\mathbb{K}^*$	$\{-1, 1\}$
$A \sim B$	$a = \pm b$
Coefficient dominant	Signe
Polynômes unitaire	$\mathbb{N}^*$
Polynômes irréductibles unitaires	Nombres premiers

2. Division euclidienne

Définition/Théorème 2.11 *Division euclidienne*[5] *polynomiale - Admis*
Soient $A, B \in \mathbb{K}[X]$. Si $B \neq 0$ alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]$ tels que

$$A = BQ + R, \quad \deg R < \deg B.$$

Alors Q est appelé *quotient* et R est appelé *reste* dans ***la division euclidienne de A par B.***

Il y a deux points importants à noter :

- Avec les notations précédentes, on remarquera que $B|A$ si, et seulement si, $R = 0$.
- Comme dans $\mathbb{Z}$, on peut effectuer l'algorithme d'Euclide (c'est-à-dire des divisions euclidiennes successives), qui donne le PGCD de A et B.

Démonstration : La preuve du théorème est similaire à celle de $\mathbb{Z}$. On peut montrer l'unicité facilement. Soient $Q_1, Q_2, R_1, R_2 \in \mathbb{K}[X]$ tels que

$$A = BQ_1 + R_1 = BQ_2 + R_2, \quad \deg R_1 < \deg B, \quad \deg R_2 < \deg B.$$

Alors

$$0 = A - A = B\left(Q_1 - Q_2\right) + \left(R_1 - R_2\right), \quad B\left(Q_2 - Q_1\right) = R_1 - R_2.$$

Si $Q_1 \neq Q_2$ alors $\deg\left(B\left(Q_2 - Q_1\right)\right) \geq \deg B > \deg\left(R_1 - R_2\right)$ ce qui est impossible. Donc $Q_1 = Q_2$ et donc $R_1 = A - BQ_1 = A - BQ_2 = R_2$. □

On admet la preuve du théorème, pour se concentrer sur la méthode effective de division euclidienne entre deux polynômes.

Exemple 2.12 :
Effectuons la division euclidienne de $3X^3 + 2X^2 - 7X + 6$ par $X + 2$:

$$\begin{array}{r|l} 3X^3+2X^2-7X+6 & X+2 \\ \cline{2-2} -4X^2-7X+6 & 3X^2-4X+1 \\ X+6 & \\ 4 & \end{array}, \qquad \begin{array}{rc} & 3X^2-4X+1 \\ X+2 & \sqrt{3X^3+2X^2-7X+6} \\ & 3X^3+6X^2 \\ \cline{2-2} & -4X^2-7X+6 \\ & -4X^2-8X \\ \cline{2-2} & X+6 \\ & X+4 \\ \cline{2-2} & 4 \end{array}$$

Donc $3X^3 + 2X^2 - 7X + 6 = (X + 2)\left(3X^2 - 4X + 1\right) + 4$. ◊

Exemple 2.13 :
Comment montrer que $X^2 + X + 1$ divise $2X^4 - X^3 - 2X + 1$? En effectuant la division euclidienne, pardi !

$$\begin{array}{r|l} 2X^4-X^3-2X+1 & X^2+X+1 \\ \cline{2-2} -3X^3-2X^2-2X+1 & 2X^2-3X \\ X^2+X+1 & \\ 0 & \end{array}$$

On en déduit que le reste dans la division euclidienne de $2X^4 - X^3 - 2X + 1$ par $X^2 + X + 1$ est 0, et donc $X^2 + X + 1$ divise $2X^4 - X^3 - 2X + 1$. ◊

Exercice 2.14 :
Déterminer une primitive de la fonction $f : \begin{array}{ccc} \mathbb{R} \setminus \{-1\} & \to & \mathbb{R} \\ x & \mapsto & \dfrac{3x^3 + x^2 + 2x + 5}{x + 1} \end{array}$.

5. Euclide (vers 300 av. J.C.) : Mathématicien grec.

Réponse

En effectuant la division euclidienne de $3X^3 + X^2 + 2X + 5$ par $1 + X$, on trouve

$$3X^3 + X^2 + 2X + 5 = (1 + X)\left(3X^2 - 2X + 4\right) + 1.$$

On en déduit que pour tout $x \neq -1, f(x) = 3x^2 - 2x + 4 + \dfrac{1}{1+x}$. Une primitive de f sur $\mathbb{R} \setminus \{-1\}$ est donc

$$F : x \mapsto x^3 - x^2 + 4x + \ln|1 + x|.$$

♢

Exercice 2.15 :
Soient $A_1, A_2, B \in \mathbb{K}[X], B \neq 0$ et soient $\lambda_1, \lambda_2 \in \mathbb{K}$. On note Q_i et R_i le quotient et le reste de la division euclidienne de A_i par B. Déterminer le reste de la division euclidienne de $\lambda_1 A_1 + \lambda_2 A_2$ par B.

Réponse

On a, pour tout $i \in \{1, 2\}$,

$$\lambda_i A_i = B(\lambda Q_i) + \lambda R_i, \quad \deg R_i < \deg B.$$

On en déduit que

$$\lambda_1 A_1 + \lambda_2 A_2 = B(\lambda_1 Q_1 + \lambda_2 Q_2) + (\lambda_1 R_1 + \lambda_2 R_2). \quad (*)$$

On remarque alors que

$$\deg(\lambda_1 R_1 + \lambda_2 R_2) \leq \max(\deg(\lambda_1 R_1), \deg(\lambda_2 R_2)) \leq \max(\deg(R_1), \deg(R_2)) < \deg B.$$

On en déduit que $(*)$ est la division euclidienne de $\lambda_1 A_1 + \lambda_2 A_2$ par B.

Note : Cela revient à montrer que le quotient et le reste dans la division euclidienne par B sont linéaires (en le polynôme A). ♢

3. Polynômes premiers entre eux

Définition/Théorème 2.16 *PGCD*

Soient $A, B \in \mathbb{K}[X], A \neq 0, B \neq 0$. On appelle *PGCD de A et B*, et on note $A \wedge B$ l'unique polynôme unitaire vérifiant

$$\forall P \in \mathbb{K}[X], \quad \begin{cases} P|A \\ P|B \end{cases} \iff P|A \wedge B.$$

Démonstration : $\boxed{\text{Unicité}}$ Soient D_1 et D_2 deux polynômes vérifiant

$$\forall P \in \mathbb{K}[X], \quad \begin{cases} P|A \\ P|B \end{cases} \iff P|D_i.$$

En particulier, $D_1|D_1$ donc $D_1|A$ et $D_1|B$, donc $D_1|D_2$. De manière similaire, on montre que D_2 divise D_1. Les polynômes D_1 et D_2 sont donc associés, c'est-à-dire qu'il existe $\lambda \in \mathbb{K}^*$ tel que $D_1 = \lambda D_2$. D'autre part, $\operatorname{dom}(D_1) = 1 = \lambda \operatorname{dom}(D_2) = \lambda$ car D_1 et D_2 sont unitaires. On en déduit que $D_1 = D_2$.

$\boxed{\text{Existence}}$ D'après l'arithmétique des entiers, un candidat pour le PGCD est le dernier reste non-nul dans l'algorithme d'Euclide. On effectue donc cet algorithme pour A et B. Il existe des polynômes $Q_0, \ldots, Q_{p+1}, R_0, \ldots, R_p \in \mathbb{K}[X]$ tels que

$$\begin{aligned}
A &= BQ_0 + R_0, \quad \deg R_0 < \deg B \\
B &= R_0 Q_1 + R_1, \quad \deg R_1 < \deg R_0 \\
R_0 &= R_1 Q_2 + R_2, \quad \deg R_2 < \deg R_1 \\
&\ldots \\
R_{p-2} &= R_{p-1} Q_p + R_p, \quad \deg R_p < \deg R_{p-1} \\
R_{p-1} &= R_p Q_{p+1} + 0
\end{aligned}$$

En notant $D(P, Q)$ les diviseurs communs de P et Q, il est clair que

$$D(A, B) = D(B, R_0) = \cdots = D(R_p, 0).$$

Donc les diviseurs de R_p sont exactement les diviseurs de A et B. On notera que R_p est non-nul mais pas forcément unitaire : il suffit de le normaliser pour obtenir le PGCD (ce qui ne change rien à la relation de divisibilité). $\square$

Définition/Théorème 2.17 *PPCM*

Soient $A, B \in \mathbb{K}[X], A \neq 0, B \neq 0$. On appelle *PPCM de A et B*, et on note $A \vee B$ l'unique polynôme unitaire vérifiant

$$\forall P \in \mathbb{K}[X], \quad \begin{cases} A|P \\ B|P \end{cases} \iff A \vee B | P.$$

Démonstration : L'unicité se traite comme l'unicité du PGCD : on démontre donc seulement l'existence d'un tel polynôme. On considère

$$N(A, B) = \{\deg P \in \mathbb{N} / A|P, B|P, P \neq 0\}.$$

$N(A, B) \neq \emptyset$ car $\deg(AB) \in N(A, B)$. C'est une partie non-vide de $\mathbb{N}$, elle admet donc un minimum d_0. Soit M un multiple commun de A et B de degré d_0 ; on va montrer que M est le PPCM de A et B. Soit $P \in \mathbb{K}[X]$. Il est clair que si $M|P$, alors $A|M$ donc $A|P$ et $B|P$. Supposons maintenant que $A|P$ et $B|P$. Alors il existe $(Q, R) \in \mathbb{K}[X]$ tels que

$$P = QM + R, \quad \deg R < \deg M.$$

Puisque $R = P - QM$ et que $M, P \in A\mathbb{K}[X] \cap B\mathbb{K}[X]$, il est clair que $R \in A\mathbb{K}[X] \cap B\mathbb{K}[X]$. Donc $R = 0$ car $\deg M = d_0 = \min N(A, B)$. Donc $M|P$. $\square$

Par convention, on pose pour tout $A \in \mathbb{K}[X]$: $A \wedge 0 = A$ et $A \vee 0 = 0$.

Proposition 2.18

Soient $A, B \in \mathbb{K}[X], A \neq 0, B \neq 0$. Il existe $r \in \mathbb{N}^*, P_1, \ldots, P_r \in \mathbb{K}[X]$ irréductibles et unitaires, il existe $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r \in \mathbb{N}$ et $\lambda, \mu \in \mathbb{K}^*$ tels que

$$A = \lambda \prod_{k=1}^{r} P_k^{\alpha_k}, \quad B = \mu \prod_{k=1}^{r} P_k^{\beta_k}.$$

Alors

(i) $A \wedge B$ est le plus grand diviseur commun unitaire de A et B (au sens du degré).

(ii) $A \wedge B = \prod_{k=1}^{r} P_k^{\min(\alpha_k,\beta_k)}$.
(iii) $A \wedge B$ est Le dernier reste non-nul dans l'algorithme d'Euclide appliqué à A et B.
(iv) $A \vee B$ est le plus petit multiple commun unitaire de A et B (au sens du degré).
(v) $A \vee B = \prod_{k=1}^{r} P_k^{\max(\alpha_k,\beta_k)}$.

Démonstration : En démontrant l'existence des PGCD et PPCM, on a déjà vérifié (iii) et (iv).

$\boxed{(i)}$ Soit P un diviseur commun de A et B. Alors $P|A \wedge B$ donc $\deg P \leq \deg(A \wedge B)$.

$\boxed{(iii) \text{ et } (v))}$ Comme dans $\mathbb{Z}$. □

Définition 2.19 *Polynômes premiers entre eux*
Soient $A, B \in \mathbb{K}[X]$. On dit que A et B sont *premiers entre eux* si $A \wedge B = 1$.

De manière équivalente, cela revient à dire que A et B sont premiers entre eux si leurs seuls diviseurs communs sont les polynômes constants non-nuls.

Exemple 2.20 :
Soient $a, b \in \mathbb{K}, a \neq b$. Montrons que $A = (X - a)$ et $B = (X - b)$ sont premiers entre eux. On a vu que A et B sont irréductibles. Les seuls diviseurs de A sont les polynômes associés à A et les polynômes de degré 0. A et B n'étant pas associés, leurs seuls diviseurs communs sont les polynômes de $\mathbb{K}^*$. Il existe donc un unique diviseur commun unitaire de A et B : $A \wedge B = 1$. ♢

Exercice 2.21 :
Déterminer le PGCD de $A = 2X^3 - 8X^2 + 18X - 72$ et $B = X^2 + (-3 + i)X + (2 - 2i)$. ♢

Théorème 2.22 *Théorème de Bézout*[6]
Soient $A, B \in \mathbb{K}[X] \setminus \{0\}$. Alors

$$A \wedge B = 1 \iff \exists U, V \in \mathbb{K}[X], AU + BV = 1.$$

Démonstration : $\boxed{\Rightarrow}$ L'important est de savoir trouver U et V en pratique : par la remontée de l'algorithme d'Euclide.

$\boxed{\Leftarrow}$ Supposons qu'il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$. Alors, pour tout polynôme P, si $P|A$ et $P|B$ alors $P|1 = AU + BV$. Puisque 1 est unitaire, alors $1 = A \wedge B$. □

Théorème 2.23 *Théorème de Gauss*[7]
Soient $A, B, C \in \mathbb{K}[X] \setminus \{0\}$. Alors

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

6. Étienne Bézout (1730-1783) : Mathématicien français.

Démonstration : Supposons que $A|BC$ et $A \wedge B = 1$. Alors il existe $P, U, V \in \mathbb{K}[X]$ tels que $AP = B$ et $AU + BV = 1$. On en déduit que

$$C = C\left(AU + BV\right) = C\left(AU + APV\right) = A\left(CU + CPV\right),$$

donc $A|C$. □

Théorème 2.24 *Lemme d'Euclide*

Soient $A, B, P \in \mathbb{K}[X] \setminus \{0\}$. Si P est irréductible alors

$$P|\left(AB\right) \Rightarrow P|A \text{ ou } P|B.$$

Démonstration : Supposons que $P|AB$ et que P ne divise pas A. Dans ce cas, les polynômes associés à P ne divisent pas A, donc les seuls diviseurs communs de A et P sont les polynômes de degré 0. Donc $A \wedge P = 1$ et $P|AB$ donc $P|B$ d'après le théorème de Gauss. □

On a vu que les trois théorèmes importants de l'arithmétique dans $\mathbb{Z}$ ont un équivalent pour les polynômes (et que les démonstrations sont rigoureusement identiques). De la même manière, leurs corollaires sont aussi applicables dans le cas des polynômes.

III Racines d'un polynôme

1. Fonction polynomiale

Définition 3.1 *Fonction polynomiale*

Soient $I \subseteq \mathbb{K}$ et $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$. On appelle *fonction polynomiale associée à P sur I* l'application

$$\widetilde{P} : \begin{array}{ccc} I & \to & \mathbb{K} \\ x & \mapsto & \sum_{k=0}^{n} a_k x^k \end{array}.$$

Il est important de différencier $\widetilde{P}$ et P, de la même manière qu'il est important de différencier x (une variable) et X (un symbole, le polynôme $\left(\delta_{1,n}\right)_{n\in\mathbb{N}}$). On ne mentionnera pas toujours I dans la suite.

Exemple 3.2 :
Soient $P = X^4 + 1$ et $Q = X^2 + 1$. Si on pose $I = \{-1, 0, 1\}$ alors on a

$$\widetilde{P}\left(-1\right) = \widetilde{P}\left(1\right) = 2, \widetilde{P}\left(0\right) = 1, \quad \widetilde{Q}\left(-1\right) = \widetilde{Q}\left(1\right) = 2, \widetilde{Q}\left(0\right) = 1.$$

Les fonctions polynomiales $\widetilde{P}$ et $\widetilde{Q}$ sont donc égales sur I, alors que les polynômes P et Q sont différents. ◇

De l'exemple précédent, on retiendra que lorsqu'on évalue des polynômes sur un ensemble fini de valeurs, on manque généralement d'informations sur ces polynômes. Pour pouvoir identifier polynôme et fonction polynomiale, c'est-à-dire pour que la fonction $P \mapsto \widetilde{P}$ soit injective, on verra un peu plus tard qu'il suffit que I soit un ensemble infini.

7. Carl Friedrich Gauss (1777-1855) : Mathématicien allemand. Légendaire.

Proposition 3.3

Soient $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. Alors

(i) $\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}$.
(ii) $\widetilde{\lambda \cdot P} = \lambda \cdot \widetilde{P}$.
(iii) $\widetilde{P \times Q} = \widetilde{P} \times \widetilde{Q}$.

Démonstration : La preuve est claire d'après la construction de $\mathbb{K}[X]$. □

2. Racines d'un polynôme

Définition 3.4 *Racine*

Soit $P \in \mathbb{K}[X]$ et $r \in \mathbb{K}$. On dit que r est une *racine de* P si $\widetilde{P}(r) = 0$. On note $Z(P)$ l'ensemble de toutes les racines de P et $Z_I(P) = Z(P) \cap I$ l'ensemble des racines de P dans $I \subseteq \mathbb{K}$.

Une racine de P est aussi appelée "zéro de P".

⚠ Comme on en a l'habitude avec les trinômes à coefficients réels, on prendra garde à distinguer les racines réelles de P, c'est-à-dire les éléments de $Z_{\mathbb{R}}(P)$ et les racines complexes de P, c'est-à-dire les éléments de $Z_{\mathbb{C}}(P)$.

Exemple 3.5 :
Soit $P = X^2 + 1 \in \mathbb{R}[X]$. Alors $Z_{\mathbb{R}}(P) = \emptyset$. On peut aussi voir P comme un polynôme de $\mathbb{C}[X]$ (puisque $\mathbb{R} \subseteq \mathbb{C}$) et dans ce cas $Z_{\mathbb{C}}(P) = \{i, -i\}$.

Soit $n \in \mathbb{N}$ et $Q = X^n - 1 \in \mathbb{C}[X]$. Alors

$$Z_{\mathbb{R}}(Q) = \begin{cases} \{1\} \text{ si } n \text{ est pair} \\ \{-1, 1\} \text{ si } n \text{ est impair} \end{cases} \quad , \quad Z_{\mathbb{C}}(Q) = \left\{ \mathrm{e}^{i\frac{2k\pi}{n}} / k \in [\![1, n]\!] \right\}.$$

♢

Lemme 3.6

Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Le reste de la division euclidienne de P par $(X - a)$ est $\widetilde{P}(a)$.

Démonstration : On sait qu'il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que

$$P = (X - a) Q + R, \quad R = P - (X - a) Q, \quad \deg R < 1.$$

Donc R est un polynôme constant. En particulier, en évaluant l'égalité précédente en a, on a

$$R = \widetilde{R}(a) = \left(P - \widetilde{(X - a)} Q\right)(a) = \widetilde{P}(a) - (a - a) Q(a) = \widetilde{P}(a).$$

□

Proposition 3.7

Soient $P \in \mathbb{K}[X]$ et $r \in \mathbb{K}$. Alors

$$r \in Z(P) \iff (X-r)\,|P.$$

Démonstration : En notant R le reste dans la division euclidienne de P par $(X-r)$, on a, d'après le lemme 3.6,

$$(X-r)\,|P \iff R=0 \iff \widetilde{P}(r)=0 \iff r \in Z(P)\,.$$

□

Proposition 3.8

Soient $P \in \mathbb{K}[X], n \geq 2$ et $r_1, \ldots, r_n \in Z(P)$ distincts. Alors

$$\prod_{k=1}^{n}(X-r_k)\,|P.$$

De plus, si $P \neq 0$ alors $\deg P \geq n$.

Démonstration : Les polynômes $(X-r_1), \ldots (X-r_n)$ sont deux à deux premiers entre eux et divisent P, donc $\prod_{k=1}^{n}(X-r_k)\,|P$. On en déduit que

$$\deg P \geq \deg\left(\prod_{k=1}^{n}(X-r_k)\right) = \sum_{k=1}^{n}\deg(X-r_k) = n.$$

□

Corollaire 3.9

Un polynôme de degré $n \in \mathbb{N}$ possède au plus n racines distinctes. En particulier, un polynôme non nul possède un nombre fini de racines.

Corollaire 3.10

Soit I un sous-ensemble infini de $\mathbb{K}$. Alors on peut identifier un polynôme à sa fonction polynomiale associée sur I.

Démonstration : Comme annoncé, on va montrer qu'une fonction polynomiale définit bien un polynôme, c'est-à-dire que $\varphi : P \mapsto \widetilde{P}$ est injective. On a vu que $\varphi \in \mathcal{L}\left(\mathbb{K}[X], \mathbb{R}^I\right)$, on va donc calculer son noyau. Soit $P \in \ker\varphi$. Alors pour tout $x \in I, \varphi(P)(x) = \widetilde{P}(x) = 0$. Donc P possède une infinité de racines, et donc $P=0$. Ce qui montre que $\ker\varphi = \{0\}$ et donc que φ est injective. □

Dans la suite, on considèrera toujours les fonctions polynomiales associées à des polynômes sur des ensembles infinis (généralement $\mathbb{K}$ lui-même). On n'écrira donc plus $\widetilde{P}(a)$ mais simplement $P(a)$. D'ailleurs, cela correspond bien à la notation de compositions de polynômes $P \circ Q = P(Q)$ lorsque $Q = a$ est un polynôme constant.

3. Formule de Taylor, multiplicité d'une racine

Théorème 3.11 *Formule de Taylor*

Soient $P \in \mathbb{K}[X], n \geq \deg P, a \in \mathbb{K}$. Alors on a

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} (X-a)^k .$$

Attention, il ne s'agit pas d'un développement limité, mais d'une égalité entre deux polynômes. En pratique, on utilise cette formule que pour $n = \deg P$. [8]

Démonstration : Soient $a \in \mathbb{K}$ et $\Psi : \mathbb{K}[X] \to \mathbb{K}[X]$ telle que, pour tout $P \in \mathbb{K}[X], \Psi(P) = \sum_{k=0}^{\infty} \frac{P^{(k)}(a)}{k!} (X-a)^k$.

Tout d'abord, Ψ est bien définie, car il s'agit d'une somme finie et donc $\Psi(P)$ est un polynôme. D'autre part, l'application $P \mapsto P'$ étant linéaire, on a $\Psi \in \mathcal{L}(\mathbb{K}[X])$. Soit $p \in \mathbb{N}$. Alors

$$(X^p)^{(k)} = \frac{p!}{(p-k)!} X^{p-k}, \quad \Psi(X^p) = \sum_{k=0}^{p} \frac{p!}{(p-k)!k!} a^{p-k} (X-a)^k = (X-a+a)^p = X^p.$$

On a donc, pour tous $n \in \mathbb{N}, P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$,

$$\sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} (X-a)^k = \Psi(P) = \Psi\left(\sum_{k=0}^{n} a_k X^k\right) = \sum_{k=0}^{n} a_k \Psi\left(X^k\right) = \sum_{k=0}^{n} a_k X^k = P.$$

□

Comme pour la formule de Taylor dans le cas des fonctions, on utilise souvent ce théorème lorsque l'on souhaite faire l'étude locale d'un polynôme, c'est-à-dire étudier un polynôme $P \in \mathbb{K}[X]$ au voisinage de $a \in \mathbb{K}$. Il permet aussi de relier l'annulation des dérivées successives de P en a et la divisibilité par de P par les puissances successives de $(X-a)$.

Définition 3.12 *Multiplicité*

Soient $P \in \mathbb{K}[X]$ et $r \in \mathbb{K}$. On définit la *multiplicité de r dans P* :

$$m_r(P) = \begin{cases} \max\{k \in \mathbb{N} / (X-r)^k \text{ divise } P\} \text{ si } P \neq 0 \\ +\infty \text{ si } P = 0 \end{cases}.$$

Si $m_r(P) = 1$, on dit que r *est une racine simple de P*.

On remarquera que par définition, pour tout $r \in \mathbb{K}, m_r(P) \leq \deg(P)$ si $P \neq 0$ D'autre part, r est une racine de P, si et seulement si, $m_r(P) \geq 1$. En pratique, pour déterminer la multiplicité d'une racine, on utilise deux critères. Voici le premier.

8. Quand on connaît $\deg P$!

Proposition 3.13

Soient $P \in \mathbb{K}[X]$ un polynôme non-nul, $r \in \mathbb{K}$ et $m \in \mathbb{N}$. Alors les propositions suivantes sont équivalentes :

(i) r est de multiplicité m dans P.
(ii) Il existe $Q \in \mathbb{K}[X]$ tel que

$$P = (X - r)^m Q, \quad Q(r) \neq 0.$$

Démonstration : $\boxed{(i) \Rightarrow (ii)}$ Par définition, il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - r)^m Q$. Donc

$$Q(r) = 0 \iff (X - r) | Q \iff \exists Q' \in \mathbb{K}[X], P = (X - r)^{m+1} Q' \iff (X - r)^{m+1} | P.$$

Donc $Q(r) \neq 0$.

$\boxed{(ii) \Rightarrow (i)}$ Il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - r)^m Q$, donc $(X - r)^m | P$. D'autre part, $Q(r) \neq 0$, et donc $(X - r)^{m+1}$ ne divise pas P. Donc $m = \max\{k \in \mathbb{N} / (X - r)^k \text{ divise } P\}$. □

Exemple 3.14 :
Déterminons les racines de $P = X^3 + 5X^2 + 8X + 4$ et leur multiplicité. On remarque que -1 est racine évidente, donc il existe $a, b, c \in \mathbb{R}$ tels que

$$X^3 + 5X^2 + 8X + 4 = (X + 1)\left(aX^2 + bX + c\right), \quad \begin{cases} a = 1 \\ a + b = 5 \\ b + c = 8 \\ c = 4 \end{cases}, \quad \begin{cases} a = 1 \\ b = 4 \\ c = 4 \end{cases}.$$

On en déduit que $P = (X + 1)\left(X^2 + 4X + 4\right) = (X + 1)(X + 2)^2$. Donc $m_1(P) = 1$ et $m_2(P) = 2$. ♢

Lemme 3.15

Soit $m \in \mathbb{N}^*$. Si r est racine de multiplicité m de P, alors r est racine de multiplicité $m - 1$ de P'.

Démonstration : D'après le critère précédent, il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - r)^m Q$, et $Q(r) \neq 0$. Alors

$$P' = Q'(X - r)^m + mQ(X - r)^{m-1} = (X - r)^{m-1}((X - r)Q' + mQ).$$

En notant $Q_1 = (X - r)Q' + mQ$, on a $P' = (X - r)^{m-1} Q_1$ et $Q_1(r) = mQ(r) \neq 0$ donc $m_r(P') = m - 1$. □

On en conclut un second critère pratique pour déterminer la multiplicité d'une racine.

Proposition 3.16

Soient $P \in \mathbb{K}[X]$ un polynôme non-nul, $r \in \mathbb{K}$ et $m \in \mathbb{N}$. Alors les propositions suivantes sont équivalentes :

(i) r est de multiplicité m dans P.
(ii) Pour tout $k \in [\![0, m - 1]\!]$, $P^{(k)}(r) = 0$ et $P^{(m)}(r) \neq 0$.

Démonstration : $\boxed{(i) \Rightarrow (ii)}$ Si $m = 0$, le résultat est évident. Sinon, par une récurrence immédiate à l'aide du lemme précédent, on a

$$m_r(P) = m, \quad m_r(P') = m-1, \dots, m_r\left(P^{(m-1)}\right) = 1, m_r\left(P^{(m)}\right) = 0.$$

Autrement dit, $P(r) = P'(r) = \cdots = P^{(m-1)}(r) = 0$ et $P^{(m)} \neq 0$.

$\boxed{(ii) \Rightarrow (i)}$ D'après la formule de Taylor, pour tout $n \geq \max(\deg P, m)$,

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(r)}{k!}(X-r)^k = \sum_{k=m}^{n} \frac{P^{(k)}(r)}{k!}(X-r)^k = (X-r)^m \sum_{k=0}^{n-m} \frac{P^{(k+m)}(r)}{(k+m)!}(X-r)^k.$$

On a donc trouvé un polynôme $Q \in \mathbb{K}[X]$ tel que $P = (X-r)^m Q$ et

$$Q(r) = \sum_{k=0}^{n-m} \frac{P^{(k+m)}(r)}{(k+m)!}(r-r)^k = \frac{P^{(m)}(r)}{m!} \neq 0.$$

□

Exemple 3.17 :
Soient $n \geq 1$ et $P_n = nX^{n+2} - (4n+1)X^{n+1} + (4n+4)X^n - 4X^{n-1}$. Déterminer la multiplicité de $m_2(P_n)$. ♢

Proposition 3.18

Soit $P \in \mathbb{K}[X] \setminus \{0\}$. Alors

$$\deg P \geq \sum_{r \in Z(P)} m_r(P).$$

Autrement dit, un polynôme de degré $n \in \mathbb{N}$ possède au plus n racines (comptées avec leur multiplicité).

Démonstration : Le résultat est évident si $Z(P) = \emptyset$. Sinon, on sait que $Z(P)$ est fini, on note donc $Z(P) = \{r_1, \dots, r_n\}$ avec $n \in \mathbb{N}^*$. Soit $k \in [\![1, n]\!]$, alors on note $m_k = m_{r_k}(P)$. On sait donc que $(X - r_k)^{m_k}$ divise P. D'autre part, les polynômes $(X-r_1)^{m_1}, \dots, (X-r_n)^{m_n}$ sont premiers entre eux donc, d'après le théorème de Gauss,

$$\left(\prod_{k=1}^{n}(X-r_k)^{m_k}\right) | P, \quad \deg P \geq \left(\prod_{k=1}^{n}(X-r_k)^{m_k}\right) = \sum_{k=1}^{n} m_{r_k}(P) = \sum_{r \in Z(P)} m_r(P).$$

□

4. Polynômes scindés, relations coefficients-racines

Définition 3.19 *Polynôme scindé*

Soit $P \in \mathbb{K}[X]$ un polynôme non-constant. On dit que P est scindé sur $\mathbb{K}$ si P possède autant de racines dans $\mathbb{K}$ (comptées avec leur multiplicité) que son degré.

Exemple 3.20 :

- Le polynôme $X^3 - X$ est scindé sur $\mathbb{R}$ et sur $\mathbb{C}$ car
$$X^3 - X = X(X-1)(X+1).$$
- Pour tout $n \in \mathbb{N}^*$, le polynôme $X^n - 1$ est scindé sur $\mathbb{C}$ car
$$X^n - 1 = \prod_{k=0}^{n-1} \left(X - \mathrm{e}^{i2k\pi/n}\right).$$
Si $n = 1$ ou 2 alors il est aussi scindé sur $\mathbb{R}$.
- X^2+1 est scindé sur $\mathbb{C}$ car $X^2+1 = (X-i)(X+i)$, mais pas sur $\mathbb{R}$. En effet, X^2+1 ne possède aucune racine réelle.

♢

D'après cet exemple, on remarquera qu'il n'est pas toujours facile de dire qu'un polynôme n'est pas scindé. En revanche, si un polynôme de $\mathbb{R}[X]$ possède des racines complexes non-réelles, alors il n'est pas scindé (sur $\mathbb{R}$). Encore une fois, on fera attention au corps $\mathbb{K}$ sur lequel on considère les polynômes.

Proposition 3.21

Soit $P \in \mathbb{K}[X]$ un polynôme non-constant. Alors on a équivalence entre :

(i) P est scindé sur $\mathbb{K}$.
(ii) Il existe $\lambda \in \mathbb{K}^*, p \in \mathbb{N}^*, m_1, \ldots, m_1, \ldots, m_p \in \mathbb{N}, r_1, \ldots, r_p \in \mathbb{K}$ tels que
$$P = \lambda \prod_{k=1}^{p} (X - r_k)^{m_k}.$$

Dans ce cas, on a alors $Z(P) = \{r_1, \ldots, r_p\}$ et
$$\forall k \in [\![1, p]\!], \quad m_{r_k}(P) = m_k.$$

Évidemment, si certains r_k sont confondus ou si certains m_k sont nuls, on peut toujours réécrire la décomposition pour supposer les r_k distincts ou les m_k strictement positifs.

Démonstration : La réciproque étant évidente, on va montrer le sens direct en supposant que P est scindé. Donc $\deg P \geq 1$ et P possède donc des racines dans $\mathbb{K}$ (distinctes) notées $r_1, \ldots, r_p$, de multiplicités respectives $m_1, \ldots, m_p$. Comme pour tout $k \in [\![1, p]\!]$, $(X - r_k)^{m_k} | P$. De plus, les $(X - r_k)$ sont deux à deux premiers entre eux donc les $(X - r_k)^{m_k}$ aussi. Donc $Q = \prod_{k=1}^{p} (X - r_k)^{m_k}$ divise Q, c'est-à-dire qu'il existe $R \in \mathbb{K}[X]$ tel que
$$P = QR, \quad \deg Q = \deg \left(\prod_{k=1}^{p} (X - r_k)^{m_k} \right) = \sum_{k=1}^{p} m_k.$$
De plus, $\deg Q = \deg P$ donc $R \in \mathbb{K}^*$. □

Proposition 3.22 *Relations coefficients-racines*

Soit $P = \sum_{k=0}^{d} a_k X^K \in \mathbb{K}[X]$ un polynôme scindé sur $\mathbb{K}$ de degré $d \in \mathbb{N}^*$ (c'est-à-dire $a_d \neq 0$). Notons $r_1, \ldots, r_d \in \mathbb{K}$ les racines de P (éventuellement confondues).

(i) Si $d = 2$ alors

$$r_1 + r_2 = -\frac{a_1}{a_2}, \quad r_1 r_2 = \frac{a_0}{a_2}.$$

(ii) Si $d = 3$ alors

$$r_1 + r_2 + r_3 = -\frac{a_2}{a_3}, \quad r_1 r_2 + r_2 r_3 + r_1 r_3 = \frac{a_1}{a_3}, \quad r_1 r_2 r_3 = -\frac{a_0}{a_3}.$$

(iii) Pour $d \geq 1$ quelconque,

$$\sum_{k=1}^{d} r_k = -\frac{a_{d-1}}{a_d}, \quad \prod_{k=1}^{d} r_k = (-1)^d \frac{a_0}{a_d}$$

Démonstration : La preuve formelle est possible par récurrence, mais ne présente qu'un intérêt limité. On retiendra simplement l'idée : si P est scindé, il existe $\lambda \in \mathbb{K}^*$ tel que

$$P = \sum_{k=1}^{n} a_k X^k = \lambda \prod_{k=1}^{d} (X - z_k).$$

On développe alors le terme de droite et en on identifie les coefficients :

$$\lambda = a_d, \quad a_{d-1} = -\lambda \sum_{k=1}^{d} r_k, \quad a_0 = \lambda \prod_{k=1}^{d} (-r_k) = (-1)^d \lambda \prod_{k=1}^{d} r_k.$$

□

On est souvent confronté à devoir montrer que deux polynômes sont égaux. Tout d'abord, cela revient à montrer que leur différence est nulle. On se concentre donc sur les méthodes pour montrer qu'un polynôme est nul.

Proposition 3.23 *Montrer qu'un polynôme est nul*

Soit $P \in \mathbb{K}[X]$. Alors on a équivalence entre les propositions suivantes :

(i) $P = 0$.
(ii) Tous les coefficients de P sont nuls.
(iii) $\deg P < 0$.
(iv) P admet strictement plus de racines (comptées avec leur multiplicité) que son degré.
(v) P admet une infinité de racines.
(vi) Il existe $a \in \mathbb{K}$ tel que, pour tout $k \in [\![0, \deg P]\!]$, $P^{(k)}(a) = 0$.

IV Factorisation en produit de polynômes irréductibles

On rappelle qu'un polynôme $P \in \mathbb{K}[X]$ est irréductible dans $\mathbb{K}[X]$ s'il est non-constant et si tous ses diviseurs sont triviaux, c'est-à-dire associés à P ou constants. On sait que les polynômes de degré 1 sont irréductibles, mais y en a-t-il d'autres ?

On rappelle également qu'on peut décomposer un polynôme $A \in \mathbb{K}[X]$ non-constant en produit de facteurs irréductibles :

$$A = \lambda \prod_{i=1}^{r} P_i^{\alpha_i},$$

et que cette décomposition est unique (à l'ordre près des facteurs P_i). Nous sommes maintenant en mesure de démontrer ce théorème, mais les questions restantes sont :

- Quels sont les polynômes irréductibles dans $\mathbb{K}[X]$?
- Comment déterminer cette factorisation en pratique ?

1. Polynômes irréductibles dans $\mathbb{C}[X]$

Dans toute cette partie, on pose $\mathbb{K} = \mathbb{C}$. Il est clair que ceci n'est pas restrictif, puisque tout polynôme à coefficients réels peut être vu comme un polynôme à coefficients complexes. Le théorème suivant est extrêmement important. Sa démonstration est difficile et est laissée en exercice (cf. TD).

Théorème 4.1 *Théorème de D'Alembert*[9]*-Gauss - Admis*
Tout polynôme non-constant admet au moins une racine dans $\mathbb{C}$.

On dit aussi que le corps $\mathbb{C}$ est algébriquement clos, ou encore que $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$ (un corps contenant les racines de tous les polynômes à coefficients réels).

Corollaire 4.2
Les polynômes irréductibles dans $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.

Démonstration : On a déjà vu qu'un polynôme du premier degré est irréductible (ses diviseurs étant de degré inférieur à 1, ils sont triviaux).

Soit P un polynôme irréductible dans $\mathbb{C}[X]$. D'après le théorème de D'Alembert-Gauss, P possède une racine $r \in \mathbb{C}$ et donc $(X - r)\,|P$. $X - r$ n'étant pas constant, il est associé à P car P est irréductible. Donc il existe $\lambda \in \mathbb{C}^*$ tel que $P = \lambda X - \lambda r$, donc $\deg P = 1$. $\square$

Corollaire 4.3
Tout polynôme non-constant est scindé sur $\mathbb{C}$.

On déduit de ce résultat que tout polynôme de degré $d \in \mathbb{N}$ admet d racines complexes (éventuellement confondues).

Démonstration : D'après la décomposition en facteurs irréductibles, et puisque les polynômes irréductibles sur $\mathbb{C}$ sont les polynômes de degré 1, il est clair que tout polynôme $P \in \mathbb{C}[X]$ non-constant s'écrit sous la forme

$$P = \lambda \prod_{i=1}^{r} (X - r_i)^{\alpha_i}, \quad r_i \in \mathbb{C}, \lambda \in \mathbb{C}^*.$$

et donc P est scindé sur $\mathbb{C}$. $\square$

2. Polynômes irréductibles dans $\mathbb{R}[X]$

Dans cette partie, on s'intéresse au cas $\mathbb{K} = \mathbb{R}$.

9. Jean-Baptiste le Rond D'Alembert (1717-1783) : Philosophe et mathématicien français.

Lemme 4.4

Soit $P \in \mathbb{R}[X]$. Alors, pour tout $z \in \mathbb{C}, m_z(P) = m_{\overline{z}}(P)$. En particulier,

$$z \in Z_{\mathbb{C}}(P) \iff \overline{z} \in Z_{\mathbb{C}}(P).$$

Démonstration : Soit $Q = \sum_{k=0}^{d} a_k X^k \in \mathbb{R}[X]$. Alors

$$Q(\overline{z}) = \sum_{k=0}^{d} a_k \overline{z}^k = \sum_{k=0}^{d} \overline{a_k}\,\overline{z^k} = \sum_{k=0}^{d} \overline{a_k z^k} = \overline{\sum_{k=0}^{d} a_k z^k} = \overline{P(z)}, \quad P(\overline{z}) = 0 \iff Q(z) = 0.$$

Donc $z \in Z_{\mathbb{C}}(P)$ si et seulement si $\overline{z} \in Z_{\mathbb{C}}(P)$. D'autre part, pour tout $k \in \mathbb{N}, P^{(k)} \in \mathbb{R}[X]$ donc

$$P^{(k)}(\overline{z}) = 0 \iff P^{(k)}(z) = 0.$$

Si $P = 0$, il est évident que $m_z(P) = +\infty = m_{\overline{z}}(P)$. Supposons donc que $P \neq 0$ et soit $m \in \mathbb{N}$. Alors

$$\begin{aligned} m_z(P) = m &\iff \begin{cases} \forall k \in [\![1, m-1]\!], P^{(k)}(z) \neq 0 \\ P^{(m)}(z) \neq 0 \end{cases} \iff \begin{cases} \forall k \in [\![1, m-1]\!], P^{(k)}(\overline{z}) \neq 0 \\ P^{(m)}(\overline{z}) \neq 0 \end{cases} \\ &\iff m_{\overline{z}}(P) = m. \end{aligned}$$

□

Théorème 4.5

Les polynômes irréductibles dans $\mathbb{R}[X]$ sont

- les polynômes de degré 1.
- les trinômes de discriminant strictement négatif.

Démonstration : Les polynômes du premier degré sont encore une fois irréductibles dans $\mathbb{R}[X]$. Soit $P \in \mathbb{R}[X]$ un trinôme dont le discriminant est strictement négatif. On sait que $\mathbb{Z}_C(P) = \{z, \overline{z}\}$ avec $z \in \mathbb{C} \setminus \mathbb{R}$ et donc $P = \operatorname{dom}(P)(X - z)(X - \overline{z})$. Par unicité de la décomposition en éléments irréductibles (dans $\mathbb{C}[X]$) il n'existe pas de polynômes $Q, R \in \mathbb{R}[X]$ tels que $QR = P$ et $\deg Q = \deg R = 1$. Donc P est irréductible.

Soit $P \in \mathbb{R}[X]$ irréductible dans $\mathbb{R}[X]$. Alors $\deg P \geq 1$, par définition. Si $\deg P = 1$, alors on a vu que P est irréductible. Supposons donc $\deg P \geq 2$. P possède au moins une racine complexe z d'après le théorème de D'Alembert-Gauss. D'autre part, P n'admet pas de racine réelle (sinon on aurait le diviseur non-trivial $X - r$, avec $r \in Z_{\mathbb{R}}(P)$). Donc $z \in \mathbb{C} \setminus \mathbb{R}$. On sait que $\overline{z}$ est aussi une racine de P, et que $\overline{z} \neq z$. Donc P est divisible par $Q = (X - z)(X - \overline{z})$. Or

$$Q = (X - z)(X - \overline{z}) = X^2 - (z + \overline{z})X + z\overline{z} = X^2 - 2\mathfrak{Re}(z)X + |z|^2,$$

donc $Q \in \mathbb{R}[X]$. Q est un polynôme non-constant donc il existe $\lambda \in \mathbb{R}^*$ tel que $P = \lambda Q$. P étant un polynôme de degré 2 admettant deux racines complexes conjuguées, son discriminant est donc strictement négatif. □

En tout cas, on retiendra le résultat suivant.

Proposition 4.6

Soit $A \in \mathbb{K}[X]$ tel que $\deg A \geq 1$. Alors :

(i) A se décompose sous la forme :

$$A = \operatorname{dom}(A) \prod_{i=1}^{p} (X - r_i)^{\alpha_i},$$

où les $r_i \in \mathbb{C}$ sont distincts.

(ii) Si $A \in \mathbb{R}[X]$ alors A se décompose sous la forme :

$$A = \operatorname{dom}(A) \prod_{i=1}^{p} (X - r_i)^{\alpha_i} \prod_{i=1}^{q} \left(X^2 + b_i X + c_i\right)^{\beta_i}, \quad (p,q) \neq (0,0),$$

où les $r_i \in \mathbb{R}, (b_i, c_i) \in \mathbb{R}^2$ sont distincts et $b_i^2 - 4c_i < 0$.

De plus, ces décompositions sont uniques, à l'ordre près des facteurs.

Exemple 4.7 :

Décomposons $P = X^6 - 1$ en facteurs irréductibles dans $\mathbb{R}[X]$. Pour cela, on commence par sa décomposition dans $\mathbb{C}[X]$. On sait que $Z_{\mathbb{C}}(P) = \{\mathrm{e}^{ik2\pi/6} / k \in [\![0,5]\!]\}$. Donc la décomposition de P en facteurs irréductibles dans $\mathbb{C}[X]$ est

$$P = \prod_{k=0}^{5} \left(X - \mathrm{e}^{ik2\pi/6}\right).$$

Pour obtenir sa décomposition en facteurs irréductibles dans $\mathbb{C}[X]$, on regroupe les racines complexes avec leurs racines conjuguées deux par deux :

$$\begin{aligned} P &= (X-1)(X+1)\left(X - \mathrm{e}^{i\pi/3}\right)\left(X - \mathrm{e}^{-i\pi/3}\right)\left(X - \mathrm{e}^{i2\pi/3}\right)\left(X - \mathrm{e}^{-i2\pi/3}\right) \\ &= (X-1)(X+1)\left(X^2 - 2\cos\left(\frac{\pi}{3}\right)X + 1\right)\left(X^2 - 2\cos\left(\frac{2\pi}{3}\right)X + 1\right) \\ &= (X-1)(X+1)\left(X^2 - X + 1\right)\left(X^2 + X + 1\right) \end{aligned}$$

Il s'agit de la décomposition en facteurs irréductibles de P sur $\mathbb{R}[X]$ car les trinômes $\left(X^2 - X + 1\right)$ et $\left(X^2 + X + 1\right)$ sont irréductibles (ils possèdent des racines complexes non-réelles). ♢

Exemple 4.8 :

Décomposons $P = iX^3 - 4iX^2 + (-2+4i)X$ en facteurs irréductibles dans $\mathbb{C}[X]$. On peut déja factoriser par iX de manière évidente, on a alors $P = iXQ$ avec $Q = X^2 - 4X + (4+2i)$. Q est un trinôme à coefficients complexes, et son discriminant vaut $\Delta = -8i$. $\Delta \neq 0$ donc Δ possède deux racines complexes distinctes : $2(1-i)$ et $-2(1-i)$. Les racines de Q sont donc $3-i$ et $1+i$. On a donc les décompositions en facteurs irréductibles :

$$Q = (X - (3-i))(X - (1+i)), \quad P = iX(X - (3-i))(X - (1+i)).$$

♢

Exercice 4.9 :

Démontrer que $X^2 - 4X - 21$ divise $P = -3X^4 + 15X^3 + 87X^2 - 207X - 756$ et en déduire la décomposition en facteurs irréductibles de P.

Réponse

Par division euclidienne on a

$$P = \left(X^2 - 4X - 21\right)\left(-3X^2 + 3X + 36\right) + 0$$

donc $\left(X^2 - 4X - 21\right) | P$. On a les factorisations suivantes :

$$X^2 - 4X - 21 = (X-7)(X+3), \quad -3X^2 + 3X - 36 = -3(X+3)(X-4).$$

Donc la décomposition de P en facteurs irréductibles est $P = -3(X+3)^2(X-4)(X-7)$ (dans $\mathbb{R}[X]$ ou dans $\mathbb{C}[X]$).

◊

Exercice 4.10 :
Décomposer $P = X^4 - X^2 - 2$ en produit de facteurs irréductibles.

Réponse

Posons $Y = X^2$. Alors $P = Y^2 - Y - 2 = (Y-2)(Y+1)$. Donc

$$P = \left(X^2 - 2\right)\left(X^2 + 1\right) = \left(X - \sqrt{2}\right)\left(X + \sqrt{2}\right)(X - i)(X + i).$$

On a donc trouvé la décomposition en facteurs irréductibles de P dans $\mathbb{C}[X]$. Sa décomposition dans $\mathbb{R}[X]$ est donc

$$P = \left(X - \sqrt{2}\right)\left(X + \sqrt{2}\right)\left(X^2 + 1\right).$$

◊

V Corps des fractions rationnelles

Dans cette partie, on s'intéresse aux fractions rationnelles, qui sont la version algébrique d'une fraction avec des termes polynomiaux au numérateur et au dénominateur. On peut aussi voir cet ensemble comme celui où l'on peut inverser les polynômes (c'est-à-dire le plus petit corps contenant $\mathbb{K}[X]$). Si l'exemple à garder en tête dans le début du chapitre était $\mathbb{Z}$, il faut maintenant comparer l'ensemble des fractions rationnelles à $\mathbb{Q}$.

On passera rapidement sur toutes les notions algébriques pour s'intéresser à la principale application des fractions rationnelles : la décomposition en éléments simples.

1. Structure de $\mathbb{K}(X)$

Définition 5.1 *Fraction rationnelle*

On appelle *fraction rationnelle* à coefficients dans $\mathbb{K}$ tout élément de la forme $F = \dfrac{A}{B}$ avec $A, B \in \mathbb{K}[X]$ et $B \neq 0$. L'ensemble des fractions rationnelles à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}(X)$.

Définition 5.2 *Représentant*

Soient $F = \frac{A}{B}, G = \frac{C}{D} \in \mathbb{K}(X)$. On identifie les deux fractions rationnelles $F = \frac{A}{B}$ et $G = \frac{C}{D}$ si, et seulement si, $AD = BC$.

On dit que $\frac{A}{B}$ est un *représentant* de F.

$\frac{A}{B}$ est appelé *représentant irréductible* si $A \wedge B = 1$.

Proposition 5.3

Toute fraction rationnelle non-nulle admet un unique représentant irréductible dont le dénominateur est unitaire.

Démonstration : Soit $F = \frac{A}{B} \in \mathbb{K}(X)$. Notons $D = \operatorname{dom}(B)(A \wedge B)$. Alors $D|A$ et $D|B$ donc il existe $\widetilde{A}, \widetilde{B} \in \mathbb{K}[X]$ tels que $A = D\widetilde{A}, B = D\widetilde{B}$. Alors $\operatorname{dom}(B) = \operatorname{dom}(D)\operatorname{dom}\left(\widetilde{B}\right) = \operatorname{dom}(B)\operatorname{dom}\left(\widetilde{B}\right)$ donc $\widetilde{B}$ est unitaire. On a déjà vu que $\widetilde{A} \wedge \widetilde{B} = 1$. De plus

$$\widetilde{A}B = \widetilde{A}D\widetilde{B} = A\widetilde{B}$$

donc F admet un représentant irréductible $\frac{\widetilde{A}}{\widetilde{B}}$ ayant un dénominateur unitaire. Supposons que $F = \frac{A}{B} = \frac{C}{D}$ avec $A, B, C, D \in \mathbb{K}[X] \setminus \{0\}$, que $A \wedge B = C \wedge D = 1$ et que $\operatorname{dom} B = \operatorname{dom} D = 1$. Alors $A|BC$ et $A \wedge B = 1$ donc, par le théorème de Gauss, $A|C$. Réciproquement, $C|A$ donc il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda C$. Donc

$$\lambda CD = BC, \quad C(\lambda D - B) = 0, \quad B = \lambda D.$$

Puisque $\operatorname{dom} B = \operatorname{dom} D = \lambda \operatorname{dom} D$, $\lambda = 1$ et donc $B = D$ et $A = C$. $\square$

Définition/Théorème 5.4 *Admis*

Pour tous $A, C \in \mathbb{K}[X], B, D \in \mathbb{K}[X] \setminus \{0\}, \lambda \in \mathbb{K}$, on définit

$$\frac{A}{B} + \frac{C}{D} = \frac{A \times D + B \times C}{BD}, \quad \frac{A}{B} \times \frac{C}{D} = \frac{A \times C}{B \times D}, \quad \lambda \cdot \frac{A}{B} = \frac{\lambda \cdot A}{B}.$$

Alors

(i) Les lois $+, \times, \cdot$ sont bien définies, c'est-à-dire ne dépendent pas du choix du représentant.
(ii) $(\mathbb{K}(X), +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.
(iii) $(\mathbb{K}(X), +, \times)$ est un corps commutatif.
(iv) $A \mapsto \frac{A}{1}$ est injectif, ce qui permet d'identifier un polynôme A à la fraction rationnelle $\frac{A}{1}$.

2. Degré, dérivation, pôles

Définition/Proposition 5.5 *Degré*

Pour toute fraction rationnelle $F = \dfrac{A}{B} \in \mathbb{K}(X)$, on définit

$$\deg(F) = \deg A - \deg B.$$

Alors

(i) deg est bien définie et prolonge l'application deg sur $\mathbb{K}[X]$.
(ii) Pour tous $F, G \in \mathbb{K}(X), \deg(FG) = \deg(F) + \deg(G)$.
(iii) Pour tous $F, G \in \mathbb{K}(X), \deg(F+G) \leq \max(\deg F, \deg G)$.
(iv) Pour tous $F \in \mathbb{K}(X)\ \lambda \in \mathbb{K}^*, \deg(\lambda F) = \deg(F)$.

Démonstration : $\boxed{(i)}$ Si $\dfrac{A}{B} = \dfrac{\widetilde{A}}{\widetilde{B}}$ alors $A\widetilde{B} = \widetilde{A}B$ et donc $\deg\left(A\widetilde{B}\right) = \deg A + \deg \widetilde{B} = \deg \widetilde{A} + \deg B = \deg\left(\widetilde{A}B\right)$. Donc $\deg A - \deg B = \deg \widetilde{A} - \deg \widetilde{B}$.

$\boxed{(ii)}$ Dans la suite, on pose $F = \dfrac{A}{B}, G = \dfrac{C}{D}$. Alors

$$\begin{aligned}\deg(FG) &= \deg \frac{AC}{BD} = \deg(AC) - \deg(BD) = \deg A - \deg B + \deg C - \deg D \\ &= \deg F + \deg G.\end{aligned}$$

$\boxed{(iii)}$ De même,

$$\begin{aligned}\deg(F+G) = \deg \frac{AD+BC}{BD} &\leq \max\left(\deg \frac{AD}{BD}, \deg \frac{BC}{BD}\right) \leq \max\left(\deg \frac{A}{B}, \deg \frac{C}{D}\right) \\ &\leq \max(\deg F, \deg G).\end{aligned}$$

$\boxed{\text{iv)}}$ Evident. □

Définition/Proposition 5.6 *Dérivation*

Pour toute fraction rationnelle $F = \dfrac{A}{B} \in \mathbb{K}(X)$, on définit la *fraction dérivée*

$$F' = \frac{A'B - AB'}{B^2}.$$

Alors

(i) $F \mapsto F'$ est bien définie et prolonge l'application "Dérivation" sur $\mathbb{K}[X]$.
(ii) Pour tous $F, G \in \mathbb{K}(X), (F+G)' = F' + G'$.
(iii) Pour tous $F, G \in \mathbb{K}(X), (FG)' = F'G + FG'$.
(iv) Pour tous $F \in \mathbb{K}(X)\ \lambda \in \mathbb{K}, (\lambda F)' = \lambda F'$.

Démonstration : On démontre simplement le point (i), le reste étant laissé en exercice (simple manipulation des définitions). Supposons que $F = \dfrac{A}{B} = \dfrac{C}{D}$ et montrons que $\left(\dfrac{A}{B}\right)' = \left(\dfrac{C}{D}\right)'$. On sait que $AD = BC$ et donc $A'D + AD' = B'C + BC'$. On calcule

$$\begin{aligned}D^2(A'B - AB') - B^2(C'D - CD') &= D^2A'B - BCDB' - B^2C'D + ADBD' \\ &= DB(A'D - CB' - BC' + AD') = 0.\end{aligned}$$

Donc $\dfrac{A'B - B'A}{B^2} = \dfrac{C'D - CD'}{D^2}$ par le critère d'égalité des fractions rationnelles. □

Définition 5.7 *Zéros et pôles*

Soit $F \in \mathbb{K}(X)$ admettant pour représentant irréductible $\dfrac{A}{B}$, avec $A, B \in \mathbb{K}[X], B \neq 0$. On appelle *zéro de F dans* $\mathbb{K}$ toute racine du polynôme A dans $\mathbb{K}$. On appelle *multiplicité du zéro* $r \in \mathbb{K}$ la multiplicité de r dans A. On appelle *pôle de F dans* $\mathbb{K}$ toute racine du polynôme B dans $\mathbb{K}$. On appelle *multiplicité du pôle* $r \in \mathbb{K}$ la multiplicité de r dans B.

Exemple 5.8 :
Soit $F = \dfrac{(X-2)^3\left(X-\sqrt{2}\right)\left(X^2+1\right)}{(X-1)(X-2)(X-3)^2}$. Un représentant irréductible de F est $\dfrac{(X-2)^2\left(X-\sqrt{2}\right)\left(X^2+1\right)}{(X-1)(X-3)^2}$ (il est clair que le numérateur et le dénominateur sont premiers entre eux d'après leur décomposition en facteurs irréductibles). Alors les zéros de F dans $\mathbb{R}$ sont 2 (de multiplicité 2), et $\sqrt{2}$ (de multiplicité 1). Les pôles de F dans $\mathbb{R}$ sont 1 (de multiplicité 1), et 3 (de multiplicité 2). ♢

3. Décomposition en éléments simples

La principale application des fractions rationnelles qui nous intéressera est la décomposition en éléments simples. En effet, cette décomposition permet d'intégrer absolument toute fraction rationnelle.

Définition 5.9 *Eléments simples*

On appelle *élément simple de* $\mathbb{K}(X)$ les fractions rationnelles suivantes :

- Les polynômes de $\mathbb{K}[X]$.
- Les éléments de $\mathbb{K}(X)$ de la forme $\dfrac{A}{B^n}$ avec $n \in \mathbb{N}^*, B \neq 0$ irréductible et $\deg A < \deg B$.

Les éléments simples de $\mathbb{C}(X)$ sont :

- Les polynômes.
- Les fractions rationnelles de la forme $\dfrac{\lambda}{(X-r)^n}$, avec $\lambda \in \mathbb{C}^*, r \in \mathbb{C}, n \in \mathbb{N}$.

Les éléments simples de $\mathbb{R}(X)$ sont :

- Les polynômes.
- Les fractions rationnelles de la forme $\dfrac{\lambda}{(X-r)^n}$, avec $\lambda \in \mathbb{R}^*, r \in \mathbb{R}, n \in \mathbb{N}$.
- Les fractions rationnelles de la forme $\dfrac{\lambda X + \mu}{(X^2+bX+c)^n}$, avec $\lambda, \mu, b, c \in \mathbb{R}, n \in \mathbb{N}$ et $b^2 - 4c < 0$.

Théorème 5.10 *Décomposition en éléments simples*

Toute fraction rationnelle se décompose de manière unique comme somme d'éléments simples.

Corollaire 5.11 *Décomposition en éléments simples complexes*

Soit $F = \dfrac{A}{B} \in \mathbb{C}(X)$, avec $B \in \mathbb{C}[X]$ unitaire admettant pour décomposition en facteurs irréductibles

$$B = \prod_{i=1}^{n} (X - r_i)^{\alpha_i}, \quad r_i \in \mathbb{C}.$$

Alors F s'écrit de manière unique sous la forme

$$F = \frac{A}{B} = Q + \sum_{i=1}^{n} \sum_{k=1}^{\alpha_i} \frac{\lambda_{i,k}}{(X - r_i)^k}$$

avec $Q \in \mathbb{C}[X]$, $\lambda_{i,k} \in \mathbb{C}$.

Corollaire 5.12 *Décomposition en éléments simples réels*

Soit $F = \dfrac{A}{B} \in \mathbb{R}(X)$, avec $B \in \mathbb{R}[X]$ unitaire admettant pour décomposition en facteurs irréductibles

$$B = \prod_{i=1}^{n} (X - r_i)^{\alpha_i} \prod_{i=1}^{m} \left(X^2 + b_i X + c_i\right)^{\beta_i}, \quad r_i, b_i, c_i \in \mathbb{R}.$$

Alors F s'écrit de manière unique sous la forme

$$F = \frac{A}{B} = Q + \sum_{i=1}^{n} \sum_{k=1}^{\alpha_i} \frac{\lambda_{i,k}}{(X - r_i)^k} + \sum_{i=1}^{m} \sum_{k=1}^{\beta_i} \frac{\mu_{i,k} X + \nu_{i,k}}{(X^2 + b_i X + c_i)^k}$$

avec $Q \in \mathbb{R}[X]$, $\lambda_{i,k}, \mu_{i,k}, \nu_{i,k} \in \mathbb{R}$.

Si $\dfrac{A}{B}$ n'est pas irréductible, c'est-à-dire si $A \wedge B \neq 1$, alors on aura trop de facteurs irréductibles dans la décomposition de B (des facteurs qu'on retrouve dans A). Cela complique inutilement les calculs, mais reste vrai.[10]

Évidemment, ces théorèmes n'ont quasiment aucun intérêt en théorie. Il convient cependant de savoir déterminer la décomposition en éléments simples de n'importe quelle fraction rationnelle $F = \dfrac{A}{B}$, à l'aide de la méthode suivante :

1. Sans plus attendre, on décompose B en facteurs irréductibles. Cela servira à l'étape 3, mais peut aussi servir avant.
2. Ensuite, on effectue la division euclidienne de A par B : on a $A = BQ + R$ avec $\deg R < \deg B$. Alors $F = Q + \dfrac{R}{B}$. Cette étape est superflue si $\deg A < \deg B$, car dans ce cas $A = R$.
3. On écrit la décomposition en éléments simples voulue, par exemple si $\mathbb{K} = \mathbb{C}$:

$$\frac{R}{B} = \sum_{i=1}^{n} \sum_{k=0}^{\alpha_i} \frac{\lambda_{i,k}}{(X - r_i)^k}.$$

   Il faut alors déterminer les coefficients $\lambda_{i,k}$.[11] Pour cela, tous les moyens sont bons :
   (a) Cas particuliers (parité, conjugaison, etc.).
   (b) Même dénominateur.

10. Heureusement, car il n'est pas toujours facile de déterminer $A \wedge B$.
11. Le cas $\mathbb{K} = \mathbb{R}$ se traite exactement de la même manière, en déterminant les coefficients $\lambda_{i,k}, \mu_{i,k}$ et $\nu_{i,k}$.

(c) Multiplication par les pôles.
(d) Equivalents.
(e) Passage du cas complexe au cas réel (uniquement lorsqu'on souhaite obtenir la décomposition en éléments simples dans $\mathbb{R}(X)$).
(f) Toute autre méthode donnant le résultat.

Exemple 5.13 :
Déterminons la décomposition en éléments simples (dans $\mathbb{R}(X)$ et dans $\mathbb{C}(X)$) de $\dfrac{A}{B} = \dfrac{5X^2+6X+16}{X^3+X^2+4X+4}$.
Tout d'abord, on remarque que

$$X^3+X^2+4X+4 = (X+1)\left(X^2+4\right) = (X+1)(X-2i)(X+2i),$$

et qu'il s'agit des décompositions en facteurs irréductibles de B dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$.

$\boxed{\text{Méthode 1 : Réduction au même dénominateur}}$ D'après le théorème, il existe $Q \in \mathbb{R}[X]$ et $a, b, c \in \mathbb{R}$ tels que

$$\begin{aligned}\frac{A}{B} &= \frac{5X^2+6X+16}{(X+1)(X^2+4)} = Q + \frac{a}{X+1} + \frac{bX+c}{X^2+4} = \frac{QB + aX^2 + 4a + bX^2 + bX + cX + c}{(X+1)(X^2+4)} \\ &= \frac{QB + (a+b)X^2 + (b+c)X + (4a+c)}{(X+1)(X^2+4)}.\end{aligned}$$

Puisque $\deg A < \deg B$, il est clair que $Q = 0$. On a alors

$$\begin{cases} a+b=5 \\ b+c=6 \\ 4a+c=16 \end{cases}, \quad \begin{cases} a=3 \\ b=2 \\ c=4 \end{cases}.$$

De même, il existe $\alpha, \beta \in \mathbb{C}$ tels que

$$\frac{2X+4}{X^2+4} = \frac{\alpha}{X-2i} + \frac{\beta}{X+2i} = \frac{(\alpha+\beta)X + 2i(\alpha-\beta)}{X^2+4}, \quad \begin{cases} \alpha = 1-i \\ \beta = 1+i \end{cases}.$$

On en déduit que

$$\frac{A}{B} = \frac{3}{X+1} + \frac{2X+4}{X^2+4} = \frac{3}{X+1} + \frac{1-i}{X-2i} + \frac{1+i}{X+2i}.$$

$\boxed{\text{Méthode 2 : Multiplication/évaluation en les pôles}}$ On commence par la décomposition complexe. On sait donc qu'il existe $\alpha, \beta, \gamma \in \mathbb{C}$ tels que

$$(*) \quad \frac{A}{B} = \frac{5X^2+6X+16}{(X+1)(X^2+4)} = \frac{\alpha}{X-2i} + \frac{\beta}{X+2i} + \frac{\gamma}{X+1}.$$

En passant au conjugué dans $(*)$, puisque $\dfrac{A}{B} \in \mathbb{R}(X)$, on a

$$\frac{A}{B} = \frac{\overline{\alpha}}{X-2i} + \frac{\overline{\beta}}{X+2i} + \frac{\overline{\gamma}}{X+1}.$$

Donc $\gamma = \overline{\gamma}$ (c'est-à-dire $\gamma \in \mathbb{R}$) et $\beta = \overline{\alpha}$. En multipliant $(*)$ par $X+1$ puis en évaluant en -1, on obtient

$$\gamma + 0 = \frac{5-6+16}{1+4} = 3.$$

De même, en multipliant $(*)$ par $X-2i$ puis en évaluant en $2i$, on obtient

$$\alpha + 0 = \frac{-20+12i+16}{(1+2i)(4i)} = \frac{-4+12i}{-8+4i} = \frac{(-4+12i)(-8-4i)}{80} = 1-i, \quad \beta = 1+i.$$

On a donc montré que

$$\frac{A}{B}=\frac{3}{X+1}+\frac{1-i}{X-2i}+\frac{1+i}{X+2i}.$$

On additionne alors les termes correspondants aux pôles conjugués entre eux (avec la même puissance) pour obtenir la décomposition dans $\mathbb{R}(X)$:

$$\frac{A}{B}=\frac{3}{X+1}+\frac{(1-i)(X+2i)+(1+i)(X-2i)}{(X-2i)(X+2i)}=\frac{3}{X+1}+\frac{2X+4}{X^2+4}.$$

$\diamondsuit$

Exercice 5.14 :
Déterminer la décomposition en éléments simples dans $\mathbb{C}(X)$ et dans $\mathbb{R}(X)$ de

$$F=\frac{2X^6+X^5-17X^3+17X^2-2X+11}{X^5-2X^3+2X^2-3X+2}.$$

Réponse

On note $A=2X^6+X^5-17X^3+17X^2-2X+11$ et $B=X^5-2X^3+2X^2-3X+2$.

1. On cherche des racines évidentes de B. On a $B(1)=B(-2)=B(i)=B(-i)=0$. Donc il existe $r\in\mathbb{R}$ tel que $B=(X-r)(X+2)(X-1)\left(X^2+1\right)$. En développant, on obtient $r=1$. Donc
$$B=(X+2)(X-1)^2(X-i)(X+i).$$
2. En faisant la division euclidienne de A par B on obtient :
$$A=BQ+R,\quad Q=2X+1,\quad R=4X^4-19X^3+21X^2-3X+9.$$
3. Alors, il existe $a,b,c,d,e,\in\mathbb{C}$ tels que
$$(*)\qquad \frac{R}{B}=\frac{4X^4-19X^3+21X^2-3X+9}{(X+2)(X-1)^2(X-i)(X+i)}=\frac{a}{X+2}+\frac{b}{X-1}+\frac{c}{(X-1)^2}+\frac{d}{X-i}+\frac{e}{X+i}.$$
   (a) Puisque $\frac{R}{B}$ est réel, il est clair que $e=\overline{d}$ et que $a,b,c\in\mathbb{R}$ en passant au conjugué dans $(*)$.
   (b) En multipliant $(*)$ par $(X+2)$ puis en évaluant en -2 on obtient $a=7$.
   (c) En multipliant par $(X-i)$ et en évaluant en i on obtient $d=2i$ et donc $e=-2i$.
   (d) En multipliant $(*)$ par $(X-1)^2$ on obtient
   $$(**)\qquad \frac{4X^4-19X^3+21X^2-3X+9}{(X+2)(X^2+1)}=c+b(X-1)+(X-1)^2\widetilde{F},$$
   avec $\widetilde{F}\in\mathbb{C}(X)$. En évaluant en 1 on obtient $c=2$.
   (e) Pour trouver b, on peut par exemple dériver $(**)$ puis en évaluer en 1, ou évaluer $(*)$ en 0. Dans tous les cas, $b=-3$.

   Donc, la décomposition en éléments simples de F dans $\mathbb{C}(X)$ est
   $$F=2X+1+\frac{7}{X+2}-\frac{3}{X-1}+\frac{2}{(X-1)^2}+\frac{2i}{X-i}-\frac{2i}{X+i}.$$
   En additionnant les éléments simples correspondant à des pôles complexes conjugués, on obtient la décomposition en éléments simples de F dans $\mathbb{R}(X)$:
   $$F=2X+1+\frac{7}{X+2}-\frac{3}{X-1}+\frac{2}{(X-1)^2}-\frac{4}{X^2+1}.$$

$\diamondsuit$

À connaître à la fin du chapitre

Arithmétique

- Employer les théorèmes importants (Bézout, Gauss, Landau) de la même manière que dans $\mathbb{Z}$.
- Manipuler une division euclidienne en pratique et en théorie.

Polynômes

- Raisonner avec le degré.
- Savoir donner la décomposition en facteurs irréductibles d'un polynôme en pratique (dans $\mathbb{C}[X]$ et/ou dans $\mathbb{R}[X]$).

Fractions rationnelles

- Donner la décomposition en éléments simples d'une fraction rationnelle en pratique.

Vrai/Faux

☐ Si $\deg P = d$ alors $\deg P' = d - 1$.
☐ Le degré de PQ' est égal au degré de $P'Q$.
☐ $(X-1)^2$ divise P si, et seulement si, $P'(1) = 0$.
☐ P ne s'annule pas sur $\mathbb{R}$ si, et seulement si, P est irréductible.
☐ Si les restes des divisions euclidiennes de P par X et $X - 1$ sont nuls, alors $X^2 - X$ divise P.
☐ Si P n'est pas constant et divise $X^{1}5 - 1$ alors les racines de P sont simples.

Pour aller plus loin

- Polynômes en plusieurs indéterminées.
- Polynômes sur un anneau commutatif quelconque.

Deuxième partie

La Énième Dimension

CHAPITRE 8

FONCTIONS – DÉRIVATION

C'est Cosinus et Exponentielle qui sont sur un bateau. Cosinus s'écrie "On dérive !". Exponentielle répond "Et alors ?".

Blague mathématique

Ce chapitre est la suite logique du cours de limite et continuité. Il est important de maîtriser ces deux concepts, qui sont sous-jacents dans tout le cours de dérivation.

Dans la suite, I est un intervalle non-trivial (non-vide et non réduit à un point) de $\mathbb{R}$.

I Dérivabilité locale

On traite d'abord le cas des fonctions à valeurs réelles, puis on verra ce qu'on peut dire pour les fonctions à valeurs complexes.

1. Nombre dérivé et tangente

Définition 1.1 *Dérivabilité*

Soit $f \in \mathcal{F}(I, \mathbb{R})$ et soit $x_0 \in I$. On dit que f *est dérivable en* x_0 si la limite suivante existe et est finie :

$$\lim_{\substack{x \to x_0 \\ x \neq x_0}} \frac{f(x) - f(x_0)}{x - x_0} \in \mathbb{R}.$$

Dans ce cas, on appelle alors *nombre dérivé de* f *en* x_0

$$f'(x_0) = \lim_{\substack{x \to x_0 \\ x \neq x_0}} \frac{f(x) - f(x_0)}{x - x_0} = \lim_{\substack{h \to 0 \\ h \neq 0}} \frac{f(x_0 + h) - f(x_0)}{h}.$$

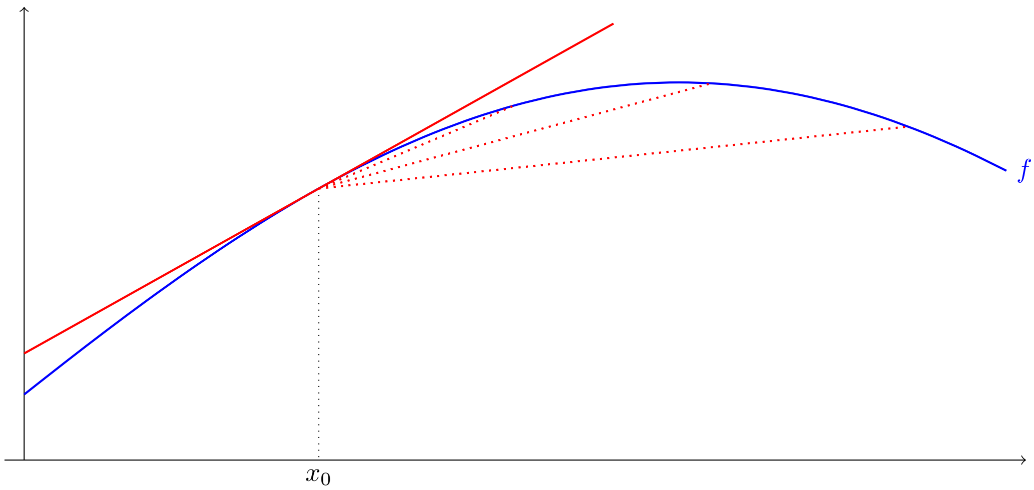
On dit que f est *dérivable sur* I si f est dérivable en tout point de I. On note $\mathcal{D}^1(I, \mathbb{R})$ l'ensemble des applications dérivables sur I à valeurs réelles.

Remarque 1.2 :

1. Si elle existe, cette limite est celle du taux d'accroissement de f entre x_0 et x lorsque x tend vers x_0. Autrement dit, $f'(x_0)$ représente la "pente" de la fonction en x_0 (voir schéma).
2. On remarquera que $f'(x_0)$ est un nombre (un élément de $\mathbb{R}$), et en aucun cas une fonction.
3. La notion de dérivabilité est *locale*, elle ne dépend que du comportement de la fonction au voisinage du point x_0.
4. S'il n'y a pas d'ambiguïté concernant l'ensemble d'arrivée, on notera simplement $f \in \mathcal{D}^1(I)$.

$\diamondsuit$

On peut faire exactement la même chose pour les fonctions à valeurs complexes, comme on le verra plus tard.



Exemple 1.3 :
Soit $n \in \mathbb{N}$. Alors la fonction $f : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^n \end{array}$ est dérivable sur $\mathbb{R}$. En effet :

- Si $n \geq 1$, soit $x_0 \in \mathbb{R}$ et soit $h \in \mathbb{R}^*$. Alors, par la formule du binôme,
$$\frac{f(x_0+h)-f(x_0)}{h} = \frac{\sum_{k=0}^{n}\binom{n}{k}x_0^k h^{n-k} - x_0^n}{h} = \sum_{k=0}^{n-1}\binom{n}{k}x_0^k h^{n-k-1}$$
$$= n x_0^{n-1} + h\sum_{k=0}^{n-2}\binom{n}{k}x_0^k h^{n-2-k}.$$
On en déduit que $\lim\limits_{\substack{h\to 0\\ h\neq 0}} \frac{f(x_0+h)-f(x_0)}{h} = n x_0^{n-1}$, donc f est dérivable en x_0 et $f'(x_0) = n x_0^{n-1}$. Donc $f \in \mathcal{D}(\mathbb{R})$.
- Si $n = 0$ alors f est constante égale à 1 et
$$\forall x_0, x \in \mathbb{R}, \quad x \neq x_0 \Rightarrow \frac{f(x)-f(x_0)}{x-x_0} = 0, \quad \lim_{\substack{x\to x_0\\ x\neq x_0}} \frac{f(x)-f(x_0)}{x-x_0} = 0.$$
Donc f est dérivable en tout $x_0 \in \mathbb{R}$ et $f'(x_0) = 0$.

$\diamondsuit$

Exemple 1.4 :
La fonction $f : \begin{array}{ccc} \mathbb{R}_+ & \to & \mathbb{R} \\ x & \mapsto & \sqrt{x} \end{array}$ n'est pas dérivable en 0. En effet,

$$\forall h > 0, \quad \frac{f(0+h)-f(0)}{h} = \frac{\sqrt{h}-0}{h} = \frac{1}{\sqrt{h}} \xrightarrow[h\to 0^+]{} +\infty,$$

donc f n'est pas dérivable en 0. $\diamondsuit$

Définition 1.5 *Nombre dérivé à droite et à gauche*

Soit $f \in \mathcal{F}(I, \mathbb{R})$ et soit $x_0 \in I$. On dit que f *est dérivable à droite, en* x_0 si la limite suivante existe et est finie :

$$\lim_{x \to x_0^+} \frac{f(x) - f(x_0)}{x - x_0} \in \mathbb{R}.$$

Dans ce cas, on appelle alors *nombre dérivé de f à droite en x_0*

$$f'_d(x_0) = \lim_{x \to x_0^+} \frac{f(x) - f(x_0)}{x - x_0} = \lim_{h \to 0^+} \frac{f(x_0 + h) - f(x_0)}{h}.$$

On définit de même, lorsqu'il existe, le *nombre dérivé de f à gauche en x_0*

$$f'_g(x_0) = \lim_{x \to x_0^-} \frac{f(x) - f(x_0)}{x - x_0} = \lim_{h \to 0^-} \frac{f(x_0 + h) - f(x_0)}{h}.$$

En particulier, on ne pourra pas parler de nombre dérivé à droite si $x_0 = \max I$ ou de nombre dérivé à gauche si $x_0 = \min I$.

Proposition 1.6

Soit $f \in \mathcal{F}(I, \mathbb{R})$ et soit $x_0 \in \mathring{I}$. Alors on a équivalence entre :

(i) f est dérivable en x_0.
(ii) f est dérivable à gauche et à droite en x_0 et $f'_g(x_0) = f'_d(x_0)$.

Dans ce cas, on a alors $f'(x_0) = f'_g(x_0) = f'_d(x_0)$.

Démonstration : C'est un résultat déjà vu dans le cours de limites : en $x_0 \in \mathring{I}$, une fonction admet une limite si et seulement si ses limites à gauche et à droite sont égales. $\square$

Exemple 1.7 :
On définit les applications

$$f: \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & |x| \end{array}, \quad g: \begin{array}{ccc} [0, +\infty[& \to & \mathbb{R} \\ x & \mapsto & |x| \end{array}.$$

La fonction f est dérivable sur $\mathbb{R}^*$ et on a

$$\forall x \in \mathbb{R}^*, \quad f'(x) = \begin{cases} 1 & \text{si } x > 0 \\ -1 & \text{si } x < 0 \end{cases}.$$

De plus, f est dérivable à gauche et à droite en 0 et

$$f'_g(0) = -1, \quad f'_d(0) = 1.$$

Par contre, $f'_g(0) \neq f'_d(0)$ donc f n'est pas dérivable en 0.

La fonction g, elle aussi, est dérivable sur $\mathbb{R}_+^*$. De plus,

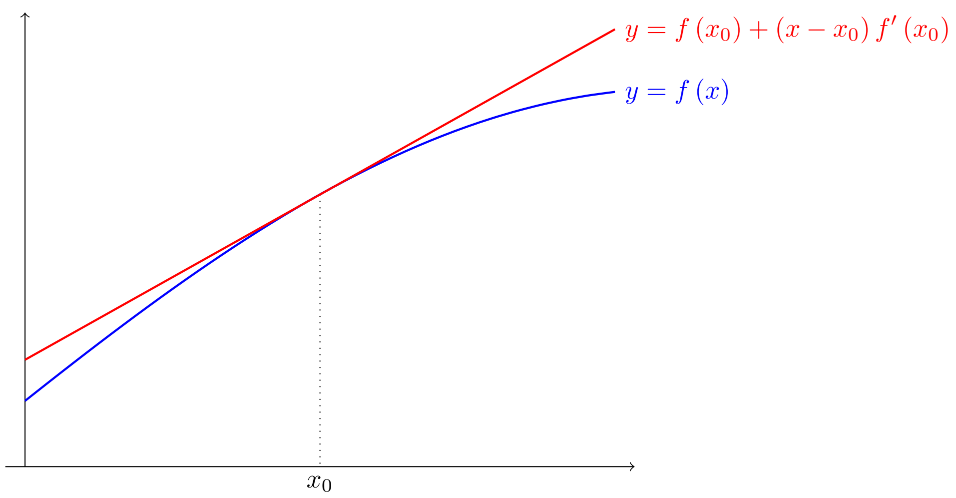
$$\lim_{\substack{h \to 0 \\ h \neq 0}} \frac{g(h) - g(0)}{h} = 1,$$

donc g est dérivable sur $\mathbb{R}_+$ et $g'(0) = 1$. ◇

Une application est la donnée de f et de son ensemble de définition.

Définition 1.8 *Tangente*
Soient $f \in \mathcal{F}(I, \mathbb{R})$ et $x_0 \in I$. On suppose que f est dérivable en x_0. On appelle alors *tangente en x_0 à la courbe représentative de f* la droite d'équation cartésienne :

$$y = f(x_0) + (x - x_0) f'(x_0).$$



La tangente en x_0 est la meilleure approximation affine de $\mathcal{C}_f$ au voisinage de x_0 : ces deux courbes passent par le point $(x_0, f(x_0))$ et le coefficient directeur de la tangente est le "taux d'accroissement local" de $\mathcal{C}_f$.

Lorsque la limite du taux d'accroissement est infinie, la fonction n'est pas dérivable, mais cela correspond quand même à une tangente verticale (cas de la fonction racine).

Définition/Proposition 1.9 *Développement limité à l'ordre 1*
Soient $f \in \mathcal{F}(I, \mathbb{R})$ et $x_0 \in I$. Alors on a équivalence entre :

(i) f est dérivable en x_0.
(ii) Il existe $\alpha, \beta \in \mathbb{R}$ tel que

$$f(x) \underset{x \to x_0}{=} \alpha + \beta(x - x_0) + o(x - x_0).$$

(iii) Il existe $\alpha, \beta \in \mathbb{R}$ tel que

$$f(x_0 + h) \underset{h \to 0}{=} \alpha + \beta h + o(h).$$

Dans ce cas, on a alors $\alpha = f(x_0)$ et $\beta = f'(x_0)$.

Les égalités (ii) et (iii) sont appelées *développement limité (DL) à l'ordre 1 de f en x_0*.

Donc f est dérivable en x_0 si, et seulement si, f admet un DL à l'ordre 1 en x_0. On verra plus tard que cette propriété est fausse pour les dérivées d'ordre plus élevé.

Démonstration : Remarquons d'abord que (ii) et (iii) sont équivalentes, par jeu de réécriture. Il reste à prouver l'équivalence avec (i).

$\boxed{(ii) \Rightarrow (i)}$ Il existe $\lambda \in \mathbb{R}$ tel que

$$f(x) \underset{x \to x_0}{=\!=} f(x_0) + \lambda (x - x_0) + o(x - x_0), \quad \frac{f(x) - f(x_0)}{x - x_0} = \lambda + o(1),$$

donc f est dérivable en x_0 et

$$f'(x_0) = \lim_{\substack{x \to x_0 \\ x \neq x_0}} \frac{f(x) - f(x_0)}{x - x_0} = \lambda.$$

$\boxed{(i) \Rightarrow (ii)}$ On suppose que f est dérivable en x_0, et on pose alors

$$\forall x \in I, \quad \varphi(x) = f(x) - f(x_0) - f'(x_0)(x - x_0).$$

Alors

$$\lim_{x \to x_0} \frac{\varphi(x)}{x - x_0} = \lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0} - f'(x_0) = 0,$$

donc $\varphi(x) \underset{x \to x_0}{=\!=} o(x - x_0)$. En notant $\lambda = f'(x_0)$, on alors vérifié le point (ii). □

Proposition 1.10

Soient $f \in \mathcal{F}(I, \mathbb{R})$ et $x_0 \in I$. Si f est dérivable en x_0 alors f est continue en x_0.

Démonstration : Si f est dérivable en x_0 alors f admet un DL à l'ordre 1 en x_0 : pour x au voisinage de x_0, on a

$$f(x) \underset{x \to x_0}{=\!=} f(x_0) + (x - x_0) f'(x_0) + o(x - x_0) \underset{x \to x_0}{=\!=} f(x_0) + O(x - x_0).$$

En particulier,

$$\lim_{x \to x_0} f(x) = \lim_{x \to x_0} f(x_0) + O(x - x_0) = f(x_0),$$

donc f est continue en x_0. □

⚠ La réciproque est évidemment fausse : on a vu que les fonctions $x \mapsto \sqrt{x}$ et $x \mapsto |x|$ sont continues mais pas dérivables en 0.

2. Règles de dérivation

Définition 1.11 *Fonction dérivée*

Soit $f \in \mathcal{F}(I, \mathbb{R})$. On appelle *fonction dérivée de f* la fonction

$$f' : \begin{array}{ccc} I & \to & \mathbb{R} \\ x & \mapsto & \lim_{\substack{h \to 0 \\ h \neq 0}} \frac{f(x+h) - f(x)}{h} \end{array}.$$

D'après ce qu'on a fait précédemment, la fonction f' n'est pas, a priori, une application. C'est-à-dire qu'il faut vérifier si elle est bien définie. De manière équivalente, cela revient à déterminer l'ensemble de dérivabilité de f.

La notation f' est réservée à la dérivée de f (quand elle existe). On ne pourra donc pas l'employer autrement, par exemple dans une phrase du type "Soient $f, f' \in \mathcal{F}(\mathbb{R}, \mathbb{R}) \dots$".

On a vu que $f'(x)$ représente le taux d'accroissement local de f en x. Il convient donc de lier le signe de f' aux variations de f.

Proposition 1.12

Soient $f, g \in \mathcal{F}(I, \mathbb{R})$, $\lambda \in \mathbb{R}$ et $x_0 \in I$. On suppose que f et g sont dérivables en x_0. Alors :

(i) $f + g$ est dérivable en x_0 et
$$(f+g)'(x_0) = f'(x_0) + g'(x_0).$$

(ii) λf est dérivable en x_0 et
$$(\lambda f)'(x_0) = \lambda f'(x_0).$$

(iii) $f \times g$ est dérivable en x_0 et
$$(f \times g)'(x_0) = f'(x_0)\, g(x_0) + f(x_0)\, g'(x_0).$$

(iv) Si $f(x_0) \neq 0$, alors $\dfrac{1}{f}$ est dérivable en x_0 et
$$\left(\frac{1}{f}\right)'(x_0) = -\frac{f'(x_0)}{f(x_0)^2}.$$

(v) Si $g(x_0) \neq 0$, alors $\dfrac{f}{g}$ est dérivable en x_0 et
$$\left(\frac{f}{g}\right)'(x_0) = \frac{f'(x_0)\, g(x_0) - f(x_0)\, g'(x_0)}{g(x_0)^2}.$$

Démonstration : (iii) Pour h au voisinage de 0, on a

$$\begin{aligned} fg(x_0+h) &= f(x_0+h)\, g(x_0+h) = (f(x_0) + hf'(x_0) + o(h))\,(g(x_0) + hg'(x_0) + o(h)) \\ &= fg(x_0) + hf'(x_0)\, g(x_0) + hf(x_0)\, g'(x_0) + h^2 f'(x_0)\, g'(x_0) + o(h) \\ &= fg(x_0) + h\,(f'(x_0)\, g(x_0) + f(x_0)\, g'(x_0)) + o(h). \end{aligned}$$

Donc fg est dérivable en x_0 et $(fg)'(x_0) = f'(x_0)\, g(x_0) + f(x_0)\, g'(x_0)$.

(iv) Supposons que $f(x_0) \neq 0$. f est dérivable donc continue en x_0. En particulier, puisque $f(x_0) \neq 0$, alors f ne s'annule pas au voisinage de x_0. On a alors, pour h au voisinage de 0

$$\frac{\left(\frac{1}{f}\right)(x_0+h) - \left(\frac{1}{f}\right)(x_0)}{h} = \frac{\frac{1}{f(x_0+h)} - \frac{1}{f(x_0)}}{h} = \frac{f(x_0) - f(x_0+h)}{hf(x_0)\, f(x_0+h)} \underset{h \to 0}{\longrightarrow} \frac{-f'(x_0)}{f(x_0)^2}.$$

Donc $\dfrac{1}{f}$ est dérivable en x_0 et $\left(\dfrac{1}{f}\right)'(x_0) = -\dfrac{f'(x_0)}{f(x_0)^2}$.

(v) Évident en remarquant que $\dfrac{f}{g} = f\varphi$ avec $\varphi = \dfrac{1}{g}$.

□

Corollaire 1.13

L'ensemble $\mathcal{D}(I,\mathbb{R})$ est un sous-espace vectoriel et un sous-anneau (commutatif) de $\mathcal{C}^0(I,\mathbb{R})$. De plus, l'application $\begin{array}{ccc} \mathcal{D}(I,\mathbb{R}) & \to & \mathcal{F}(I,\mathbb{R}) \\ f & \mapsto & f' \end{array}$ est un morphisme d'espaces vectoriels.

Proposition 1.14 *Règle de la chaîne("chain rule")*

Soient I, J deux intervalles de $\mathbb{R}$ et $f \in \mathcal{F}(I,J), g \in \mathcal{F}(J,\mathbb{R})$ et $x_0 \in I$. Si f est dérivable en x_0 et si g est dérivable en $f(x_0)$, alors $g \circ f$ est dérivable en x_0 et

$$(g \circ f)'(x_0) = f'(x_0) \times g'(f(x_0)).$$

Démonstration : Puisque f et g sont dérivables, il existe des fonctions h_1, h_2 telles que $\lim\limits_0 h_1 = \lim\limits_0 h_2 = 0$ et, pour x au voisinage de x_0 et y au voisinage de $f(x_0)$,

$$\begin{aligned} f(x) &= f(x_0) + (x - x_0)(f'(x_0) + h_1(x - x_0)), \\ g(y) &= g(f(x_0)) + (y - f(x_0))(g'(f(x_0)) + h_2(y - f(x_0))). \end{aligned}$$

Par continuité de f en x_0, $\lim\limits_{x \to x_0} f(x) = f(x_0)$, et donc

$$\begin{aligned} g(f(x)) &= g(f(x_0)) + (f(x) - f(x_0))(g'(f(x_0)) + h_2(y - f(x_0))) \\ &= g(f(x_0)) + (x - x_0)(f'(x_0) + h_1(x - x_0))(g'(f(x_0)) + h_2(y - f(x_0))) \\ &= g(f(x_0)) + (x - x_0) f'(x_0) g'(f(x_0)) + (x - x_0) h_3(x - x_0), \end{aligned}$$

avec $\lim\limits_0 h_3 = 0$. On en déduit que $g \circ f$ est dérivable en x_0 et que $(g \circ f)'(x_0) = f'(x_0) \times g'(f(x_0))$. □

Proposition 1.15

Soient I, J deux intervalles de $\mathbb{R}$ et f une bijection continue entre I et J. Soit $x_0 \in I$, et on note $y_0 = f(x_0)$. Si f est dérivable en x_0 et que $f'(x_0) \neq 0$, alors f^{-1} est dérivable en y_0 et

$$\left(f^{-1}\right)'(y_0) = \frac{1}{f'\left(f^{-1}(y_0)\right)}.$$

Démonstration : Pour y au voisinage de y_0, $y \neq y_0$, on a

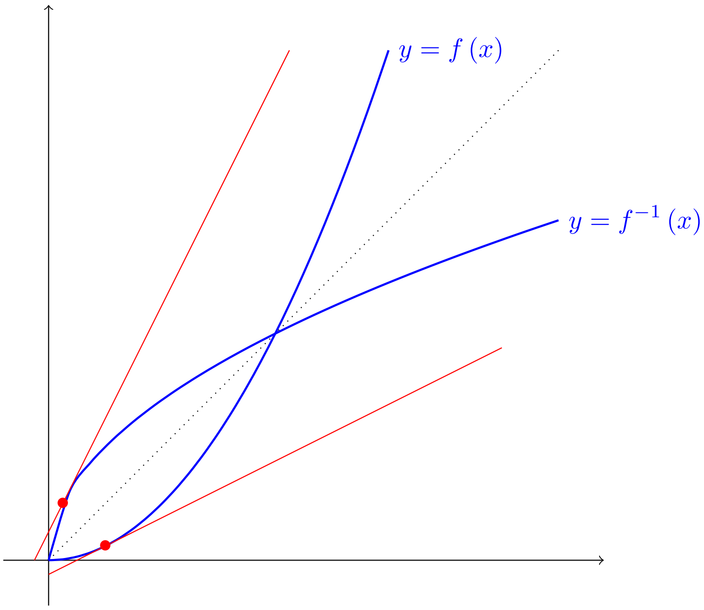
$$\frac{f^{-1}(y) - f^{-1}(y_0)}{y - y_0} = \frac{f^{-1}(y) - f^{-1}(y_0)}{f\left(f^{-1}(y)\right) - f\left(f^{-1}(y_0)\right)} = \frac{f^{-1}(y) - x_0}{f\left(f^{-1}(y)\right) - f(x_0)}.$$

Puisque f est continue sur I, alors f^{-1} est continue sur J, et en particulier en y_0. Donc $\lim\limits_{y \to y_0} f^{-1}(y) = f^{-1}(y_0)$. Et donc, puisque f est dérivable en x_0 et que $f'(x_0) \neq 0$,

$$\lim_{y \to y_0} \frac{f^{-1}(y) - f^{-1}(y_0)}{y - y_0} = \lim_{y \to y_0} \frac{f^{-1}(y) - x_0}{f\left(f^{-1}(y)\right) - f(x_0)} = \frac{1}{f'(x_0)} = \frac{1}{f'\left(f^{-1}(y_0)\right)}.$$

□

Remarque 1.16 : Les courbes représentatives de f et f' sont symétriques par rapport à la droite d'équation $y = x$. C'est pourquoi leurs tangentes respectives en x_0 et y_0, lorsqu'elles existent, sont aussi symétriques, et leurs coefficients directeurs sont inverses l'un de l'autre.



En particulier, l'une des courbes admet une tangente verticale (correspondant à une "dérivée infinie") si, et seulement si, l'autre admet une tangente horizontale (correspondant à une dérivée nulle). ♢

Pour retrouver la formule, on peut aussi simplement dériver l'égalité $f \circ f^{-1} = \mathrm{Id}$ (cela ne prouve pas que f^{-1} est dérivable).

Proposition 1.17 *Dérivées usuelles*

Les fonctions polynomiales, trigonométriques, trigonométriques hyperboliques, exp et ln sont dérivables sur leur domaine de définition. La fonction $x \mapsto \sqrt{x}$ est dérivable sur $]0, +\infty[$.

On a les formules suivantes, $a \neq 0$, et pour x convenablement choisi :

$f(x)$	x^a	e^x	$\cos x$	$\sin x$	$\tan x$	$\arccos x$	$\arcsin x$	$\arctan x$
$f'(x)$	ax^{a-1}	e^x	$-\sin x$	$\cos x$	$1 + \tan^2 x$	$-\frac{1}{\sqrt{1-x^2}}$	$\frac{1}{\sqrt{1-x^2}}$	$\frac{1}{1+x^2}$

$f(x)$	$\ln x$	$\mathrm{ch}\, x$	$\mathrm{sh}\, x$	$\mathrm{th}\, x$	$\mathrm{argch}\, x$	$\mathrm{argsh}\, x$	$\mathrm{argth}\, x$
$f'(x)$	$\frac{1}{x}$	$\mathrm{sh}\, x$	$\mathrm{ch}\, x$	$1 - \mathrm{th}^2\, x$	$\frac{1}{\sqrt{x^2-1}}$	$\frac{1}{\sqrt{1+x^2}}$	$\frac{1}{1-x^2}$

La fonction $x \mapsto x^a$ est définie sur $]0, +\infty[$, sauf si $a \in \mathbb{Z}$, auquel cas elle est définie sur sur $\mathbb{R}^*$ ou $\mathbb{R}$ (dans le cas général, penser à l'écriture exponentielle).

On remarquera (et c'est bien normal) que la dérivée des fonctions correspond à l'opérateur "dérivation" rencontré dans le chapitre sur les polynômes (et évoqué pour les fractions rationnelles). Il faut juste faire attention au domaine de dérivabilité des fonctions considérées (ici, la dérivée n'est plus un objet abstrait mais une fonction dont on doit connaître le domaine de définition).

Avant de dériver brutalement une fonction, on précisera toujours si celle-ci est dérivable en les points d'intérêt (même si c'est évident).

Exercice 1.18 :
Soit I un intervalle ouvert non-vide de $\mathbb{R}$ et soit $f \in \mathcal{D}^1(I, \mathbb{R})$.

1. Trouver une condition nécessaire et suffisante sur f et f' pour que $|f|$ soit dérivable sur I.
2. Soit $g \in \mathcal{D}^1(I, \mathbb{R})$. Trouver une condition nécessaire et suffisante sur f, f', g, g' pour que $\max(f, g)$ soit dérivable sur I.

Réponse

1. On commence par faire un dessin pour deviner la réponse, et on montre que

$$|f| \in \mathcal{D}^1(I, \mathbb{R}) \iff \forall x \in I, \Big(f(x) = 0 \Rightarrow f'(x) = 0\Big).$$

Supposons que $|f|$ soit dérivable sur I, et soit $x \in I$ tel que $f(x) = 0$. Alors, pour h au voisinage de 0,

$$\frac{|f(x+h)| - |f(x)|}{h} = \frac{|f(x+h)|}{h} = \operatorname{sgn}(h) \left| \frac{f(x+h) - f(x)}{h} \right|,$$

Donc

$$|f|'(x) = \lim_{h \to 0^-} \frac{|f(x+h)| - |f(x)|}{h} = -|f'(x)|,$$
$$|f|'(x) = \lim_{h \to 0^+} \frac{|f(x+h)| - |f(x)|}{h} = |f'(x)|.$$

On en déduit que $|f'(x)| = |f|'(x) = 0$.
Réciproquement, soit $x \in I$.
   - Si $f(x) \neq 0$, alors $f \neq 0$ au voisinage de x (par continuité). $|f|$ coïncide avec f (ou $-f$) au voisinage de x, et est donc dérivable en x.
   - Si $f(x) = 0$, alors $f'(x) = 0$, et

$$\frac{|f(x+h)| - |f(x)|}{h} = \frac{|f(x+h)|}{h} \xrightarrow[h \to 0]{} 0.$$

   Donc $|f|$ est dérivable en x, et donc sur I.
2. On a

$$\max(f+g) = \frac{f+g}{2} + \frac{|f-g|}{2}.$$

On déduit de la question précédente que

$$\max(f, g) \in \mathcal{D}^1(I, \mathbb{R}) \iff \forall x \in I, \Big(f(x) = g(x) \Rightarrow f'(x) = g'(x)\Big).$$

♢

3. Dérivées d'ordre supérieur

Définition 1.19 *Dérivée seconde*
Soit $f \in \mathcal{F}(I, \mathbb{R})$. On dit que f *est 2 fois dérivable sur* I si f est dérivable sur I et si f' est dérivable sur I.

On définit alors la *dérivée seconde de f*

$$f^{(2)}:\begin{array}{ccc} I & \to & \mathbb{R} \\ x & \mapsto & (f')'(x) \end{array}.$$

Il s'agit d'une notion locale, même si on l'écrit sur tout I par souci de simplicité ; en effet, f' doit être définie au voisinage de x_0 et donc f doit être dérivable sur tout un voisinage de x_0.

On définit alors par récurrence les dérivées d'ordre supérieur de f (lorsque c'est possible), et on note :

$$f^{(0)} = f, \quad \forall n \in \mathbb{N}, f^{(n+1)} = \left(f^{(n)}\right)'.$$

On remarquera qu'on a bien $f^{(n+1)} = \left(f^{(n)}\right)' = (f')^{(n)}$.

Définition 1.20 *Classes $\mathcal{C}^n$ et $\mathcal{D}^n$*

Soit $n \in \mathbb{N}^*$. On définit

$$\begin{aligned} \mathcal{D}^n(I,\mathbb{R}) &= \{f \in \mathcal{F}(I,\mathbb{R}) / f \text{ est } n \text{ fois dérivable sur } I\}, \\ \mathcal{C}^n(I,\mathbb{R}) &= \{f \in \mathcal{D}^n(I,\mathbb{R}) / f^{(n)} \text{ est continue sur } I\} \\ \mathcal{C}^\infty(I,\mathbb{R}) &= \bigcap_{n=0}^{+\infty} \mathcal{C}^n(I,\mathbb{R}) = \{f \in \mathcal{F}(I,\mathbb{R}) / \forall n \in \mathbb{N}, f \in \mathcal{C}^n(I,\mathbb{R})\}. \end{aligned}$$

Ces notations sont bien consistantes avec les notations $\mathcal{C}^0(I), \mathcal{D}^1(I), \mathcal{D}^2(I)$ rencontrées auparavant (on ne précisera pas l'ensemble d'arrivée lorsqu'il n'y a pas d'ambiguïté).

A noter :

$$\mathcal{C}^0(I) \supseteq \mathcal{D}^1(I) \supseteq \mathcal{C}^1(I) \supseteq \mathcal{D}^2(I) \supseteq \cdots \supseteq \mathcal{D}^n(I) \supseteq \mathcal{C}^n(I) \supseteq \cdots \supseteq \mathcal{C}^\infty(I).$$

On parle de "régularité" des fonctions, et on pourra qualifier une fonction $\mathcal{C}^\infty$ de "régulière" (terme non-mathématique, mais assez parlant).

Exemple 1.21 :
Les fonctions polynomiales, exp et ln sont de classe $\mathcal{C}^\infty$ sur leurs ensembles de définition respectifs. ♢

Exemple 1.22 :
On définit la fonction $f:\begin{array}{ccc} \mathbb{R}^* & \to & \mathbb{R} \\ x & \mapsto & x^2 \sin\left(\frac{1}{x}\right) \end{array}$. D'abord, remarquons que $\lim\limits_0 f = 0$ car sin est bornée, et donc on peut prolonger par continuité la fonction f en

$$\forall x \in \mathbb{R}, \quad \widetilde{f}(x) = \begin{cases} x^2 \sin \frac{1}{x} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases}.$$

Ensuite, par composition de fonctions dérivables, $\widetilde{f}$ est évidemment dérivable sur $\mathbb{R}^*$ et

$$\forall x \in \mathbb{R}^*, \quad \widetilde{f}'(x) = 2x \sin \frac{1}{x} - \cos \frac{1}{x}.$$

On remarque que

$$\lim_{x \to 0} \frac{\widetilde{f}(x)}{x} = \lim_{x \to 0}\left(x \sin \frac{1}{x}\right) = 0, \quad \widetilde{f}(x) \underset{x \to 0}{=} o(x).$$

Autrement dit, $\widetilde{f}$ admet un DL d'ordre 1 en 0 :

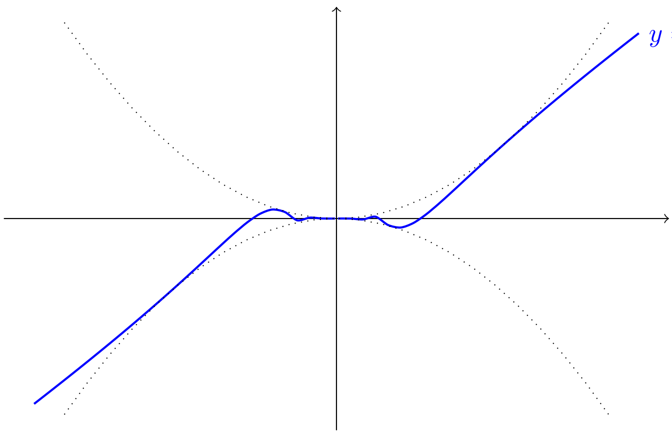
$$\widetilde{f}(x) = 0 + x \times 0 + o(x),$$

ce qui prouve que $\widetilde{f}$ est dérivable en 0, et que $\widetilde{f}'(0) = 0$. Ainsi, $\widetilde{f} \in \mathcal{D}^1(\mathbb{R})$.

Enfin,

$$\lim_{x\to 0}\left(2x\sin\frac{1}{x}\right) = 0, \quad \lim_{x\to 0}\cos\frac{1}{x} \text{ n'existe pas,}$$

donc $\widetilde{f}'$ n'admet pas de limite en 0. Autrement dit, $\widetilde{f}'$ n'est pas continue en 0.



◇

Remarque 1.23 : L'exemple 1.22 fournit un exemple très important de fonction dérivable mais pas $\mathcal{C}^1$. On a donc montré que $\mathcal{C}^1(\mathbb{R}) \subsetneq \mathcal{D}^1(\mathbb{R})$. De même, en considérant les fonctions de la forme $x \mapsto x^p \sin\left(\frac{1}{x}\right)$, on peut montrer que toutes les inclusions $\mathcal{C}^n(\mathbb{R}) \subseteq \mathcal{D}^n(\mathbb{R})$ et $\mathcal{D}^{n+1}(\mathbb{R}) \subseteq \mathcal{C}^n(\mathbb{R})$ sont strictes. ◇

Proposition 1.24

Pour tout $n \in \mathbb{N}^*$, les classes $\mathcal{C}^n, \mathcal{D}^n$ et $\mathcal{C}^\infty$ sont stables par combinaison linéaire, par produit, par inverse et par composition (lorsque ces opérations sont bien définies).

Proposition 1.25 *Formule de Leibniz*[1]

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

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

Démonstration : On démontre cette formule par récurrence sur $n \in \mathbb{N}$.

Initialisation Il est clair que $(fg)^{(0)} = fg = f^{(0)}g^{(0)} = \sum_{k=0}^{0} \binom{0}{k} f^{(k)} g^{(0-k)}$.

1. Gottfried Wilhelm Leibniz (1646-1716) : Philosophe, juriste et scientifique allemand.

Hérédité Soit $n \in \mathbb{N}$ et supposons que $(fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n-k)}$. Alors

$$\begin{aligned}
(fg)^{(n+1)} &= \left(\sum_{k=0}^{n} \binom{n}{k} f^{(k)} \times g^{(n-k)}\right)' = \sum_{k=0}^{n} \binom{n}{k} \left(f^{(k)} g^{(n-k)}\right)' \\
&= \sum_{k=0}^{n} \binom{n}{k} \left(f^{(k+1)} g^{(n-k)} + f^{(k)} g^{(n+1-k)}\right) \\
&= \sum_{k=0}^{n} \binom{n}{k} f^{(k+1)} g^{(n-k)} + \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n+1-k)} \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} f^{(k)} g^{(n+1-k)} + \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n+1-k)} \\
&= f^{(n+1)} g^{(0)} + \sum_{k=0}^{n} \left[\binom{n}{k} + \binom{n}{k-1}\right] f^{(k)} g^{(n+1-k)} + f^{(0)} g^{(n+1)} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} f^{(k)} g^{(n+1-k)},
\end{aligned}$$

ce qui achève l'hérédité. □

Exemple 1.26 :
On pose $f : x \mapsto \left(2x^2 - 4x + 1\right) \mathrm{e}^{2x}$. On note

$$g : x \mapsto 2x^2 - 4x + 1, \quad h : x \mapsto \mathrm{e}^{2x}.$$

Tout d'abord, g et h, et donc f, sont de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$. On va calculer les dérivées successives de f avec la formule de Leibniz. Pour tout $n \geq 2$, et pour tout $x \in \mathbb{R}$,

$$\begin{aligned}
f^{(n)}(x) &= \sum_{k=0}^{n} \binom{n}{k} g^{(k)}(x)\, h^{(n-k)}(x) = \sum_{k=0}^{2} \binom{n}{k} g^{(k)}(x)\, h^{(n-k)}(x) \\
&= 2^n \left(2x^2 - 4x + 1\right) \mathrm{e}^{2x} + 2^{n-1} n (4x - 4) \mathrm{e}^{2x} + \frac{n(n-1)}{2} 2^{n-2} 4\, \mathrm{e}^{2x} \\
&= \left[2^n \left(2x^2 - 4x + 1\right) + 2^{n+1} n (x-1) + n(n-1) 2^{n-1}\right] \mathrm{e}^{2x} \\
&= \left[2^n x^2 + (n-2) 2^{n+1} x + 2^{n-1} \left(n^2 - 5n + 2\right)\right] \mathrm{e}^{2x}.
\end{aligned}$$

On remarque que la formule précédente reste vraie si $n = 0$ ou $n = 1$ (pas besoin de refaire les calculs, les termes de rangs 1 et 2 de la somme s'annule lorsqu'il le faut). ◇

Proposition 1.27

Soient I, J deux intervalles de $\mathbb{R}$ et f une bijection entre I et J. Supposons que $f \in \mathcal{D}^n(I, J)$ (resp. $f \in \mathcal{C}^n(I, J)$, resp. $f \in \mathcal{C}^\infty(I, J)$) et que f' ne s'annule pas sur I. Alors $f^{-1} \in \mathcal{D}^n(J, I)$ (resp. $f^{-1} \in \mathcal{C}^n(J, I)$, resp. $f^{-1} \in \mathcal{C}^\infty(J, I)$).

Démonstration : Supposons que, pour tout $x \in I$, $f'(x) \neq 0$. On démontre par récurrence que, pour tout $n \in \mathbb{N}$, si $f \in \mathcal{C}^n(I)$ alors $f^{-1} \in \mathcal{C}^n(J)$.

Initialisation Si $f \in \mathcal{C}^1(I)$ alors, puisque f' ne s'annule pas sur I, on sait que f^{-1} est dérivable (donc continue) sur I et que et $\left(f^{-1}\right)' = \dfrac{1}{f' \circ f^{-1}}$. Par composition de fonctions continues, $\left(f^{-1}\right)'$ est donc continue sur I.

$\boxed{\text{Hérédité}}$ Soit $n \in \mathbb{N}$ et supposons que

$$f \in \mathcal{C}^n(I) \Longrightarrow f^{-1} \in \mathcal{C}^n(J).$$

On suppose que $f \in \mathcal{C}^{n+1}(I)$. Par hypothèse de récurrence, $f^{-1} \in \mathcal{C}^n(J)$. D'autre part, $\left(f^{-1}\right)' = \dfrac{1}{f' \circ f^{-1}}$ et, par composition de fonctions de classe $\mathcal{C}^n$, la fonction $\left(f^{-1}\right)'$ est donc de classe $\mathcal{C}^n$ sur J. On en déduit que $f^{-1} \in \mathcal{C}^{n+1}(J)$, ce qui achève l'hérédité.

On démontre de la même manière le résultat pour la classe $\mathcal{D}^n$. Le résultat pour la classe $\mathcal{C}^\infty$ est alors évident par définition. □

Définition 1.28 *Difféomorphisme*

Soit $f \in \mathcal{F}(I,\mathbb{R})$, soit $p \in \mathbb{N}$ et soit J un intervalle de $\mathbb{R}$. On dit que f *est un $\mathcal{C}^p$-difféomorphisme de I vers J* si f est une bijection de I sur J et f et f^{-1} sont de classe $\mathcal{C}^p$.

4. Cas d'une fonction à valeurs complexes

Tout ce qu'on a vu dans cette première section reste rigoureusement vrai pour les fonctions à valeurs complexes (tant que la variable est réelle), ce qui exclut donc les résultats sur les bijections réciproques.

Proposition 1.29

Soient $f \in \mathcal{F}(I,\mathbb{C})$ et $x_0 \in I$. Alors on a équivalence entre :

(i) f est dérivable en x_0.
(ii) $\mathfrak{Re}\, f$ et $\mathfrak{Im}\, f$ sont dérivables en x_0.
(iii) $\overline{f}$ est dérivable en x_0.

Dans ce cas, on a alors

$$(\mathfrak{Re}\, f)' = \mathfrak{Re}\,(f'), \quad (\mathfrak{Im}\, f)' = \mathfrak{Im}\,(f'), \quad \left(\overline{f}\right)' = \overline{f'}.$$

Aucune difficulté, c'est un simple résultat sur les limites de fonctions complexes.

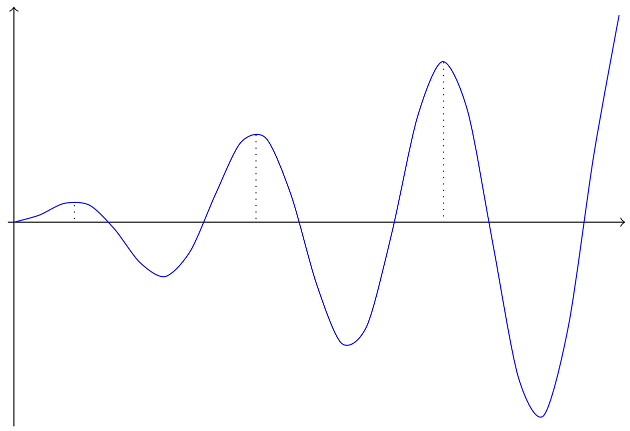
Exemple 1.30 :
La fonction $\varphi : x \mapsto \mathrm{e}^{ix}$ est dérivable sur $\mathbb{R}$ et $\varphi' : x \mapsto i\,\mathrm{e}^{ix}$. ♢

II Dérivée globale

Puisque cette section traite d'extrema et de variations de fonctions, il est assez clair que l'on ne va parler que de fonctions réelles. Pour cause, la plupart des résultats énoncés ici sont faux pour les fonctions à valeurs complexes, à l'exception de l'inégalité des accroissements finis.

1. Extrema locaux et points critiques

On rappelle qu'un extremum local est un point ou une fonction admet un maximum ou un minimum local. Une fonction f admet un maximum local en x_0 si $f \leq f(x_0)$ au voisinage de x_0.



Définition 2.1 *Point critique*

Soient $f \in \mathcal{F}(I, \mathbb{R})$ et $x_0 \in I$. On dit que x_0 est un point critique de f si f est dérivable en x_0 et si $f'(x_0) = 0$.

Proposition 2.2

Soit $f \in \mathcal{F}(I, \mathbb{R})$ et $x_0 \in \mathring{I}$. Supposons que f admette un extremum local en x_0 et que f soit dérivable en x_0. Alors $f'(x_0) = 0$.

Autrement dit, si une fonction admet un extremum local en un point à l'intérieur de I, alors celui-ci est un point critique.

Démonstration : Quitte à considérer $-f$, on peut supposer que x_0 est un maximum local. Autrement dit, il existe $\alpha > 0$ tel que

$$\forall h \in [-\alpha, \alpha], \quad f(x_0 + h) \leq f(x_0).$$

f est dérivable en x_0, et donc $f'_g(x_0) = f'(x_0) = f'_d(x_0)$. On a alors

$$\forall h \in [-\alpha, 0[, \quad \frac{f(x_0 + h) - f(x_0)}{h} \geq 0, \quad f'_g(x_0) = \lim_{h \to 0^-} \frac{f(x_0 + h) - f(x_0)}{h} \geq 0.$$

De même,

$$\forall h \in]0, \alpha], \quad \frac{f(x_0 + h) - f(x_0)}{h} \leq 0, \quad f'_d(x_0) = \lim_{h \to 0^+} \frac{f(x_0 + h) - f(x_0)}{h} \leq 0.$$

Donc $f'(x_0) = 0$. □

Ce résultat est faux si x_0 est une borne de I (on a contre-exemple avec n'importe quelle fonction strictement monotone sur un segment).

La réciproque est fausse également. En effet, 0 est un point critique pour la fonction $x \mapsto x^3$, mais cette fonction est strictement croissante au voisinage de 0 (il n'est donc pas un extremum local).

En pratique, pour trouver les extrema locaux d'une fonction, on commencera par trouver les points critiques (et on étudiera alors précisément chacun d'entre eux).

Théorème 2.3 *Théorème de Rolle*[2]

Soient $a, b \in \mathbb{R}$ tels que $a < b$, et soit $f \in \mathcal{F}([a,b], \mathbb{R})$. On suppose que f est continue sur $[a,b]$, dérivable sur $]a,b[$ et que $f(a) = f(b)$. Alors il existe $c \in]a,b[$ tel que $f'(c) = 0$.

Démonstration : La fonction f est continue sur le segment $[a,b]$, elle est donc bornée et atteint ses bornes. Il existe donc $m, M \in \mathbb{R}$ et $c_1, c_2 \in [a,b]$ tels que $m = \min\limits_{[a,b]} f = f(c_1)$ et $M = \max\limits_{[a,b]} f = f(c_2)$.

Si $m = M$, alors f est constante sur $[a,b]$ et donc le théorème est vrai avec $c = \dfrac{a+b}{2}$.

Si $m < M$, et puisque $f(a) = f(b)$, on a forcément $c_1 \in]a,b[$ (on pose alors $c = c_1$) ou $c_2 \in]a,b[$ (on pose alors $c = c_2$). Dans tous les cas, $c \in]a,b[$ et c est un extremum local de f. De plus, f est dérivable en c, c est un point critique de f, et donc $f'(c) = 0$. □

Exercice 2.4 :
Soit $P \in \mathbb{R}[X]$ un polynôme de degré $n \geq 2$ possédant n racines distinctes $r_1, \ldots, r_n$.

1. Montrer que $P - P'$ possède $n-1$ racines réelles distinctes.
2. Montrer que toutes les racines de $P - P'$ sont réelles.

Réponse

1. On définit la fonction $f : x \mapsto P(x)\,\mathrm{e}^{-x}$. f est dérivable sur $\mathbb{R}$, comme produit de deux fonctions dérivables. De plus,
$$\forall x \in \mathbb{R}, \quad f'(x) = P'(x)\,\mathrm{e}^{-x} - P(x)\,\mathrm{e}^{-x} = -[P(x) - P'(x)]\,\mathrm{e}^{-x}.$$
Enfin, pour tout $i \in [\![1, n-1]\!]$, on a $f(r_i) = 0 = f(r_{i+1})$, donc d'après le théorème de Rolle, il existe $c_i \in]r_i, r_{i+1}[$ tel que $f'(c_i) = 0$. Donc $(P - P')(c_i) = 0$. Il existe donc des nombres réels distincts $c_1, \ldots c_{n-1}$ tels que $(P-P')(c_1) = \cdots = (P-P')(c_{n-1})\,0$. Autrement dit, $P - P'$ possède $n-1$ racines réelles distinctes.
2. $P - P'$ est de degré n (car $\deg P = n$ et $\deg P' = n-1$) et $P - P'$ possède $n-1$ racines réelles distinctes, donc il existe $c_n \in \mathbb{C}$ tel que
$$Z(P - P') = \{c_1, \ldots c_{n-1}, c_n\}.$$
Supposons, par l'absurde, que $c_n \in \mathbb{C} \setminus \mathbb{R}$. Puisque $P - P' \in \mathbb{R}[X]$, alors $\overline{c}_n \in Z(P - P')$. Or $c_1, \ldots, c_{n-1} \in \mathbb{R}$ et $\overline{c}_n \notin \mathbb{R}$ donc $\overline{c}_n = c_n$, ce qui est impossible. Donc $c_n \in \mathbb{R}$. Toutes les racines de $P - P'$ sont donc réelles.

◇

Proposition 2.5 *Règle de L'Hôpital*[3]

Soient $x_0 \in \overline{I}$ et $f, g \in \mathcal{D}^1(I \setminus \{x_0\}, \mathbb{R})$. On suppose que $\lim\limits_{x_0} f = \lim\limits_{x_0} g = 0$ ou $\pm\infty$. S'il existe $\ell \in \overline{\mathbb{R}}$ tel que
$$\lim_{x \to x_0} \frac{f'(x)}{g'(x)} = \ell,$$

2. Michel Rolle (1652-1719) : Mathématicien français.

alors

$$\lim_{x \to x_0} \frac{f(x)}{g(x)} = \ell.$$

Cette règle permet de lever certaines formes indéterminées de la forme $\frac{0}{0}$ ou $\frac{\pm\infty}{\pm\infty}$.

2. Théorème et inégalité des accroissements finis

Théorème 2.6 *Théorème des accroissements finis*

Soient $a, b \in \mathbb{R}$ tels que $a < b$, et soit $f \in \mathcal{F}([a,b], \mathbb{R})$. On suppose que f est continue sur $[a,b]$ et dérivable sur $]a,b[$. Alors il existe $c \in]a,b[$ tel que $f'(c) = \dfrac{f(b) - f(a)}{b - a}$.

Démonstration : Cette méthode est classique : on veut appliquer le théorème de Rolle à une fonction bien choisie g. Pour cela, on remarque que

$$f'(c) = \frac{f(b) - f(a)}{b - a} \iff f'(c) - \frac{f(b) - f(a)}{b - a} = 0.$$

On cherche donc g une primitive de $c \mapsto f'(c) - \dfrac{f(b) - f(a)}{b - a}$. On pose donc

$$g : x \mapsto f(x) - \frac{f(b) - f(a)}{b - a} x.$$

On a alors

$$g(a) = f(a) - \frac{a[f(b) - f(a)]}{b - a} = \frac{(b-a) f(a) - a[f(b) - f(a)]}{b - a} = \frac{bf(a) - af(b)}{b - a},$$
$$g(b) = f(b) - \frac{b[f(b) - f(a)]}{b - a} = \frac{(b-a) f(b) - b[f(b) - f(a)]}{b - a} = \frac{bf(a) - af(b)}{b - a} = g(a),$$

De plus, g est continue sur $[a,b]$ et dérivable sur $]a,b[$. D'après le théorème de Rolle, il existe $c \in]a,b[$ tel que

$$g'(c) = f'(c) - \frac{f(b) - f(a)}{b - a} = 0, \quad f'(c) = \frac{f(b) - f(a)}{b - a}.$$

□

Le théorème des accroissements finis généralise le théorème de Rolle lorsque $f(a) \neq f(b)$. On remarquera que ces deux théorèmes donnent un résultat d'existence ("il existe c tel que...") mais ne permettent pas de trouver le point d'intérêt en pratique.

Corollaire 2.7 *Inégalité des accroissements finis*

Soient $a, b \in \mathbb{R}$ tels que $a < b$, et soit $f \in \mathcal{F}([a,b], \mathbb{R})$. On suppose que f est continue sur $[a,b]$ et dérivable sur $]a,b[$. S'il existe $M > 0$ tel que, pour tout $x \in]a,b[, |f'(x)| \leq M$, alors

$$|f(b) - f(a)| \leq M|b - a|.$$

3. Guillaume François Antoine de L'Hôpital (1661-1704) : mathématicien français.

Démonstration : D'après le théorème des accroissements finis, il existe $c \in]a, b[$ tel que

$$f'(c) = \frac{f(b) - f(a)}{b - a}, \quad \frac{|f(b) - f(a)|}{|b - a|} = |f'(c)| \leq M.$$

□

Le résultat est faux si f' est simplement majorée ; on n'oubliera donc pas la valeur absolue !

Par définition, les propriétés du taux d'accroissement sont transmises à la dérivée (il s'agit en effet d'une limite). Le théorème et l'inégalité des accroissements finis fournissent une sorte de réciproque à cette proposition : avoir des informations concernant f' sur $]a, b[$ permet d'obtenir des informations sur le taux d'accroissement de f entre a et b.

Exemple 2.8 :
La fonction sin est dérivable sur $\mathbb{R}$, et $\sin' = \cos$ qui est bornée par 1. Soit $x \in \mathbb{R}$. On a alors, d'après l'inégalité des accroissements finis sur $[0, x]$,

$$|\sin x - \sin 0| \leq |x - 0| \times \sup_{[0,x]} |\cos| = |x|, \quad |\sin x| \leq |x|.$$

♢

Corollaire 2.9

Soient $a, b \in \mathbb{R}$ tels que $a < b$, et soit $f \in \mathcal{C}^1([a, b], \mathbb{R})$. Alors f est lipschitzienne sur $[a, b]$.

Démonstration : f est $\mathcal{C}^1$ sur $[a, b]$ donc f' existe et est continue sur le segment $[a, b]$. On en déduit que f' est bornée (et atteint ses bornes) sur $[a, b]$. D'après l'inégalité des accroissements finis, pour tous $x, y \in [a, b]$,

$$|f(x) - f(y)| \leq |x - y| \times \sup_{]x,y[} |f'| \leq |x - y| \times \sup_{[a,b]} |f'|.$$

Par définition, f est donc lipschitzienne sur $[a, b]$, de constante de Lipschitz $\sup_{[a,b]} |f'|$. □

Exemple 2.10 :
Soit (u_n) la suite définie par

$$u_0 \in \mathbb{R}, \quad u_{n+1} = \frac{u_n + \cos\left(\frac{u_n}{2}\right)}{2}.$$

Étudier la convergence de la suite (u_n).

Réponse

On pose, pour tout $x \in \mathbb{R}$,

$$f(x) = \frac{x + \cos\frac{x}{2}}{2}, \quad g(x) = f(x) - x = \frac{\cos\frac{x}{2} - x}{2}.$$

Les fonctions f et g sont de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$, comme combinaisons linéaires de fonctions régulières. On a, pour tout $x \in \mathbb{R}$,

$$|f'(x)| = \left|\frac{1}{2} - \frac{1}{4}\sin\frac{x}{2}\right| \leq \frac{1}{2} + \frac{1}{4}\left|\sin\frac{x}{2}\right| \leq \frac{3}{4},$$
$$g'(x) = -\frac{1}{2} - \frac{1}{4}\sin\frac{x}{2} < 0.$$

D'une part, on sait que $\lim\limits_{-\infty} g = +\infty$ et $\lim\limits_{+\infty} g = -\infty$ et g est continue sur $\mathbb{R}$, donc d'après le théorème des valeurs intermédiaires (à rédiger proprement), il existe $\ell \in \mathbb{R}$ tel que $g(\ell) = 0$, c'est-à-dire $f(\ell) = \ell$. De plus, g' étant strictement négative, la fonction g est strictement décroissante sur $\mathbb{R}$ donc injective, donc

$$\exists! \ell \in \mathbb{R}, \quad f(\ell) = \ell.$$

D'autre part, d'après l'inégalité des accroissements finis,

$$\forall n \in \mathbb{N}, \quad |u_{n+1} - \ell| = |f(u_n) - f(\ell)| \leq \frac{3}{4}|u_n - \ell|.$$

Par une récurrence immédiate, on en déduit que

$$|u_n - \ell| \leq \left(\frac{3}{4}\right)^n |u_0 - \ell| \xrightarrow[n \to +\infty]{} 0,$$

donc $\lim\limits_{n \to +\infty} u_n = \ell$.

$\diamondsuit$

Exemple 2.11 :
Soit (u_n) la suite définie par

$$u_0 \in [0, 1], \quad u_{n+1} = \frac{1}{1 + u_n^2}.$$

Étudier la convergence de la suite (u_n). $\diamondsuit$

Toute cette partie devrait vous rappeler le cours sur les suites définies par récurrence et leurs points fixes, vu dans le chapitre de limite et continuité.

Remarque 2.12 : On pourra noter que l'inégalité des accroissements finis est vraie dans le cas d'une fonction à valeurs complexes. En revanche, le théorème de Rolle (et le théorème des accroissements finis, qui le généralise) sont faux : prendre l'exemple de $x \mapsto \mathrm{e}^{ix}$ sur $[0, 2\pi]$. $\diamondsuit$

3. Signe de la dérivée et variations

Proposition 2.13

Soit $f \in \mathcal{D}^1(I, \mathbb{R})$. Alors :

(i) f est croissante (resp. décroissante) sur I si, et seulement si

$$\forall x \in I, f'(x) \geq 0 \quad (\text{resp. } \forall x \in I, f'(x) \leq 0).$$

(ii) f est constante sur I si, et seulement si, pour tout $x \in I$, $f'(x) = 0$.

(iii) Si f' est positive (resp. négative) sur I et si f' s'annule seulement en un nombre fini de points, alors f est strictement croissante (resp. strictement décroissante) sur I.

Démonstration : Quitte à considérer $-f$, on ne démontre que les propriétés pour les fonctions croissantes.

(i) $\boxed{\Rightarrow}$ Si f est croissante, alors pour tout $x_0 \in I$, f est dérivable en x_0 et

$$\forall x \in I, \quad \frac{f(x) - f(x_0)}{x - x_0} \geq 0,$$

donc en passant à la limite, $f'(x_0) \geq 0$.
$\boxed{\Leftarrow}$ Soient $x, y \in I, x < y$. Alors d'après le théorème des accroissements finis, il existe $c \in]x, y[$ tel que

$$f'(c) = \frac{f(y) - f(x)}{y - x} \geq 0.$$

Or $y - x > 0$ donc $f(y) - f(x) \geq 0$, ce qui entraîne que f est croissante sur I.

(ii) D'après (i), on a

$$f \text{ constante} \iff f \text{ croissante et décroissante} \iff \begin{cases} \forall x \in I, & f'(x) \geq 0 \\ \forall x \in I, & f'(x) \leq 0 \end{cases} \iff \forall x \in I, \quad f'(x) = 0.$$

(iii) Puisque f' est positive, alors f est croissante sur I. Supposons, par l'absurde, que f ne soit pas strictement croissante sur I, c'est-à-dire qu'il existe $x, y \in I, x < y$ tels que $f(x) = f(y)$. Alors f est constante sur $[x, y]$ et donc $f' = 0$ sur $[x, y]$, qui est un ensemble infini), ce qui est impossible car f' ne s'annule qu'en un nombre fini de points.

□

Remarque 2.14 : Le point (iii) n'est qu'une condition suffisante pour qu'une fonction soit strictement positive ; c'est la condition qui sert en pratique. f pourrait aussi s'annuler en un nombre dénombrable de points, par exemple $x \mapsto x - \sin x$. ♢

Exercice 2.15 :
Déterminer les extrema locaux et globaux de la fonction

$$f : x \mapsto \left(x^4 - 4x^3 + 11x^2 - 22x + 22\right) \mathrm{e}^x .$$

Réponse

Puisque la fonction f est dérivable sur $\mathbb{R}$, les extrema locaux de f sont solutions de l'équation $f'(x) = 0$. On a, pour tout $x \in \mathbb{R}$,

$$f'(x) = \left(x^4 - 4x^3 + 11x^2 - 22x + 22 + 4x^3 - 12x^2 + 22x - 22\right) \mathrm{e}^x = \left(x^4 - x^2\right) \mathrm{e}^x .$$

Donc

$$f'(x) = 0 \iff x^4 - x^2 = 0 \iff x^2\left(x^2 - 1\right) = 0 \iff x = 0 \text{ ou } x = 1 \text{ ou } x = -1.$$

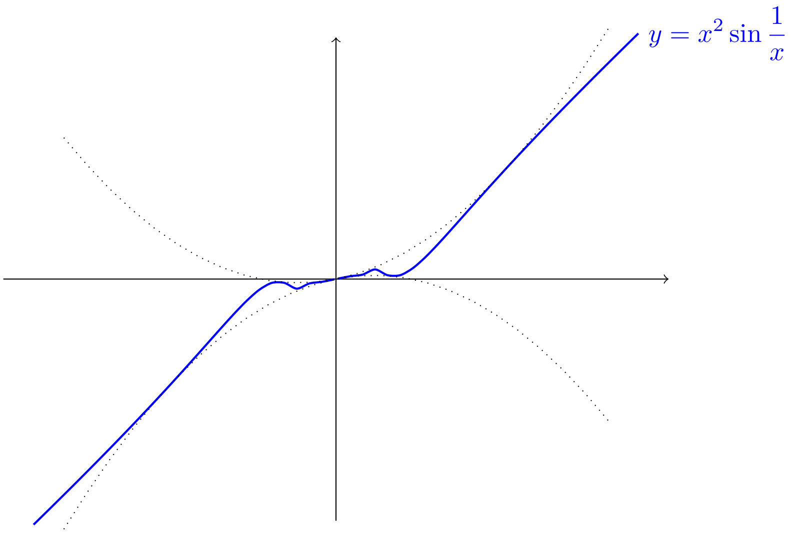
De plus, on a le tableau de variations suivant :

x	$-\infty$		-1		0		1		$+\infty$
$f'(x)$		$+$	0	$-$	0	$-$	0	$+$	
f	0	$\nearrow$	$60\,\mathrm{e}^{-1}$	$\searrow$	22	$\searrow$	$8\,\mathrm{e}$	$\nearrow$	$+\infty$

Donc 1 et -1 sont des extrema locaux de f, mais 0 n'en est pas un. De plus, $8\,\mathrm{e} > 0$ donc f d'admet pas d'extrema globaux.

◊

Remarque 2.16 : Attention, si $f'(x) > 0$, alors cela n'implique pas que f est croissante au voisinage de x_0 (c'est vrai si la fonction f est $\mathcal{C}^1$, auquel cas f' est positive au voisinage de x_0). On peut s'inspirer de l'exemple de $x \mapsto x^2 \sin \frac{1}{x}$ pour trouver un contre-exemple avec une dérivée positive en 0 :



On considèrera par exemple la fonction $\varphi : x \mapsto x^2 \sin \frac{1}{x} + \frac{x}{2}$, dont la courbe est coincée entre les courbes des fonctions $x \mapsto x^2 + \frac{x}{2}$ et $x \mapsto -x^2 + \frac{x}{2}$. ◊

4. Théorèmes d'extension et de prolongement

Théorème 2.17 *Extension de la dérivée*

Soient $x_0 \in I$. Soit $f \in \mathcal{F}(I, \mathbb{R})$. Si $f \in \mathcal{C}^0(I)$ et $f \in \mathcal{D}^1(I \setminus \{x_0\})$, et si f' admet une limite finie ℓ en x_0, alors $f \in \mathcal{D}^1(I)$ et $f'(x_0) = \ell$.

En particulier, f' est continue en x_0.

Démonstration : Il suffit de montrer que f est dérivable en x_0. Soit $x \in I \setminus \{x_0\}$. On note $S_x =]x_0, x[\cup]x, x_0[$. Alors f est continue sur $\overline{S}_x$ et dérivable sur S_x, on peut donc lui appliquer le théorème des accroissements finis : il existe $c_x \in S_x$ tel que

$$f'(c_x) = \frac{f(x) - f(x_0)}{x - x_0}.$$

On a alors

$$x_0 - x \leq c_x \leq x_0 + x, \quad \lim_{\substack{x \to x_0 \\ x \neq x_0}} c_x = x_0, \quad \lim_{\substack{x \to x_0 \\ x \neq x_0}} \frac{f(x) - f(x_0)}{x - x_0} = \lim_{\substack{x \to x_0 \\ x \neq x_0}} f'(c_x) = \ell,$$

donc $f'(x_0) = \ell$. □

Une variante de la démonstration utilise l'inégalité des accroissements finis, et permet donc d'étendre ce résultat au cas des fonctions à valeurs complexes.

Théorème 2.18 *Prolongement $\mathcal{C}^p$*

Soient $p \in \mathbb{N}^*$ et $x_0 \in I$. Soit $f \in \mathcal{F}(I \setminus \{x_0\}, \mathbb{R})$. Si $f \in \mathcal{C}^p(I \setminus \{x_0\})$, et si

$$\forall k \in [\![0, p]\!], \quad \lim_{\substack{x \to x_0 \\ x \neq x_0}} f^{(k)}(x) = \ell_k \in \mathbb{R}.$$

alors f se prolonge en une fonction de de classe $\mathcal{C}^p$ sur I vérifiant

$$\forall k \in [\![0, p]\!], \quad f^{(k)}(x_0) = \ell_k.$$

Évidemment, on pourra appliquer ce théorème pour prolonger des fonctions de classe $\mathcal{C}^\infty$.

Démonstration : Montrons par récurrence finie sur $k \in [\![0, p]\!]$ que f se prolonge en une fonction $\mathcal{C}^k(I)$ et que $f^{(k)}(x_0) = \ell_k$.

Initialisation D'après le théorème de prolongement par continuité, f admet une limite finie en x_0 donc se prolonge en une fonction continue en x_0 (on la note encore f) vérifiant $f(x_0) = \ell_0$.

Hérédité Soit $k \in [\![0, p-1]\!]$, on suppose qu'on a prolongé f en une fonction de classe $\mathcal{C}^k$ sur I et que $f^{(k)}(x_0) = \ell_k$. Alors $f^{(k)}$ est continue en x_0, dérivable sur $I \setminus \{x_0\}$, et sa dérivée admet une limite finie en x_0. Donc par le théorème d'extension de la dérivée $f^{(k)}$ est dérivable et $f^{(k+1)}(x_0) = \ell_{k+1}$, ce qui démontre l'hérédité. □

La différence principale avec le théorème d'extension de la dérivée, c'est qu'on ne suppose plus que f est continue (ni même définie) en a : c'est bien un théorème de prolongement.

Remarque 2.19 : Hors-programme : si x_0 est une borne de l'intervalle, alors on a juste besoin d'une limite pour la dérivée p-ème, et toutes les autres dérivées se raccordent automatiquement. ◊

Exemple 2.20 :
On pose

$$\forall x \in \mathbb{R}^*, \quad f : x \mapsto \begin{cases} x\,\mathrm{e}^{-\frac{1}{x}} & \text{si } x > 0 \\ 0 & \text{si } x < 0 \end{cases}.$$

Montrer que f se prolonge en une fonction de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$, et déterminer $f^{(p)}(0)$ pour tout $p \in \mathbb{N}$.

Réponse

Il est évident que f est $\mathcal{C}^\infty$ sur $\mathbb{R}^*$. On montre alors par récurrence directe que, pour tout $p \in \mathbb{N}$, il existe $F_p \in \mathbb{R}(X)$ vérifiant

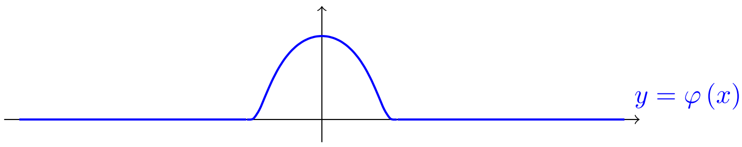
$$\forall x > 0, \quad f^{(p)}(x) = F_p(x)\,\mathrm{e}^{-\frac{1}{x}}.$$

Par croissances comparées, on en déduit que, pour tout $p \in \mathbb{N}$, $\lim_{x \to 0^+} f^{(p)}(x) = 0$. D'après le théorème de prolongement $\mathcal{C}^p$, on en déduit donc que f se prolonge en une fonction de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$ et, pour tout $p \in \mathbb{N}$, $f^{(p)} = 0$.

◊

Remarque 2.21 : Avec ce genre d'exemple, on peut construire des fonctions de classe $\mathcal{C}^\infty$ nulles en dehors d'un segment. Par exemple, la fonction φ, définie par

$$\forall x \in \mathbb{R}, \quad \varphi(x) = \begin{cases} \exp\left(\frac{1}{x^2-1}\right) & \text{si } x \in [-1,1] \\ 0 & \text{sinon} \end{cases}.$$



◇

III Développements limités

1. Définition et manipulation

Définition/Proposition 3.1 *Développement limité*

Soient $f \in \mathcal{F}(I)$, $x_0 \in I$ et $n \in \mathbb{N}$. On dit que f *admet un développement limité (DL) à l'ordre n en x_0* s'il existe $a_0, \ldots, a_n \in \mathbb{R}$ tels que :

$$f(x) \underset{x \to x_0}{=\!=} \sum_{k=0}^{n} a_k (x - x_0)^k + o\left((x - x_0)^n\right),$$

ou, de manière équivalente,

$$f(x_0 + h) \underset{h \to 0}{=\!=} \sum_{k=0}^{n} a_k h^k + o(h^n).$$

S'il existe, le développement limité est unique.

Dans cette définition, les coefficients a_k dépendent bien entendu de x_0 !

Démonstration : Supposons qu'il existe $a_0, \ldots, a_n, b_0, \ldots, b_n \in \mathbb{R}$ tels que

$$f(x_0 + h) \underset{h \to 0}{=\!=} \sum_{k=0}^{n} a_k h^k + o(h^n) = \sum_{k=0}^{n} b_k h^k + o(h^n).$$

Alors, pour h au voisinage de 0,

$$\sum_{k=0}^{n} (a_k - b_k) h^k \underset{h \to 0}{=\!=} o(h^n).$$

Supposons, par l'absurde, qu'il existe $k \in [\![0, n]\!]$ tel que $a_k \neq b_k$. On pose alors $p = \min\{k \in [\![0, n / a_k \neq b_k\}$ (qui existe par hypothèse, l'ensemble étant une partie non-vide de $\mathbb{N}$). On a alors $p \leq n$ et

$$\sum_{k=0}^{n} (a_k - b_k) h^k = \sum_{k=p}^{n} (a_k - b_k) h^k \underset{h \to 0}{=\!=} (a_p - b_p) h^p + o(h^p) \underset{h \to 0}{=\!=} o(h^n),$$

et donc

$$a_p - b_p + o(1) \underset{h \to 0}{=\!=} o\left(h^{n-p}\right).$$

Ceci est absurde, car le terme de droite tend vers 0 mais $a_p \neq b_p$. Il s'en suit que, pour tout $k \in [\![0,n]\!]$, $a_k = b_k$. $\square$

On n'oubliera pas le terme en "$o(h^n)$", ce qui donne vraiment une très mauvaise impression le jours du concours ou de l'examen. Pour rappel, on peut écrire $o(h^n)$ sous la forme :

$$o(h^n) = h^n \varepsilon(h), \quad \lim_{h\to 0} \varepsilon(h) = 0.$$

Exemple 3.2 :
Soit $n \in \mathbb{N}$. Pour tout $h \in]-1,1[$, on sait que $\displaystyle\sum_{k=0}^{n} h^k = \frac{1-h^{n+1}}{1-h}$, donc $\displaystyle\frac{1}{1-h} = \sum_{k=0}^{n} h^k + \frac{h^{n+1}}{1-h}$. Or

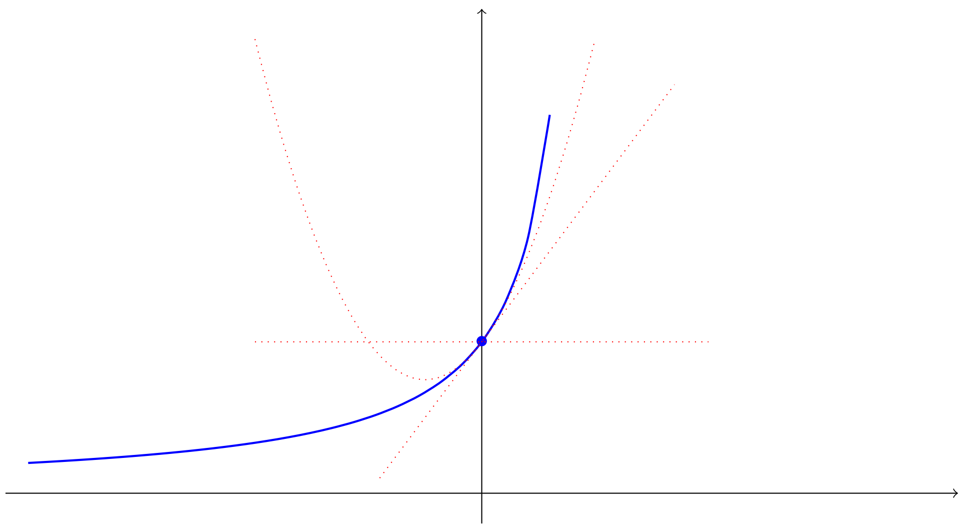
$$\frac{1}{h^n} \times \frac{h^{n+1}}{1-h} = \frac{h}{1-h} \xrightarrow[h\to 0]{} 0, \quad \frac{h^{n+1}}{1-h} \underset{h\to 0}{=} o(h^n),$$

donc la fonction $x \mapsto \dfrac{1}{1-x}$ admet un développement limité à l'ordre n en 0, qui est

$$\frac{1}{1-x} \underset{x\to 0}{=} \sum_{k=0}^{n} x^k + o(x^n).$$

$\diamondsuit$

Remarque 3.3 : Le polynôme $\displaystyle\sum_{k=0}^{n} a_k X^k$ est la fonction polynômiale de degré inférieur à n qui approche le mieux la courbe de f au point x_0.



$\diamondsuit$

Proposition 3.4
Soient $f \in \mathcal{F}(I)$ et $n \in \mathbb{N}$. Supposons que $0 \in I$ et que f admette un DL à l'ordre n en 0. Si f est paire (resp. impaire) alors le DL ne contient que des puissances paires (resp. impaires).

Démonstration : Supposons que f soit paire (le cas impair se traite de façon similaire). Il existe $a_0, \ldots, a_n \in \mathbb{R}$ tels que

$$f(x) \underset{x\to 0}{=} \sum_{k=0}^{n} a_k x^k + o(x^n).$$

D'autre part, f étant paire, on a

$$f(x) = f(-x) \underset{x\to 0}{=} \sum_{k=0}^{n} (-1)^k a_k x^k + o(x^n).$$

Par unicité du DL, on en déduit que, pour tout $k \in [\![0, n]\!]$, $a_k = (-1)^k a_k$, et donc $a_k = 0$ si k est impair. □

Exemple 3.5 :
On sait que la fonction sin est impaire, et son DL à l'ordre 8 en 0 est :

$$\sin x \underset{x\to 0}{=} x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + o\left(x^8\right).$$

♢

Remarque 3.6 :

- On ne peut évidemment rien dire en un point autre que 0.
- La réciproque est également fausse (si l'on connaît les n premiers termes du DL, on ne connaît pas toute la fonction f. Par exemple, la fonction f définie par

  $$f(x) = 1 + x^2 + x^3 \underset{x\to 0}{=} 1 + x^2 + o\left(x^2\right)$$

  admet un DL à l'ordre 2 possédant uniquement des termes pairs, et pourtant f n'est pas paire.
- Cela reste vrai si la fonction possède à n'importe quel ordre un DL composé de puissances paires : voir exemple 2.20.

♢

Proposition 3.7

Soient $f \in \mathcal{F}(I)$ et $x_0 \in I$. Alors

(i) f admet un DL à l'ordre 0 en x_0 si, et seulement si, f est continue en x_0.
(ii) f admet un DL à l'ordre 0 en x_0 si, et seulement si, f est dérivable en x_0.

Dans ces cas, on peut alors identifier les deux premiers termes du DL avec $f(x_0)$ et $f'(x_0)$.

Proposition 3.8

Soient $f \in \mathcal{D}^1(I)$, $x_0 \in I$ et $n \in \mathbb{N}$.

(i) Si f' admet un DL à l'ordre n en x_0, alors f admet un DL à l'ordre $n+1$ en x_0 obtenu en intégrant terme à terme celui de f'.
(ii) Si f admet un DL à l'ordre $n+1$ et f' admet un DL à l'ordre n, alors celui-ci est obtenu en intégrant terme à terme celui de f.

Démonstration : (i) Par définition, il existe $a_0, \ldots, a_n \in \mathbb{R}$ tels que, pour tout x au voisinage de x_0,

$$f'(x) = \sum_{k=0}^{n} a_k (x - x_0)^k + (x - x_0)^n h(x - x_0),$$

avec $\lim\limits_{0} h = 0$. Alors

$$\begin{aligned} f(x) = f(x_0) + \int_{x_0}^{x} f'(t)\, dt &= f(x_0) + \int_{x_0}^{x} \left(\sum_{k=0}^{n} a_k (t - x_0)^k + (t - x_0)^n h(t - x_0) \right) dt \\ &= f(x_0) + \sum_{k=0}^{n} \frac{a_k}{k+1} (x - x_0)^{k+1} + \int_{x_0}^{x} (t - x_0)^n h(t - x_0)\, dt \\ &= f(x_0) + \sum_{k=1}^{n+1} \frac{a_{k-1}}{k} (x - x_0)^k + \int_{0}^{x - x_0} s^n h(s)\, ds. \end{aligned}$$

Par définition, pour tout $\varepsilon > 0$, il existe $\alpha > 0$ tel que

$$\forall s \in I \cap [-\alpha, \alpha], \quad |h(s)| \leq \varepsilon.$$

On a alors, pour $x \in [x_0, x_0 + \alpha] \cap I$,

$$\left| \int_{0}^{x - x_0} s^n h(s)\, ds \right| \leq \int_{0}^{x - x_0} s^n |h(s)|\, ds \leq \varepsilon \int_{0}^{x - x_0} s^n ds = \frac{\varepsilon}{n+1} (x - x_0)^{n+1} = \frac{\varepsilon}{n+1} |x - x_0|^{n+1}.$$

De même, pour $x \in [x_0 - \alpha, x_0] \cap I$,

$$\left| \int_{0}^{x - x_0} s^n h(s)\, ds \right| \leq \int_{x - x_0}^{0} |s^n| |h(s)|\, ds \leq \varepsilon \int_{x - x_0}^{0} (-s)^n\, ds = \varepsilon \int_{0}^{x_0 - x} t^n dt = \frac{\varepsilon}{n+1} |x - x_0|^{n+1}.$$

Donc $\displaystyle\int_{0}^{x - x_0} s^n h(s)\, ds \underset{x \to x_0}{=\!=} o\left((x - x_0)^{n+1} \right)$, et donc f admet un DL à l'ordre $n+1$ en x_0.

(ii) Par hypothèse, il existe $a_0, \ldots, a_n, b_0, \ldots, b_{n+1} \in \mathbb{R}$ tels que

$$f'(x) \underset{x \to x_0}{=\!=} \sum_{k=0}^{n} a_k (x - x_0)^k + o((x - x_0)^n), \quad f'(x) \underset{x \to x_0}{=\!=} \sum_{k=0}^{n+1} b_k (x - x_0)^k + o\left((x - x_0)^{n+1} \right).$$

D'après (i), on sait que

$$b_0 = f(x_0), \quad \forall k \in [\![1, n+1]\!], \quad b_k = \frac{a_{k-1}}{k}.$$

Donc

$$f'(x) \underset{x \to x_0}{=\!=} \sum_{k=0}^{n} (k+1) b_{k+1} (x - x_0)^k + o((x - x_0)^n).$$

$\square$

Si f' admet un DL, alors f en admet un à l'ordre supérieur, mais la réciproque n'est pas vrai. Toujours, le classique contre-exemple $x^2 \sin\left(\dfrac{1}{x}\right)$ qui admet un DL à l'ordre 1 en 0 (car dérivable) mais dont la dérivée n'admet pas de DL à l'ordre 0 en 0 (car non-continue).

Remarque 3.9 : Soient f, g des fonctions admettant un DL à l'ordre n en x_0.

(i) Pour obtenir les DL de la combinaison linéaire, du produit ou de la composée de f et g, on part des DL de f et g avec les règles de calcul habituelles.

(ii) Pour obtenir le DL de $\dfrac{1}{f}$, on utilise le DL de $u \mapsto \dfrac{1}{1+u}$.

(iii) Pour obtenir le DL de f' s'il existe, on dérive terme à terme le DL de f :

$$f(x_0+h) = a_0 + a_1 h + a_2 h^2 + \cdots + a_n h^n + o(h^n), \quad f'(x_0+h) = a_1 + 2a_2 h + \cdots + n a_n h^{n-1} + o\left(h^{n-1}\right).$$

(iv) Pour obtenir le DL de f si f' admet un DL, on intègre terme à terme le DL de f' :

$$f'(x_0+h) = a_0 + a_1 h + \cdots + a_n h^n + o(h^n), \quad f(x_0+h) = f(x_0) + a_0 h + \frac{a_1}{2} h^2 + \cdots + \frac{a_n}{n+1} h^{n+1} + o\left(h^{n+1}\right).$$

$\diamondsuit$

Exemple 3.10 :
La fonction arctan admet un DL à tout ordre en 0. En effet, elle est dérivable sur $\mathbb{R}$ et

$$\forall x \in \mathbb{R}, \quad f'(x) = \frac{1}{1+x^2}.$$

Soit $n \in \mathbb{N}$. On a déjà vu que

$$\frac{1}{1-x} \underset{x\to 0}{=\!=} \sum_{k=0}^{n} x^k + o(x^n).$$

On en déduit que

$$\frac{1}{1+x^2} \underset{x\to 0}{=\!=} \sum_{k=0}^{n} (-1)^k x^{2k} + o\left(x^{2n}\right), \quad \arctan(x) \underset{x\to 0}{=\!=} \arctan(0) + \sum_{k=0}^{n} \frac{(-1)^k}{2k+1} x^{2k+1} + o\left(x^{2n+1}\right).$$

Donc

$$\arctan(x) \underset{x\to 0}{=\!=} x - \frac{x^3}{3} + \frac{x^5}{5} + \cdots + (-1)^n \frac{x^{2n+1}}{2n+1} + o\left(x^{2n+1}\right).$$

$\diamondsuit$

Exercice 3.11 :
Obtenir le DL à l'ordre 4 en 0 de $x \mapsto \cos(\ln(1+x))$.

Réponse

On a

$$\ln(1+x) \underset{x\to 0}{=\!=} x - \frac{x^2}{2} + \frac{x^3}{3} + o\left(x^3\right), \quad \cos(u) \underset{u\to 0}{=\!=} 1 - \frac{u^2}{2} + \frac{u^4}{24} + o\left(u^4\right).$$

En posant $u(x) = \ln(1+x)$, on a alors $\lim\limits_{x\to 0} u(x) = 0$ et

$$u(x)^2 = x^2 - x^3 + \frac{x^4}{4} + \frac{2x^4}{3} + o\left(x^4\right), \quad u(x)^4 = x^4 + o\left(x^4\right).$$

Donc

$$\cos(\ln(1+x)) \underset{x\to 0}{=\!=} 1 - \frac{x^2}{2} + \frac{x^3}{2} - \frac{5x^4}{12} + o\left(x^4\right).$$

Pousser le DL de $\ln(1+x)$ à l'ordre 2 ne suffit pas !

$\diamondsuit$

2. Formules de Taylor

Souvent considérées à tort comme de simples développements limités, les formules de Taylor [4] sont des outils puissants pour comparer une fonction à son approximation polynomiale en un point. On les énonce ici pour des fonctions à valeurs réelles ; elles restent vraies (sauf la formule de Taylor-Lagrange) pour des fonctions complexes.

Théorème 3.12 *Formule de Taylor avec reste intégral*
Soient $n \in \mathbb{N}, x_0 \in I$ et $f \in \mathcal{C}^{n+1}(I)$. Alors :

$$\forall x \in I, \quad f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(x_0)}{k!}(x-x_0)^k + \int_{x_0}^{x} \frac{f^{(n+1)}(t)}{n!}(x-t)^n \, dt.$$

Démonstration : On montre par récurrence sur $n \in \mathbb{N}$ que toute fonction $f \in \mathcal{C}^{n+1}(I)$vérifie cette relation.

$\boxed{\text{Initialisation}}$ Supposons que $f \in \mathcal{C}^1(I)$. Alors

$$f(x) = f(x_0) + \int_{x_0}^{x} f'(t)\, dt = \sum_{k=0}^{0} \frac{f^{(k)}(x_0)}{k!}(x-x_0)^k + \int_{x_0}^{x} \frac{f^{(1)}(t)}{0}(x-t)^0 \, dt.$$

$\boxed{\text{Hérédité}}$ Soit $n \in \mathbb{N}$ et supposons que la propriété soit vraie au rang n. Soit $f \in \mathcal{C}^{n+2}(I)$. Alors l'hypothèse de récurrence s'applique à f, et on a donc, pour tout $x \in I$,

$$f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(x_0)}{k!}(x-x_0)^k + \int_{x_0}^{x} \frac{f^{(n+1)}(t)}{n!}(x-t)^n \, dt.$$

Alors, par intégration par parties, les fonctions $f^{(n+1)}$ et $t \mapsto (x-t)^{n+1}$ étant $\mathcal{C}^1$ sur I,

$$\begin{aligned}\int_{x_0}^{x} f^{(n+1)}(t)(x-t)^n \, dt &= -\left[\frac{(x-t)^{n+1}}{n+1} f^{(n+1)}(t)\right]_{t=x_0}^{x} + \int_{x_0}^{x} \frac{(x-t)^{n+1}}{n+1} f^{(n+2)}(t)\, dt \\ &= \frac{(x-x_0)^{n+1}}{n+1} f^{(n+1)}(x_0)\, \frac{(x-t)^{n+1}}{n+1} f^{(n+2)}(t)\, dt,\end{aligned}$$

et on en déduit que

$$\begin{aligned}f(x) &= \sum_{k=0}^{n} \frac{f^{(k)}(x_0)}{k!}(x-x_0)^k + \frac{f^{(n+1)}(x_0)}{(n+1)!}(x-x_0)^{n+1} + \int_{x_0}^{x} \frac{f^{(n+2)}(t)}{(n+1)!}(x-t)^{n+1}\, dt \\ &= \sum_{k=0}^{n+1} \frac{f^{(k)}(x_0)}{k!}(x-x_0)^k + \int_{x_0}^{x} \frac{f^{(n+2)}(t)}{(n+1)!}(x-t)^{n+1}\, dt.\end{aligned}$$

$\square$

Exercice 3.13 :
Soit $f \in \mathcal{C}^{\infty}(\mathbb{R}, \mathbb{R})$. Montrer que

$$\begin{aligned} f \text{ est un polynôme} &\iff \exists n \in \mathbb{N}, \quad f^{(n)} = 0 \\ &\iff \exists n \in \mathbb{N}, \forall k \geq n \quad f^{(k)} = 0.\end{aligned}$$

4. Brook Taylor (1685-1731) : artiste et mathématicien anglais. Ne pas confondre avec Chuck Taylor, le joueur de basket.

Réponse

La deuxième équivalence est évidente (la réciproque est claire, et l'implication est une récurrence directe). On démontre maintenant la première équivalence.

Si f est un polynôme, soit $n \geq \deg(f)$, alors on sait d'après le cours sur les polynômes que $f^{(n)} = 0$. Réciproquement, supposons qu'il existe $n \in \mathbb{N}$ tel que $f^{(n)} = 0$. Par hypothèse, f est de classe $\mathcal{C}^n$ sur $\mathbb{R}$ et donc, d'après la formule de Taylor avec reste intégral, pour tout $x \in \mathbb{R}$, on a

$$f(x) = \sum_{k=0}^{n-1} \frac{f^{(k)}(0)}{k!} x^k + \int_0^x \frac{f^{(n)}(t)}{(n-1)!} (x-t)^{n-1} \, dt = \sum_{k=0}^{n-1} \frac{f^{(k)}(0)}{k!} x^k,$$

donc $f = \displaystyle\sum_{k=0}^{n-1} \frac{f^{(k)}(0)}{k!} X^k$.

$\diamondsuit$

Théorème 3.14 *Formule de Taylor-Lagrange*[5]

Soient $a, b \in \mathbb{R}$ tels que $a \neq b$, $n \in \mathbb{N}$ et $f \in \mathcal{F}([a,b], \mathbb{R})$. Notons $S = [a,b] \cup [b,a]$. Si f est de classe $\mathcal{C}^n$ sur S et $\mathcal{D}^{n+1}$ sur $\mathring{S}$ alors il existe $c \in \mathring{S}$ tel que

$$f(b) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!} (b-a)^k + \frac{f^{(n+1)}(c)}{(n+1)!} (b-a)^{n+1}.$$

À écrire entre x_0 et x.

Démonstration : Pour $\lambda \in \mathbb{R}$, on pose

$$\varphi_\lambda(x) = f(x) - f(b) + \sum_{k=1}^{n} \frac{(b-x)^k}{k!} f^{(k)}(x) + \lambda \frac{(b-x)^{n+1}}{(n+1)!}.$$

D'une part, $\varphi_\lambda(b) = 0$. Puisque $b > a$, on fixe alors

$$\lambda = \frac{(n+1)!}{(b-a)^{n+1}} \left(f(b) - \sum_{k=0}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a) \right),$$

et $\varphi_\lambda(a) = 0$ aussi. D'autre part, la fonction φ_λ est continue sur $[a,b]$ et dérivable sur $]a,b[$, et $\varphi_\lambda(a) = \varphi_\lambda(b) = 0$. D'après le théorème de Rolle, il existe $c \in]a,b[$ tel que $\varphi'_\lambda(c) = 0$. On a donc

$$\varphi'_\lambda(c) = f'(c) + \sum_{k=1}^{n} \frac{(b-c)^k}{k!} f^{(k+1)}(c) - \sum_{k=1}^{n} \frac{(b-c)^{k-1}}{(k-1)!} f^{(k)}(c) - \lambda \frac{(b-c)^n}{n!} = \frac{(b-c)^n}{n!} \left(f^{(n+1)}(c) - \lambda \right).$$

D'où $f^{(n+1)}(c) = \lambda$. Donc

$$f(b) = \sum_{k=0}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a) + \frac{(b-a)^{n+1}}{(n+1)!} f^{n+1}(c).$$

$\square$

5. Joseph Louis Lagrange (1736-1813) : mathématicien italien naturalisé français.

Puisqu'elle utilise le théorème de Rolle pour sa démonstration, cette formule n'est vraie que dans $\mathbb{R}$ (dans les autres espaces, on ne va pas forcément de a à b en ligne droite). Si $f \in \mathcal{C}^{n+1}([a,b],\mathbb{R})$, l'inégalité de Taylor-Lagrange est alors une conséquence directe de la formule de Taylor-Lagrange.

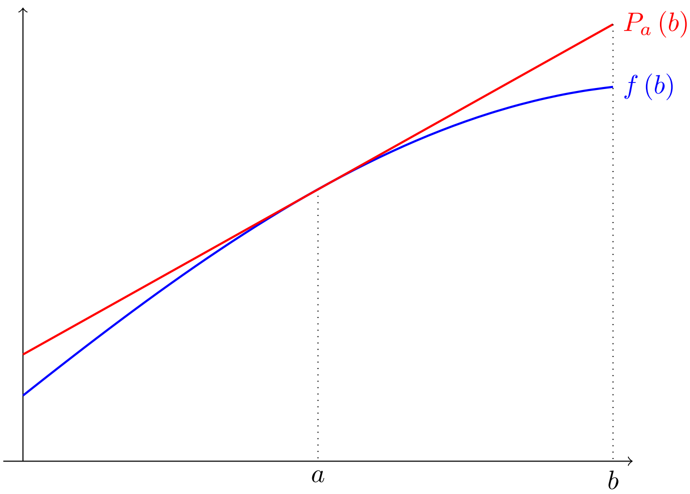
On remarquera que la formule de Taylor-Lagrange généralise le théorème des accroissements finis.

Corollaire 3.15 *Inégalité de Taylor-Lagrange*

Soient $a, b \in \mathbb{R}$ tels que $a < b$, $n \in \mathbb{N}$ et $f \in \mathcal{F}([a,b],\mathbb{R})$. Notons $S = [a,b] \cup [b,a]$. On suppose que f est de classe $\mathcal{C}^n$ sur S et $\mathcal{D}^{n+1}$ sur $\mathring{S}$. S'il existe $M > 0$ tel que, pour tout $x \in \mathring{S}$, $|f^{(n+1)}(x)| \leq M$, alors :

$$\left| f(b) - \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(b-a)^k \right| \leq M \frac{|b-a|^{(n+1)}}{(n+1)!}.$$

La preuve est une simple application de la formule de Taylor-Lagrange. L'inégalité de Taylor-Lagrange permet de contrôler l'erreur entre $f(b)$ et l'approximation polynomiale de f en a, notée P_a au point b.



Remarque 3.16 : Si $f \in \mathcal{C}^{n+1}(I)$ et si $x_0 \in I$, alors f admet un DL à l'ordre n en x_0. En effet, puisque $x_0 \in I$, il existe un segment J inclus dans I contenant x_0. Par restriction, $f \in \mathcal{C}^{n+1}(J)$ et donc $f^{(n+1)}$ est continue donc bornée (par un certain $M > 0$) sur J. Alors

$$\lim_{x \to x_0} \left(\frac{1}{(x-x_0)^n} M \frac{|x-x_0|^{(n+1)}}{(n+1)!} \right) = 0, \quad M \frac{|x-x_0|^{(n+1)}}{(n+1)!} \underset{x \to x_0}{=\!=} o\left((x-x_0)^n\right).$$

D'après l'inégalité de Taylor-Lagrange (sur J), on a alors

$$f(x) - \sum_{k=0}^{n} \frac{f^{(k)}(x_0)}{k!}(x-x_0)^k \underset{x \to x_0}{=\!=} o\left((x-x_0)^n\right).$$

Autrement dit, f admet un DL à l'ordre n en x_0. ♢

On va voir qu'on peut affaiblir cette hypothèse de classe $\mathcal{C}^{n+1}$ nécessaire pour que f admette un DL en x_0.

Théorème 3.17 *Formule de Taylor-Young*[6]

Soient $n \in \mathbb{N}^*, x_0 \in I$ et $f \in \mathcal{D}^n(I)$. Alors f admet un DL à l'ordre n en x_0 donné par :

$$f(x) \underset{x \to x_0}{=\!=} \sum_{k=0}^{n} \frac{f^{(k)}(x_0)}{k!}(x - x_0)^k + o\left((x - x_0)^n\right)$$

ou, de manière équivalente,

$$f(x_0 + h) \underset{h \to 0}{=\!=} \sum_{k=0}^{n} \frac{f^{(k)}(x_0)}{k!} h^k + o(h^n).$$

Démonstration : On montre par récurrence sur $n \in \mathbb{N}^*$ que cette égalité est vraie pour toute fonction de classe $\mathcal{D}^n$ sur I.

Initialisation Soit $f \in \mathcal{D}^1(I)$. Alors on a déjà vu que f admet un DL à l'ordre 1 en x_0 et que

$$f(x) \underset{x \to x_0}{=\!=} f(x_0) + f'(x_0)(x - x_0) + o(x - x_0).$$

Hérédité Soit $n \in \mathbb{N}$ et supposons que la propriété soit vraie pour toute fonction de classe $\mathcal{D}^n$ sur I. Soit $f \in \mathcal{D}^{n+1}(I)$. Alors $f \in \mathcal{D}^n(I)$ et, d'après l'hypothèse de récurrence, f' admet un DL à l'ordre n en x_0 donné par :

$$f'(x) \underset{x \to x_0}{=\!=} \sum_{k=0}^{n} \frac{f^{(k+1)}(x_0)}{k!}(x - x_0)^k + o\left((x - x_0)^n\right).$$

Alors f admet un DL à l'ordre $n+1$ en x_0 obtenu en intégrant terme à terme :

$$\begin{aligned} f(x) &\underset{x \to x_0}{=\!=} f(x_0) + \sum_{k=0}^{n} \frac{f^{(k+1)}(x_0)}{k!} \frac{(x - x_0)^{k+1}}{k+1} + o\left((x - x_0)^{n+1}\right) \\ &\underset{x \to x_0}{=\!=} \sum_{k=0}^{n+1} \frac{f^{(k)}(x_0)}{k!}(x - x_0)^k + o\left((x - x_0)^{n+1}\right), \end{aligned}$$

ce qui achève l'hérédité. □

Remarque 3.18 : Les trois (ou quatre) formules de Taylor sont ici énoncées de la plus précise à la moins précise, mais les hypothèses sont de plus en plus faibles (pour arriver finalement à "n fois dérivable). On ne s'embêtera pas à retenir les hypothèses précises des trois premières formules, la classe $\mathcal{C}^{n+1}$ étant bien suffisante en pratique.

- Le reste intégral donne une expression précise du reste dans la formule de Taylor, et permet notamment d'étudier sa régularité. Elle donne des informations sur tout l'intervalle I.
- La formule et l'inégalité de Taylor-Lagrange donne des renseignements partiels (en un point, ou une inégalité) sur tout segment de I.
- La formule de Taylor-Young est plus vague et donne seulement des informations au voisinage de x_0.

◊

⚠ La formule de Taylor-Young donne l'implication :

$f$est n fois dérivable $\Longrightarrow f$ admet un DL à l'ordre n en tout $x_0 \in I$.

6. William Henry Young (1863-1942) : Mathématicien anglais.

On a équivalence pour $n = 1$ (c'est la proposition 1.9), mais la réciproque est fausse pour $n \geq 2$. En effet, posons

$$f : x \mapsto \begin{cases} x^3 \sin\left(\frac{1}{x}\right) & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases}.$$

Alors f est dérivable sur $\mathbb{R}$ et

$$\forall x \in \mathbb{R}, \quad f'(x) = \begin{cases} 3x^2 \sin\left(\frac{1}{x}\right) - x \cos\left(\frac{1}{x}\right) & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases}.$$

Or, pour $x \neq 0$,

$$\frac{f'(x) - f'(0)}{x} = 3x \sin\left(\frac{1}{x}\right) - \cos\left(\frac{1}{x}\right)$$

qui n'admet pas de limite quand $x \to 0$, donc f' n'est pas dérivable en 0. Autrement dit, f n'est pas deux fois dérivable en 0. Par contre, f admet un DL à l'ordre 2 en 0 :

$$f(x) = 0 + 0 + x^2 \left(x \sin \frac{1}{x}\right) \underset{x \to 0}{=\!=} 0 + 0 + o\left(x^2\right).$$

3. Développements limités usuels

Les fonctions usuelles sont de classe $\mathcal{C}^\infty$, et on peut donc obtenir des DL à tout ordre en tout point. Il est conseillé de retenir les premiers termes des DL usuels, et de là retrouver la formule théorique au rang n, plutôt que l'inverse (sous peine de se tromper dans les signes ou dans les factorielles).

Proposition 3.19 *Développements limités usuels en 0*

Soit $n \in \mathbb{N}$. On a les formules suivantes, pour x tendant vers 0 :

$$\mathrm{e}^x = \sum_{k=0}^{n} \frac{x^k}{k!} + o(x^n)$$

$$\cos(x) = \sum_{k=0}^{n} \frac{(-1)^k x^{2k}}{(2k)!} + o\left(x^{2n+1}\right)$$

$$\sin(x) = \sum_{k=0}^{n} \frac{(-1)^k x^{2k+1}}{(2k+1)!} + o\left(x^{2n+2}\right)$$

$$\mathrm{ch}(x) = \sum_{k=0}^{n} \frac{x^{2k}}{(2k)!} + o\left(x^{2n+1}\right)$$

$$\mathrm{sh}(x) = \sum_{k=0}^{n} \frac{x^{2k+1}}{(2k+1)!} + o\left(x^{2n+2}\right)$$

$$(1+x)^\alpha = \sum_{k=0}^{n} \frac{x^k}{k!} \left(\prod_{i=0}^{k-1} (\alpha - i)\right) + o(x^n)$$

$$\frac{1}{1-x} = \sum_{k=0}^{n} x^k + o(x^n)$$

$$\frac{1}{1+x} = \sum_{k=0}^{n} (-1)^k x^k + o(x^n)$$

$$\ln(1+x) = \sum_{k=1}^{n} (-1)^{k+1} \frac{x^k}{k} + o(x^n)$$

$$\arctan(x) = \sum_{k=0}^{n} (-1)^k \frac{x^{2k+1}}{2k+1} + o\left(x^{2n+1}\right)$$

$$\mathrm{argth}(x) = \sum_{k=0}^{n} \frac{x^{2k+1}}{2k+1} + o\left(x^{2n+1}\right)$$

Démonstration : On ne fait pas les calculs entiers. Pour exp et $x \mapsto (1+x)^\alpha$, il s'agit de la formule de Taylor-Young (en calculant les dérivées successives en 0). On déduit du DL de l'exponentielle les DL des fonctions trigonométriques. On connaît déjà les DL de $x \mapsto \dfrac{1}{1-x}$ et $x \mapsto \dfrac{1}{1+x}$, et on les intègre pour obtenir les DL de $x \mapsto \ln(1+x)$, arctan et argth. ☐

On notera que les DL usuels sont majoritairement issus de deux familles : l'exponentielle (on en déduit les fonctions trigonométriques circulaires et hyperboliques) et la somme géométrique (on en déduit les fonctions inverses et logarithmiques).

Exemple 3.20 :
Montrer que

$$\tan(x) \underset{x\to 0}{=\!=} x + \frac{x^3}{3} + \frac{2x^5}{15} + o\left(x^6\right), \quad \operatorname{th}(x) \underset{x\to 0}{=\!=} x - \frac{x^3}{3} + \frac{2x^5}{15} + o\left(x^6\right).$$

Réponse

D'après la propriété précédente, on a

$$\tan(x) \underset{x\to 0}{=\!=} \frac{x - \frac{x^3}{6} + \frac{x^5}{5!} + o\left(x^6\right)}{1 - \frac{x^2}{2} + \frac{x^4}{4!} + o\left(x^5\right)}.$$

Le premier terme du DL de $\cos x$ étant 1, on doit arrêter le DL de $\sin(x)$ à $o\left(x^6\right)$. Le premier terme du DL de $\sin(x)$ étant x, on peut par contre arrêter le DL de $\cos(x)$ à $o\left(x^5\right)$. En posant $u : x \mapsto -\frac{x^2}{2} + \frac{x^4}{4!} + o\left(x^5\right)$, on a alors

$$\begin{aligned}
\tan x &= \left(x - \frac{x^3}{6} + \frac{x^5}{5!} + o\left(x^6\right)\right)\left(1 - u(x) + u^2(x) - u^3(x) + o\left(u(x)^3\right)\right)\\
&= \left(x - \frac{x^3}{6} + \frac{x^5}{5!} + o\left(x^6\right)\right)\left(1 + \frac{x^2}{2} - \frac{x^4}{4!} + \frac{x^4}{4} + o\left(x^6\right)\right)\\
&= \left(x - \frac{x^3}{6} + \frac{x^5}{5!} + o\left(x^6\right)\right)\left(1 + \frac{x^2}{2} + \frac{5x^4}{24} + o\left(x^6\right)\right)\\
&= x + \frac{x^3}{2} - \frac{x^3}{6} + \frac{x^5}{120} + \frac{5x^5}{24} - \frac{x^5}{12} + o\left(x^6\right)\\
&\underset{x\to 0}{=\!=} x + \frac{1}{3}x^3 + \frac{2}{15}x^5 + o\left(x^6\right).
\end{aligned}$$

Le calcul du DL de th est similaire en utilisant ch et sh.

◇

Remarque 3.21 : Pour obtenir des DL de fonctions en un point différent de 0, on se ramènera aux formules usuelles en 0 (en priorité), ou on utilisera la formule de Taylor-Young (si l'on n'a pas d'autre idée) ◇

Exemple 3.22 :
Pour déterminer le DL à l'ordre 4 de ln en 2, on pose $f : t \mapsto \ln(2+t)$, et l'on se ramène donc à trouver un DL de f en 0 (qui existe, car $f \in \mathcal{C}^\infty(]-2, +\infty[)$). On a alors, pour t au voisinage de 0,

$$\ln(2+t) = \ln\left(2\left(1 + \frac{t}{2}\right)\right) = \ln 2 + \ln\left(1 + \frac{t}{2}\right) \underset{t\to 0}{=\!=} \ln 2 + \frac{t}{2} - \frac{t^2}{8} + \frac{t^3}{24} - \frac{t^4}{64} + o\left(t^4\right).$$

◇

Exemple 3.23 :
Pour déterminer le DL à l'ordre 4 de cos en 2, on pose $f : t \mapsto \cos(2+t)$, et l'on se ramène donc à trouver un DL de f en 0 (qui existe, car $f \in \mathcal{C}^\infty(\mathbb{R})$). On a alors, pour t au voisinage de 0,

$$\begin{aligned}
\cos(2+t) &= \cos 2 \cos t - \sin 2 \sin t = \cos 2\left(1 - \frac{t^2}{2} + \frac{t^4}{24} + o\left(t^4\right)\right) - \sin 2\left(t - \frac{t^3}{6} + o\left(t^4\right)\right)\\
&\underset{t\to 0}{=\!=} \cos 2 - (\sin 2)\, t - \frac{\cos 2}{2}t^2 + \frac{\sin 2}{6}t^3 + \frac{\cos 2}{24}t^4 + o\left(t^4\right).
\end{aligned}$$

◇

4. Applications

Les développements limités ont de nombreuses applications : calculs de limites sous formes indéterminées, étude des positions relatives d'une courbe et de sa tangente, développements asymptotiques, positions relatives d'une courbe et de son asymptote. . .

Exemple 3.24 :
Déterminons la limite lorsque $x \to 0$ de $\dfrac{x(\mathrm{e}^x+1)-2(\mathrm{e}^x-1)}{x^3}$. On sait que $\exp \in \mathcal{C}^\infty(\mathbb{R})$ et on a donc

$$x(\mathrm{e}^x+1)-2(\mathrm{e}^x-1) = x\left(2+x+\frac{x^2}{2}+o\left(x^2\right)\right)-2\left(x+\frac{x^2}{2}+\frac{x^3}{3!}+o\left(x^3\right)\right)=\frac{x^3}{6}+o\left(x^3\right).$$

On en déduit que

$$\frac{x(\mathrm{e}^x+1)-2(\mathrm{e}^x-1)}{x^3} \underset{x\to 0}{\sim} \frac{\frac{x^3}{6}}{x^3} \underset{x\to 0}{\sim} \frac{1}{6}, \quad \frac{x(\mathrm{e}^x+1)-2(\mathrm{e}^x-1)}{x^3} \xrightarrow[x\to 0]{} \frac{1}{6}.$$

◇

Exemple 3.25 :
Montrons que la courbe représentative de exp est au-dessus de toutes ses tangentes. Soit $x_0 \in \mathbb{R}$. On sait que $\exp \in \mathcal{C}^\infty(\mathbb{R})$ et, d'après la formule de Taylor avec reste intégral,[7] on a

$$\forall x \in \mathbb{R}, \quad \mathrm{e}^x = \mathrm{e}^{x_0}+(x-x_0)\,\mathrm{e}^{x_0}+\int_{x_0}^{x}\mathrm{e}^t\,(x-t)\,dt.$$

Notons $\mathscr{C}$ la courbe représentative de exp et Δ sa tangente en x_0, d'équation $y = \mathrm{e}^{x_0}+(x-x_0)\,\mathrm{e}^{x_0}$. On sait alors que

$$\forall x \in \mathbb{R}, \quad \mathrm{e}^x - \mathrm{e}^{x_0}+(x-x_0)\,\mathrm{e}^{x_0} = \int_{x_0}^{x}\mathrm{e}^t\,(x-t)\,dt \geq 0,$$

et donc $\mathscr{C}$ est au-dessus de Δ. ◇

Exercice 3.26 :
Montrer que la courbe représentative de la fonction $f : x \mapsto x\exp\left(\dfrac{3}{x}\right)$ admet une asymptote oblique Δ en $+\infty$ et $-\infty$ et étudier la position de la courbe par rapport à cette asymptote aux voisinages de $+\infty$ et $-\infty$.

Réponse

On note $\mathscr{C}_f$ la courbe représentative de f. f est définie sur $\mathbb{R}^*$, et on a

$$\lim_{x\to\pm\infty}\frac{3}{x}=0, \quad \mathrm{e}^{3/x} \underset{x\to\pm\infty}{=\!=} 1+\frac{3}{x}+o\left(\frac{1}{x}\right), \quad f(x)-x-3 \xrightarrow[x\to\pm\infty]{} 0.$$

Donc $\mathscr{C}_f$ admet la droite Δ d'équation $y = x+3$ pour asymptote oblique en $+\infty$ et $-\infty$. Il est difficile d'étudier le signe de $x \mapsto f(x)-(x+3)$, mais on peut se servir du DL pour obtenir son signe aux voisinages de $+\infty$ et $-\infty$. En effet, on a

$$\mathrm{e}^{3/x} \underset{x\to\pm\infty}{=\!=} 1+\frac{3}{x}+\frac{3}{2x^2}+o\left(\frac{1}{x^2}\right), \quad f(x)-(x+3) \underset{x\to\pm\infty}{\sim} \frac{3}{2x}.$$

Or on sait que les équivalents sont localement strictement de même signe, donc $\mathscr{C}_f$ est au-dessus de Δ au voisinage de $+\infty$ et en-dessous au voisinage de $-\infty$.

◇

7. Ici on utilisera ça, ou la formule de Taylor-Lagrange : les autres ne donnent pas de résultat valable sur $\mathbb{R}$ tout entier.

À connaître à la fin du chapitre

Dérivabilité théorique

- Exemples et contre-exemples classiques : $\sqrt{x}, |x|, x^2 \sin\left(\frac{1}{x}\right)$.
- Pour calculer une dérivée, se ramener à un calcul de limite si nécessaire.
- Savoir utiliser les théorèmes importants : Rolle, accroissements finis, prolongement $\mathcal{C}^p$,...
- Savoir ce qui reste valable pour les fonctions à valeurs complexes.

Dérivabilité pratique

- Connaître les dérivées usuelles et savoir les manipuler.

Développements limités

- Connaître les DL usuels.
- Connaître les quatre formules de Taylor (la formule, pas les hypothèses exactes) et savoir les appliquer.

Vrai/Faux

☐ Si f est dérivable à gauche et à droite en x_0, alors f est dérivable en x_0.
☐ Si f est dérivable à droite en x_0 alors f est continue à droite en x_0.
☐ Si f' n'admet pas de limite en x_0 alors f n'est pas dérivable en x_0.
☐ Si f' est dérivable sur I, alors f est $\mathcal{C}^1$ sur I.
☐ x_0 est un extremum local de f si, et seulement si, $f'(x_0) = 0$.
☐ Si f est strictement croissante sur I alors f' est strictement positive sur I.
☐ Si $f'(x_0) > 0$ alors f est croissante au voisinage de x_0.
☐ f est paire si, et seulement si, f' est impaire.
☐ f est impaire si, et seulement si, f' est paire.

Pour aller plus loin

- Théorème de Rolle généralisé
- Différentiabilité et dérivées partielles de fonctions de plusieurs variables

CHAPITRE 9

ALGÈBRE LINÉAIRE – DIMENSION FINIE

Ce chapitre s'appuie fortement sur le chapitre introductif d'algèbre linéaire. En particulier, les notions suivantes doivent être connues et maîtrisées :

- $\mathbb{K}-$espace vectoriel, $\mathbb{K}-$sous-espace vectoriel
- application linéaire, image, noyau
- famille de vecteurs, espace vectoriel engendré
- sous-espaces vectoriels en somme directe, supplémentaires
- projecteur, symétrie, forme linéaire, hyperplan

L'objectif de ce chapitre est d'introduire rigoureusement la notion de dimension, que l'on pourra relier de manière naturelle à ce que l'on connaît en physique (plan de dimension 2, espace de dimension 3, etc.). On verra que dans le cas particulier de la dimension finie, de nombreux résultats facilitent beaucoup les raisonnements que l'on a appris à faire auparavant.

Dans tout ce chapitre, sauf mention contraire, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ et E et F sont des $\mathbb{K}$-espaces vectoriels.

I Famille de vecteurs

1. Famille libre, famille liée

Définition 1.1 *Famille*

On appelle *famille* finie de vecteurs de E tout $n-$uplet d'éléments de E, avec $n \in \mathbb{N}$.

On définit, pour tous $n, p \in \mathbb{N}^*, x_1, \ldots, x_n, y_1, \ldots, y_p \in E$:

- $(x_1, \ldots, x_n) \cup (y_1, \ldots, y_p) = (x_1, \ldots, x_n, y_1, \ldots, y_p)$.
- $(x_1, \ldots, x_n, y_1, \ldots, y_p) \setminus (y_1, \ldots, y_p) = (x_1, \ldots, x_n)$.

Dans le cadre de ce chapitre, on ne considèrera que des familles finies ou indexées par $\mathbb{N}$ ou $\mathbb{Z}$.

Il faut imaginer une famille comme un ensemble (ordonné quand la famille est finie) et autorisant la répétition. En particulier, la famille vide () est une famille (n'ayant aucun élément).

Il convient de faire la différence entre une famille de vecteurs $(\dots)$ et un ensemble de vecteurs $\{\dots\}$: dans une famille, la répétition et l'ordre sont importants : $(x,x,y) \neq (x,y) \neq (y,x)$.

Exemple 1.2 :

(i) Soient $E = \mathbb{R}^2, x_1 = (-1,2), x_2 = (3,-6)$. Les vecteurs x_1 et x_2 sont colinéaires car $x_2 = -3x_1$. On peut aussi écrire $3x_1 + x_2 = 0$.
(ii) Soient $E = \mathbb{R}^3, x_1 = (1,0,0), x_2 = (0,1,0), x_3 = (1,1,0)$. Les vecteurs x_i sont non-colinéaires deux à deux, mais $x_1 + x_2 = x_3$: on parle de vecteurs coplanaires. On peut aussi écrire $x_1 + x_2 - x_3 = 0$.

$\diamondsuit$

Définition 1.3 *Famille libre*

Soient $n \in \mathbb{N}$ et $x_1, \dots, x_n \in E$. On dit que la famille finie $(x_1, \dots, x_n)$ est *libre* si

$$\forall \lambda_1, \dots, \lambda_n \in \mathbb{K}, \quad \left(\sum_{i=1}^{n} \lambda_i x_i = 0 \Rightarrow \forall i \in [\![1,n]\!], \lambda_i = 0 \right).$$

Les vecteurs $x_1, \dots, x_n$ sont aussi dits *linéairement indépendants.*

Une famille (éventuellement infinie) A est dite *libre* si toute sous-famille finie extraite de A est libre, c'est-à-dire :

$$\forall A' \subseteq A, \quad (|A'| < \infty \Rightarrow A' \text{ est libre}).$$

Une famille qui n'est pas libre est dite *liée.*

Quelques exemples fondamentaux à connaître :

- La famille vide $A = ()$ est libre (cohérent d'un point de vue logique).
- Si $0 \in A$ alors A est liée.
- Pour $x \in E$, la famille (x) est libre si, et seulement si, $x \neq 0$.
- Si un vecteur est répété dans une famille, alors celle-ci est liée.

Exemple 1.4 :
Si $E = \mathbb{R}^2$, posons $x_1 = (1,0), x_2 = (1,2), x_3 = (-2,3)$. Montrons que la famille (x_1, x_2) est libre. Soient $\lambda_1, \lambda_2 \in \mathbb{R}$, tels que $\lambda_1 x_1 + \lambda_2 x_2 = 0$. Alors

$$(\lambda_1 + \lambda_2, 2\lambda_2) = 0, \quad \begin{cases} \lambda_1 + \lambda_2 = 0 \\ 2\lambda_2 = 0 \end{cases}, \quad \lambda_1 = \lambda_2 = 0.$$

Que dire de la famille (x_1, x_2, x_3) ? Pour tous $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$,

$$\lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3 = 0 \iff \begin{cases} \lambda_1 + \lambda_2 - 2\lambda_3 = 0 \\ 2\lambda_2 + 3\lambda_3 = 0 \end{cases} \iff \begin{cases} \lambda_1 - \dfrac{3}{2}\lambda_3 - 2\lambda_3 = 0 \\ \lambda_2 = -\dfrac{3}{2}\lambda_3 \end{cases}$$
$$\iff \begin{cases} \lambda_1 = \dfrac{7}{2}\lambda_3 \\ \lambda_2 = -\dfrac{3}{2}\lambda_3 \end{cases}$$

Donc, si $\lambda_1 = 7, \lambda_2 = -3, \lambda_3 = 2$ alors $\lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3 = 0$. $\diamondsuit$

Exercice 1.5 :
Montrer que la famille $A = \left(x \mapsto \mathrm{e}^{x}, x \mapsto \mathrm{e}^{2x}, x \mapsto \mathrm{e}^{3x}\right)$ est libre dans $\mathcal{F}(\mathbb{R}, \mathbb{R})$.

Réponse

Notons $f_1 : x \mapsto e^x, f_2 : x \mapsto e^{2x}, f_3 : x \mapsto e^{3x}$. Soient $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ tels que $\sum_{i=1}^{3} \lambda_i f_i = 0$. En évaluant cette combinaison linéaire de fonctions en $x = 0, \ln 2, \ln 3$ cela nous donne le système

$$\begin{cases} \lambda_1 + \lambda_2 + \lambda_3 = 0 \\ \lambda_1 + 2\lambda_2 + 4\lambda_3 = 0 \\ \lambda_1 + 3\lambda_2 + 9\lambda_3 = 0 \end{cases}, \quad \begin{cases} \lambda_1 + \lambda_2 + \lambda_3 = 0 \\ \lambda_2 + 3\lambda_3 = 0 \\ 2\lambda_2 + 8\lambda_3 = 0 \end{cases}, \quad \begin{cases} \lambda_1 + \lambda_2 + \lambda_3 = 0 \\ \lambda_2 + 3\lambda_3 = 0 \\ 2\lambda_3 = 0 \end{cases}.$$

Donc $\lambda_1 = \lambda_2 = \lambda_3 = 0$, la famille A est donc libre.

♢

La liberté ne dépend ni de E, ni de l'ordre des vecteurs dans la famille. Elle dépend en revanche de $\mathbb{K}$, on fera donc bien attention à préciser si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ lorsque ce n'est pas clair.

Exercice 1.6 :
Etudier la liberté des familles suivantes dans $\mathcal{F}(\mathbb{R}, \mathbb{R})$.

$$(\cos, \sin, x \mapsto \sin(x+2)), \quad (\cos, \sin, x \mapsto \sin(2x)).$$

Réponse

On note $f : x \mapsto \sin(x+2)$ et $g : x \mapsto \sin(2x)$.

1. Pour tout $x \in \mathbb{R}$,

   $$\sin(x+2) = f(x) = \sin 2 \cos x + \cos 2 \sin x, \quad \sin 2 \cos x + \cos 2 \sin x - f(x) = 0.$$

   Puisque $\sin 2 \cos + \cos 2 \sin - f = 0$, on a trouvé une combinaison linéaire non-triviale annulant $(\cos, \sin, f)$, la famille est donc liée.
2. Montrons que $(\cos, \sin, g)$ est libre. Soient $\lambda, \mu, \nu \in \mathbb{R}$ tels que $\varphi = \lambda \cos + \mu \sin + \nu g = 0$. On a alors

   $$\varphi(0)\, \lambda = 0, \quad \varphi\left(\frac{\pi}{2}\right) = \mu = 0,$$

   et donc $\nu = 0$ car $g \neq 0$. La famille $(\cos, \sin, g)$ est donc libre.

♢

Proposition 1.7

Soit $(x_1, \dots, x_n)$ une famille de E. Alors on a l'équivalence suivante :

(i) $(x_1, \dots, x_n)$ est liée.
(ii) L'un des x_i est combinaison linéaire des autres.

En particulier, on remarque que la notion de "famille liée" correspond à la notion de "colinéarité" dans le cas de deux vecteurs" et à celle de "coplanarité" dans le cas de trois vecteurs.

Démonstration : $\boxed{(i) \Rightarrow (ii)}$ Il existe $\lambda_1, \dots, \lambda_n \in \mathbb{K}$ tels que $\sum_{k=1}^{n} \lambda_i x_i = 0$ et les λ_i ne sont pas tous nuls.

Quitte à les réorganiser, on peut supposer $\lambda_n \neq 0$, et alors $x_n = -\sum_{i=1}^{n-1} \frac{\lambda_i}{\lambda_n} x_i$.

$\boxed{(ii) \Rightarrow (i)}$ Quitte à réorganiser les x_i, on peut supposer qu'il existe $\alpha_1, \ldots, \alpha_{n-1} \in \mathbb{K}$ tels que $x_n = \sum_{k=1}^{n-1} \alpha_i x_i$.
Donc $\sum_{k=1}^{n-1} \alpha_i x_i - x_n = 0$. □

Proposition 1.8

(i) Toute sous-famille d'une famille libre est libre.
(ii) Toute sur-famille d'une famille liée est liée.

Démonstration : (i) On se restreint au cas des familles finies. Soit $A = (x_1, \ldots, x_n)$ une famille libre de E. Soit $A' = (x_1, \ldots, x_d)$ une sous-famille non-vide de A, avec $d \leq n$. Soient $\lambda_1, \ldots, \lambda_d \in \mathbb{K}$ tels que $\sum_{i=1}^{d} \lambda_i x_i = 0$. Alors

$$\sum_{i=1}^{d} \lambda_i x_i = \sum_{i=1}^{d} \lambda_i x_i + \sum_{i=d+1}^{n} 0 x_i = \sum_{i=1}^{n} \lambda_i x_i = 0.$$

en notant $\lambda_{d+1} = \cdots = \lambda_n = 0$. La famille A étant libre,

$$\lambda_1 = \cdots = \lambda_d = \lambda_{d+1} = \cdots = \lambda_n = 0.$$

Donc A' est libre.
(ii) Evident par l'absurde.

□

Proposition 1.9

Soit $(x_1, \ldots, x_n)$ une famille libre de E et soit $x_{n+1} \in E$. Alors

$$(x_1, \ldots, x_n, x_{n+1}) \text{ est libre} \iff x_{n+1} \notin \operatorname{Vect}(x_1, \ldots, x_n).$$

Démonstration : $\boxed{\text{Si } (x_1, \ldots, x_{n+1}) \text{ est libre}}$ Evident d'après la proposition 1.7.

$\boxed{\text{Si } (x_1, \ldots, x_{n+1}) \text{ est liée}}$ Alors il existe $\lambda_1, \ldots, \lambda_{n+1} \in \mathbb{K}$ tels que $\sum_{k=1}^{n+1} \lambda_i x_i \neq 0$ et les λ_i ne sont pas tous nuls. Puisque $(x_1, \ldots, x_n)$ est libre, il est clair que $\lambda_{n+1} \neq 0$. Donc

$$x_{n+1} = -\sum_{i=1}^{n} \frac{\lambda_i}{\lambda_{n+1}} x_i.$$

□

Exercice 1.10 :
Soit $n \in \mathbb{N}$. Montrer que la famille $A_n = \left(X^k\right)_{k \in [\![0,n]\!]}$ est une famille libre de $\mathbb{K}[X]$. En déduire que $A = \left(X^k\right)_{k \in \mathbb{N}}$ est libre.

Réponse

Soient $\lambda_0, \ldots, \lambda_n \in \mathbb{K}$. D'après le chapitre sur les polynômes, on sait que $\sum_{k=0}^{n} \lambda_k X^k = 0$ si, et seulement si, $\lambda_0 = \cdots = \lambda_n = 0$. Donc la famille A_n est libre.

Soit A' une sous-famille finie de A. Si A' est vide alors A' est libre. Sinon, notons $d = \max\{\deg P / P \in A'\}$. Donc A' est une sous-famille de A_d qui est libre. Donc A' est libre et donc A est libre.

$\diamondsuit$

Définition 1.11 *Famille de polynômes échelonnée en degrés*

Soit $I \subseteq \mathbb{N}$. On dit qu'une famille $(P_i)_{i \in I}$ de $\mathbb{K}[X]$ est *échelonnée en degrés* si les polynômes P_i sont tous non-nuls et leurs degrés sont deux à deux distincts.

Proposition 1.12

Toute famille de polynômes échelonnée en degrés est libre.

Démonstration : On considère uniquement le cas I fini, puisque si I est infini on sera amené à prendre une sous-famille finie. Soit $(P_i)_{i \in [\![1,n]\!]}$ de $\mathbb{K}[X]$ une famille échelonnée en degrés. Quitte à réorganiser les P_i, on peut supposer que pour tout $i \in [\![1, n-1]\!], \deg P_i < \deg P_{i+1}$. Soient $\lambda_1, \ldots, \lambda_n \in \mathbb{K}^n$ tels que $\sum_{i=1}^{n} \lambda_i P_i = 0$. Supposons, par l'absurde, qu'au moins l'un des λ_i soit non-nul, et notons $m = \max\{i \in [\![1, n]\!], \lambda_i \neq 0\}$. Alors $\lambda_m \neq 0$ et pour tout $i > m, \lambda_i = 0$. Donc

$$\deg\left(\sum_{i=1}^{n} \lambda_i P_i\right) = \deg\left(\sum_{i=1}^{m} \lambda_i P_i\right) = \deg(P_m),$$

ce qui est impossible car $\sum_{i=1}^{n} \lambda_i P_i = 0$ et $P_m \neq 0$. Donc $\lambda_1 = \cdots = \lambda_n = 0$.

On peut aussi traiter cette preuve par récurrence descendante, après avoir réordonné les P_i, en montrant que $\lambda_n = 0$, puis que $\lambda_{n-1} = 0$, et ainsi de suite... $\square$

2. Famille génératrice

Définition 1.13 *Famille génératrice*

Soit A une famille de E. On dit que A est *génératrice* de E si $\operatorname{Vect}(A) = E$.

S'il n'y a pas d'ambiguïté sur l'espace vectoriel considéré, on parlera simplement de famille génératrice.

Dans le cas simple où $A = (x_1, \ldots, x_n)$, A est génératrice si, et seulement si,

$$\forall x \in E, \exists \lambda_1, \ldots, \lambda_n, x = \sum_{i=1}^{n} \lambda_i x_i.$$

On rappelle que

$$\operatorname{Vect} A = \left\{ x \in E / \exists n \in \mathbb{N}, \exists x_1, \ldots, x_n \in A, \exists \lambda_1, \ldots, \lambda_n \in \mathbb{K}, x = \sum_{i=1}^{n} \lambda_i x_i \right\}.$$

Autrement dit, si A est infinie, $\operatorname{Vect} A$ est l'ensemble des combinaisons linéaires finies de A.

Exemple 1.14 :

- La famille $((1,0),(0,1))$ est génératrice dans $\mathbb{R}^2$.
- La famille $((1,0,0),(0,1,0),(0,0,1))$ est génératrice dans $\mathbb{R}^3$.
- La famille $\left(X^k\right)_{k\in\mathbb{N}}$ est génératrice de $\mathbb{K}[X]$ (encore une fois, les combinaisons linéaires sont finies)

$\diamondsuit$

Proposition 1.15

Toute sur-famille d'une famille génératrice est génératrice.

Proposition 1.16

Soit $(x_1, \ldots, x_n, x_{n+1})$ une famille génératrice de E. Alors

$$(x_1, \ldots, x_n) \text{ est génératrice } \iff x_{n+1} \in \operatorname{Vect}(x_1, \ldots, x_n).$$

Démonstration : L'implication étant évidente, on se concentre sur la réciproque. Supposons donc qu'il existe $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ tels que $x_{n+1} = \sum_{i=1}^{n} \lambda_i x_i$. Alors, puisque $(x_1, \ldots, x_{n+1})$ est génératrice, pour tout $x \in E$, il existe $\alpha_1, \ldots, \alpha_{n+1} \in \mathbb{K}$ tels que

$$x = \sum_{k=1}^{n+1} \alpha_i x_i = \sum_{k=1}^{n} \alpha_i x_i + \alpha_{n+1} \sum_{i=1}^{n} \lambda_i x_i = \sum_{i=1}^{n} (\alpha_i + \alpha_{n+1}\lambda_i) x_i.$$

Donc $(x_1, \ldots, x_n)$ est génératrice $\square$

3. Base

Définition 1.17 *Base*

On dit qu'une famille B est une *base* de E si c'est une famille libre et génératrice.

Exemple 1.18 :
La famille $((1,0,0),(0,1,0),(0,0,1))$ est une base de $\mathbb{R}^3$. $\diamondsuit$

La famille vide est une base de $\{0\}$. On pourra retenir que dans une base, il y a juste le bon nombre de vecteurs : il y en a suffisamment pour que la famille soit génératrice, et pas trop pour que la famille soit libre.

Définition 1.19 *Base canonique*
On appelle *base canonique* d'un espace vectoriel la base "naturelle" de cet espace.

Un $\mathbb{K}$-ev admet généralement une infinité de bases.

Par exemple, la base canonique de $\mathbb{R}^n$ la famille $(e_1, \ldots, e_n)$, où

$$\forall i \in [\![1, n]\!], \quad e_i = (\delta_{1,i}, \ldots, \delta_{n,i}) = \left(\underbrace{0, \ldots, 0}_{i-1}, 1, 0, \ldots, 0\right).$$

Exercice 1.20 :
Quelle est la base canonique de $\mathbb{C}^n$?

Réponse
La base canonique de $\mathbb{C}^n$ est aussi $(e_1, \ldots, e_n)$, avec $e_i = (\delta_{1,i}, \ldots, \delta_{n,i})$. Attention, la différence est qu'ici, les combinaisons linéaires se font avec des scalaires de $\mathbb{C}$ et pas de $\mathbb{R}$.

◇

Définition/Théorème 1.21 *Coordonnées*
Soient $n \in \mathbb{N}^*$ et $B = (b_1, \ldots, b_n)$ une famille de E. Les propriétés suivantes sont équivalentes :

(i) B est une base de E.

(ii) $\forall x \in E, \exists! \, (x_1, \ldots, x_n) \in \mathbb{K}^n, x = \sum_{i=1}^{n} x_i b_i$.

Dans ce cas, le n-uplet $(x_1, \ldots, x_n)$ est appelé *coordonnées de x dans la base B.*

Démonstration : $\boxed{(i) \Rightarrow (ii)}$ Soit $x \in E$. Puisque B est génératrice, il existe $(x_1, \ldots, x_n) \in \mathbb{K}^n$ tel que $x = \sum_{i=1}^{n} x_i b_i$. Soit $(x'_1, \ldots, x'_n) \in \mathbb{K}^n$ tel que $x = \sum_{i=1}^{n} x'_i b_i$. Alors $\sum_{i=1}^{n} (x_i - x'_i)\, b_i = 0$ et, puisque B est libre, il s'en suit que pour tout $i \in [\![1, n]\!], x_i - x'_i = 0$ donc $x_i = x'_i$, d'où unicité.

$\boxed{(ii) \Rightarrow (i)}$ Le vecteur nul s'écrivant de manière unique $0 = \sum_{i=1}^{n} 0 \times b_i$, la famille B est libre. En effet, pour tous $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$,

$$\sum_{i=1}^{n} \lambda_i b_i = 0 \Longrightarrow \sum_{i=1}^{n} \lambda_i b_i = \sum_{i=1}^{n} 0 \times b_i \Longrightarrow \forall i \in [\![1, n]\!], \lambda_i = 0.$$

D'autre part, pour tout $x \in E$, il existe $(x_1, \ldots, x_n) \in \mathbb{K}^n$ tel que $x = \sum_{i=1}^{n} x_i b_i$, donc B est génératrice. C'est donc une base. □

On remarquera que l'existence des coordonnées est équivalente au caractère générateur de B tandis que son unicité est équivalente à la liberté de B.

Définition 1.22

Soit A une famille de E. On dit que A est *libre maximale* si A est libre et s'il n'existe aucune famille libre contenant strictement A. On dit que A est *génératrice minimale* si A est génératrice s'il n'existe aucune famille génératrice strictement incluse dans A.

Théorème 1.23

Soit B une famille de E. Alors les propositions suivantes sont équivalentes :

(i) B est une base de E.
(ii) B est génératrice minimale.
(iii) B est libre maximale.

Démonstration : $\boxed{(i) \Rightarrow (ii)}$ Par hypothèse, B est génératrice. Si B est vide, alors B ne possède pas de sous-famille stricte, le résultat est donc évident. Sinon, prenons $x \in B$. Puisque B est libre, $x \notin \operatorname{Vect}(B \setminus (x))$ donc $B \setminus (x)$ n'est pas génératrice. B est donc génératrice minimale.

$\boxed{(ii) \Rightarrow (iii)}$ Supposons, par l'absurde, que B soit liée. Alors il existe $x \in B$ tel que $x \in \operatorname{Vect}(B \setminus (x))$, et donc $B \setminus (x)$ est encore génératrice, ce qui est impossible car B est génératrice minimale. Donc B est libre. De plus, pour tout $x' \in E, x' \in \operatorname{Vect}(B)$ donc $B \cup (x)$ est liée. Donc B est libre maximale.

$\boxed{(iii) \Rightarrow (i)}$ Par hypothèse, B est libre, il reste à montrer qu'elle est génératrice. Soit $x \in E$. La famille $B \cup (x)$ est liée, donc $x \in \operatorname{Vect}(B)$ et donc B est génératrice. □

4. Applications linéaires et familles

Théorème 1.24 *Caractérisation d'une application linéaire par l'image d'une base*

Soient $(e_1, \ldots, e_n)$ une base de E et $(u_1, \ldots, u_n)$ une famille de F. Alors il existe une unique application linéaire $f \in \mathcal{L}(E, F)$ telle que, pour tout $i \in [\![1, n]\!], f(e_i) = u_i$.

Démonstration : Notons $B = (e_1, \ldots, e_n)$.

$\boxed{\text{Existence}}$ Soit $x \in E$ de coordonnées $(x_1, \ldots, x_n)$ dans la base B. Posons $f(x) = \sum_{i=1}^{n} x_i u_i$ et montrons que f convient :

- f est bien définie, par unicité des coordonnées.
- f est linéaire. En effet, pour tous $x, y \in E$ et $\lambda, \mu \in \mathbb{K}$, il existe $x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathbb{K}$ tels que

$$x = \sum_{i=1}^{n} x_i e_i, \quad y = \sum_{i=1}^{n} y_i e_i.$$

Alors,

$$\begin{aligned} f(\lambda x + \mu y) &= f\left(\sum_{i=1}^{n} (\lambda x_i + \mu y_i) e_i\right) = \sum_{i=1}^{n} (\lambda x_i + \mu y_i) u_i = \lambda \sum_{i=1}^{n} x_i u_i + \mu \sum_{i=1}^{n} y_i u_i \\ &= \lambda f(x) + \mu f(y). \end{aligned}$$

- Pour tout $k \in [\![1, n]\!]$,

$$e_k = \sum_{i=1}^{n} \delta_{i,k} e_i, \quad f(e_k) = \sum_{i=1}^{n} \delta_{i,k} u_i = u_k.$$

Unicité Soient $f, g \in \mathcal{L}(E, F)$ telles que, pour tout $i \in [\![1, n]\!]$, $f(e_i) = g(e_i) = u_i$. Alors, pour tout $x = \sum_{i=1}^{n} x_i \in E$,

$$f(x) = f\left(\sum_{i=1}^{n} x_i e_i\right) = \sum_{i=1}^{n} x_i f(e_i) = \sum_{i=1}^{n} x_i u_i = \sum_{i=1}^{n} x_i g(e_i) = g\left(\sum_{i=1}^{n} x_i e_i\right) = g(x).$$

Donc $f = g$, d'où unicité. □

Lemme 1.25

Soit $f \in \mathcal{L}(E, F)$ et soit $A = (x_1, \ldots, x_n)$ une famille de E. Alors

(i) Si A est libre et f est injective, alors $f(A)$ est libre.
(ii) Si A est génératrice et f est surjective, alors $f(A)$ est génératrice.

Démonstration : (i) Pour tous $\lambda_1, \ldots, \lambda_n \in F$,

$$\sum_{i=1}^{n} \lambda_i f(x_i) = 0 \Rightarrow f\left(\sum_{i=1}^{n} \lambda_i x_i\right) = 0 \Rightarrow \sum_{i=1}^{n} \lambda_i x_i = 0 \Rightarrow \lambda_1 = \cdots = \lambda_n = 0.$$

Donc $f(A)$ est libre.

(ii) Pour tout $y \in F$, il existe $x \in E$ tel que $f(x) = y$. Il existe $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ tels que $x = \sum_{i=1}^{n} \lambda_i x_i$ et donc

$$y = f\left(\sum_{i=1}^{n} \lambda_i x_i\right) = \sum_{i=1}^{n} \lambda_i f(x_i).$$

Donc $f(A)$ est génératrice.

□

Théorème 1.26

Soient $f \in \mathcal{L}(E, F)$ et B une base de E. Alors

(i) f est injective $\iff$ $f(B)$ est libre.
(ii) f est surjective $\iff$ $f(B)$ est génératrice.
(iii) f est bijective $\iff$ $f(B)$ est une base.

Démonstration : Le théorème est clair si $B = ()$, auquel cas $E = \{0\}$. Sinon, $B = (e_1, \ldots, e_n)$.

(i) D'après le lemme 1.25, l'implication est évidente puisque B est libre. Supposons donc que $f(B)$ soit libre. Soit $x = \sum_{i=1}^{n} x_i e_i \in \ker f$. Alors

$$f(x) = \sum_{i=1}^{n} x_i f(e_i) = 0, \quad x_1 = \cdots = x_n = 0, \quad x = 0.$$

Donc $\ker f = \{0\}$ donc f est injective.

(ii) D'après le lemme 1.25, l'implication est évidente puisque B est génératrice. Supposons donc que $f(B)$ soit génératrice. Pour tout $y \in F$, il existe $y_1, \ldots, y_n \in \mathbb{K}$ tels que

$$y = \sum_{i=1}^{n} y_i f(e_i) = f\left(\sum_{i=1}^{n} y_i e_i\right)$$

donc y possède un antécédent par f. On en déduit que f est surjective.

(iii) Evident par définition.

□

Puisqu'une application linéaire est caractérisée par son image d'une base, il est logique de lier des propriétés de l'application aux propriétés de l'image. Encore une fois, on pourra faire le lien entre unicité, injectivité et liberté d'une part, et existence, surjectivité et caractère générateur d'autre part.

II Dimension

1. Dimension finie

Définition 2.1 *Dimension finie*

On dit que E est de *dimension finie* s'il possède une famille génératrice finie. Sinon, on dira évidemment qu'il est de dimension infinie.

Exemple 2.2 :
La famille $((1,0),(1,1),(1,2))$ est une famille génératrice de $\mathbb{R}^2$ donc $\mathbb{R}^2$ est de dimension finie. De manière générale, on a vu que $\mathbb{R}^n$ admettait une base (donc famille génératrice) finie. Donc $\mathbb{R}^n$ est de dimension finie. $\mathbb{C}$ est aussi un $\mathbb{R}$ espace vectoriel de dimension finie. ♢

Exercice 2.3 :
Les espaces $\mathbb{K}_n[X]$ et $\mathbb{K}[X]$ sont-ils de dimension finie ?

Réponse

Il est clair que $\mathbb{K}_n[X] = \text{Vect}\left(X^0, \ldots, X^n\right)$ donc il est de dimension finie. En revanche, $\mathbb{K}[X]$ n'est pas de dimension finie. Soit A une famille finie de $\mathbb{K}[X]$. Notons $d = \max\{\deg(P) / P \in A\}$. Toute combinaison linéaire d'éléments de A étant de degré inférieur à d, on en déduit que $\text{Vect}(A) \subseteq \mathbb{K}_d[X] \subsetneq \mathbb{K}[X]$.

♢

Lemme 2.4

Tout espace vectoriel de dimension finie admet (au moins) une base finie.

Démonstration : Soit $G_0 = (x_1, \ldots, x_n)$ une famille génératrice finie de E.

1. Si G_0 est libre, il s'agit d'une base.
2. Sinon, quitte à permuter les x_i, on peut supposer que $x_n \in \text{Vect}(x_1, \ldots, x_{n-1})$, et donc $G_1 = (x_1, \ldots, x_{n-1})$ est génératrice. On revient à l'étape 1 : si G_1 est libre, on a trouvé une base de E, sinon on continue à retirer des vecteurs jusqu'à obtenir une famille libre.[1] Cet algorithme termine en au plus n étapes.

1. Dans le pire des cas (si $E = \{0\}$), on retire tous les x_i et la famille () est libre.

□

En pratique, pour extraire une base d'une famille génératrice, on utilisera plutôt le théorème 2.7 avec $B = ()$. Cela revient à ajouter des vecteurs un par un à $()$, plutôt que de les retirer de G : les calculs sont plus pratiques.

Théorème 2.5 *Théorème fondamental de la dimension - Admis*

Si E est un espace vectoriel de dimension finie admettant une famille génératrice de n vecteurs, alors toute famille de $(n+1)$ vecteurs de E est liée.

Corollaire 2.6

Si L est une famille libre et G est une famille génératrice finie, alors L est finie et $|L| \leq |G|$. En particulier, toutes les bases de E sont finies.

Théorème 2.7 *Théorème de la base incomplète*

Soit E un espace vectoriel de dimension finie. Soient L une famille libre et G une famille génératrice finie telles que $L \subseteq G$. Alors il existe une base B de E telle que $L \subseteq B \subseteq G$.

Démonstration : Si $G = ()$ ou $L = ()$, le résultat est évident. Sinon, notons $L = (x_1, \ldots, x_n)$ et $G = (x_1, \ldots, x_n, y_1, \ldots, y_d)$. Notons $L_0 = L$.

1. Si L_0 est génératrice, on a trouvé une base de E.
2. Sinon, il existe $i \in [\![1, d]\!]$ tel que $y_i \notin \operatorname{Vect}(L_0)$ (évident par l'absurde). Quitte à réordonner les y_i, on peut supposer que $y_1 \notin \operatorname{Vect}(L_0)$, et on pose alors $L_1 = L_0 \cup (y_1)$. On revient à l'étape 1 : si L_1 est génératrice, on a trouvé une base de E, sinon on continue à ajouter des y_i jusqu'à obtenir une famille libre.

□

Exercice 2.8 :
Soient $u = (0, 1, 0, 1), v = (1, 2, 0, 0) \in \mathbb{R}^4$.

1. Montrer que la famille $A = (u, v)$ est libre.
2. Compléter A en une base de $\mathbb{R}^4$.

Réponse

1. A est libre car u et v ne sont pas colinéaires. En effet,

$$\forall \lambda, \mu \in \mathbb{R}, \quad \lambda u + \mu v = 0 \Rightarrow (\mu, \lambda + 2\mu, 0, \lambda) = (0,0,0,0) \iff \lambda = \mu = 0.$$

2. Pour appliquer l'algorithme du théorème, on considère les familles $L_0 = A$ et $G = A \cup B$, avec $B = (e_1, \ldots, e_4)$ la base canonique de $\mathbb{R}^4$. Soient $\lambda, \mu \in \mathbb{K}$.

$$e_1 = \lambda u + \mu v \iff \begin{cases} \mu = 1 \\ \lambda + 2\mu = 0 \\ \lambda = 0 \end{cases} \iff \begin{cases} 0 = 2 \\ \mu = 1 \\ \lambda = 0 \end{cases}$$

donc $e_1 \notin \operatorname{Vect} L_0$. On pose donc $L_1 = L_0 \cup (e_1)$, qui est libre. L_1 n'est pas génératrice, car il existe une famille libre de 4 vecteurs dans $\mathbb{R}^4$. Enfin, il est clair que $e_3 \notin \operatorname{Vect} A_1$. On pose donc $L_2 = (u, v, e_1, e_3)$, qui est libre. Puisque $\mathbb{R}^4$ possède une famille génératrice de 4 vecteurs, toute famille de 5 vecteurs sera liée. Donc L_2 est libre maximale, c'est donc une base de $\mathbb{R}^4$.

$\diamondsuit$

On retiendra que, dans un espace de dimension finie :

- on peut extraire une base de toute famille génératrice ;
- on peut compléter toute famille libre en une base.

2. Définition et caractérisation des bases

Définition/Proposition 2.9 *Dimension*

Soit E un espace vectoriel de dimension finie. Alors toutes les bases de E ont le même nombre d'éléments. Leur cardinal commun est appelé *dimension* de E et noté $\dim(E)$.

Démonstration : Soient B et B' deux bases de E. Puisque B est libre et B' est génératrice, $|B| \leq |B'|$. De même, $|B'| \leq |B|$ donc $|B| = |B'|$. $\square$

Comme max ou lim, on ne pourra écrire $\dim E$ que si l'on a déjà vérifié au préalable que E est de dimension finie. Ecrire $\dim E = +\infty$ peut conduire à des absurdités, car tous les espaces de dimension infinie ne sont pas de la même "taille" (par exemple, $\mathbb{R}^{\mathbb{R}}$ et $\mathbb{R}^{\mathbb{N}}$). Par abus de notation, on pourra écrire, en revanche, $\dim E < +\infty$.

$\{0\}$ est de dimension 0 (c'est le seul ev de dimension 0).

Proposition 2.10 *Espaces de dimension finie de référence*

- Pour tout $n \in \mathbb{N}^*, \mathbb{K}^n$ est un $\mathbb{K}$-espace vectoriel de dimension finie et $\dim \mathbb{K}_n = n$.
- Pour tout $n \in \mathbb{N}, \mathbb{K}_n[X]$ est un $\mathbb{K}$-espace vectoriel dimension finie et $\dim \mathbb{K}_n[X] = n + 1$.
- Les solutions d'une équation différentielle linéaire d'ordre 2 du type
$$y'' + \alpha y' + \beta y = 0, \quad \alpha, \beta \in \mathbb{K}$$
forment un espace-vectoriel de dimension 2.
- L'ensemble des suites définies par une relation de récurrence du type
$$\forall n \in \mathbb{N}, \quad u_{n+2} + \alpha u_{n+1} + \beta u_n = 0, \quad \alpha, \beta \in \mathbb{K}$$
forment un espace-vectoriel de dimension 2.

Démonstration : On sait que $\mathbb{K}_n[X]$ admet $\left(1, X, X^2, \ldots, X^n\right)$ pour base (on l'appelle base canonique de $\mathbb{K}_n[X]$), et que la base canonique de $\mathbb{K}^n$ admet n éléments. Le reste a déjà été vu. $\square$

Définition 2.11

Un espace vectoriel de dimension 1 est appelé *droite vectorielle.* Un espace vectoriel de dimension 2 est appelé *plan vectoriel.*

Proposition 2.12

Soient E un espace vectoriel de dimension $n \in \mathbb{N}$ et A une famille de E. Alors :

(i) Si A est libre, alors $|A| \leq n$ avec égalité si, et seulement si, A est une base.
(ii) Si A est génératrice, alors $|A| \geq n$ avec égalité si, et seulement si, A est une base.
(iii) Si A possède n vecteurs, alors

$$A \text{ est une base} \iff A \text{ est libre} \iff A \text{ est génératrice.}$$

Démonstration : Soit B une base de E de cardinal n.

(i) B est génératrice donc $|A| \leq |B| = n$. A est libre donc on peut la compléter en une base A' contenant A. Alors $|A'| = n$.

$$|A| = n \iff A = A' \iff A \text{ est une base.}$$

(ii) B est libre donc $n = |B| \leq |A|$. A est génératrice donc on peut en extraire une base A'' incluse dans A. Alors $|A''| = n$.

$$|A| = n \iff A = A'' \iff A \text{ est une base.}$$

(iii) Direct en utilisant (i) et (ii).

□

Proposition 2.13

Un espace vectoriel est de dimension infinie si, et seulement si, il admet une famille libre infinie.

En pratique, pour montrer qu'un espace est de dimension infinie, on cherchera à construire une famille libre de cardinal aussi grand qu'on veut.

Démonstration : Si E est de dimension finie, alors toute famille libre est finie et de cardinal inférieur à $\dim E$, donc E n'admet pas de famille libre infinie. Supposons maintenant que E soit de dimension infinie, et construisons une famille libre infinie par récurrence.

Initialisation $E \neq \{0\}$ (qui est de dimension finie) donc on peut choisir n'importe quel vecteur $x_1 \neq 0$ de E tel que (e_1) soit libre.

Hérédité Soit $n \in \mathbb{N}^*$ et supposons qu'on puisse construire une famille libre $A = (x_1, \ldots, x_n)$. Alors A n'est pas génératrice car E n'est pas de dimension infinie, donc il existe $x_{n+1} \in E \setminus \operatorname{Vect}(A)$. La famille $(x_1, \ldots, x_{n+1})$ est donc libre. □

Proposition 2.14 *Espaces de dimension infinie de référence*

Soit I un intervalle non-trivial de $\mathbb{R}$. Alors les espaces suivants sont de dimension infinie :

1. $\mathcal{F}(I, \mathbb{R})$.
2. $\mathcal{C}^n(I, \mathbb{R})$, pour tout $n \in \mathbb{N} \cup \{\infty\}$.
3. $\mathcal{D}^n(I, \mathbb{R})$, pour tout $n \in \mathbb{N}^*$.
4. $\mathbb{K}^{\mathbb{N}}$.
5. $\mathbb{K}[X]$.
6. $\mathbb{K}(X)$.

Proposition 2.15

Soit $n \in \mathbb{N}^*$. Alors les propositions suivantes sont équivalentes :

(i) E est de dimension finie et $\dim E = n$.
(ii) E est isomorphe à $\mathbb{K}^n$.

Démonstration : $\boxed{(i) \Rightarrow (ii)}$ Soit $B'\left(e_1', \dots, e_n'\right)$ une base de E et soit

$$\Phi : \begin{array}{ccc} \mathbb{K}^n & \to & E \\ (\lambda_1, \dots, \lambda_n) & \mapsto & \sum_{i=1}^n \lambda_i e_i' \end{array}.$$

Par linéarité de la somme, Φ est linéaire. De plus, en notant $B = (e_1, \dots, e_n)$ la base canonique de $\mathbb{K}^n$, pour tout $i \in [\![1, n]\!]$, $f(e_i) = e_i'$. Donc $f(B) = B'$, et B est une base. Donc f est bijective et E et $\mathbb{K}^n$ sont isomorphes.

$\boxed{(ii) \Rightarrow (i)}$ Soit $\Phi : B \to E$ un isomorphisme. En particulier, pour toute base B de $\mathbb{K}^n$, $\Phi(B)$ est une base à n éléments de E. Donc $\dim(E) = n$. □

Corollaire 2.16

Soient E et F deux espaces vectoriels.

(i) Si E et F sont de dimension finie, alors E et F sont isomorphes si, et seulement si, $\dim E = \dim F$.
(ii) Si E et F sont isomorphes et $\dim E = n$, alors F est de dimension finie et $\dim F = n$.

III Propriétés de la dimension

1. Produit cartésien

Rappel : on dit que deux espaces vectoriels E et F sont isomorphes, et on note $E \cong F$, s'il existe $f \in \mathcal{L}(E, F)$ bijective.

Théorème 3.1

Soient E et F deux espaces vectoriels de dimension finie. Alors $E \times F$ est de dimension finie et

$$\dim E \times F = \dim E + \dim F.$$

Démonstration : Si $E = \{0\}$ ou $F = \{0\}$ alors le résultat est clair car $E \times \{0\} \cong E$ et $\{0\} \times F \cong F$. Supposons donc que $n = \dim E \geq 1$ et $m = \dim F \geq 1$. E et F sont respectivement isomorphes à $\mathbb{K}^n$ et $\mathbb{K}^m$. Autrement dit, il existe des isomorphismes $\varphi \in \mathcal{L}(E, \mathbb{K}^n), \psi \in \mathcal{L}(f, \mathbb{K}^m)$. Posons $\Phi : E \times F \to \mathbb{K}^{n+m}$ telle que, pour tout $(u, v) \in E \times F$,

$$\Phi(u, v) = \left(\varphi(u)_1, \dots, \varphi(u)_n, \psi(v)_1, \dots, \psi(v)_m\right).$$

Par linéarité de φ et ψ, il est clair que $\Phi \in \mathcal{L}\left(E \times F, \mathbb{K}^{n+m}\right)$. De plus, φ et ψ étant bijectives, il est clair que Φ est bijective (le vérifier). Donc $E \times F \cong \mathbb{K}^{n+m}$. On en déduit que $E \times F$ est de dimension finie et $\dim E \times F = n + m = \dim E + \dim F$. □

2. Sous-espace vectoriel

Théorème 3.2 *Dimension du produit d'espaces vectoriels*

Soient F un sous-espace vectoriel de E. Si E est de dimension finie, alors F est de dimension finie et $\dim F \leq \dim E$, avec égalité si, et seulement si, $F = E$.

En pratique, on utilisera

$$\begin{cases} F \text{sev de } E \\ \dim F = \dim E \end{cases} \Rightarrow F = E.$$

Démonstration : Si $E = \{0\}$ ou $F = \{0\}$, le résultat est clair. Supposons donc que $\{0\} \subsetneq F$ et notons $n = \dim E \in \mathbb{N}^*$. Soit $x_1 \in F \setminus \{0\}$ et posons $A_1 = (x_1)$.

1. Si $\operatorname{Vect} A_1 = F$, alors on a trouvé une base de F et
$$\dim F = |A_1| = 1 \leq n = \dim E.$$
2. Sinon, soit $x_2 \in F \setminus \operatorname{Vect} A_1$ et on pose $A_2 = A_1 \cup (x_2)$. On reprend alors à la première étape en considérant A_2.

Cet algorithme termine en au plus n étapes. [2] Il existe donc $p \in [\![1, n]\!]$ tel que A_p est une base de F, donc F est de dimension finie, et

$$\dim F = |A_p| = p \leq n = \dim E.$$

D'autre part, comme on l'a dit,

$$p = n \iff \begin{cases} E = \operatorname{Vect} A_p \\ F = \operatorname{Vect} A_p \end{cases} \iff E = F.$$

□

Cet algorithme ne permet pas de construire une base de F en pratique, car il faut choisir des vecteurs $x_1, \ldots, x_p$ sans vraiment savoir lesquels prendre. Pour trouver une base de F, on manipulera plutôt des systèmes linéaires comme on en a déjà l'habitude (pour décrire le noyau ou l'image d'un morphisme, par exemple).

Corollaire 3.3

Soit E un espace vectoriel de dimension finie et F un sous-espace vectoriel de E. Alors F admet au moins un supplémentaire dans E.

Démonstration : Soit B_F une base de E. D'après le théorème de la base incomplète, on peut compléter B_F en une base B de E et poser $B_G = B \setminus B_F$ et $G = \operatorname{Vect} B$. Alors on a

$$F + G = \operatorname{Vect} B_F + \operatorname{Vect} B_G = \operatorname{Vect} (B_F \cup B_G) = \operatorname{Vect} B = E.$$

Soit $x \in F \cap G$. Notons (si $F \neq \{0\}$ et $G \neq \{0\}$) $B_F = (x_1, \ldots, x_p)$ et $G = (x_{p+1}, \ldots, x_n)$. Alors il existe $\lambda_1, \ldots, \lambda_n$ tels que

$$x = \sum_{i=1}^{p} \lambda_i x_i = \sum_{i=p+1}^{n} \lambda_i x_i, \quad \sum_{i=1}^{p} \lambda_i x_i - \sum_{i=p+1}^{n} \lambda_i x_i = 0, \quad \lambda_1 = \cdots = \lambda_n = 0$$

car B est libre, donc $x = 0$, donc $F \cap G = \{0\}$ et $F \oplus G = E$. □

2. Si on en arrive à construire $A_1 \subsetneq \cdots \subsetneq A_n$, alors il est clair que $E = \operatorname{Vect} A_n$: A_n est libre et de cardinal n, c'est une base de E.

3. Somme et somme directe

Lemme 3.4
Soient F et G deux sous-espaces vectoriels de E. Si F et G sont en somme directe et de dimension finie, alors $F \oplus G$ est de dimension finie et $\dim F \oplus G = \dim F + \dim G$.

Démonstration : La fonction

$$\Phi : \begin{array}{ccc} F \times G & \to & F \oplus G \\ (u,v) & \mapsto & u+v \end{array}.$$

est linéaire, injective (car $F \cap G = \{0\}$) et surjective (évident). Φ est donc un isomorphisme d'espaces vectoriels, $F \oplus G$ est de dimension finie et $\dim F \oplus G = \dim F \times G = \dim F + \dim G$. $\square$

Théorème 3.5 *Formule de Grassmann*
Soit E un espace vectoriel de dimension finie et soient F, G deux sous-espaces vectoriels de E. Alors $F + G$ est de dimension finie et

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

Démonstration : D'abord, $F, G, F \cap G$ et $F + G$ sont de dimension finie, car ce sont des sev de E. $F \cap G$ est un sev de G donc il admet un supplémentaire dans G, qu'on note G'. On a ainsi

$$F \cap G \oplus G' = G.$$

Montrons que $F \oplus G' = F + G$. Soit $x \in F + G$. Alors il existe $(f, g) \in F \times G$ tel que $x = f + g$. Et il existe $(f', g') \in (F \cap G) \times G'$ tel que $g = f' + g'$. Alors

$$x = (f + f') + g' \in F + G'.$$

De plus, puisque $G' \subseteq G$,

$$F \cap G' = F \cap (G' \cap G) = (F \cap G) \cap G' = \{0\}.$$

Donc $F \oplus G' = F + G$. D'après le lemme 3.4, on a

$$\begin{aligned} \dim G' &= \dim G - \dim (F \cap G), \\ \dim (F+G) &= \dim F + \dim G' = \dim F + \dim G - \dim (F \cap G). \end{aligned}$$

$\square$

Il s'agit exactement de la même formule que $|A| \cup B = |A| + |B| - |A \cap B|$. Et c'est normal, puisque manipuler des dimensions revient à manipuler des bases.

Théorème 3.6 *Caractérisation dimensionnelle de la somme directe*
Soit E un espace vectoriel de dimension finie et soient F, G deux sous-espaces vectoriels de E. Si $\dim F + \dim G = \dim E$, alors on a équivalence entre les trois propriétés suivantes :

(i) $F \cap G = \{0\}$.
(ii) $F + G = E$.
(iii) $F \oplus G = E$.

Démonstration : On a

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

Puisque $F + G \subseteq E$, on a

$$F + G = E \iff \dim F + G = \dim E \iff \dim F \cap G = 0 \iff F \cap G = \{0\}.$$

Donc $(i) \iff (ii)$. De plus, par définition,

$$(i) \wedge (ii) \iff (iii),$$

ce qui achève la preuve. □

Proposition 3.7

Soit E un espace vectoriel de dimension $n \in \mathbb{N}^*$ et H un sous-espace vectoriel de E. Alors

$$H \text{ est un hyperplan de } E \iff \dim H = n - 1.$$

Démonstration : Par définition, H est un hyperplan si, et seulement si, il existe $u \in E \setminus \{0\}$ tel que $H \oplus \mathbb{K}u = E$, et, pour tout $u \in E \setminus \{0\}, \dim(\mathbb{K}u) = 1$. L'implication est donc évidente. Réciproquement, supposons que $\dim H = n-1$. Alors il existe $u \in E \setminus H$. Donc $\mathbb{K}u \cap H = \{0\}$ et $\dim H + \dim \mathbb{K}u = \dim E$ donc $H \oplus \mathbb{K}u = E$. Donc H est un hyperplan de E. □

Lemme 3.8 *Caractérisation des formes linéaires*

Soit $n \in \mathbb{N}^*$ et soient $\lambda_1, \ldots, \lambda_n \in \mathbb{K}^n$. Alors l'application

$$\begin{array}{cccc} f & \mathbb{K}^n & \to & \mathbb{K} \\ & (x_1, \ldots, x_n) & \mapsto & \displaystyle\sum_{i=1}^{n} \lambda_i x_i \end{array}$$

est une forme linéaire de $\mathbb{K}^n$.

Démonstration : Evident par définition. □

On pourra utiliser ce résultat pour montrer plus rapidement que des sous-ensembles de $\mathbb{K}^n$ sont des sev.

Exercice 3.9 :
Soient

$$F = \{(x,y,z,t) \in \mathbb{R}^4 / 2x + y - z + t = 0 = 0 \text{ et } 3x - t = 0\}, \quad G = \{(x,y,z,t) \in \mathbb{R}^4 / y = z = t\}.$$

1. Montrer que F et G sont des espaces vectoriels de dimension finie et déterminer leur dimension.
2. Montrer que $F \oplus G = \mathbb{R}^4$.

Réponse

1. Les applications

$$\begin{array}{cccc} f & \mathbb{R}^4 & \to & \mathbb{R} \\ & (x,y,z,t) & \mapsto & 2x+y-z+t \end{array}, \quad \begin{array}{cccc} g & \mathbb{R}^4 & \to & \mathbb{R} \\ & (x,y,z,t) & \mapsto & 3x-t \end{array}.$$

sont des formes linéaires de $\mathbb{R}^4$. Alors $F = \ker f \cap \ker g$, donc F est un sev de $\mathbb{R}^4$. C'est donc un espace vectoriel de dimension finie et $\dim F \leq 4$. De même, G est un sev de $\mathbb{R}^4$. Pour tout $u = (x,y,z,t) \in \mathbb{R}^4$, on a

$$u \in F \iff \begin{cases} 2x+y-z+t=0=0 \\ 3x-t=0 \end{cases} \iff \begin{cases} z=5x+y \\ t=3x \end{cases}$$
$$\iff u = x\,(1,0,5,3) + y\,(0,1,1,0)\,.$$

Donc $F = \text{Vect}\left((1,0,5,3)\,,(0,1,1,0)\right)$ et ces deux vecteurs ne sont pas colinéaires, ils forment donc une base de F. Donc $\dim F = 2$. De même, $G = \text{Vect}\left((1,0,0,0)\,,(0,1,1,1)\right)$ et $\dim G = 2$.

2. Pour tout $u = (x,y,z,t) \in \mathbb{R}^4$, on a

$$u \in F \cap G \iff \begin{cases} 2x+y-z+t=0=0 \\ 3x-t=0 \\ t=y \\ z=y \end{cases} \iff x=y=z=t=0$$

Donc $F \cap G = \{0\}$. De plus, $\dim F + \dim G = 4 = \dim \mathbb{R}^4$ donc $F \oplus G = \mathbb{R}^4$.

◊

IV Dimension et applications linéaires

1. Rang d'une famille de vecteurs

Définition 4.1 *Rang d'une famille*

Soit A une famille de vecteurs de E. Si $\text{Vect}\,A$ est de dimension finie, on dit que A est de rang fini et on définit le rang de A par

$$\text{rg}\,(A) = \dim\left(\text{Vect}\,(A)\right).$$

On remarquera que si A est une famille de cardinal fini, alors elle est nécessairement de rang fini.

Proposition 4.2

Soit A une famille finie d'un espace vectoriel E. Alors

(i) Si E est de dimension finie, alors $\text{rg}\,A \le \dim E$.
(ii) $\text{rg}\,A \le |A|$ avec égalité si et seulement si A est libre.

Exercice 4.3 :
Soit $E = \mathbb{R}^3$ et soient $u_1 = (1,2,-2)\,, u_2 = (3,-6,-2)\,, u_3 = (1,-10,2)$. Déterminer le rang de (u_1,u_2,u_3).

Réponse

La famille A est liée (car $u_3 = u_2 - 2u_1$). D'autre part, (u_1,u_2) est libre, c'est donc une base de $\text{Vect}\,A$. Donc $\text{rg}\,A = \dim \text{Vect}\,A = 2$.

◊

2. Rang d'une application linéaire

Lemme 4.4

Si A est une famille de E, alors $f(\operatorname{Vect} A) = \operatorname{Vect} f(A)$. En particulier, si A est une famille génératrice de E, alors $\operatorname{Im} f = \operatorname{Vect} A$.

Ce lemme est évident par linéarité de f. Il donne de plus une nouvelle méthode pour déterminer l'image d'une application linéaire.

Définition 4.5 *Rang d'une application linéaire*

Soit $f \in \mathcal{L}(E, F)$. Si $\operatorname{Im} f$ est de dimension finie, on dit que f est de rang fini et on définit le rang de f par

$$\operatorname{rg}(f) = \dim(\operatorname{Im}(f)).$$

Exercice 4.6 :
Soit $E = \mathbb{R}^3$ et soient $u_1 = (1, 2, -2), u_2 = (3, -6, -2), u_3 = (1, -10, 2)$. On note $A = (u_1, u_2, u_3)$ et $B = (e_1, e_2, e_3)$ la base canonique de E.

1. Déterminer le rang de A.
2. (a) Montrer qu'il existe une unique application linéaire $f \in \mathcal{L}(E)$ telle que, pour tout $i \in [\![1, 3]\!]$, $f(e_i) = u_i$.
   (b) Exprimer $f(x, y, z)$ pour tout $(x, y, z) \in \mathbb{R}^3$.
   (c) Déterminer $\operatorname{rg} f$.

Réponse

1. On a déjà démontré à l'exercice précédent que $\operatorname{rg} A = 2$.
2. (a) Evident d'après le théorème 1.24.
   (b) On a $f(x, y, z) = (x + 3y + z, 2x - 6y - 10z, -2x - 2y + 2z)$ pour tout $(x, y, z) \in \mathbb{R}^3$.
   (c) On pourrait déterminer à la main $\operatorname{Im} f$ et montrer que $\dim \operatorname{Im} f = 2$. Mais en toute généralité, on a

$$\operatorname{Im}(f) = f(E) = f(\operatorname{Vect} B) = \operatorname{Vect} f(B) = \operatorname{Vect} A.$$

   Donc $\operatorname{rg} f = \operatorname{rg} A$.

$\diamondsuit$

Proposition 4.7

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

(i) Si E est de dimension finie, alors f est de rang fini et

$$\operatorname{rg} f \leq \dim E$$

avec égalité si, et seulement si, f est injective.

(ii) Si F est de dimension finie, alors f est de rang fini et

$$\operatorname{rg} f \leq \dim F$$

avec égalité si, et seulement si, f est surjective.

(iii) Si E et F sont de dimension finie, alors

$$f \text{ est bijective } \iff \dim E = \dim F = \operatorname{rg} f.$$

Démonstration : (i) Soit B une base de E. Alors $\operatorname{Im} f = \operatorname{Vect} f(B)$ d'après le lemme précédent. Donc $\operatorname{rg} f = \dim \operatorname{Im} f \leq \dim E$. De plus,

$$f \text{ est injective } \iff f(B) \text{ est libre } \iff f(B) \text{ est une base de } \operatorname{Im} f \iff \operatorname{rg} f = \dim E.$$

(ii) $\operatorname{Im} f$ est de dimension finie car c'est un sev de F. De plus,

$$f \text{ est surjective } \iff \operatorname{Im} f = F \iff \operatorname{rg} \operatorname{Im} f = \dim F.$$

(iii) Evident d'après (i) et (ii).

□

3. Théorème du rang

Théorème 4.8 *Isomorphisme entre un supplémentaire du noyau et image*

Soit $f \in \mathcal{L}(E, F)$. Supposons que E soit de dimension finie, et soit H un supplémentaire de $\ker f$ dans E. Alors

$$\widetilde{f} : \begin{array}{ccc} H & \to & \operatorname{Im} f \\ x & \mapsto & f(x) \end{array}$$

est un isomorphisme d'espaces vectoriels.

Démonstration : Puisque E est de dimension finie, $\ker f$ admet un supplémentaire H dans E :

$$\ker f \oplus H = E, \quad \dim H = \dim E - \dim \ker f.$$

Notons $\widetilde{f} = f_{|H}$. $\widetilde{f}$ est une application linéaire (en tant que restriction d'une application linéaire à un sev). D'autre part, $\operatorname{Im} \widetilde{f} \subseteq \operatorname{Im} f$ donc $\widetilde{f} \in \mathcal{L}(H, \operatorname{Im} f)$.

Montrons que $\widetilde{f}$ est un isomorphisme. Soit $x \in \ker \widetilde{f}$. Alors $f(x) = 0$ donc $x \in H \cap \ker f = \{0\}$ donc $x = 0$ donc $\widetilde{f}$ est injective. Soit $y \in \operatorname{Im} f$. Alors il existe $x \in E$ et $(x_K, x_H) \in \ker f \times H$ tels que

$$y = f(x), \quad x = x_K + x_H, \quad \widetilde{f}(x_H) = f(x) - f(x_K) = f(x) = y.$$

Donc $y \in \operatorname{Im} \widetilde{f}$ donc $\widetilde{f}$ est surjective donc bijective. □

Corollaire 4.9 *Théorème du rang*

Soit $f \in \mathcal{L}(E, F)$. Si E est de dimension finie, alors

$$\dim E = \operatorname{rg} f + \dim(\ker f).$$

Démonstration : Avec les notations du théorème précédent, H et $\operatorname{Im} f$ étant isomorphes, $\operatorname{Im} f$ est de dimension finie et

$$\operatorname{rg} f = \dim \operatorname{Im} f = \dim H = \dim E - \dim \ker f.$$

□

Théorème 4.10 *Caractérisation des isomorphismes en dimension finie*

Soient E et F deux espaces vectoriels de dimension finie tels que $\dim E = \dim F = n \in \mathbb{N}$. Alors on a équivalence entre les propriétés suivantes :

(i) f est bijective
(ii) f est injective
(iii) f est surjective
(iv) $\operatorname{rg} f = n$.

Démonstration : Remarquons que, par définition,

$$(iii) \iff (iv), \quad (i) \iff (ii) \wedge (iii).$$

De plus, d'après le théorème du rang,

$$(i) \iff \ker f = \{0\} \iff \dim \ker f = 0 \iff \operatorname{rg} f = n \iff (iv) \iff (iii).$$

□

Evidemment, ce résultat est grossièrement faux en dimension infinie, ou si E et F n'ont pas même dimension.

Exercice 4.11 :
Soit $D : \mathbb{C}[X] \to \mathbb{C}[X]$ telle que, pour $P \in \mathbb{C}[X]$, $D(P) = P'$. On a déjà vu que D est un endomorphisme de $\mathbb{C}[X]$.

1. Déterminer $\ker D$.
2. En considérant $D_{|\mathbb{C}_n[X]}$, déterminer $\operatorname{Im} D$.
3. Conclure.

Réponse

1. Soit $P \in \mathbb{C}[X]$. On sait que $P' = 0$ si, et seulement si, $P \in \mathbb{C}_0[X]$. Donc $\ker D = \mathbb{C}_0[X]$.
2. Soit $n \in \mathbb{N}^*$. Pour tout $P \in \mathbb{C}_n[X]$,

   $$\deg (D(P)) \leq \deg P \leq n$$

   donc $\mathbb{C}_n[X]$ est stable par D. Notons $D_n = D_{|\mathbb{C}_n[X]} \in \mathcal{L}(\mathbb{C}_n[X])$. De plus, puisque

   $$\ker D \subseteq \mathbb{C}_n[X], \quad \ker D_n = \ker D.$$

   Donc d'après le théorème du rang, $\operatorname{rg} D_n = n$. De plus, pour tout $P \in \mathbb{C}_n[X]$, si $\deg P = n$ alors $\deg (D_n(P)) = n-1$ donc $\operatorname{Im} D_n \subseteq \mathbb{C}_{n-1}[X]$ et $\dim(\operatorname{Im} D_n) = \dim(\mathbb{C}_{n-1}[X])$. Donc

   $$\operatorname{Im} D_n = \mathbb{C}_{n-1}[X].$$

   Finalement, pour tout $Q \in \mathbb{C}[X]$, il existe $n \in \mathbb{N}^*$ tel que $Q \in \mathbb{C}_{n-1}[X]$. Donc

   $$\exists P \in \mathbb{C}_n[X], Q = D_n(P) = D(P).$$

   Donc D est surjective.
3. En dimension infinie, une application linéaire surjective n'est donc pas nécessairement injective.

$\diamondsuit$

Exercice 4.12 :
Soit $f : \mathbb{R}^{\mathbb{N}} \to \mathbb{R}^{\mathbb{N}}$ telle que, pour $(u_n) \in \mathbb{R}^{\mathbb{N}}$,

$$f\left((u_0, u_1, u_2, u_3, \dots)\right) = (0, u_0, u_1, u_2, \dots).$$

1. Montrer que f est un endomorphisme de $\mathbb{R}^{\mathbb{N}}$.
2. Déterminer $\ker f$.
3. Montrer que f n'est pas surjective
4. Conclure.

Réponse

1. Evident en revenant à la définition.
2. Pour toute suite $(u_n) \in \mathbb{R}^{\mathbb{N}}$, on a

$$(u_n) \in \ker f \iff (0, u_0, u_1, \dots) = (0, 0, 0, \dots) \iff \forall n \in \mathbb{N}, u_n = 0 \iff (u_n) = 0.$$

   Donc $\ker f = \{0\}$ et donc f est injective.
3. Il est clair que $1 \notin \operatorname{Im} f$ donc f n'est pas surjective.
4. En dimension infinie, une application linéaire injective n'est donc pas nécessairement surjective.

$\diamondsuit$

V À connaître à la fin du chapitre

1. Familles

- Déterminer si une famille est libre/génératrice/base.
- Comparer les cardinaux de familles libres et génératrices.
- Compléter une famille libre en une base. Extraire une base d'une famille génératrice.

2. Applications linéaires

- Connaître les liens entre libre/générateur et injectif/surjectif.
- Déterminer l'image d'une application linéaire à l'aide d'une partie génératrice de l'espace de départ.
- Déterminer le rang ou la dimension du noyau d'un morphisme, et savoir l'appliquer au calcul de l'injectivité et de la surjectivité.
- Savoir utiliser la dimension pour optimiser les raisonnements.

3. Espaces vectoriels

- Reconnaître les espaces de dimension finie de référence.
- Montrer qu'un espace vectoriel est de dimension finie et en déterminer une base.
- Connaître les liens entre bases et espaces supplémentaires.
- Passer de l'équation cartésienne à une base et inversement pour les sous-espaces de $\mathbb{R}^n$.
- Savoir utiliser la dimension pour optimiser les raisonnements.

CHAPITRE 10

INTÉGRATION SUR UN SEGMENT

C'est Sinus qui emmène son pote Cosinus dans un boîte qu'il connaît, remplie de sinus. Alors que Sinus picole et drague, Cosinus se morfond au bar. Sinus arrive et lui dit "Allez viens mon vieux, je vais t'aider à t'intégrer".

Blague mathématique

Ce chapitre est la suite (et fin) du cours d'analyse de première année, à la suite du cours de continuité et de celui de dérivation. Il est important de connaître et de comprendre ces deux sujets.

Dans la suite, a et b sont des nombres réels tels que $a < b$ et $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. On introduit dans ce chapitre la notion d'intégrale sur le segment $[a, b]$, avant de voir dans un prochain chapitre comment on peut intégrer sur un ensemble plus général.

I Construction de l'intégrale de Riemann

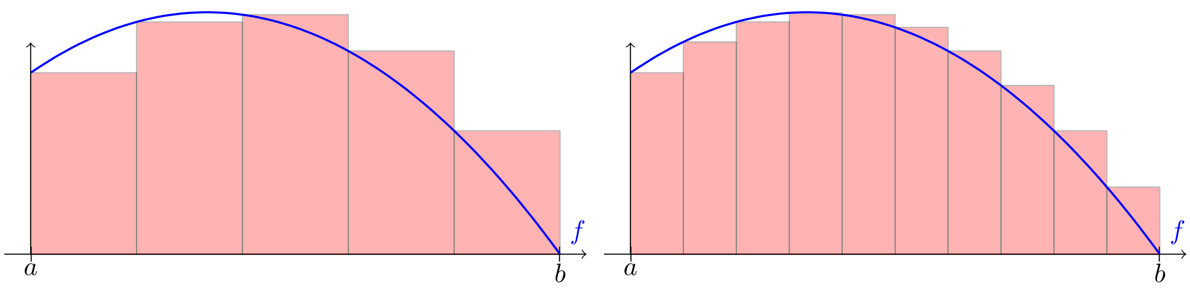
Cette première partie est relativement théorique, et nous allons la couvrir rapidement sans rentrer dans les détails des preuves. L'idée est de comprendre comment on construit l'intégrale de Riemann.[1] Il s'agit de la seule intégrale enseignée en cycle préparatoire, mais il est possible de créer d'autres intégrales (pour d'autres types de fonctions).

1. Idée principale

L'intégrale d'une fonction f est l'aire algébrique (positive ou négative) sous la courbe de f. Pour pouvoir définir une telle quantité, on a besoin de considérer f dans une certaine classe de fonctions. Par exemple, si $f = \mathbb{1}_{\mathbb{Q}}$, on aura bien du mal à donner un sens à l'aire sous la courbe.

La classe de fonctions que l'on choisit ici sont les fonctions continues par morceaux (on pourra simplement penser aux fonctions continues dans un premier temps). On peut approcher l'aire sous la courbe d'une fonction continue par une somme d'aires de rectangles bien choisis. La limite de cette somme donnera l'aire sous la courbe :

1. Bernhard Riemann (1826-1866) : Mathématicien allemand.



2. Définition de l'intégrale

Définition 1.1 *Subdivision*

On appelle *subdivision de l'intervalle* $[a,b]$ toute famille $(x_0,\dots,x_n)$ avec $n\in\mathbb{N}^*$ telle que

$$a=x_0<x_1<\cdots<x_{n-1}<x_n=b.$$

On appelle *subdivision régulière de l'intervalle* $[a,b]$ *de pas* $\frac{1}{n}$ la subdivision $(x_0,\dots,x_n)$ définie par

$$\forall i\in[\![0,n]\!],\quad x_i=a+\frac{i\,(b-a)}{n}.$$

Définition 1.2 *Fonction en escalier*

Soit $\varphi\in\mathcal{F}([a,b],\mathbb{K})$. On dit que φ est *en escalier sur* $[a,b]$ s'il existe une subdivision $(x_0,\dots,x_n)$ telle que, pour tout $i\in[\![1,n]\!]$, φ est constante sur $]x_{i-1},x_i[$.

On note $\mathcal{E}([a,b],\mathbb{K})$ l'ensemble des fonctions en escalier sur $[a,b]$ à valeurs dans $\mathbb{K}$.

On dira qu'une telle subdivision est *adaptée* à φ.

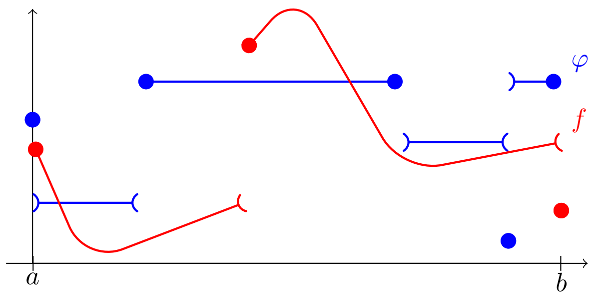
Définition 1.3 *Continuité par morceaux*

Soit $f\in\mathcal{F}([a,b],\mathbb{K})$. On dit que f est *continue par morceaux sur* $[a,b]$ s'il existe une subdivision $(x_0,\dots,x_n)$ telle que, pour tout $i\in[\![1,n]\!]$, f est continue sur $]x_{i-1},x_i[$, admet une limite à droite finie en x_{i-1} et une limite à gauche finie en x_i.

On note $\mathcal{C}^0_m([a,b],\mathbb{K})$ l'ensemble des fonctions continues par morceaux sur $[a,b]$ à valeurs dans $\mathbb{K}$.

On remarquera qu'on n'impose rien sur les valeurs de $f(x_i)$, mais les fonctions continues par morceaux doivent avoir des limites finies à gauche et à droite en tout point de la subdivision.

Modifier la valeur d'une fonction continue par morceaux <u>en un point</u> ne change pas sa nature.



Exemple 1.4 :
La fonction partie entière E est en escalier (donc continue par morceaux) sur $[-2.5, 2.5]$.

La fonction f définie par

$$\forall x \in [-1,1], \quad f(x) = \begin{cases} \sin x & \text{si } x < 0 \\ -1 & \text{si } x = 0 \\ \mathrm{e}^x & \text{si } x > 0 \end{cases}$$

est continue par morceaux sur $[-1, 1]$.

La fonction g définie par

$$\forall x \in [0,1], \quad g(x) = \begin{cases} \cos \frac{1}{x} & \text{si } x > 0 \\ 0 & \text{si } x = 0 \end{cases}$$

n'est pas continue par morceaux sur $[0, 1]$. ♢

Proposition 1.5
Une fonction continue par morceaux sur un segment est bornée.

Démonstration : Soit $f \in \mathcal{C}^0_m([a,b])$ et soit $(x_0, \ldots, x_n)$ une subdivision adaptée à f. Soit $k \in [\![1, n]\!]$. Par définition, f admet une limite finie en x_{k-1} et en x_k et est continue sur $]x_{k-1}, x_k[$, elle est donc prolongeable par continuité sur $[x_{k-1}, x_k]$ (on note $\widetilde{f}$ son prolongement). Alors $\widetilde{f}$ est continue sur un segment, donc bornée, donc f est bornée sur $]x_{k-1}, x_k[$. On en déduit que f est bornée sur $[a,b] \setminus \{x_0, \ldots, x_n\}$. On en déduit finalement que f est bornée sur $[a, b]$. □

⚠ Contrairement aux fonctions continues, les fonctions continues par morceaux n'atteignent pas forcément leurs bornes.

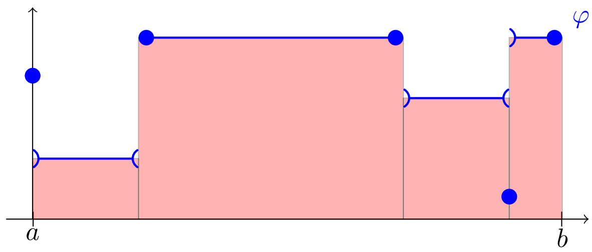
Définition/Théorème 1.6 *Intégrale d'une fonction en escalier*
Soit $\varphi \in \mathcal{E}([a,b], \mathbb{R})$. Soit $(x_0, \ldots, x_n)$ une subdivision adaptée à φ. On note

$$\forall i \in [\![1, n]\!], \quad \lambda_i = \varphi\left(\frac{x_{i-1} + x_i}{2}\right).$$

On appelle *intégrale de φ sur $[a, b]$* le nombre

$$\int_{[a,b]} \varphi = \int_a^b \varphi = \int_a^b \varphi(t)\, dt = \sum_{i=1}^{n} \lambda_i (x_i - x_{i-1}).$$

Ce nombre est indépendant de la subdivision $(x_0, \dots, x_n)$ choisie.



L'intégrale de φ est simplement l'aire algébrique sous la courbe, c'est-à-dire comptée positivement si $\lambda_i \geq 0$ et négativement si $\lambda_i \leq 0$.

On se sert de cette définition pour définir l'aire d'une fonction continue par morceaux sur un segment.

Définition/Théorème 1.7 *Intégrale d'une fonction continue par morceaux réelle*

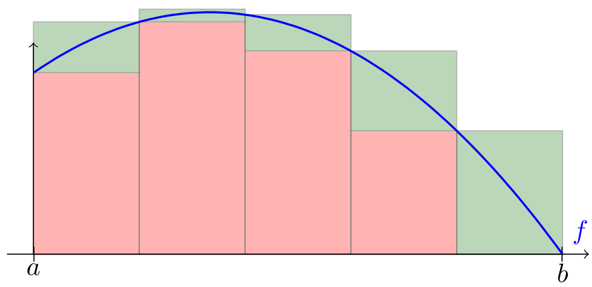
Soit $f \in \mathcal{C}^0_m([a,b], \mathbb{R})$. On définit

$$A_f = \left\{ \int_a^b \varphi(t)\, dt \Big/ \varphi \in \mathcal{E}([a,b]), \varphi \leq f \right\} \subseteq \mathbb{R}$$

$$B_f = \left\{ \int_a^b \psi(t)\, dt \Big/ \psi \in \mathcal{E}([a,b]), f \leq \psi \right\} \subseteq \mathbb{R}$$

Alors A_f admet une borne supérieure, B_f admet une borne inférieure et ces deux nombres sont égaux. On appelle *intégrale de f sur* $[a,b]$ le nombre

$$\int_{[a,b]} f = \int_a^b f = \int_a^b f(t)\, dt = \sup A_f = \inf B_f.$$



En pratique, on n'utilise évidemment pas cette définition pour calculer des intégrales : on utilise les primitives et formules classiques qu'on reverra un peu plus tard.

Définition 1.8 *Intégrale d'une fonction continue par morceaux complexe*

Soit $f \in \mathcal{C}^0_m([a,b], \mathbb{C})$. Alors on définit

$$\int_a^b f = \int_a^b \mathfrak{Re}(f) + i \int_a^b \mathfrak{Im}(f).$$

Modifier la valeur d'une fonction continue par morceaux en un point ne change pas son intégrale.

Remarque 1.9 : Par convention, on pose pour $a < b$

$$\int_b^a f = -\int_a^b f.$$

Cela permet de simplifier l'écriture de nombreux calculs, mais on fera très attention lors des inégalités, notamment lorsqu'on manipule des fonctions positives ou lorsqu'on utilise l'inégalité triangulaire. $\diamondsuit$

3. Sommes de Riemann

La définition de l'intégrale d'une fonction f continue par morceaux (comme borne supérieure ou inférieure d'un ensemble) n'est pas commode pour faire des calculs pratiques. Par contre, on peut aussi voir l'intégrale de f comme limite d'intégrales de fonctions en escalier bien choisies.

Définition/Théorème 1.10

Soit $f \in \mathcal{C}^0_m([a,b],\mathbb{K})$ et soit $\left(x_0^{(n)},\dots,x_n^{(n)}\right)$ la subdivision régulière de $[a,b]$, c'est-à-dire que

$$\forall n \in \mathbb{N}^*, \forall k \in [\![1,n]\!], \quad x_k^{(n)} = a + \frac{k(b-a)}{n}.$$

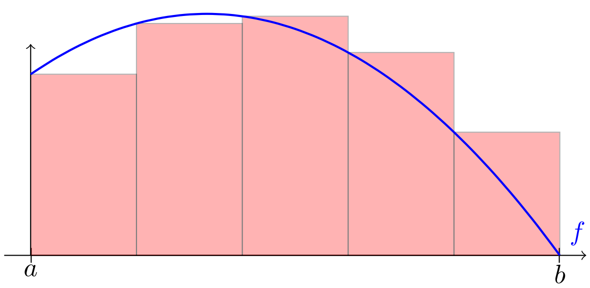
On appelle *somme de Riemann de f* tout nombre de la forme

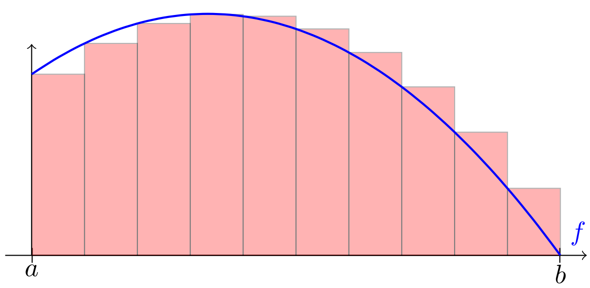
$$S_n = \frac{b-a}{n}\sum_{k=1}^{n} f\left(\omega_k^{(n)}\right), \quad \forall k \in [\![1,n]\!], \quad \omega_k^{(n)} \in \left[x_{k-1}^{(n)}, x_k^{(n)}\right].$$

On a alors

$$\lim_{n\to+\infty} S_n = \int_a^b f.$$

Autrement dit, la limite de toute somme de Riemann d'une fonction converge vers l'intégrale de cette dernière. On notera que S_n dépend du choix des $\omega_k^{(n)}$. Lorsque $\omega_k^{(n)} = x_{k-1}^{(n)}$ ou $\omega_k^{(n)} = x_k^{(n)}$, cela s'appelle la méthode des rectangles (pour calculer l'intégrale de f).



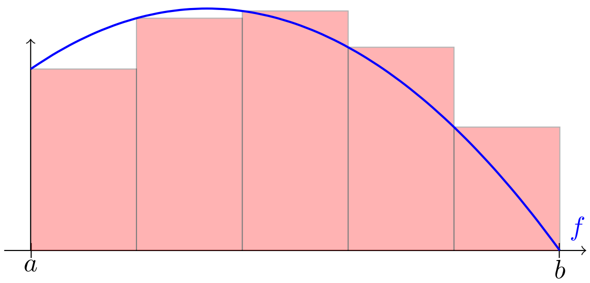


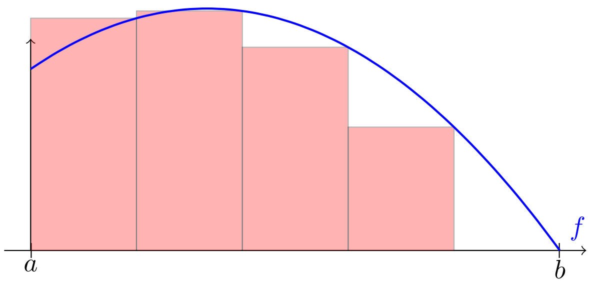
Proposition 1.11 *Méthode des rectangles*

Soit $f \in \mathcal{C}^0_m([a,b],\mathbb{K})$. Alors

$$\frac{b-a}{n}\sum_{k=0}^{n-1} f\left(a+\frac{k(b-a)}{n}\right) \xrightarrow[n\to+\infty]{} \int_a^b f, \quad \frac{b-a}{n}\sum_{k=1}^{n} f\left(a+\frac{k(b-a)}{n}\right) \xrightarrow[n\to+\infty]{} \int_a^b f.$$

On parle de méthode des rectangles à gauche (si $\omega_k^{(n)} = x_{k-1}^{(n)}$) ou à droite (si $\omega_k^{(n)} = x_k^{(n)}$) pour calculer une intégrale. Il s'agit de méthodes que l'on peut implémenter facilement sur n'importe quel logiciel de programmation. [2]





Proposition 1.12 *Méthode des trapèzes*

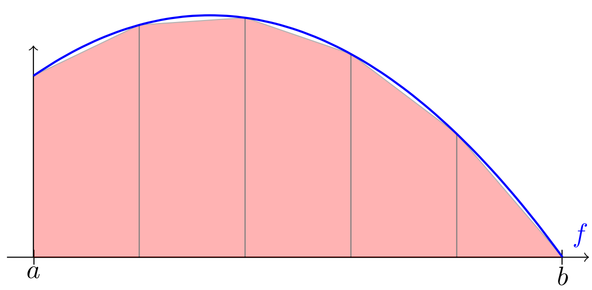
Soit $f \in \mathcal{C}^0_m([a,b],\mathbb{K})$. Alors

$$\frac{b-a}{n}\sum_{k=1}^{n} \frac{f\left(a+\frac{(k-1)(b-a)}{n}\right)+f\left(a+\frac{k(b-a)}{n}\right)}{2} \xrightarrow[n\to+\infty]{} \int_a^b f.$$

Démonstration : D'après les méthodes des rectangles,

$$\begin{aligned}
&\frac{b-a}{n}\sum_{k=1}^{n} \frac{f\left(a+\frac{(k-1)(b-a)}{n}\right)+f\left(a+\frac{k(b-a)}{n}\right)}{2}\\
&= \frac{1}{2}\left[\frac{b-a}{n}\sum_{k=0}^{n-1} f\left(a+\frac{k(b-a)}{n}\right)+\frac{b-a}{n}\sum_{k=1}^{n} f\left(a+\frac{k(b-a)}{n}\right)\right]\\
&\xrightarrow[n\to+\infty]{} \frac{1}{2}\left[\int_a^b f+\int_a^b f\right] = \int_a^b f.
\end{aligned}$$

□



2. En pratique, toutefois, ce n'est pas la méthode que les logiciels de calcul utilisent de nos jours.

Dans les exercices, toutefois, il est souvent plus facile de calculer une intégrale qu'une somme. On utilisera alors les résultats de convergence des sommes de Riemann pour calculer la limite d'une suite (en fonction d'une intégrale).

Exemple 1.13 :
Déterminons la limite de la suite (u_n) définie par

$$\forall n \in \mathbb{N}^*, \quad u_n = \frac{1}{n}\sum_{k=0}^{n-1} \frac{k}{\sqrt{4n^2 - k^2}}.$$

On a, pour tout $n \in \mathbb{N}^*$,

$$u_n = \sum_{k=0}^{n-1} \frac{\frac{k}{n}}{n\sqrt{4 - \left(\frac{k}{n}\right)^2}} = \frac{1}{n}\sum_{k=0}^{n-1} f\left(\frac{k}{n}\right), \quad f : x \mapsto \frac{x}{\sqrt{4 - x^2}}.$$

La fonction f est continue sur $[0,1]$, et (u_n) est la suite de ses sommes de Riemann (ici, c'est la méthode des rectangles à gauche). De plus, on a

$$\int_0^1 \frac{t}{\sqrt{4-t^2}}dt = [-\sqrt{4-t^2}]_{t=0}^1 = \sqrt{4} - \sqrt{3}.$$

On en déduit que

$$\lim_{n\to+\infty} u_n = \sqrt{4} - \sqrt{3}.$$

$\diamondsuit$

Remarque 1.14 : Avant de passer aux calculs pratiques, on pourrait se demander quels sont les problèmes qui se posent lorsque l'on cherche à définir l'intégrale sur un intervalle I quelconque. Ils sont principalement de deux types :

- Si I n'est pas borné, l'aire sous la courbe peut être "infinie". Il est assez facile de comprendre que $\displaystyle\int_{[0,+\infty[} 1$ va poser des problèmes.
- Même si I est borné, on peut avoir des problèmes si I est ouvert en a ou b. De la même manière, on peut se douter que $\displaystyle\int_{]0,1]} \frac{dt}{t}$ risque de poser quelques problèmes de définition.

$\diamondsuit$

II Propriétés de l'intégrale

1. Manipulation de l'intégrale

Proposition 2.1

Soient $f, g \in \mathcal{C}_m^0([a,b],\mathbb{K})$. Alors

(i) Linéarité : Pour tous $\lambda, \mu \in \mathbb{K}$, on a

$$\int_a^b (\lambda f + \mu g) = \lambda\int_a^b f + \mu\int_a^b g.$$

(ii) Positivité : Si $\mathbb{K} = \mathbb{R}$ et $f \geq 0$ sur $[a,b]$ alors $\displaystyle\int_a^b f \geq 0$.

(iii) Monotonie : Si $\mathbb{K} = \mathbb{R}$ et $f \leq g$ sur $[a,b]$ alors $\displaystyle\int_a^b f \leq \int_a^b g$.

(iv) Inégalité triangulaire : On a

$$\left|\int_a^b f\right| \leq \int_a^b |f|.$$

(v) Relation de Chasles[3] : Pour tout $c \in [a,b]$, on a

$$\int_a^b f = \int_a^c f + \int_c^b f.$$

Démonstration : On ne démontre pas ces résultats, qui sont plus techniques qu'il n'y paraît. Il faut en effet les démontrer pour les fonctions en escalier puis les étendre aux fonctions continues par morceaux. □

On notera que la relation de Chasles se généralise à tous a, b, c, sans tenir compte de l'ordre. Dès qu'on peut écrire ces intégrales, on a

$$\int_a^b f = \int_a^c f + \int_c^b f.$$

Lemme 2.2

Soit $f \in \mathcal{C}^0([a,b], \mathbb{R})$. Si f est positive, alors

$$\left(\int_a^b f = 0\right) \Longrightarrow f = 0.$$

Démonstration : Raisonnons par contraposée. Supposons qu'il existe $x \in [a,b]$ tel que $f(x) > 0$. Alors, par continuité de f en x, il existe $\alpha > 0$ tel que $f \geq \dfrac{f(x)}{2}$ sur $S = [x-\alpha, x+\alpha] \cap [a,b]$. Alors S est un segment non-vide, et on pose

$$g : t \mapsto \begin{cases} \frac{f(t)}{2} & \text{si } t \in S \\ 0 & \text{sinon} \end{cases}.$$

Alors

$$f \geq g, \quad \int_a^b f \geq \int_a^b g = \int_S g > 0.$$

□

⚠ Ce résultat est faux si f n'est pas continue ou si f n'est pas positive. Quels contre-exemples choisir ?

Exercice 2.3 :

Soit $f \in \mathcal{C}^0([a,b], \mathbb{R})$. Montrer qu'il existe $c \in [a,b]$ tel que $f(c) = \dfrac{1}{b-a}\displaystyle\int_a^b f$. Ce nombre est appelé *valeur moyenne de f sur $[a,b]$*.

3. Michel Chasles (1793-1880) : Mathématicien français.

Réponse

Notons $\lambda = \dfrac{1}{b-a}\displaystyle\int_a^b f$. Considérons la fonction continue $g = f - \lambda$, et supposons que g ne s'annule pas sur $[a, b]$. g étant continue, elle est strictement positive (ou strictement négative) sur $[a, b]$ et son intégrale est donc non-nulle. On a donc

$$\int_a^b g = \int_a^b (f - \lambda) = \int_a^b f - (b-a)\lambda = \int_a^b f - \int_a^b f \neq 0,$$

ce qui est absurde. On en déduit qu'il existe $c \in [a, b]$ tel que $g(c) = 0$, et donc $f(c) = \lambda$.

◊

Exercice 2.4 :
Déterminer les fonctions $f \in \mathcal{C}^0([0,1],[0,1])$ vérifiant

$$\int_0^1 f = \int_0^1 f^2.$$

Réponse

Analyse Soit $f \in \mathcal{C}^0([0,1],[0,1])$ une telle fonction. Alors $f - f^2$ est une fonction continue et positive sur $[0,1]$, car $\operatorname{Im} f \subseteq [0,1]$. De plus,

$$\int_0^1 f - \int_0^1 f^2 = \int_0^1 (f - f^2) = 0,$$

donc $f = f^2$ sur $[0,1]$. Donc $\operatorname{Im} f \subseteq \{0,1\}$. Puisque f est continue, on en déduit que $f = 0$ ou $f = 1$.

Synthèse Il est évident que les fonctions constantes 0 et 1 sont solutions du problèmes.

Conclusion On a montré que les solutions du problèmes sont les fonctions constantes 0 et 1.

◊

2. Inégalité de Cauchy-Schwarz

Théorème 2.5 *Inégalité de Cauchy*[4]*-Schwarz*[5]

Soient $f, g \in \mathcal{C}_m^0([a,b],\mathbb{R})$. Alors

$$\left|\int_a^b fg\right| \leq \sqrt{\int_a^b f^2}\sqrt{\int_a^b g^2}.$$

De plus, si f et g sont continues, alors on a égalité si, et seulement si, la famille (f, g) est liée.

Démonstration : On fait la démonstration dans le cas où les fonctions f et g sont continues. On définit

$$\forall \lambda \in \mathbb{R},\quad P = \int_a^b (f + \lambda g)^2 = \int_a^b \left(f^2 + 2fg\lambda + \lambda^2 g^2\right) = \int_a^b f^2 + 2\lambda \int_a^b fg + \lambda^2 \int_a^b g^2.$$

4. Augustin Cauchy (1789-1857) : Mathématicien français.
5. Hermann Schwarz (1843-1921) : Mathématicien allemand.

On en déduit que P est un polynôme de degré au plus 2.

- Si $g = 0$ alors on a l'égalité voulue $(0 = 0)$.
- Si $g \neq 0$, alors $\displaystyle\int_a^b g^2 \neq 0$ et $\deg P = 2$. De plus, pour tout $\lambda \in \mathbb{R}, P(\lambda) \geq 0$ donc le discriminant Δ de P est négatif. On a

$$\Delta = 4\left(\int_a^b fg\right)^2 - 4\int_a^b f^2 \int_a^b g^2 \leq 0,$$

$$\left(\int_a^b fg\right)^2 \leq \int_a^b f^2 \int_a^b g^2,$$

$$\left|\int_a^b fg\right| \leq \sqrt{\int_a^b f^2}\sqrt{\int_a^b g^2}.$$

De plus,

$$\begin{aligned}\left|\int_a^b fg\right| = \sqrt{\int_a^b f^2}\sqrt{\int_a^b g^2}\Delta = 0 &\iff \exists\lambda \in \mathbb{R}, \quad P(\lambda) = 0\\ &\iff \exists\lambda \in \mathbb{R}, \quad \int_a^b (f + \lambda g)^2 = 0 \iff \exists\lambda \in \mathbb{R}, \quad f = -\lambda g\\ &\iff (f, g) \text{ est liée}\end{aligned}$$

Attention, la dernière équivalence est vraie car $g \neq 0$. □

Remarque 2.6 : L'inégalité de Cauchy-Schwarz reste vrai dans un cadre beaucoup plus général, les espaces euclidiens. Un espace euclidien est un $\mathbb{R}$-espace vectoriel muni d'un produit scalaire, c'est-à-dire qu'il existe une application $\Phi : E^2 \to E$ vérifiant :

- Φ est bilinéaire :
$$\forall x, y, z \in E, \quad \forall\lambda\mu \in \mathbb{R}, \quad \begin{cases}\Phi(\lambda x + \mu z, y) = \lambda\Phi(x, y) + \mu\Phi(z, y)\\ \Phi(x, \lambda y + \mu z) = \lambda\Phi(x, y) + \mu\Phi(x, z)\end{cases}.$$
- Φ est symétrique :
$$\forall x, y \in E, \quad \Phi(x, y) = \Phi(y, x).$$
- Φ est positive :
$$\forall x \in E, \quad \Phi(x, x) \geq 0.$$
- Φ est définie :
$$\forall x \in E, \quad \Phi(x, x) = 0 \iff x = 0.$$

Dans ce cas, on a alors

$$\forall x, y \in E, \quad |\Phi(x, y)| \leq \sqrt{\Phi(x, x)}\sqrt{\Phi(y, y)}.$$

Ici, on considèrerait l'application

$$\Phi : \begin{array}{ccc}\mathcal{C}^0([a, b], \mathbb{R})^2 & \to & \mathcal{C}^0([a, b], \mathbb{R})\\ (f, g) & \mapsto & \int_a^b f(t)\, g(t)\, dt\end{array}$$

qui vérifie bien les quatre propriétés des produits scalaires, sur le $\mathbb{R}$-espace vectoriel $\mathcal{C}^0([a, b], \mathbb{R})$. ♢

Exercice 2.7 :

On considère une suite de fonctions $(f_n)_{n\in\mathbb{N}} \in \mathcal{C}^0_m([a, b])^{\mathbb{N}}$. On suppose que $\displaystyle\lim_{n\to+\infty}\int_a^b f_n^2 = 0$. Montrer que $\displaystyle\lim_{n\to+\infty}\int_a^b f_n = 0$.

Réponse

Tout d'abord, les f_n^2 sont bien continues par morceaux, donc l'exercice a bien un sens. Ensuite, d'après l'inégalité de Cauchy-Schwarz,

$$\forall n \in \mathbb{N}, \quad \left| \int_a^b f_n \right| = \left| \int_a^b 1 \times f_n \right| \leq \sqrt{\int_a^b 1^2} \sqrt{\int_a^b f_n^2} = \sqrt{b-a} \sqrt{\int_a^b f_n^2}.$$

Le membre de droite tendant vers 0 lorsque $n \to +\infty$, on en déduit que $\lim\limits_{n \to +\infty} \int_a^b f_n = 0$.

$\diamondsuit$

3. Intégrale et primitive

Dans toute cette partie, on considère un intervalle non-trivial $I \subseteq \mathbb{R}$.

Définition 2.8

Soit $f \in \mathcal{F}(I, \mathbb{K})$. On dit que f est continue par morceaux sur I si f est continue par morceaux sur tout segment inclus dans I.

On note $\mathcal{C}_m^0(I, \mathbb{K})$ l'ensemble des fonctions continues par morceaux sur I.

Définition 2.9 *Primitive*

Soit $f \in \mathcal{F}(I, \mathbb{K})$. On appelle primitive de f sur I toute fonction $F \in \mathcal{F}(I, \mathbb{K})$ telle que $F' = f$ sur I.

On utilise traditionnellement des lettres majuscules pour nommer les primitives, mais ce n'est absolument pas une obligation.

Exemple 2.10 :

- La fonction sin est une primitive de cos sur $\mathbb{R}$.
- La fonction ln est une primitive de $x \mapsto \dfrac{1}{x}$ sur $]0, +\infty[$, pas sur $\mathbb{R}^*$.

$\diamondsuit$

Proposition 2.11

Soit $f \in \mathcal{F}(I, \mathbb{K})$. Si F et G sont deux primitives de f sur I, alors

$$\exists c \in \mathbb{K}, \forall x \in I, \quad F = G + c.$$

Démonstration : On a $F' - G' = (F - G)' = 0$ donc $F - G$ est constante sur I. Autrement dit, il existe $c \in \mathbb{K}$ tel que, pour tout $x \in I$

$$F(x) - G(x) = c, \quad F(x) = G(x) + c.$$

$\square$

Exemple 2.12 :
Déterminons toutes les primitives de la fonctions $f : x \mapsto \dfrac{1}{x}$ sur $\mathbb{R}^*$. Posons $F : x \mapsto \ln|x|$. On sait que la fonction ln est dérivable sur $\mathbb{R}_+^*$ donc F est dérivable sur $\mathbb{R}^*$ et

$$\forall x > 0, \quad F'(x) = \frac{1}{x} = f(x), \quad \forall x < 0, \quad F'(x) = \frac{-1}{-x} = f(x).$$

On a donc trouvé une primitive de f sur $\mathbb{R}^*$. Soit $G \in \mathcal{F}(\mathbb{R}^*, \mathbb{R})$. D'après la proposition 2.11,

$$\forall x \in \mathbb{R}^*, \quad G'(x) = f(x) \iff \exists A, B \in \mathbb{R}, \forall x \in \mathbb{R}^*, \quad G(x) = \begin{cases} A + \ln(-x) & \text{si } x < 0 \\ B + \ln(x) & \text{si } x > 0 \end{cases}.$$

◇

Exercice 2.13 :
Montrer que la fonction partie entière E n'admet pas de primitive sur $\mathbb{R}$.

Réponse
Supposons, par l'absurde, que E possède une primitive, qu'on note F. F est dérivable donc continue en tout point de $\mathbb{R}$, en particulier en 1. On a $F' = 0$ sur $[0, 1[$ donc il existe $c_0 \in \mathbb{K}$ tel que

$$\forall x \in [0, 1[, \quad F(x) = c_0.$$

De même, $F' = 1$ sur $[1, 2[$ donc il existe $c_1 \in \mathbb{K}$ tel que

$$\forall x \in [1, 2[, \quad F(x) = x + c_1.$$

Par continuité, on a

$$F(1) = 1 + c_1 = c_0 = \lim_{1^-} F.$$

Donc

$$\forall x \in [0, 2[, \quad F(x) = \begin{cases} c_0 & \text{si } x \leq 1 \\ x + c_0 - 1 & \text{si } x > 1. \end{cases}$$

On en déduit que F n'est pas dérivable en 1, car $F'_g(1) = 0$ et $F'_d(1) = 1$, ce qui est absurde.

◇

Une fonction discontinue peut admettre une primitive, ou pas, mais si c'est le cas, celle-ci ne sera pas $\mathcal{C}^1$: penser à $x^2 \sin \dfrac{1}{x}$. Attention, la dérivée de $x^2 \sin \dfrac{1}{x}$ n'est pas continue par morceaux sur $[0, 1]$ (limite oscillante en 0^+).

Théorème 2.14 *Théorème fondamental de l'analyse*
Soit $f \in \mathcal{C}^0(I, \mathbb{K})$. Soit $a \in I$, et on définit

$$F : x \mapsto \int_a^x f(t)\, dt.$$

Alors :

(i) La fonction F est de classe $\mathcal{C}^1$ sur I, et c'est l'unique primitive de f sur I vérifiant $F(a) = 0$.

(ii) Pour toute primitive G de f sur I, et pour tout $b \in I$ on a

$$\int_a^b f(t)\,dt = G(b) - G(a).$$

Démonstration : (i) Soit $x \in I$. Pour simplifier, on suppose que $x \in \mathring{I}$. Puisque f est continue en x, il existe $\alpha > 0$ tel que,

$$\forall t \in [x-\alpha, x+\alpha], \quad |f(x) - f(t)| \leq \varepsilon.$$

Alors, pour tout $h \in [-\alpha, \alpha] \setminus \{0\}$,

$$\begin{aligned}\left|\frac{F(x+h)-F(x)}{h} - f(x)\right| &= \left|\frac{1}{h}\left(\int_a^{x+h} f - \int_a^x f\right) - f(x)\right| = \left|\frac{1}{h}\int_x^{x+h} f(t)\,dt - f(x)\right| \\ &= \left|\frac{1}{h}\int_x^{x+h} (f(t) - f(x))\,dt\right| \\ &\leq \frac{1}{h}\int_x^{x+h} |f(t)-f(x)|dt \leq \frac{1}{h}\int_x^{x+h} \varepsilon dt \\ &\leq \varepsilon.\end{aligned}$$

Attention, on a utilisé l'inégalité triangulaire, il convient de faire très attention au signe de h. D'où,

$$\lim_{\substack{h \to 0 \\ h \neq 0}} \frac{F(x+h)-F(x)}{h} = f(x),$$

donc $F'(x) = f(x)$ par définition. On en déduit que F est dérivable sur I et que $F' = f$. Or f est continue, donc $F \in \mathcal{C}^1(I)$. On a bien montré que F est une primitive de f, et il est clair que $F(a) = 0$. D'après la proposition 2.11, il est clair qu'on a unicité.

(ii) Soit G une primitive de f sur I. Alors il existe $c \in \mathbb{K}$ tel que $G = F + c$ sur I. En particulier, on a

$$G(a) = F(a) + c = c, \quad \forall b \in I, \quad F(b) = \int_a^b f(t)\,dt = G(b) - c = G(b) - G(a).$$

□

On écrira généralement $\int_a^b f(t)\,dt = \Big[F(t)\Big]_{t=a}^b$.

Corollaire 2.15

Toute fonction continue sur un intervalle admet des primitives.

Corollaire 2.16

Soit $f \in \mathcal{C}^1(I, \mathbb{K})$. Alors

$$\forall a, b \in I, \quad \int_a^b f'(t)\,dt = f(b) - f(a).$$

On peut étendre ce théorème aux fonctions continues par morceaux sur un intervalle. En général, on prendra quand même garde de travailler avec des fonctions continues sur $[a, b]$ pour éviter les problèmes de "primitive à constante près".

Proposition 2.17

Soit $f \in \mathcal{C}_m^0(I, \mathbb{K})$. Soit $a \in I$, on définit

$$F : x \mapsto \int_a^x f(t)\, dt.$$

Alors

(i) F est continue sur I.
(ii) F est dérivable en tout point de continuité $x_0 \in I$ de f, et $F' = f$.
(iii) Si $x_0 \in I$ est un point de discontinuité de f, F est dérivable à gauche et à droite en x_0 (lorsque cela a un sens) et on a

$$F_g'(x_0) = \lim_{x_0^-} f, \quad F_d'(x_0) = \lim_{x_0^+} f.$$

Démonstration : La démonstration de la dérivabilité (générale, à gauche ou à droite) se fait comme pour le théorème fondamental de l'analyse. La fonction F est donc dérivable à gauche et à droite sur I, donc continue à gauche et à droite sur I. On en déduit que F est continue sur I.

On pourrait aussi montrer que F est lipschitzienne sur tout segment, donc continue (la fonction f étant continue par morceaux, elle est bornée sur tout segment). $\square$

III Calcul pratique d'intégrales

Dans toute cette partie, la question que l'on se pose est "comment calculer une intégrale (ou une primitive) en pratique ?", ce qui est le principal intérêt de ce chapitre (en mathématiques, en physique, en biologie, etc.).

On voit régulièrement des calculs du genre : $\displaystyle\int x\, dx = \frac{x^2}{2} + \texttt{cste}$, pour signifier qu'une primitive de la fonction $x \mapsto x$ est une fonction du type $x \mapsto \dfrac{x^2}{2} + C$. C'est en général une mauvaise idée (à part au brouillon, éventuellement), le problème principal des débutants étant de mettre du x partout (sans faire attention s'il s'agit d'une borne ou de la variable d'intégration). On écrira donc plutôt :

$$\int^x t\, dt = \frac{x^2}{2} + \texttt{cste}.$$

Cette écriture a l'avantage de rappeler le théorème fondamental (la borne supérieure de l'intégrale étant x) et permet de dissocier x et t.

Cette écriture sert simplement à faire des calculs, et ne tient pas compte, par exemple, de l'intervalle sur lequel on fait ce calcul.

1. Intégration par parties

La dérivation étant une opération linéaire, il est facile de trouver la primitive d'une combinaison linéaire de fonctions simples. Mais pour le produit, c'est plus compliqué, et on utilise l'intégration par parties.

Théorème 3.1 *Intégration par parties (IPP)*
Soient $u, v \in \mathbb{C}^1([a,b], \mathbb{K})$. Alors

$$\int_a^b u(t)\, v'(t)\, dt = u(b)\, v(b) - u(a)\, v(a) - \int_a^b u'(t)\, v(t)\, dt.$$

Démonstration : La fonction $u \times v$ est $\mathcal{C}^1$ sur $[a,b]$ et, d'après le théorème fondamental de l'analyse,

$$\begin{aligned} u(b)\, v(b) - u(a)\, v(a) &= \int_a^b (uv)'(t)\, dt = \int_a^b [u'(t)\, v(t) + u(t)\, v'(t)] dt \\ &= \int_a^b u'(t)\, v(t)\, dt + \int_a^b u(t)\, v'(t)\, dt. \end{aligned}$$

□

L'intégration par parties sert principalement pour obtenir la primitive d'un produit de fonctions simples. Pour itnégrer uv', le terme uv aura beau être très compliqué, cela ne pose aucun problème : il suffit de savoir intégrer $u'v$.

Exemple 3.2 :
Déterminons une primitive de ln sur $\mathbb{R}_+^*$. Soit $x > 0$.On applique la formule d'intégration par parties avec $u : t \mapsto \ln t$ et $v : t \mapsto t$, qui sont $\mathcal{C}^1$ sur $[1, x] \cup [x, 1]$.

$$\int_1^x \ln(t)\, dt = \int_1^x u(t)\, v'(t)\, dt = [t \ln t]_{t=1}^x - \int_1^x \frac{t}{t} dt = x \ln x - [t]_{t=1}^x = x \ln x - x - 1.$$

Une primitive de ln sur $\mathbb{R}_+^*$ est donc $x \mapsto x \ln x - x$. ♢

Exemple 3.3 :
Calculons $\int_0^2 3t\, \mathrm{e}^{2t}\, dt$. On applique la formule d'intégration par parties avec $u : t \mapsto 3t$ et $v : t \mapsto \frac{\mathrm{e}^{2t}}{2}$, qui sont $\mathcal{C}^1$ sur $[0, 2]$.

$$\begin{aligned} \int_0^2 t\, \mathrm{e}^{2t}\, dt = \int_0^2 t\, \mathrm{e}^{2t}\, dt &= \left[\frac{3}{2} t\, \mathrm{e}^{2t}\right]_{t=0}^2 - \frac{3}{2} \int_0^2 \mathrm{e}^{2t}\, dt \\ &= 3\, \mathrm{e}^4 - \frac{3}{4} \left[\mathrm{e}^{2t}\right]_{t=0}^2 = \frac{9}{4}\, \mathrm{e}^4 + \frac{3}{4}. \end{aligned}$$

♢

On prendra soin d'indiquer que les deux fonctions qui nous intéressent sont $\mathcal{C}^1$ sur le segment voulu.

Exercice 3.4 :
Déterminer de deux façons différentes les primitives de $f : x \mapsto \sin(2x)\, \mathrm{e}^x$ sur $\mathbb{R}$.

Réponse

Méthode 1 Par intégration par parties, les fonctions sin, cos, exp étant $\mathcal{C}^1$ sur $\mathbb{R}$,

$$\begin{aligned} \int^x \sin(2t)\, \mathrm{e}^t\, dt &= [\sin(2t)\, \mathrm{e}^t]^x - 2 \int^x \cos(2t)\, \mathrm{e}^t\, dt = \sin(2x)\, \mathrm{e}^x - 2[\cos(2t)\, \mathrm{e}^t]^x - 4 \int^x \sin(2t)\, \mathrm{e}^t\, dt \\ (1+4) \int^x \sin(2t)\, \mathrm{e}^t\, dt &= \sin(2x)\, \mathrm{e}^x - 2 \cos(2x)\, \mathrm{e}^x \\ \int^x \sin(2t)\, \mathrm{e}^t\, dt &= \frac{\sin(2x) - 2\cos(2x)}{5}\, \mathrm{e}^x \end{aligned}$$

Méthode 2 En passant aux complexes, on a

$$\begin{aligned}\int^x \sin(2t)\,\mathrm{e}^t\,dt &= \int^x \left(\frac{\mathrm{e}^{i2t}-\mathrm{e}^{-i2t}}{2i}\right)\mathrm{e}^t\,dt = \frac{1}{2i}\int^x \left(\mathrm{e}^{(1+2i)t}-\mathrm{e}^{(1-2i)t}\right)dt \\ &= \frac{1}{2i}\left(\frac{\mathrm{e}^{(1+2i)x}}{1+2i}-\frac{\mathrm{e}^{(1-2i)x}}{1-2i}\right) = \frac{1}{10i}\left[(1-2i)\,\mathrm{e}^{2ix}-(1+2i)\,\mathrm{e}^{-2ix}\right]\mathrm{e}^x \\ &= \frac{\left(\mathrm{e}^{2ix}-\mathrm{e}^{-2ix}\right)-2i\left(\mathrm{e}^{2ix}+\mathrm{e}^{-2ix}\right)}{2i}\,\frac{\mathrm{e}^x}{5} \\ &= \frac{\sin(2x)-2\cos(2x)}{5}\,\mathrm{e}^x\end{aligned}$$

Bilan Les primitives de f sur $\mathbb{R}$ sont donc de la forme

$$x \mapsto \frac{\sin(2x)-2\cos(2x)}{5}\,\mathrm{e}^x + \texttt{cste}.$$

Remarque : Même si les nombres complexes font habituellement un peu peur (à tort), la méthode 2 est beaucoup plus efficace (moins de risques d'erreurs de signe ou de coefficient !)

♢

2. Changement de variable

On peut faire des changements de variables sur des intervalles, à peu près de la même façon que sur des segments.

Théorème 3.5 *Changement de variable*
Soient $\alpha < \beta \in \mathbb{R}$ et $\Phi \in \mathcal{C}^1([\alpha,\beta], I)$. Soit $f \in \mathcal{C}^0(I)$. Alors

$$\int_\alpha^\beta f(\Phi(t))\,\Phi'(t)\,dt \underset{u=\Phi(t)}{=\!=\!=} \int_{\Phi(\alpha)}^{\Phi(\beta)} f(u)\,du.$$

On dit qu'on fait le changement de variable $u = \Phi(t)$.

Démonstration : f étant continue sur I, elle admet une primitive F qui est $\mathcal{C}^1$ sur I. D'après le théorème fondamental de l'analyse, on a alors

$$\int_{\Phi(\alpha)}^{\Phi(\beta)} f(u)\,du = F(\Phi(\beta)) - F(\Phi(\alpha)).$$

D'autre part, $F \circ \Phi \in \mathcal{C}^1([\alpha,\beta])$ et

$$(F\circ\Phi)' = F'\circ\Phi \times \Phi' = f\circ\Phi\times\Phi'.$$

On en déduit que $F\circ\Phi$ est une primitive de $f\circ\Phi\times\Phi'$ et donc que

$$\int_\alpha^\beta f(\Phi(t))\,\Phi'(t)\,dt = F(\Phi(\beta)) - F(\Phi(\alpha)) = \int_{\Phi(\alpha)}^{\Phi(\beta)} f(u)\,du.$$

□

On traite ici un cas particulier, où f est continue et non plus continue par morceaux.

Remarque 3.6 : En pratique, on aura plutôt des intégrales du type $\int_a^b f(\Psi(u))\,du$, et on veut donc pouvoir écrire :

$$\int_a^b f(\Psi(u))\,du \underset{t=\Psi(u)}{=\!=\!=} \int_{\Psi(a)}^{\Psi(b)} f(t)\left(\Psi^{-1}\right)'(t)\,dt.$$

Une condition suffisante pour effectuer un tel changement de variable est donc "Φ (resp. Ψ) est un $\mathcal{C}^1$-difféomorphisme sur $[\alpha, \beta]$ (resp. $[a, b]$)". $\diamondsuit$

⚠ Lors d'un changement de variable, on fera attention à bien changer <u>trois</u> parties dans l'intégrale :

- les bornes
- l'intégrande "$f(t)$"
- le "dt"

Exemple 3.7 :
Pour appliquer le théorème de changement de variable, il n'est pas nécessaire que Φ soit injective. On a par exemple

$$\int_{-\sqrt{\frac{\pi}{2}}}^{2\sqrt{\frac{\pi}{2}}} t\cos\left(t^2\right)dt \underset{u=t^2}{=\!=\!=} \int_{\frac{\pi}{2}}^{2\pi} \frac{\cos u}{2}du = \left[\frac{\sin u}{2}\right]_{u=\frac{\pi}{2}}^{2\pi} = -\frac{1}{2}.$$

Ceci dit, on aurait pu trouver une primitive directement en remarquant que l'intégrande est sous la forme $u'\cos u$, d'où

$$\int_{-\sqrt{\frac{\pi}{2}}}^{2\sqrt{\frac{\pi}{2}}} t\cos\left(t^2\right)dt = \left[\frac{\sin\left(t^2\right)}{2}\right]_{t=-\sqrt{\frac{\pi}{2}}}^{2\sqrt{\frac{\pi}{2}}} = -\frac{1}{2}.$$

$\diamondsuit$

Exercice 3.8 :
Calculer $\displaystyle\int_1^9 \frac{dt}{1+\sqrt{t}}$.

Réponse
On a

$$\int_1^9 \frac{dt}{1+\sqrt{t}} \underset{s=\sqrt{t}}{=\!=\!=} \int_1^3 \frac{2s}{1+s}ds = 2\int_1^3\left(1-\frac{1}{1+s}\right)ds = 2\left[s-\ln(1+s)\right]_{s=1}^3 = 4-\ln 4.$$

$\diamondsuit$

Exercice 3.9 :
Calculer $\displaystyle\int_0^{\frac{1}{2}} \mathrm{e}^{\arcsin t}\,dt$.

Réponse
On a

$$\int_0^{\frac{1}{2}} \mathrm{e}^{\arcsin t}\,dt \underset{u=\arcsin t}{=\!=\!=\!=} \int_0^{\frac{\pi}{6}} \cos u\,\mathrm{e}^u\,du = \left[\frac{\mathrm{e}^u}{2}(\sin u+\cos u)\right]_0^{\frac{\pi}{6}} = \frac{(1+\sqrt{3})\,\mathrm{e}^{\frac{\pi}{6}}-2}{4}$$

◇

3. Périodicité et parité

Evidemment, on peut utiliser les propriétés de périodicité, de parité et d'imparité des fonctions pour calculer leurs intégrales, à l'aide du théorème de changement de variable.

Proposition 3.10

Soit $f \in \mathcal{C}_m^0([a,b])$ une fonction T-périodique. Alors

$$\int_{a+T}^{b+T} f(t)\,dt = \int_a^b f(t)\,dt.$$

Démonstration : On effectue simplement le changement de variable $u = t - T$. □

Proposition 3.11

Soit $a > 0$ et $f \in \mathcal{C}_m^0([-a,a])$. Alors

(i) Si f est paire, alors

$$\int_{-a}^{a} f(t)\,dt = 2\int_0^a f(t)\,dt.$$

(ii) Si f est impaire, alors

$$\int_{-a}^{a} f(t)\,dt = 0.$$

Démonstration : On fait le changement de variable $u = -t$ dans les intégrales considérées. □

4. Fonctions trigonométriques

Exercice 3.12 :
Déterminer les primitives de $x \mapsto \sin^2 x \cos^3 x$ sur $\mathbb{R}$.

Réponse

Il faut linéariser les fonctions $\sin^2$ et $\cos^3$. On peut pour cela utiliser les formules de trigonométrie, ou l'exponentielle complexe. Pour tout $t \in \mathbb{R}$, on a

$$\begin{aligned}
\sin^2 t \cos^3 t &= \left(\frac{\mathrm{e}^{it} - \mathrm{e}^{-it}}{2i}\right)^2 \left(\frac{\mathrm{e}^{it} + \mathrm{e}^{-it}}{2}\right)^3 = \frac{\left(\mathrm{e}^{i2t} - 2 + \mathrm{e}^{-i2t}\right)\left(\mathrm{e}^{i3t} + 3\,\mathrm{e}^{it} + 3\,\mathrm{e}^{-it} + \mathrm{e}^{-3it}\right)}{-32} \\
&\frac{\mathrm{e}^{i5t} + \mathrm{e}^{i3t} - 2\,\mathrm{e}^{it} - 2\,\mathrm{e}^{-it} + \mathrm{e}^{-i3t} + \mathrm{e}^{-i5t}}{-32} \\
&= \frac{\cos t}{8} - \frac{\cos(3t)}{16} - \frac{\cos(5t)}{16}
\end{aligned}$$

On en déduit que

$$\int^x \sin^2 t \cos^3 t \; dt = \frac{1}{16}\int^x [2\cos t - \cos(3t) - \cos(5t)]dt = \frac{\sin x}{8} - \frac{\sin(3x)}{48} - \frac{\sin(5x)}{80} + \texttt{cste}.$$

$\diamondsuit$

Les règles de Bioche[6] sont des règles pour calculer des intégrales avec des fonctions trigonométriques.

Proposition 3.13 *Règles de Bioche*

Pour calculer l'intégrale d'une fonction rationnelle composée de fonctions trigonométriques f, on pose le changement de variable suivant :

(i) Si $f(x)\,dx$ est invariant par $-x$, on pose $t = \cos x$.
(ii) Si $f(x)\,dx$ est invariant par $\pi - x$, on pose $t = \sin x$.
(iii) Si $f(x)\,dx$ est invariant par $\pi + x$, on pose $t = \tan x$.

Dans tous les cas, on peut tenter le changement de variable "universel" $u = \tan\frac{x}{2}$. Alors,

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

Il faut quand même que ces changements de variables soit légitimes.

Idée de démonstration : On démontre juste les formules du changement de variable "universel". Soient $x \in]-\pi,\pi[$, on pose $u = \tan\frac{x}{2}$. Alors

$$\frac{2u}{1+u^2} = \frac{2\tan\frac{x}{2}}{1+\tan^2\frac{x}{2}} = \frac{2\cos\frac{x}{2}\sin\frac{x}{2}}{\cos^2\frac{x}{2}+\sin^2\frac{x}{2}} = \frac{\sin\left(2\times\frac{x}{2}\right)}{1} = \sin x.$$
$$\frac{1-u^2}{1+u^2} = \frac{1-\tan^2\frac{x}{2}}{1+\tan^2\frac{x}{2}} = \frac{\cos^2\frac{x}{2}-\sin^2\frac{x}{2}}{\cos^2\frac{x}{2}+\sin^2\frac{x}{2}} = \frac{\cos\left(2\times\frac{x}{2}\right)}{1} = \cos x.$$
$$\frac{2u}{1-u^2} = \frac{\sin x}{\cos x} = \tan x.$$
$$dx = 2\arctan'(u)\,du = \frac{2du}{1+u^2}.$$

$\square$

On retiendra que les invariances suggérées sont exactement celles du changement de variable :

$$\forall x \in \mathbb{R}, \quad \cos(-x) = \cos x, \quad \sin(\pi - x) = \sin x, \quad \tan(\pi + x) = \tan x.$$

Exercice 3.14 :
Calculer $\displaystyle\int_0^{\frac{\pi}{3}} \frac{\tan x}{1+\cos x}dx$.

6. Charles Bioche (1859-1949) : Mathématicien français.

Réponse

Première méthode D'après les règles de Bioche, on remarque qu'il est conseillé d'effectuer le changement de variable $t = \cos x$. On a alors $dt = -\sin x\ dx$:

$$\int_0^{\frac{\pi}{3}} \frac{\tan x}{1+\cos x} dx = \int_0^{\frac{\pi}{3}} \frac{\sin x}{\cos x\,(1+\cos x)} dx \underset{t=\cos x}{=\!=\!=} \int_1^{\frac{1}{2}} \frac{-dt}{t\,(1+t)} = \int_{\frac{1}{2}}^1 \left(\frac{1}{t} - \frac{1}{1+t}\right) dt$$
$$= \left[\ln \frac{t}{1+t}\right]_{t=\frac{1}{2}}^1 = \ln\frac{1}{2} - \ln\frac{1}{3} = \ln\frac{3}{2}.$$

Deuxième méthode On fait le changement de variable $u = \tan \dfrac{x}{2}$ (aucun problème sur l'intervalle $[0, \pi/3]$) :

$$\int_0^{\frac{\pi}{3}} \frac{\tan x}{1+\cos x} dx \underset{u=\tan\frac{x}{2}}{=\!=\!=} \int_0^{\frac{1}{\sqrt{3}}} \frac{\left(\frac{2u}{1-u^2}\right)\left(\frac{2du}{1+u^2}\right)}{1+\frac{1-u^2}{1+u^2}} = 2\int_0^{\frac{1}{\sqrt{3}}} \frac{\left(\frac{u}{1-u^2}\right)\left(\frac{1}{1+u^2}\right)}{\frac{1}{1+u^2}} du$$
$$= \int_0^{\frac{1}{\sqrt{3}}} \frac{2u}{1-u^2} du = \left[-\ln\left(1-u^2\right)\right]_{u=0}^{\frac{1}{\sqrt{3}}} = \ln\frac{3}{2}.$$

$\diamondsuit$

5. Fractions rationnelles

Comme on l'a vu dans le chapitre consacré aux fractions rationnelles et aux polynômes, l'outil fondamental pour intégrer des fractions rationnelles est la décomposition en éléments simples. Si la plupart des éléments simples, comme leur nom l'indique, sont facilement intégrables à l'aide des fonctions puissances et ln, il y a quand même quelques exceptions qu'il faut savoir traiter.

Exemple 3.15 :
Déterminons la primitive suivante :

$$\int^x \frac{dt}{(1+t^2)^2} = \int^x \frac{1+t^2-t^2}{(1+t^2)^2} dt = \int^x \left(\frac{1}{1+t^2} - \frac{t^2}{(1+t^2)^2}\right) dt = \arctan x + \int^x \frac{-t^2}{(1+t^2)^2} dt$$
$$= \arctan x + \frac{x}{2\,(1+x^2)} - \int^x \frac{dt}{2\,(1+t^2)} = \frac{\arctan x}{2} + \frac{x}{2\,(1+x^2)} + \texttt{cste}.$$

$\diamondsuit$

Exercice 3.16 :

Déterminer les primitive de la fonction $f : \begin{array}{ccc} \mathbb{R}\setminus\{-1\} & \to & \mathbb{R} \\ x & \mapsto & \dfrac{3x^3+x^2+2x+5}{x+1} \end{array}$.

Réponse

En effectuant la division euclidienne de $3X^3 + X^2 + 2X + 5$ par $1 + X$, on trouve

$$3X^3 + X^2 + 2X + 5 = (1+X)\left(3X^2 - 2X + 4\right) + 1.$$

On en déduit que pour tout $x \neq -1$, $f(x) = 3x^2 - 2x + 4 + \dfrac{1}{1+x}$. Les primitives de f sur $\mathbb{R}\setminus\{-1\}$ est donc de la forme

$$F : x \mapsto \begin{cases} x^3 - x^2 + 4x + \ln|1+x| + C_1 & \text{si } x > -1 \\ x^3 - x^2 + 4x + \ln|1+x| + C_2 & \text{si } x < -1 \end{cases}, \quad \text{avec } C_1, C_2 \in \mathbb{R}.$$

$\diamondsuit$

À connaître à la fin du chapitre

Définition de l'intégrale

- Reconnaître et calculer la limite d'une somme de Riemann.
- Théorème fondamental de l'analyse, lien entre primitive et intégrale.

Calcul pratique d'intégrales

- Connaître et savoir utiliser les différentes méthodes à votre disposition pour calculer efficacement des intégrales : passages aux complexes, changement de variable, intégration par parties, fractions rationnelles, règles de Bioche...
- Attention à l'ordre des bornes lors des inégalités classiques (inégalité triangulaire et inégalité de Cauchy-Schwarz).

Pour aller plus loin

- Intégrale de Lebesgue, d'Itô ou de Stieltjes.
- Intégration sur un intervalle quelconque (intégrale généralisée)
- Méthodes d'intégration : Simpson, Runge-Kutta,...

CHAPITRE 11

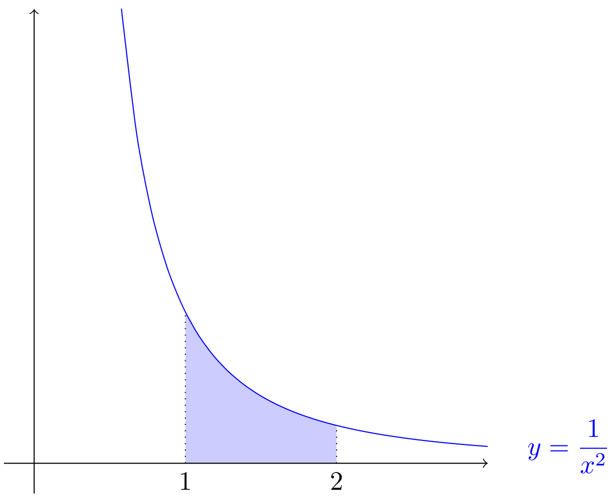
INTÉGRALES GÉNÉRALISÉES

Ce chapitre est la suite directe du cours d'intégration sur un segment, et les notions suivantes doivent naturellement être connues et maîtrisées :

- Lien avec les primitives, théorème fondamental de l'analyse
- Intégration par parties, changement de variables
- Techniques classiques de calcul d'intégrales

Dans le chapitre précédent, on a appris à construire l'intégrale d'une fonction continue par morceaux sur un segment $[a,b]$: il s'agit de l'aire sous la courbe entre a et b. On sait par exemple calculer

$$\int_1^2 \frac{dt}{t^2} = \left[-\frac{1}{t}\right]_{t=1}^{2} = \frac{1}{2}.$$



Mais que peut-on dire de l'aire sous la courbe de la fonction $t \mapsto \dfrac{1}{t^2}$ entre 0 et $+\infty$? Ce chapitre sert à répondre à cette question. Remarquons qu'il y a deux problèmes :

- La fonction $t \mapsto \dfrac{1}{t^2}$ n'est pas définie en 0 et $\lim\limits_{t\to 0^+} \dfrac{1}{t^2} = +\infty$. Ainsi l'aire peut potentiellement être infinie au voisinage de 0 : on dit que 0 est un point incertain.

- Le domaine d'intégration est de longueur infinie. Ainsi l'aire peut potentiellement être infinie "au voisinage de $+\infty$" : c'est un point incertain aussi.

Dans tout ce chapitre, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

I Intégrale généralisée

1. Intégration sur un intervalle

Définition 1.1 *Continuité par morceaux*

Soient $a < b \in \mathbb{R}$. On dit que $f : [a,b] \to \mathbb{K}$ est *continue par morceaux* sur $[a,b]$ s'il existe une subdivision $(a_0, \ldots, a_n)$ de $[a,b]$ telle que, pour tout $i \in [\![1,n]\!]$,

(i) f est continue sur $]a_{i-1}, a_i[$.
(ii) f admet une limite finie à droite en a_{i-1} et une limite finie à gauche en a_i.

On note $\mathcal{C}_m^0\left([a,b], \mathbb{K}\right)$ l'ensemble des fonctions continues par morceaux sur $[a,b]$.

Soit I un intervalle non-trivial de $\mathbb{R}$. On dit que $f : I \to \mathbb{R}$ est *continue par morceaux* sur I si f est continue par morceaux sur tout segment inclus dans I. On note $\mathcal{C}_m^0\left(I, \mathbb{K}\right)$ l'ensemble des fonctions continues par morceaux sur I.

Pour définir l'intégrale, on s'est restreint aux fonctions continues par morceaux sur un segment. On peut maintenant étendre cette notion à une classe plus vaste de fonctions en se basant sur la relation de Chasles.

Définition 1.2 *Intégrale généralisée à droite*

Soit $f \in \mathcal{C}_m^0\left([a,b[, \mathbb{K}\right)$ avec $a < b \leq +\infty$. On dit que l'intégrale généralisée $\displaystyle\int_a^b f(t)\,dt$ *converge* si $\displaystyle\lim_{x\to b^-} \int_{[a,x]} f(t)\,dt$ existe et est finie. On définit alors

$$\int_a^b f(t)\,dt = \lim_{x\to b^-} \int_{[a,x]} f(t)\,dt.$$

Sinon, on dit que l'intégrale généralisée $\displaystyle\int_a^b f(t)\,dt$ *diverge.*

On dit que b est un *point incertain* pour l'intégrale $\displaystyle\int_a^b f(t)\,dt$.

On parle d'intégrale généralisée (ou d'intégrale *impropre*) car il ne s'agit plus tout à fait de l'intégrale de Riemann construite au chapitre précédent. Il s'agit d'une généralisation de cette intégrale aux fonctions continues par morceaux sur un intervalle semi-ouvert. Cette définition a bien un sens car f est bien continue par morceaux sur $[a,x]$ pour tout $x \in]a,b[$.

On remarque que, si $f \in \mathcal{C}_m^0\left([a,b]\right)$ alors $\displaystyle\int_a^b f(t)\,dt$ converge et elle coïncide avec l'intégrale de Riemann :

$$\int_a^b f(t)\,dt = \int_{[a,b]} f(t)\,dt.$$

Exemple 1.3 :
Notons $f(t) = \dfrac{1}{t^2}$. Pour tout $x \in]1,+\infty[$, la fonction f est continue sur $[1,x]$ donc $f \in \mathcal{C}_m^0\left([1,+\infty[\right)$. Étudions

l'intégrale généralisée $\int_1^{+\infty} f(t)\,dt$. On a, pour tout $x > 1$,

$$\int_1^x \frac{dt}{t^2} = \left[-\frac{1}{t}\right]_{t=1}^x = 1 - \frac{1}{x}.$$

Donc $\int_1^{+\infty} f(t)\,dt$ converge et

$$\int_1^{+\infty} f(t)\,dt = \lim_{x\to+\infty} 1 - \frac{1}{x} = 1.$$

$\diamondsuit$

Proposition 1.4 *Relation de Chasles*

Soit $f \in \mathcal{C}_m^0([a,b[,\mathbb{K})$ avec $a < b \leq +\infty$. Alors

$$\int_a^b f(t)\,dt \text{ converge } \iff \forall c \in]a,b[, \int_c^b f(t)\,dt \text{ converge.}$$

Dans ce cas on a

$$\int_a^b f(t)\,dt = \int_a^c f(t)\,dt + \int_c^b f(t)\,dt.$$

Démonstration : Pour tout $c \in]a,b[$ et pour tout $x \in [c,b[$,

$$\int_a^x f(t)\,dt = \int_a^c f(t)\,dt + \int_c^x f(t)\,dt.$$

Lorsque $x \to b^-$, le membre de gauche admet une limite si et seulement si le membre de droite admet une limite, et dans ce cas on a

$$\lim_{x\to b^-} \int_a^x f(t)\,dt = \int_a^c f(t)\,dt + \lim_{x\to b^-} \int_c^x f(t)\,dt.$$

$\square$

Définition 1.5 *Intégrale généralisée à gauche*

Soit $f \in \mathcal{C}_m^0(]a,b],\mathbb{K})$ avec $-\infty \leq a < b$. On dit que l'intégrale généralisée $\int_a^b f(t)\,dt$ *converge* si $\lim_{x\to a^+} \int_{[x,b]} f(t)\,dt$ existe et est finie. On définit alors

$$\int_a^b f(t)\,dt = \lim_{x\to b^-} \int_{[x,b]} f(t)\,dt.$$

Sinon, on dit que l'intégrale généralisée $\int_a^b f(t)\,dt$ *diverge*.

On dit que a est un *point incertain* pour l'intégrale $\int_a^b f(t)\,dt$.

Exemple 1.6 :
Notons $f(t) = \dfrac{1}{t^2}$. Pour tout $x \in]0,1[$, la fonction f est continue sur $[x,1]$ donc $f \in \mathcal{C}^0_m(]0,1])$. Étudions l'intégrale généralisée $\displaystyle\int_0^1 f(t)\,dt$. On a, pour tout $x \in]0,1[$,

$$\int_x^1 \frac{dt}{t^2} = \left[-\frac{1}{t}\right]_{t=x}^1 = \frac{1}{x} - 1.$$

Donc $\displaystyle\int_1^{+\infty} f(t)\,dt$ diverge car $\displaystyle\lim_{x\to 0} \frac{1}{x} - 1 = +\infty$. ◇

Proposition 1.7 *Relation de Chasles*
Soit $f \in \mathcal{C}^0_m(]a,b],\mathbb{K})$ avec $-\infty \leq a < b$. Alors

$$\int_a^b f(t)\,dt \text{ converge} \iff \forall c \in]a,b[, \int_a^c f(t)\,dt \text{ converge.}$$

Dans ce cas on a

$$\int_a^b f(t)\,dt = \int_a^c f(t)\,dt + \int_c^b f(t)\,dt.$$

Définition 1.8 *Intégrale généralisée*
Soit $f \in \mathcal{C}^0_m(]a,b[,\mathbb{K})$ avec $-\infty \leq a < b \leq +\infty$. On dit que l'intégrale généralisée $\displaystyle\int_a^b f(t)\,dt$ *converge* s'il existe $c \in]a,b[$ tel que $\displaystyle\int_a^c f(t)\,dt$ et $\displaystyle\int_c^b f(t)\,dt$ convergent. On pose alors

$$\int_a^b f(t)\,dt = \int_a^c f(t)\,dt + \int_c^b f(t)\,dt.$$

Sinon, on dit que l'intégrale $\displaystyle\int_a^b f(t)\,dt$ *diverge.*

On pourra noter $\displaystyle\int_a^b f = \int_a^b f(t)\,dt$.

⚠ On n'a pas défini l'intégrale généralisée à gauche et à droite d'un seul coup. Il est en effet crucial de ne traiter qu'un seul point incertain à la fois, c'est-à-dire une seule limite à la fois !

Proposition 1.9
Soit $f \in \mathcal{C}^0_m(]a,b[,\mathbb{K})$ avec $-\infty \leq a < b \leq +\infty$. La convergence de l'intégrale généralisée $\displaystyle\int_a^b f$ ne dépend pas du point $c \in]a,b[$ choisi. Autrement dit,

$$\int_a^b f(t)\,dt \text{ converge} \iff \forall c \in]a,b[, \int_a^c f \text{ et } \int_c^b f \text{ convergent.}$$

C'est évident par les relation de Chasles établies précédemment : le problème de convergence d'une intégrale généralisée est un problème local, aux bornes de l'intervalle d'intégration.

Exemple 1.10 :
$\displaystyle\int_0^{+\infty} \frac{dt}{t^2}$ diverge, car on a trouvé $c \in]0, +\infty[$ tel que $\displaystyle\int_0^{c} \frac{dt}{t^2}$ diverge. ♢

Exercice 1.11 :
Soient $p \in \mathbb{N}^*$, I un intervalle de $\mathbb{R}$ et $x_0 \in I$. Soit $f \in \mathcal{F}(I \setminus \{x_0\}, \mathbb{R})$. Montrer que, si $f \in \mathcal{C}^p(I \setminus \{x_0\})$, et si $f^{(p)}$ admet une limite finie en x_0, alors f se prolonge en une fonction de de classe $\mathcal{C}^p$ sur I.

Réponse

$\boxed{\text{Cas } p = 1}$ Soit $x_1 \in I \setminus \{x_0\}$. Puisque f' admet une limite finie en x_0, l'intégrale généralisée $\displaystyle\int_{x_0}^{x_1} f'(t)\,dt$ converge donc. On a alors

$$f(x) = f(x_1) - \int_x^{x_1} f'(t)\,dt \xrightarrow[x \to x_0]{} f(x_1) - \int_{x_0}^{x_1} f'(t)\,dt.$$

Autrement dit, f possède une limite finie en x_0, et donc f se prolonge par continuité en x_0 (on note encore son prolongement f). Par le théorème d'extension de la dérivée, f est alors dérivable en x_0 et $f'(x_0) = \ell$. On en déduit que $f' \in \mathcal{C}^0(I)$ et donc $f \in \mathcal{C}^1(I)$.

$\boxed{\text{Cas } p \in \mathbb{N}^*}$ On démontre par récurrence finie descendante sur $k \in [\![0, p-1]\!]$ que $f^{(k)}$ se prolonge en une fonction de classe $\mathcal{C}^1$ dont la dérivée est le prolongement de $f^{(k+1)}$ en utilisant le cas $p = 1$ démontré plus haut.

♢

2. Propriétés héritées de l'intégrale sur un segment

Proposition 1.12

Soient I un intervalle non-trivial de $\mathbb{R}$ et $f, g \in \mathcal{C}_m^0(I, \mathbb{K})$. Alors

(i) Si $\displaystyle\int_I f$ et $\displaystyle\int_I g$ convergent, alors pour tous $\lambda, \mu \in \mathbb{K}$, $\displaystyle\int_I (\lambda f + \mu g)$ converge et

$$\int_I (\lambda f + \mu g) = \lambda \int_I f + \mu \int_I g.$$

(ii) Si $\mathbb{K} = \mathbb{R}$ et $f \geq 0$ et $\displaystyle\int_I f$ converge alors $\displaystyle\int_I f(t)\,dt \geq 0$.

(iii) Si $\mathbb{K} = \mathbb{R}$ et $f \leq g$ et $\displaystyle\int_I f$ et $\displaystyle\int_I g$ convergent, alors $\displaystyle\int_I f \leq \int_I g$.

(iv) Si $\mathbb{K} = \mathbb{C}$, alors

$$\int_I f \text{ converge} \iff \begin{cases} \int_I \Re(f) \text{ converge} \\ \int_I \operatorname{Im}(f) \text{ converge} \end{cases} \iff \int_I \overline{f} \text{ converge.}$$

De plus, si ces intégrales convergent, alors

$$\Re\left(\int_I f\right) = \int_I \Re(f), \quad \operatorname{Im}\left(\int_I f\right) = \int_I \operatorname{Im}(f), \quad \overline{\int_I f} = \int_I \overline{f}.$$

Démonstration : Notons $a = \inf I$ et $b = \sup I$ (potentiellement $a = -\infty$ ou $b = +\infty$). Soit $x, c, y \in \mathring{I}$ tels que $x < c < y$.

(i) Soient $\lambda, \mu \in \mathbb{K}$. Remarquons que $\lambda f + \mu g \in \mathcal{C}_m^0\left(]a, b[\right)$, et alors

$$\int_x^c (\lambda f + \mu g) = \lambda \int_x^c f + \mu \int_x^c g.$$

Puisque $\displaystyle\int_I f$ et $\displaystyle\int_I g$ convergent, alors $\displaystyle\lim_{x \to a^-} \int_x^c (\lambda f + \mu g)$ existe et

$$\int_a^c (\lambda f + \mu g) = \lambda \int_a^c f + \mu \int_a^c g.$$

De même,

$$\int_c^b (\lambda f + \mu g) = \lambda \int_c^b f + \mu \int_c^b g.$$

Donc

$$\int_a^b (\lambda f + \mu g) = \lambda \int_a^b f + \mu \int_a^b g.$$

(ii) Puisque $f \geq 0$, et $\displaystyle\int_I f$ converge, on a

$$\int_x^c f \geq 0, \quad \int_a^c f = \lim_{x \to a^+} \int_x^c f \geq 0.$$

De même, $\displaystyle\int_c^b f \geq 0$. Donc $\displaystyle\int_a^b f = \int_a^c f + \int_c^b f \geq 0$.

(iii) On applique simplement les résultats (i) et (ii) à $g - f$, qui est une fonction positive sur I.

(iv) On remarque que pour tous $x, y \in \mathring{I}$,

$$\int_x^y f = \int_x^y \Re(f) + i \int_x^y \operatorname{Im}(f), \quad \int_x^y \overline{f} = \overline{\int_x^y f},$$

puis on applique le même type de raisonnement que précédemment.

□

Exercice 1.13 :
Etudier la nature des intégrales $\displaystyle\int_1^{+\infty} \frac{dt}{t + t^2}$ et $\displaystyle\int_{-\infty}^{+\infty} \sin t dt$.

Réponse

1. Posons pour tout $t \geq 1, f(t) = \dfrac{1}{t + t^2}$. Alors $f \in \mathcal{C}_m^0([1, +\infty[)$. Le seul point incertain est donc $+\infty$. On a, pour tout $x > 1$,

$$\int_1^x f(t)\, dt = \int_1^x \frac{dt}{t} - \int_1^x \frac{dt}{1+t} = \left[\ln\left(\frac{t}{1+t}\right)\right]_{t=1}^x = \ln 2 - \ln\left(\frac{x}{1+x}\right).$$

Donc $\displaystyle\int_1^{+\infty} f(t)\, dt$ converge et

$$\int_1^{+\infty} \frac{dt}{t + t^2} = \lim_{x \to +\infty} \left(\ln 2 - \ln\left(\frac{x}{1+x}\right)\right) = \ln 2.$$

Par contre, on ne peut pas écrire

$$\int_1^{+\infty} \frac{dt}{t+t^2} = \int_1^{+\infty} \frac{dt}{t} - \int_1^{+\infty} \frac{dt}{1+t}.$$

2. $\sin \in \mathcal{C}_m^0(\mathbb{R})$ donc $-\infty$ et $+\infty$ sont deux points incertains. On a, pour tout $x > 0$,

$$\int_0^x \sin t dt = [-\cos t]_{t=0}^x = 1 - \cos x.$$

On sait que $\cos$ n'admet pas de limite en $+\infty$ donc $\int_0^{+\infty} \sin t dt$ diverge, et par suite $\int_{-\infty}^{+\infty} \sin t dt$ diverge.

Par contre, pour tout $x > 0$, on a

$$\int_{-x}^x \sin t dt = 0, \qquad \lim_{x\to+\infty} \int_{-x}^x \sin t dt = 0.$$

◇

3. Intégrales de Riemann

Théorème 1.14 *Critère de Riemann*

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

(i) L'intégrale $\int_0^1 \frac{dt}{t^\alpha}$ converge si, et seulement si, $\alpha < 1$.

(ii) L'intégrale $\int_1^{+\infty} \frac{dt}{t^\alpha}$ converge si, et seulement si, $\alpha > 1$.

Démonstration : Notons $f_\alpha : t \mapsto^{-\alpha}$. Remarquons que la fonction f^α est continue sur $\mathbb{R}_+^*$ donc $f \in \mathcal{C}_m^0(\mathbb{R}_+^*)$. Notons, pour $t > 0$,

$$F_\alpha(t) = \begin{cases} \frac{t^{1-\alpha}}{1-\alpha} & \text{si } \alpha \neq 0 \\ \ln t & \text{si } \alpha = 0 \end{cases}.$$

La fonction F_α est une primitive de f_α sur $\mathbb{R}_+^*$.

(i) Pour tout $x \in]0,1[$, on a

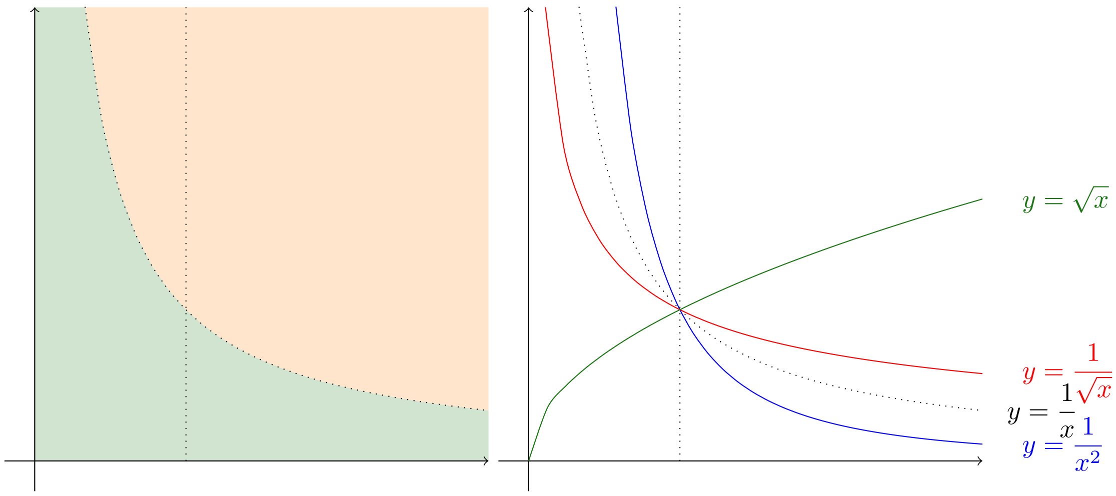
$$\int_x^1 f_\alpha = F_\alpha(1) - F_\alpha(x), \qquad \lim_{x\to 0^+} F_\alpha(x) \in \mathbb{R} \iff 1-\alpha > 0 \iff \alpha < 1.$$

(ii) Pour tout $y \in]1,+\infty[$, on a

$$\int_1^y f_\alpha = F_\alpha(y) - F_\alpha(1), \qquad \lim_{y\to+\infty} F_\alpha(y) \in \mathbb{R} \iff 1-\alpha < 0 \iff \alpha > 1.$$

□

Les intégrales de Riemann sont fondamentales, car elles donnent une idée de "quelle intégrale converge ou ne converge pas" (pour des fonctions positives).



II Fonctions positives et intégrabilité

Dans la première section de ce chapitre, on a vu comment généraliser l'intégration sur un segment à l'intégration sur un intervalle. Mais pour l'instant, la seule méthode de justification de l'existence d'une intégrale est celle du calcul effectif de cette intégrale, c'est-à-dire de trouver une primitive de l'intégrande.

On va voir que pour les fonctions positives (et par extension, les fonctions de signe constant), on dispose de nombreuses méthodes pour justifier que l'intégrale converge sans avoir à déterminer une primitive de l'intégrande.

Dans tout ce qui suit, I est un intervalle non-trivial de $\mathbb{R}$.

1. Intégrale d'une fonction positive

Théorème 2.1 *Admis*

Soit $f \in \mathcal{C}^0_m(I, \mathbb{R})$. Si $f \geq 0$, alors

$$\int_I f \text{ converge} \iff \exists M > 0, \forall a, b \in I, \int_{[a,b]} f \leq M.$$

Dans ce cas, on a alors $\displaystyle\int_I f = \sup_{a,b \in I} \int_{[a,b]} f$.

Idée de la démonstration : Dans le cas où $I = [a, b[$ avec $a < b \leq +\infty$, on pose

$$F : x \mapsto \int_a^x f(t)\, dt.$$

Puisque f est positive, F est croissante sur $[a, b[$. Donc

$$\lim_{x \to b} F(x) \text{ existe} \iff F \text{ est majorée sur } I.$$

Dans ce cas, on a

$$\lim_{x \to b} F(x) = \sup_I F.$$

$\square$

Corollaire 2.2

Si $f, g \in \mathcal{C}_m^0(I, \mathbb{R})$, si $0 \leq f \leq g$ et si $\displaystyle\int_I g$ converge, alors $\displaystyle\int_I f$ converge et

$$0 \leq \int_I f \leq \int_I g.$$

Exercice 2.3 :
Montrer que $\dfrac{dt}{t+t^2}$ est convergente sans déterminer la primitive de l'intégrande. $\diamondsuit$

2. Comparaison de fonctions positives

Dans le cas des fonctions positives, grâce au résultat précédent, on est désormais en mesure de donner des critères de convergence de $\displaystyle\int_I f$ sans savoir calculer cette intégrale.

Théorème 2.4 *Comparaison de fonction positives*

Soient $f, g \in \mathcal{C}_m^0([a, b[, \mathbb{R})$ avec $a < b \leq +\infty$. Si f et g sont positives sur $[a, b[$, alors

(i) Si $f(t) \underset{t \to b^-}{\sim} g(t)$ alors

$$\int_I g \text{ converge} \iff \int_I f \text{ converge.}$$

(ii) Si $f(t) \underset{t \to b^-}{=} O(g(t))$ alors

$$\int_I g \text{ converge} \Rightarrow \int_I f \text{ converge.}$$

(iii) Si $f(t) \underset{t \to b^-}{=} o(g(t))$ alors

$$\int_I g \text{ converge} \Rightarrow \int_I f \text{ converge.}$$

Dans le cas où $f = o(g)$ ou $f = O(g)$, on utilisera aussi souvent la contraposée, qui fournit un critère de divergence :

$$\int_I f \text{ diverge} \Rightarrow \int_I g \text{ diverge.}$$

Démonstration : $\boxed{(ii)}$ Par définition, il existe $c \in]a, b[$ et $M > 0$ tels que

$$\forall x \in [c, b[, \quad 0 \leq f(x) \leq M g(x), \quad \int_{[c,x]} f \leq M \int_{[c,x]} g \leq M \int_c^b g$$

Donc $\displaystyle\int_c^b f$ converge.

$\boxed{(i)}$ Si $f \sim g$ alors $f = O(g)$ et $g = O(f)$.

$\boxed{(iii)}$ Si $f = o(g)$ alors $f = O(g)$. $\square$

Exercice 2.5 :
Pour $t > 0$, on pose $f(t) = \dfrac{\ln t}{1+t+t^3}$.

1. Montrer que $\displaystyle\int_1^{+\infty} \frac{\ln t}{t^3} dt$ converge.
2. Montrer que $\displaystyle\int_0^1 \ln t dt$ converge.
3. En déduire que $\displaystyle\int_0^{+\infty} f(t)\, dt$ converge.

Réponse

Tout d'abord, les fonctions considérées sont continues par morceaux sur $]0, +\infty[$.

1. Remarquons que $t \mapsto \dfrac{\ln t}{t^3}$ est positive au voisinage de $+\infty$.
$$t^2 \frac{\ln t}{t^3} \xrightarrow[t \to +\infty]{} 0, \qquad \frac{\ln t}{t^3} \underset{t\to+\infty}{=} o\left(\frac{1}{t^2}\right).$$
Or $\displaystyle\int_1^{+\infty} \frac{dt}{t^2}$ est une intégrale de Riemann convergente car $2 > 1$. Donc $\displaystyle\int_1^{+\infty} \frac{\ln t}{t^3} dt$ converge.
2. Pour tout $x \in]0, 1[$, on a
$$\int_x^1 \ln t dt = [t \ln t - t]_{t=x}^1 = x - x \ln x - 1, \qquad \int_0^1 \ln t dt = -1,$$
donc $\displaystyle\int_0^1 \ln t dt$ converge.
3. Pour tout $t \in [1, +\infty[$, on a
$$f(t) \geq 0, \quad \frac{\ln t}{t^3} \geq 0, \quad f(t) \underset{t\to+\infty}{\sim} \frac{\ln t}{t^3},$$
donc $\displaystyle\int_1^{+\infty} f$ converge. De plus, pour $t \in]0, 1]$,
$$-f(t) \geq 0, \quad -\ln t \geq 0, \quad -f(t) \underset{t\to 0^+}{\sim} -\ln t.$$
Donc $\displaystyle\int_0^1 (-f)$ converge donc $\displaystyle\int_0^1 f$ converge. Donc $\displaystyle\int_0^{+\infty} f$ converge.

♢

Remarque 2.6 : Le théorème 2.4 est extrêmement important lorsqu'on ne sait pas calculer directement la primitive d'une fonction dont on souhaite déterminer si son intégrale généralisée converge. Comme on l'a déjà vu dans l'exemple précédent, les conclusions du théorème 2.4 restent valable dans plusieurs cas plus généraux (pour des fonctions à valeurs réelles) :

- f et g sont positives sur un voisinage (à gauche) de b (on restreint l'intervalle à $[c, b[$).
- f et g sont négatives sur un voisinage (à gauche) de b (on considère $-f$ et $-g$).
- on effectue une intégrale généralisée "à gauche" (avec les relations de comparaison correspondantes en a^+).

♢

Ce résultat est faux pour les fonctions complexes ou de signe quelconque. En effet, par exemple,

$$f(t) = \frac{|\sin t|}{t}, \quad g(t) = \frac{\sin t}{\sqrt{t}}, \quad f(t) \underset{t \to +\infty}{=} o(g(t)),$$

or on verra plus tard que

$$\int_1^{+\infty} f(t)\, dt \text{ diverge}, \quad \int_1^{+\infty} g(t)\, dt = \text{ converge.}$$

3. Intégrabilité sur un intervalle

Définition 2.7 *Absolue convergence et intégrabilité*

Soit $f \in \mathcal{C}_m^0(I, \mathbb{K})$. On dit que $\int_I f$ est *absolument convergente* si $\int_I |f(t)|dt$ converge. On dit aussi que f est *intégrable* sur I

Si $\int_I f$ converge mais que f n'est pas intégrable, on dit que $\int_I f$ est *semi-convergente*.

Contrairement à ce qu'on pourrait croire au premier abord, f n'est pas intégrable si son intégrale existe, mais bien si $\int_I |f|$ existe. On note aussi $f \in L^1(I)$.

Si f est positive (ou plus généralement, de signe constant au voisinage des points incertains), alors f est intégrable si, et seulement si, son intégrale converge.

Théorème 2.8

Soit $f \in \mathcal{C}_m^0(I, \mathbb{K})$. Alors

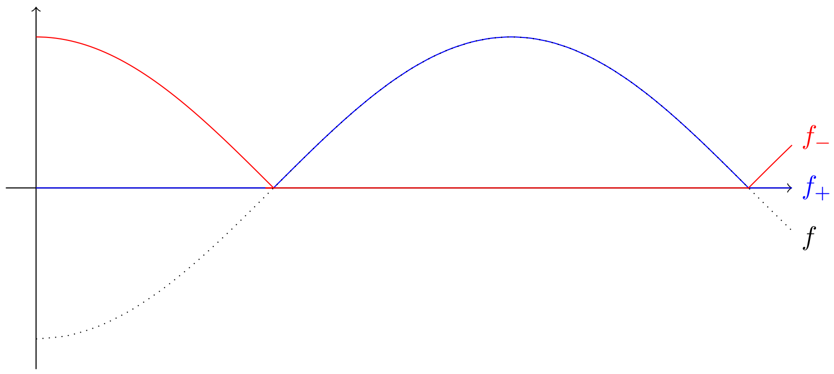
$$\int_I f \text{ converge absolument} \Rightarrow \int_I f \text{ converge.}$$

Il existe des fonctions donc l'intégrale est semi-convergente. A l'exercice 3.9, on verra que

$$\int_0^{+\infty} \frac{\sin t}{t} dt \text{ converge}, \quad \int_0^{+\infty} \frac{|\sin t|}{t} dt \text{ diverge.}$$

Démonstration : On fait la preuve uniquement dans le cas où f est à valeurs réelles. Notons $f_- = -\min(0, f)$ et $f_+ = \max(0, f)$; on a

$$f_+ \geq 0, \quad f_- \geq 0, \quad f = f_+ - f_-, \quad |f| = f_+ + f_-.$$



Supposons que f soit intégrable sur I, alors pour tout $a, b \in I$,

$$f_+ \leq |f|, \quad \int_{[a,b]} f_+ \leq \int_{[a,b]} |f| \leq \int_I |f|,$$

donc $\int_I f_+$ converge. De même, $\int_I f_-$ converge. Donc $\int_I f = \int_I (f_+ - f_-)$ converge. □

Proposition 2.9 *Inégalité triangulaire*

Soit $f \in \mathcal{C}_m^0(I, \mathbb{K})$. Si $\int_I f$ converge absolument alors

$$\left|\int_I f(t)\,dt\right| \leq \int_I |f(t)|dt.$$

Démonstration : Supposons que f soit intégrable sur I. Alors $\int_I f$ converge et on a

$$-|f| \leq f \leq |f|, \quad -\int_I |f| \leq \int_I f \leq \int_I |f|, \quad \left|\int_I f\right| \leq \int_I |f|.$$

□

4. Plan d'étude

Soient $-\infty \leq a < b \leq +\infty$ et $f \in \mathcal{C}_m^0(]a, b[)$. Pour déterminer si $\int_a^b f$ converge :

0. On vérifie que la fonction f est bien continue (ou continue par morceaux) sur $]a, b[$.
1. Si a ou b sont finis, on vérifie d'abord s'il y a un problème : on se demande si $\lim\limits_{a^+} f$ ou $\lim\limits_{b^-} f$ sont finies.
2. On découpe l'intervalle en $]a, c]$ et $[c, b[$ et on traite un problème à la fois.
3. Si possible, on détermine une primitive F de f et on étudie $\lim\limits_{a^+} F$ et $\lim\limits_{b^-} F$.
4. Sinon, on considère $|f|$:
   (a) Si possible, on trouve un équivalent simple de f dont on connait l'intégrabilité sur $]a, b[$.
   (b) Sinon, on essaie de comparer $|f|$ à une fonction simple dont on connaît l'intégrabilité.
5. Si l'on n'a pas réussi à montrer que $\int_a^b |f|$ converge, on ne sait pas quoi dire (pour l'instant).

Exemple 2.10 :

Déterminons la nature de $\int_0^{+\infty} \frac{\sin t}{t^{3/2}} dt$.

1. Posons $f : t \mapsto \dfrac{\sin t}{t^{3/2}}$. La fonction f est continue sur $]0, +\infty[$ (comme composée de fonctions continues sur leurs domaines de définition). $+\infty$ est évidemment un point incertain. De plus, $\lim\limits_{t\to 0^+} f(t) = +\infty$ donc 0 est aussi un point incertain.
2. On étudie la convergence des intégrales $\displaystyle\int_0^1 f(t)\,dt$ et $\displaystyle\int_1^{+\infty} f(t)\,dt$.
3. Puisqu'on ne reconnait pas de primitive pour f, on doit procéder autrement.
4. (a) La fonction f est positive sur $]0, 1]$. De plus, on a
$$f(t) \underset{t\to 0^-}{\sim} \frac{t}{t^{3/2}} = \frac{1}{t^{1/2}}.$$
La fonction $t \mapsto t^{-1/2}$ est continue par morceaux et positive sur $]0, 1]$, et $\displaystyle\int_0^1 t^{-1/2}$ converge d'après le critère de Riemann. Donc $\displaystyle\int_0^1 f$ converge.

   (b) La fonction f n'est pas de signe constant sur $[1, +\infty[$ (elle oscille en $+\infty$). Par contre, on a
$$|f(t)| = \left|\frac{\sin t}{t^{3/2}}\right| \leq \frac{1}{t^{3/2}}.$$
La fonction $t \mapsto t^{-3/2}$ est continue par morceaux et positive sur $[1, +\infty[$, et $\displaystyle\int_1^{+\infty} t^{-3/2}$ converge d'après le critère de Riemann. Donc $\displaystyle\int_1^{+\infty} f$ converge.

En conclusion, $\displaystyle\int_0^{+\infty} \frac{\sin t}{t^{3/2}} dt$ converge. ◊

III Intégrales généralisées en pratique

1. Intégrales de Bertrand

<u>Théorème 3.1</u> *Critère de Bertrand*

Soient $\alpha, \beta \in \mathbb{R}$. Alors

(i) L'intégrale $\displaystyle\int_0^{1/2} \frac{dt}{t^\alpha |\ln t|^\beta}$ converge si, et seulement si, $\alpha < 1$ ou ($\alpha = 1$ et $\beta > 1$).

(ii) L'intégrale $\displaystyle\int_2^{+\infty} \frac{dt}{t^\alpha \ln^\beta t}$ converge si, et seulement si, $\alpha > 1$ ou ($\alpha = 1$ et $\beta > 1$).

Démonstration : Remarquons que la fonction $f_{\alpha,\beta}$ définie par
$$\forall t > 0, \quad f_{\alpha,\beta}(t) = \frac{1}{t^\alpha |\ln t|^\beta}$$
est continue et positive sur $]0, 1/2]$ et sur $[2, +\infty[$.

1. (i) Cas 1 : $\alpha > 1$. Posons $\varepsilon = \dfrac{\alpha - 1}{2}$. Alors, par croissances comparées,
$$f_{\alpha,\beta}(t) = \frac{1}{t^\varepsilon |\ln t|^\beta} \times \frac{1}{t^{1+\varepsilon}} = \underset{t\to+\infty}{=} o\left(\frac{1}{t^{1+\varepsilon}}\right) \text{ qui est intégrable sur } [2, +\infty[.$$
Donc $\displaystyle\int_2^{+\infty} f_{\alpha,\beta}(t)\,dt$ converge.

(i) Cas 2 : $\alpha < 1$. Posons $\varepsilon = \dfrac{1-\alpha}{2}$. Alors, par croissances comparées,

$$\frac{\ln^\beta t}{t^\varepsilon} \xrightarrow[t\to+\infty]{} 0, \quad \frac{1}{t^{1-\varepsilon}} = \frac{\ln^\beta t}{t^{1-\varepsilon} t^\varepsilon \ln^\beta t} = \frac{\ln^\beta t}{t^\varepsilon} f_{\alpha,\beta}(t) \underset{t\to+\infty}{=} o\left(f_{\alpha,\beta}(t)\right)$$

et $\displaystyle\int_2^{+\infty} \frac{dt}{t^{1-\varepsilon}}$ diverge d'après le critère de Riemann. Donc $\displaystyle\int_0^{1/2} f_{\alpha,\beta}(t)\,dt$ diverge.

(i) Si $\alpha = 1$, $f_{1,\beta}$ possède une primitive sur $[2,+\infty[$ définie par

$$\forall t \in [2,+\infty[, \quad F_{1,\beta}(t) = \begin{cases} \frac{|\ln t|^{1-\beta}}{1-\beta} & \text{si } \beta \neq 1 \\ \ln(|\ln t|) & \text{si } \beta = 1 \end{cases}.$$

Alors,

$$\beta \leq 1 \Rightarrow \lim_{t\to+\infty} F_{1,\beta}(t) = +\infty, \quad \beta > 1 \Rightarrow \lim_{t\to+\infty} F_{1,\beta}(t) = 0.$$

On en déduit que $\displaystyle\int_2^{+\infty} f_{\alpha,\beta}$ converge si, et seulement si, $\alpha < 1$ ou ($\alpha = 1$ et $\beta > 1$).

2. Soit $a > 2$. Alors, avec le changement de variable $u = \dfrac{1}{t}$,

$$\int_{\frac{1}{a}}^{\frac{1}{2}} \frac{dt}{t^\alpha |\ln t|^\beta} = -\int_a^2 u^{\alpha-2} \left|\ln \frac{1}{u}\right|^\beta du = \int_2^a \frac{du}{u^{2-\alpha} \ln^\beta u}.$$

D'après (i), on a donc

$$\begin{aligned} \int_2^{+\infty} \frac{dt}{t^\alpha \ln^\beta t} \text{ converge } &\iff 2-\alpha > 1 \text{ ou } (2-\alpha = 1 \text{ et } \beta > 1) \\ &\iff \alpha < 1 \text{ ou } (\alpha = 1 \text{ et } \beta > 1) \end{aligned}$$

□

Exemple 3.2 :
Etudions la nature de $\displaystyle\int_2^{+\infty} f(t)\,dt$ avec $f(t) = \sqrt{t^2+3t} \ln\left(\cos\frac{1}{t}\right) \sin^2\left(\frac{1}{\ln t}\right)$. La fonction $f \in \mathcal{C}^0_m([2,+\infty[)$, le seul point incertain est donc $+\infty$. De plus,

$$\ln\left(\cos\frac{1}{t}\right) \xrightarrow[t\to+\infty]{} 0^-, \quad \sin^2\left(\frac{1}{\ln t}\right) \xrightarrow[t\to+\infty]{} 0^+, \quad \sqrt{t^2+3t} \xrightarrow[t\to+\infty]{} +\infty.$$

donc f est négative au voisinage de $+\infty$. De plus, on a, pour t au voisinage de $+\infty$,

$$\begin{aligned} \sqrt{t^2+3t} &= t\sqrt{1+\frac{3}{t}} = t\,(1+o(1)) \underset{t\to+\infty}{\sim} t, \\ \ln\left(\cos\frac{1}{t}\right) &= \ln\left(1-\frac{1}{2t^2}+o\left(\frac{1}{t^2}\right)\right) = -\frac{1}{2t^2}+o\left(\frac{1}{t^2}\right) \underset{t\to+\infty}{\sim} -\frac{1}{2t^2}, \\ \sin^2\left(\frac{1}{\ln t}\right) &= \left(\frac{1}{\ln t}+o\left(\frac{1}{\ln t}\right)\right)^2 = \frac{1}{\ln^2 t}+o\left(\frac{1}{\ln^2 t}\right) \underset{t\to+\infty}{\sim} \frac{1}{\ln^2 t}, \\ f(t) &\underset{t\to+\infty}{\sim} \frac{1}{-2t\ln^2 t}. \end{aligned}$$

La fonction $t \mapsto \dfrac{1}{-2t\ln^2 t}$ est négative au voisinage de $+\infty$ donc les intégrales associées sont de même nature. Or $\displaystyle\int_2^{+\infty} \frac{dt}{-2t\ln^2 t}$ converge (c'est une intégrale de Bertrand), donc $\displaystyle\int_2^{+\infty} f(t)\,dt$ converge. ◇

2. Changement de variable

On peut faire des changements de variables sur des intervalles, à peu près de la même façon que sur des segments.

Théorème 3.3 *Changement de variable*

Soient $-\infty \leq \alpha < \beta \leq +\infty$ et I un intervalle non-trivial de $\mathbb{R}$. Soit $\Phi \in \mathcal{C}^1\left(]\alpha, \beta[, I\right)$. Si f est continue sur I et si Φ est monotone, alors, en notant $\Phi(\alpha) = \lim\limits_{\alpha^+} \Phi$ et $\Phi(\beta) = \lim\limits_{\beta^-} \Phi$,

$$\int_{\Phi(\alpha)}^{\Phi(\beta)} f(u)\,du \text{ converge } \iff \int_{\alpha}^{\beta} f(\Phi(t))\,\Phi'(t)\,dt \text{ converge.}$$

Si les intégrales convergent alors on a

$$\int_{\Phi(\alpha)}^{\Phi(b)} f(u)\,du = \int_{\alpha}^{\beta} f(\Phi(t))\,\Phi'(t)\,dt.$$

On dit qu'on fait le changement de variable $u = \Phi(t)$.

Démonstration : Puisque Φ est monotone, $\Phi(\alpha) = \lim\limits_{\alpha^+} \Phi$ et $\Phi(\beta) = \lim\limits_{\beta^-} \Phi$ existent toujours (dans $\overline{\mathbb{R}}$). Pour simplifier, supposons que Φ est croissante. La fonction f est continue sur I donc sur $]\Phi(\alpha), \Phi(\beta)[$. De même, par composition de fonctions continues, la fonction $(f \circ \Phi)\,\Phi'$ est continue sur $]\alpha, \beta[$. Les intégrales sont donc bien définies. $f \in \mathcal{C}^0(I)$ donc f possède une primitive F sur I On a alors, pour tous $x < y \in]\alpha, \beta[$

$$(\star) \quad \int_{\Phi(x)}^{\Phi(y)} f(u)\,du = F(\Phi(y)) - F(\Phi(x)) = \int_x^y (F \circ \Phi)'(t)\,dt = \int_x^y f(\Phi(t))\,\Phi'(t)\,dt.$$

C'est la formule du changement de variable pour l'intégrale sur le segment $[x, y]$. L'intégrale de gauche dans $(\star)$ admet une limite quand $y \to \beta^-$ si et seulement si l'intégrale de droite en admet une, ce qui donne

$$\int_{\Phi(x)}^{\Phi(\beta)} f(u)\,du \text{ converge } \iff \int_{x}^{\beta} f(\Phi(t))\,\Phi'(t)\,dt \text{ converge.}$$

On a évidemment de la même manière,

$$\int_{\Phi(\alpha)}^{\Phi(y)} f(u)\,du \text{ converge } \iff \int_{\alpha}^{y} f(\Phi(t))\,\Phi'(t)\,dt \text{ converge.}$$

Si toutes ces intégrales convergent, on a, en passant à la limite dans $(\star)$,

$$\int_{\Phi(\alpha)}^{\Phi(b)} f(u)\,du = \int_{\alpha}^{\beta} f(\Phi(t))\,\Phi'(t)\,dt.$$

Si Φ est décroissante, $(\star)$ devient

$$\int_{\Phi(x)}^{\Phi(y)} f(u)\,du = -\int_{\Phi(y)}^{\Phi(x)} f(u)\,du = -[F(\Phi(x)) - F(\Phi(y))] = \int_x^y f(\Phi(t))\,\Phi'(t)\,dt.$$

□

On traite ici un cas particulier, où f est continue et non plus continue par morceaux. On veillera donc simplement à découper les intégrales suivant une subdivison adaptée pour se retrouver avec des fonctions continues.

En pratique, on aura plutôt des intégrales du type $\int_a^b f(\Psi(u))\,du$ avec $-\infty \leq a < b \leq +\infty$. On veut donc pouvoir écrire (sous réserve de convergence des intégrale) :

$$\int_a^b f(\Psi(u))\,du \underset{t=\Psi(u)}{=} \int_{\Psi(a)}^{\Psi(b)} f(t)\left(\Psi^{-1}\right)'(t)\,dt.$$

Une condition suffisante pour effectuer un changement de variable est donc "Φ (resp. Ψ) est un difféomorphisme sur $]\alpha,\beta[$ (resp. $]a,b[$)".

Un changement de variable peut changer une intégrale "classique" en une intégrale généralisée et vice-versa. A condition de le remarquer, il n'y a aucun problème d'intégrabilité.

Exemple 3.4 :

Déterminons la valeur de $\int_{-\pi}^{\pi} \frac{du}{2+\cos u}$. Remarquons que la fonction $f(u) = \frac{1}{2+\cos u}$ est continue sur $[-\pi,\pi]$. Donc $\int_{-\pi}^{\pi} f(u)\,du$ converge. Alors, d'après les règles de Bioche,

$$\int_{-\pi}^{\pi} \frac{du}{2+\cos u} \underset{t=\tan(u/2)}{=} \int_{-\infty}^{+\infty} \frac{2dt}{3+t^2} = \frac{2}{3}\int_{-\infty}^{+\infty} \frac{dt}{1+\left(\frac{t}{\sqrt{3}}\right)^2} \underset{x=t/\sqrt{3}}{=} \frac{2}{\sqrt{3}}\int_{-\infty}^{+\infty} \frac{dx}{1+x^2},$$

et toutes ces intégrales sont convergentes (tous les changements de variables sont des bijections $\mathcal{C}^1$ sur les intervalles considérés). On a donc

$$\int_{-\pi}^{\pi} \frac{du}{2+\cos u} = \frac{2}{\sqrt{3}}\left[\arctan x\right]_{x=-\infty}^{+\infty} = \frac{2\pi}{\sqrt{3}}.$$

$\diamondsuit$

Exercice 3.5 :

1. Déterminer la nature de $\int_0^{+\infty} \frac{\cos u}{\sqrt{u}}du$.
2. En déduire la nature de $\int_{-\infty}^{+\infty} \cos\left(x^2\right)dx$.

Réponse

1. Posons $f : u \mapsto \frac{\cos u}{\sqrt{u}}$. $f \in \mathcal{C}^0(]0,+\infty[)$ donc il y a deux points incertains : 0 et $+\infty$ (on découpera donc par exemple l'intégrale en 1).
   $\boxed{\text{En } 0}$ Pour tout $u \in]0,1]$, on a $|f(u)| \leq u^{-1/2}$. La fonction $u \mapsto u^{-1/2}$ est intégrable sur $]0,1]$ d'après le critère de Riemann, donc $\int_0^1 f$ converge absolument (donc converge).
   $\boxed{\text{En } +\infty}$ La majoration habituelle $|\cos| \leq 1$ ne donne rien ici, on raisonne donc par IPP. On a, pour tout $a > 1$,
   $$\int_1^a \frac{\cos u}{\sqrt{u}}du = \left[\frac{\sin u}{\sqrt{u}}\right]_1^a + \int_1^a \frac{\sin u}{2u^{3/2}}du = \frac{\sin a}{\sqrt{a}} - \sin(1) + \int_1^a \frac{\sin u}{2u^{3/2}}du.$$
   L'intégrale $\int_1^{+\infty} \frac{\sin u}{2u^{3/2}}du$ converge absolument (encore une fois par le critère de Riemann) et
   $$\lim_{a\to+\infty} \frac{\sin a}{\sqrt{a}} = 0.$$

On en déduit donc que $\displaystyle\int_1^{+\infty} f(u)\,du$ converge.

Conclusion : $\displaystyle\int_0^{+\infty} \frac{\cos u}{\sqrt{u}} du$ converge.

2. La fonction $g : x \mapsto \cos\left(x^2\right)$ est continue sur $\mathbb{R}$ donc les deux points incertains sont $-\infty$ et $+\infty$. On sépare donc l'intégrale en $\displaystyle\int_{-\infty}^{0} \cos\left(x^2\right) dx$ et $\displaystyle\int_0^{+\infty} \cos\left(x^2\right) dx$. En effectuant le changement de variable $t = -x$ dans la première intégrale, on a

$$\int_{-\infty}^{0} \cos\left(x^2\right) dx \text{ converge} \underset{t=-x}{\iff} \int_0^{+\infty} \cos\left(t^2\right) dt \text{ converge,}$$

donc il suffit de déterminer la nature de $\displaystyle\int_0^{+\infty} g(x)\,dx$. Par changement de variable $u = x^2$, on a

$$\int_0^{+\infty} \cos\left(x^2\right) dx \text{ converge} \underset{u=x^2}{\iff} \int_0^{+\infty} \frac{\cos u}{2\sqrt{u}} du \text{ converge.}$$

D'après la question 1, $\displaystyle\int_{-\infty}^{+\infty} \cos\left(x^2\right) dx$ converge.

$\diamondsuit$

Exercice 3.6 :

Déterminer la nature de l'intégrale $\displaystyle\int_0^{+\infty} \mathrm{e}^{-\sqrt{x}}\,dx$ et déterminer sa valeur si elle converge.

Réponse

Soit $f : x \mapsto \mathrm{e}^{-\sqrt{x}}$. $f \in \mathcal{C}^0\left(\mathbb{R}_+\right)$ donc le seul point incertain est en $+\infty$. Remarquons que f est positive sur $\mathbb{R}_+$. De plus, on a

$$x^2 f(x) \xrightarrow[x\to+\infty]{} 0, \quad f(x) = \underset{x\to+\infty}{=} o\left(\frac{1}{x^2}\right).$$

La fonction $x \mapsto x^{-2}$ est positive, continue par morceaux et intégrable sur $[1, +\infty[$ donc $\displaystyle\int_1^{+\infty} f(x)\,dx$ converge donc $\displaystyle\int_0^{+\infty} f(x)\,dx$ converge. On a alors

$$\int_0^{+\infty} \mathrm{e}^{-\sqrt{x}}\,dx \underset{t=\sqrt{x}}{=} 2\int_0^{+\infty} t\,\mathrm{e}^{-t}\,dt.$$

Pour tout $a > 0$, on a

$$\int_0^{a} t\,\mathrm{e}^{-t}\,dt = \left[-t\,\mathrm{e}^{-t}\right]_{t=0}^{a} + \int_0^{a} \mathrm{e}^{-t}\,dt = -a\,\mathrm{e}^{-a} + \left[-\,\mathrm{e}^{-t}\right]_{t=0}^{a} = 1 - (a+1)\,\mathrm{e}^{-a} \xrightarrow[a\to+\infty]{} 1.$$

Donc $\displaystyle\int_0^{+\infty} \mathrm{e}^{-\sqrt{x}}\,dx = 2\int_0^{+\infty} t\,\mathrm{e}^{-t}\,dt = 2.$

$\diamondsuit$

3. Intégration par parties

La règle à retenir est la suivante : on ne fait pas d'intégration par parties avec des intégrales généralisées. Par exemple, dans le cas de fonctions continues par morceaux sur $[a, b[$, on fera le changement de variable ou l'intégration par parties classiques sur $[a, x]$ avant de faire tendre x vers b.

Exemple 3.7 :
La fonction $t \mapsto \dfrac{\ln t}{(1+t)^2}$ étant continue et négative sur $]0,1]$, on montre facilement par comparaison de fonctions négatives que $\displaystyle\int_0^1 \frac{\ln t}{(1+t)^2}$ converge. Les fonctions ln et $t \mapsto \dfrac{-1}{1+t}$ sont bien de classe $\mathcal{C}^1$ sur $]0,1]$, mais ça n'a aucun sens d'écrire

$$\int_0^1 \frac{\ln t}{(1+t^2)} dt = \left[\frac{-\ln t}{1+t}\right]_0^1 + \int_0^1 \frac{dt}{t(1+t)}.$$

En effet, les deux quantités dans le membre de droite sont en fait des limites (d'une intégrale sur $[x, 1]$ quand $x \to 0$) et les deux divergent. Pour traiter ce cas, on calcule, pour tout $x \in]0,1[$,

$$\int_x^1 \frac{\ln t}{(1+t^2)} dt = \left[\frac{-\ln t}{1+t}\right]_x^1 + \int_x^1 \frac{dt}{t(1+t)} = \frac{\ln x}{1+x} + [\ln t - \ln(1+t)]_x^1 = -\ln 2 + \ln(1+x) - \frac{x \ln x}{1+x}.$$

En passant à la limite, on a alors, par croissances comparées,

$$\lim_{x \to 0} x \ln x = 0, \quad \int_0^1 \frac{\ln t}{(1+t)^2} = \lim_{x \to 0} \int_x^1 \frac{\ln t}{(1+t^2)} dt = -\ln 2.$$

♢

Exemple 3.8 :
Calculons de deux manières différentes l'intégrale $\displaystyle\int_0^{+\infty} \sin t \, \mathrm{e}^{-2t} \, dt$.

$\boxed{\text{Méthode 1}}$ Soit $f : t \mapsto \sin t \, \mathrm{e}^{-2t}$. $f \in \mathcal{C}_m^0(\mathbb{R}_+)$, donc le seul point incertain est $+\infty$. Alors

$$|f(t)| \leq \mathrm{e}^{-2t}, \quad \int_0^{+\infty} \mathrm{e}^{-2t} \, dt \text{ converge.}$$

Donc f est intégrable sur $\mathbb{R}_+$. De plus, pour tout $x > 0$,

$$\begin{aligned}
\int_0^x \sin t \, \mathrm{e}^{-2t} \, dt &= \left[-\cos t \, \mathrm{e}^{-2t}\right]_{t=0}^x - 2 \int_0^x \cos t \, \mathrm{e}^{-2t} \, dt \\
&= 1 - \cos x \, \mathrm{e}^{-2x} - 2 \left[\sin t \, \mathrm{e}^{-2t}\right]_{t=0}^x - 4 \int_0^x \sin t \, \mathrm{e}^{-2t} \, dt \\
&= \frac{1 - \cos x \, \mathrm{e}^{-2x} - 2 \sin x \, \mathrm{e}^{-2x}}{5},
\end{aligned}$$

donc

$$\int_0^{+\infty} \sin t \, \mathrm{e}^{-2t} \, dt = \lim_{x \to +\infty} \frac{1 - \cos x \, \mathrm{e}^{-2x} - 2 \sin x \, \mathrm{e}^{-2x}}{5} = \frac{1}{5}.$$

$\boxed{\text{Méthode 2}}$ Notons $g : t \mapsto \mathrm{e}^{(-2+i)t}$. On a alors $f = \mathrm{Im}(g)$ et $f, g \in \mathcal{C}_m^0(\mathbb{R}_+)$. On sait que g est intégrable sur $\mathbb{R}_+$, car $\Re(-2+i) = -2$, donc f est aussi intégrable sur $\mathbb{R}_+$. De plus, une primitive de g sur $]0, +\infty[$ est

$$\forall t \in \mathbb{R}, \quad G(t) = \frac{1}{-2+i} \mathrm{e}^{(-2+i)t} = -\frac{2+i}{5} \mathrm{e}^{(-2+i)t}, \quad \lim_{t \to +\infty} G(t) = 0.$$

On en déduit que

$$\int_0^{+\infty} g(t)\,dt = \lim_{t\to+\infty} G(t) - G(0) = \frac{2+i}{5}, \qquad \int_0^{+\infty} f(t)\,dt = \mathrm{Im}\left(\int_0^{+\infty} g(t)\,dt\right) = \frac{1}{5}.$$

♢

Dans l'exemple précédent, on remarque que le calcul dans $\mathbb{C}$ fournit une primitive évidente et occasionne beaucoup moins d'erreurs de signes.

Formellement, on pourrait écrire

$$\int_0^{+\infty} \sin t\,\mathrm{e}^{-2t}\,dt = \left[-\cos t\,\mathrm{e}^{-2t} - 2\sin t\,\mathrm{e}^{2t}\right]_0^{+\infty} - 4\int_0^{+\infty} \sin t\,\mathrm{e}^{-2t}\,dt,$$

en prenant la limite dans le terme entre crochets. Néanmoins, cela reste dangereux car on ne s'assure pas de l'existence des quantités manipulées (intégrales, limites...) Il existe des théorèmes permettant de faire des intégration par parties sur des intervalles, mais ils sont délicats à manipuler et n'offrent pas de réel gain de temps ou de calculs.

4. Intégrale de fonction oscillante

Soit $f \in \mathcal{C}_m^0([a,b[,\mathbb{R})$ avec $a < b \leq +\infty$. On dit que f est oscillante si son signe n'est pas constant au voisinage de b. On ne peut alors utiliser aucun théorème de comparaison de fonctions de signe constant. Par exemple :

- La fonction $x \mapsto \cos x$ est de signe constant au voisinage de 0 mais oscille en $+\infty$.
- La fonction $x \mapsto \cos\frac{1}{x}$ est de signe constant au voisinage de $+\infty$ mais oscille en 0.

Question : que faire si l'intégrale d'une fonction oscillante n'est pas absolument convergente ?

Exercice 3.9 :
On appelle intégrale de Dirichlet l'intégrale $\displaystyle\int_0^{\infty} \frac{\sin t}{t}dt$.

1. Montrer que l'intégrale de Dirichlet converge.
2. Montrer que l'intégrale de Dirichlet ne converge pas absolument.

Réponse

Remarquons que la fonction $f : t \mapsto \dfrac{\sin t}{t}$ est continue sur $]0,+\infty[$. Il y a deux points incertains : 0 et $+\infty$. Tout d'abord, la majoration standard $|\sin| \leq 1$ ne donne rien car $t \mapsto \dfrac{1}{t}$ n'est intégrable ni sur $]0,1]$ ni sur $[1,+\infty[$.

1. Montrons que l'intégrale est convergente.
   (a) f est positive sur $]0,1[$ et, pour tous $x, y \in]0,1[$,

   $$\int_x^y \frac{\sin t}{t}dt \leq \int_x^y \frac{t}{t}dt \leq \int_0^1 dt = 1.$$

   Donc $\displaystyle\int_0^1 f(t)\,dt$ converge.

   (b) Pour tout $x > 1$ on a

   $$\int_1^x \frac{\sin t}{t}dt = \left[-\frac{\cos t}{t}\right]_{t=1}^x - \int_1^x \frac{\cos t}{t^2}dt = \cos 1 - \frac{\cos x}{x} - \int_1^x \frac{\cos t}{t^2}dt.$$

On a $\lim\limits_{x\to+\infty} \frac{\cos x}{x} = 0$. Etudions donc la nature de $\int_1^{+\infty} \frac{\cos t}{t^2} dt$. On a

$$\left|\frac{\cos t}{t^2}\right| \leq \frac{1}{t^2}, \quad \left|\frac{\cos t}{t^2}\right| = O\left(\frac{1}{t^2}\right).$$

La fonction $t \mapsto \frac{1}{t^2}$ est continue, positive et intégrable sur $[1, +\infty[$, d'après le critère de Riemann. Donc $\int_1^{+\infty} \frac{\cos t}{t^2} dt$ converge absolument, donc converge. Donc

$$\lim_{x\to+\infty} \left(\cos 1 - \frac{\cos x}{x} - \int_1^x \frac{\cos t}{t^2} dt\right) \text{ existe et est finie,} \quad \int_1^{\infty} \frac{\sin t}{t} dt \text{ converge.}$$

Donc $\int_0^{+\infty} \frac{\sin t}{t} dt$ converge.

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

$$\begin{aligned} \int_1^{2n\pi} \frac{|\sin t|}{t} dt &\geq \sum_{k=1}^{n} \int_{2(k-1)\pi}^{2k\pi} \frac{|\sin t|}{t} dt \geq \sum_{k=1}^{n} \frac{1}{2k\pi} \int_{2(k-1)\pi}^{2k\pi-\pi} \sin t dt \\ &\geq \sum_{k=1}^{n} \frac{1}{2k\pi} \int_0^{\pi} \sin t dt = \sum_{k=1}^{n} \frac{\cos 0 - \cos \pi}{2k\pi} = \frac{1}{\pi} \sum_{k=1}^{n} \frac{1}{k} \end{aligned}$$

Or on sait que $\lim\limits_{n\to+\infty} \sum_{k=1}^{n} \frac{1}{k} = +\infty$. Donc $\int_0^{\infty} \frac{|\sin t|}{t} dt$ diverge.

◇

5. Fonctions continues sauf en un nombre fini de points

Définition 3.10

Soit $n \in \mathbb{N}^*$ et $f \in \mathcal{C}^0\left(\cup_{i=1}^{n}]a_{i-1}, a_i[, \mathbb{K}\right)$ avec $-\infty \leq a_0 < a_1 < \cdots < a_n \leq +\infty$. On dit que $\int_{a_0}^{a_n} f$ *converge* si $\int_{a_{i-1}}^{a_i} f$ converge pour tout $i \in [\![1, n]\!]$.

Quelle est la différence entre une fonction continue par morceaux et une fonction continue sauf en un nombre fini de points ?

Exercice 3.11 :

Déterminer la nature de $\int_{-2}^{2} \frac{dt}{\sqrt[3]{t^2 - 1}}$.

Réponse

Notons

$$f : t \mapsto \frac{1}{\sqrt[3]{t^2 - 1}} = \frac{1}{(t-1)^{1/3} (t+1)^{1/3}}.$$

La fonction f est continue sur $\mathbb{R} \setminus \{-1, 1\}$ comme composée de fonctions continues sur leurs domaines de définition. Il y a deux points incertains : -1 et 1. Puisque f est paire, on va juste étudier la nature des intégrales $\displaystyle\int_1^2 f(t)\,dt$ et $\displaystyle\int_0^1 f(t)\,dt$.

- Sur $]1,2]$, d'après le théorème du changement de variable avec $u = t-1$,
$$\int_1^2 \frac{dt}{(t-1)^{1/3}(t+1)^{1/3}} \text{ converge} \iff \int_0^1 \frac{du}{u^{1/3}(u+2)^{1/3}} \text{ converge.}$$
Or
$$\frac{1}{u^{1/3}(u+2)^{1/3}} \underset{u\to 0^+}{\sim} \frac{1}{2^{1/3}} \times \frac{1}{u^{1/3}}$$
qui est positive et intégrable sur $]0,1]$ d'après le critère de Riemann. Donc $\displaystyle\int_1^2 f$ converge.
- On effectue le changement de variable $u = 1-t$ sur $[0,1[$:
$$\int_0^1 \frac{dt}{(t-1)^{1/3}(t+1)^{1/3}} \text{ converge} \iff \int_0^1 \frac{du}{-u^{1/3}(2-u)^{1/3}} \text{ converge.}$$
Par comparaison de fonctions négatives, cette fois, $\displaystyle\int_0^1 f$ converge.

Donc $\displaystyle\int_0^2 \frac{dt}{\sqrt[3]{t^2-1}}$ converge. De plus, par changement de variable $u=-t$,
$$\int_0^2 \frac{dt}{\sqrt[3]{t^2-1}} \text{ converge} \iff \int_{-2}^0 \frac{dt}{\sqrt[3]{t^2-1}} \text{ converge.}$$
Donc $\displaystyle\int_{-2}^2 \frac{dt}{\sqrt[3]{t^2-1}}$ converge.

♢

6. Plan d'étude

Comment déterminer la nature de $\displaystyle\int_a^b f$?

0. On vérifie que la fonction f est bien continue (ou continue par morceaux) sur $]a,b[$, sauf éventuellement en un nombre fini de points. Auquel cas, on se ramène à étudier plusieurs intégrales du type $\displaystyle\int_{a_{i-1}}^{a_i} f$. On étudie aussi la parité de f pour réduire le domaine d'étude.
1. Si a ou b sont finis, on vérifie s'il y a un problème : on se demande si $\lim_{a^+} f$ ou $\lim_{b^-} f$ sont finies.
2. On découpe l'intervalle en $]a,c]$ et $[c,b[$ et on traite un problème à la fois.
3. Si possible, on détermine une primitive F de f et on étudie $\lim_{a^+} F$ et $\lim_{b^-} F$.
4. Sinon, on considère $|f|$:
   (a) Si possible, on trouve un équivalent simple de f dont on connait l'intégrabilité sur $]a,b[$.
   (b) Sinon, on essaie de comparer $|f|$ à une fonction simple dont on connaît l'intégrabilité. Dans le cas classique $a=0, b=+\infty$, on pourra étudier $t^\gamma f(t)$ pour utiliser le critère de Riemann.
5. Sinon, on essaie de se ramener à une autre intégrale plus facile à étudier par IPP ou CDV.

À connaître à la fin du chapitre

Intégrales de référence

- Connaître (et reconnaître) les intégrales de Riemann ou de Bertrand.
- Connaître des exemples (et les méthodes) d'intégrales semi-convergentes.
- Connaître des contre-exemples aux relations de comparaison.

Fonctions positives

- Déterminer la convergence (ou l'absolue convergence) d'une intégrale à l'aide d'un équivalent, d'une majoration, ou de relations de comparaison.

Méthodes d'intégration

- Effectuer un changement de variable ou une intégration par parties pour déterminer la nature et/ou la valeur d'une intégrale.

CHAPITRE 12

ALGÈBRE LINÉAIRE – MATRICES

CHAPITRE 13

SÉRIES NUMÉRIQUES

La notion de série a été brièvement introduite dans le chapitre sur les suites. La grande question est "une somme avec une infinité de termes est-elle finie ?". Puisque la quantité d'intérêt est l'incrément (le u_n dans $\sum_{k=0}^{n} u_k$), cela lie d'emblée la notion de série (sur $[\![0,+\infty[\![$) à celle d'intégrale (sur $[0,+\infty[$). C'est pourquoi les deux chapitres suivants sont des pré-requis fondamentaux :

- Suites numériques
- Intégrales généralisées

Dans tout ce chapitre, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

I Généralités sur les séries

1. Définition

Définition 1.1 *Série*

Soit $(u_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ une suite à valeurs dans $\mathbb{K}$. On appelle *série de terme général* u_n la suite $(S_n)_{n\in\mathbb{N}}$ définie par

$$\forall N \in \mathbb{N}, \quad S_N = \sum_{n=0}^{N} u_n.$$

On note $(S_n)_{n\in\mathbb{N}} = \sum_n u_n$. Pour tout $n \in \mathbb{N}$, on appelle u_n le terme général ou le terme d'indice n de la série $\sum_n u_n$ et le nombre S_N est la *somme partielle d'indice* N de la série $\sum_n u_n$.

Remarque 1.2 :

- Comme pour les suites, on pourra bien évidemment définir une série à partir d'un certain rang $n_0 \in \mathbb{N}$.
- Une série est, par définition, une suite (c'est juste une suite un peu particulière, qu'on étudiera avec des outils un peu particuliers).

- Attention à ne pas confondre la série $\sum_n u_n$, la somme partielle $\sum_{n=0}^{N} u_n$ et la somme de la série $\sum_{n=0}^{+\infty} u_n$ (lorsqu'elle existe).

$\diamondsuit$

Exemple 1.3 :
La série $\sum_{n \geq 1} n^2$ est une série définie à partir du rang $n = 1$, de terme général n^2, dont la somme partielle vaut :

$$\forall N \geq 1, \quad \sum_{n=1}^{N} u_n = \frac{N(N+1)(2N+1)}{6}.$$

$\diamondsuit$

Exemple 1.4 :
On a évidemment déjà rencontré des séries sans le dire. Une suite arithmétique est un exemple de série dont le terme général est constant. $\diamondsuit$

Dans la suite, sauf mention contraire, $(u_n) \in \mathbb{K}^n$ est une suite et on note $(S_n)_{n \in \mathbb{N}} = \sum_n u_n$ la série de terme général u_n.

⚠ Il est crucial de comprendre qu'une série est une suite. Réciproquement, on peut étudier une suite en tant que série :

$$\forall n \in \mathbb{N}, \quad u_n = u_0 + \sum_{k=0}^{n-1} (u_{k+1} - u_k).$$

Il faudra savoir passer de suite à série et inversement.

2. Séries de référence

Dans cette partie, on introduit quelques séries de référence. Soit $\sum_n u_n$ une série à valeurs dans $\mathbb{K}$ et on note S_N sa somme partielle d'indice N.

⚠ Si la suite commence au rang 0 alors la somme partielle S_N possède $N + 1$ termes.

Définition/Proposition 1.5 *Série arithmétique*

On dit que $\sum_n u_n$ est une *série arithmétique* si (u_n) est une suite arithmétique, c'est-à-dire s'il existe $(u_0, r) \in \mathbb{K}^2$ tel que

$$\forall n \in \mathbb{N}, \quad u_{n+1} = u_n + r, \quad u_n = u_0 + nr.$$

Dans ce cas,

$$\forall N \in \mathbb{N}, \quad S_N = (N+1) u_0 + \frac{N(N+1)}{2} r.$$

Définition/Proposition 1.6 *Série géométrique*

On dit que $\sum_n u_n$ est une *série géométrique* si (u_n) est une suite géométrique, c'est-à-dire s'il existe $u_0 \in \mathbb{K}, q \in \mathbb{K} \setminus \{1\}$ tels que

$$\forall n \in \mathbb{N}, \quad u_{n+1} = u_n \times q, \quad u_n = u_0 \times q^n.$$

Dans ce cas,

$$\forall N \in \mathbb{N}, \quad S_N = u_0 \frac{1 - q^{N+1}}{1 - q}.$$

Démonstration : Soit $N \in \mathbb{N}$. En reconnaissant une somme télescopique, on a alors

$$(1-q) \sum_{n=0}^{N} q^n = \sum_{n=0}^{N} \left(q^n - q^{n+1}\right) = 1 - q^{N+1}.$$

On en déduit que

$$\sum_{n=0}^{N} q^n = \frac{1 - q^{N+1}}{1 - q}, \quad S_N = u_0 \frac{1 - q^{N+1}}{1 - q}.$$

□

Définition 1.7 *Série exponentielle*

On dit que $\sum_n u_n$ est une *série exponentielle* s'il existe $z \in \mathbb{K}$ tel que

$$\forall n \in \mathbb{N}, \quad u_n = \frac{z^n}{n!}.$$

Dans ce cas,

$$\forall N \in \mathbb{N}, \quad S_N = \sum_{n=0}^{N} \frac{z^n}{n!}.$$

On rappelle que $0! = 1$ par définition. On remarque que, de manière informelle, il s'agit du polynôme de Taylor apparaissant dans le développement limité de l'exponentielle.

Définition 1.8 *Séries de Riemann*[1] *et de Bertrand*[2]

On dit que $\sum_n u_n$ est une *série de Bertrand* s'il existe $(\alpha, \beta) \in \mathbb{R}^2$ tel que

$$\forall n \geq 2, \quad u_n = \frac{1}{n^\alpha \ln^\beta n}.$$

On dira que $\sum_n u_n$ est une *série de Riemann* dans le cas particulier où $\beta = 0$ (dans ce cas on peut la considérer à partir du rang $n_0 = 1$).

Définition/Proposition 1.9 *Série télescopique*

On dit que $\sum_n u_n$ est une *série télescopique* s'il existe $(a_n) \in \mathbb{K}^{\mathbb{N}}$ tel que

$$\forall n \in \mathbb{N}, \quad u_n = a_{n+1} - a_n.$$

Dans ce cas,

$$\forall N \in \mathbb{N}, \quad S_N = a_{N+1} - a_0.$$

Enfin, quelques cas particuliers :

- La *série harmonique* est la série $\sum_n \frac{1}{n}$ (c'est la série de Riemann correspondant à $\alpha = 1$).
- La *série harmonique alternée* est la série $\sum_n \frac{(-1)^n}{n}$, parfois aussi $\sum_n \frac{(-1)^n}{n+1}$.

3. Convergence d'une série

Définition 1.10 *Somme d'une série*

Soit $\sum_n u_n$ une série à valeurs dans $\mathbb{K}$. On dit que la série $\sum_n u_n$ converge si la suite des sommes partielles $\left(\sum_{n=0}^{N} u_n\right)_{N \in \mathbb{N}}$ admet une limite finie (lorsque $N \to +\infty$). On appelle alors *somme de la série* le nombre

$$\sum_{n=0}^{+\infty} u_n = \lim_{N \to +\infty} \sum_{n=0}^{N} u_n.$$

Sinon, on dit que la série $\sum_n u_n$ diverge.

Il s'agit de l'équivalent de limite pour une série. On parle de "nature" de la série (convergente ou divergente).

Exemple 1.11 :
En reprenant l'exemple précédent, $\sum_n n^2$ diverge car $\lim_{N \to +\infty} \frac{N(N+1)(2N+1)}{6} = +\infty$. ◇

Proposition 1.12

Soit $\sum_n u_n$ une série. Soient $n_0 \leq n_1 \in \mathbb{N}$. Alors

$$\sum_{n \geq n_0} u_n \text{ converge} \iff \sum_{n \geq n_1} u_n \text{ converge}$$

1. Berhard RIEMANN (1826-1866) : Mathématicien allemand.
2. Joseph BERTRAND (1822-1900) : Mathématicien français.

Si ces séries convergent, alors on a

$$\sum_{n=n_0}^{+\infty} u_n = \sum_{n=n_0}^{n_1-1} u_n + \sum_{n=n_1}^{+\infty} u_n.$$

Autrement dit, les séries $\sum_{n\geq n_0} u_n$ et $\sum_{n\geq n_1} u_n$ sont de même nature : c'est l'équivalent de la relation de Chasles pour les intégrales. On remarquera aussi qu'on ne modifie pas la nature d'une intégrale en changeant un nombre fini de termes.

Proposition 1.13

Soient $u_0, q, r, x \in \mathbb{K}$, $q \neq 1$. Alors :

(i) La série arithmétique $\sum_n (u_0 + nr)$ est convergente si, et seulement si, $u_0 = r = 0$. Dans ce cas, $\sum_{n=0}^{+\infty} u_n = 0$.

(ii) La série géométrique $\sum_n u_0 q^n$ est convergente si, et seulement si, $u_0 = 0$ ou $|q| < 1$. Dans ce cas,

$$\sum_{n=0}^{+\infty} u_n = \frac{u_0}{1-q}.$$

(iii) La série télescopique $\sum_n (a_{n+1} - a_n)$ est convergente si, et seulement si, la suite (a_n) est convergente. Dans ce cas,

$$\sum_{n=0}^{+\infty} u_n = \lim (a_n) - a_0.$$

Démonstration : (i) Si $r \neq 0$, alors

$$|S_N| \underset{n\to+\infty}{\sim} \frac{N^2|r|}{2}, \quad \lim_{N\to+\infty} |S_N| = +\infty, \quad (S_N) \text{ diverge.}$$

Si $r = 0$ et $u_0 \neq 0$, alors

$$|S_N| \underset{N\to+\infty}{\sim} N|u_0|, \quad \lim_{N\to+\infty} |S_N| = +\infty, \quad (S_N) \text{ diverge.}$$

Si $u_0 = r_0 = 0$ alors (S_N) converge.

(ii) Si $u_0 = 0$, (S_N) est convergente. Si $u_0 \neq 0$, alors

$$\forall N \geq 0, \quad S_N = \frac{u_0}{1-q} - \frac{u_0}{1-q} q^{N+1}.$$

Donc

$$(S_N) \text{ converge} \iff \left(q^{N+1}\right) \text{ converge} \iff |q| < 1.$$

Dans ce cas, on a $\lim_{N\to+\infty} q^{N+1} = 0$ donc $\lim_{N\to+\infty} S_N = \dfrac{u_0}{1-q}$.

(iii) Évident.

□

Remarquons qu'étudier la nature d'une série télescopique revient à étudier la nature d'une suite (et inversement). Les séries télescopiques sont le moyen principal d'utiliser des outils de séries dans le cadre des suites.[3]

La convergence des séries exponentielle, harmonique, harmonique alternée, de Bertrand et de Riemann étant moins élémentaire, on verra cette étude un peu plus loin dans le cours.

Proposition 1.14 *Propriétés des séries convergentes*

Soient $(u_n), (v_n) \in \mathbb{K}^{\mathbb{N}}$.

(i) Si $\sum_n u_n$ et $\sum_n v_n$ convergent, alors, pour tous $\lambda, \mu \in \mathbb{K}$, $\sum_n (\lambda u_n + \mu v_n)$ converge et

$$\sum_{n=0}^{+\infty} (\lambda u_n + \mu v_n) = \lambda \sum_{n=0}^{+\infty} u_n + \mu \sum_{n=0}^{+\infty} v_n.$$

(ii) Si $\mathbb{K} = \mathbb{R}$ et $\forall n \in \mathbb{N}, u_n \geq 0$ et $\sum_n u_n$ converge, alors $\sum_{n=0}^{+\infty} u_n \geq 0$.

(iii) Si $\mathbb{K} = \mathbb{R}$ et $\forall n \in \mathbb{N}, u_n \leq v_n$ et $\sum_n u_n$ et $\sum_n v_n$ convergent, alors $\sum_{n=0}^{+\infty} u_n \leq \sum_{n=0}^{+\infty} v_n$.

(iv) Si $\mathbb{K} = \mathbb{C}$, alors

$$\sum_n u_n \text{ converge} \iff \begin{cases} \sum_n \mathfrak{Re}\,(u_n) \text{ converge} \\ \sum_n \mathfrak{Im}\,(u_n) \text{ converge} \end{cases} \iff \sum_n \overline{u}_n \text{ converge.}$$

Dans ce cas, on a

$$\sum_{n=0}^{+\infty} u_n = \sum_{n=0}^{+\infty} \mathfrak{Re}\,(u_n) + i \sum_{n=0}^{+\infty} \mathfrak{Im}\,(u_n), \quad \overline{\sum_{n=0}^{+\infty} u_n} = \sum_{n=0}^{+\infty} \overline{u}_n.$$

Démonstration : Ces résultats sont des propriétés déjà vues dans le cadre des suites, mais appliquées aux sommes partielles. □

On notera que, si $\sum_n u_n$ converge et $\sum_n v_n$ diverge, alors $\sum_n (u_n + v_n)$ diverge (évident par l'absurde).

Évidemment, on ne peut rien dire de la combinaison linéaire de deux série divergentes. En effet, si $\sum_n u_n$ est une série divergente, alors $\sum_n (u_n - u_n)$ est constante égale à 0, donc convergente.

Exercice 1.15 :
Après avoir montré que la série $\sum_n \frac{1}{n^2 + n}$ converge, calculer sa somme.

3. La réciproque est vraie aussi, mais moins utilisée en pratique.

Réponse

Pour tout $n \geq 1$, on a

$$\frac{1}{n^2+n} = \frac{1}{n\,(n+1)} = \frac{1}{n} - \frac{1}{n+1}.$$

La série $\sum_n \frac{1}{n^2+n}$ est donc une série télescopique. Puisque la suite $\left(\frac{1}{n}\right)$ converge, alors $\sum_n \frac{1}{n^2+n}$ est une série convergente. De plus, on a pour tout $N \in \mathbb{N}^*$,

$$\sum_{n=1}^{N} \frac{1}{n^2+n} = \sum_{n=1}^{N} \left(\frac{1}{n} - \frac{1}{n+1}\right) = 1 - \frac{1}{N+1} \xrightarrow[N\to+\infty]{} 1.$$

Donc $\sum_{n=1}^{+\infty} \frac{1}{n^2+n} = 1$.

◊

Définition 1.16 *Reste*

Soit $\sum_n u_n$ une série convergente. Pour $N \in \mathbb{N}$, on définit son *reste d'indice N* :

$$R_N = \sum_{n=0}^{+\infty} u_n - \sum_{n=0}^{N} u_n = \sum_{n=N+1}^{+\infty} u_n.$$

⚠ On parle de reste uniquement dans le cas d'une série convergente, sinon cela n'a strictement aucun sens. Dans ce cas, les deux sommes $\sum_{n=0}^{+\infty} u_n$ et $\sum_{n=N+1}^{+\infty} u_n$ sont bien définies.

Proposition 1.17

Soit $\sum_n u_n$ une série convergente. Alors la suite des restes de $\sum_n u_n$ converge vers 0.

Exemple 1.18 :

Le reste de rang N de la série géométrique $\sum_n q^n$ est $\frac{q^{N+1}}{1-q}$. ◊

Proposition 1.19

Soit $\sum_n u_n$ une série. Alors

$$\sum_n u_n \text{ converge} \Rightarrow \lim_{n\to+\infty} u_n = 0.$$

La réciproque est fausse!!! On sait (ou on reverra bientôt) que la série harmonique $\sum_n \frac{1}{n}$ diverge, mais $\lim_{n\to+\infty} \frac{1}{n} = 0$.

Démonstration : Soit $\sum_n u_n$ une série convergente. Notons pour $N \in \mathbb{N}$, $S_N = \sum_{n=0}^{N} u_n$ la somme partielle de la série. Par définition, (S_N) et (S_{N-1}) convergent vers la même limite. Donc

$$u_n = \sum_{k=0}^{n} u_k - \sum_{k=0}^{n-1} u_k = S_n - S_{n-1} \xrightarrow[n\to+\infty]{} 0.$$

□

Définition/Proposition 1.20 *Divergence grossière*
Soit $(u_n) \in \mathbb{K}^n$. Si (u_n) ne converge pas vers 0, alors la série $\sum_n u_n$ diverge. On dit que $\sum_n u_n$ *diverge grossièrement.*

Exercice 1.21 :
Soit $a \in \mathbb{R}$ et $f \in \mathcal{C}^0_m([a, +\infty[)$. La proposition suivante est-elle vraie ou fausse ?

$$\int_a^{+\infty} f \text{ converge} \overset{?}{\Longrightarrow} \lim_{x\to+\infty} f(x) = 0.$$

Réponse
La proposition est fausse. En effet, on peut construire une fonction dont la limite en $+\infty$ n'existe pas mais qui sera intégrable sur $[a, +\infty[$. Posons $a = 1$ et

$$\forall x \in [1, +\infty[, \quad f(x) = \sum_{n=1}^{+\infty} \mathbb{1}_{\{n<x<n+1/n^2\}}.$$

La fonction f est une fonction en escalier positive sur tout segment $[1, N]$ avec ≥ 2, et on a

$$\int_1^N f(x)\,dx = \int_1^N \sum_{n=1}^{N} \mathbb{1}_{\{n<x<n+1/n^2\}} dx = \sum_{n=1}^{N} \int_1^N \mathbb{1}_{\{n<x<n+1/n^2\}} dx = \sum_{n=1}^{N} \int_n^{n+\frac{1}{n^2}} dx$$
$$= \sum_{n=1}^{N} \frac{1}{n^2}.$$

On sait (ou on reverra bientôt) que la série $\sum_n \frac{1}{n^2}$ converge, donc $\int_1^{+\infty} f(x)\,dx$ converge.

♢

Exercice 1.22 :
Montrer que la série $\sum_{n\geq 1} nq^n$ converge pour tout $q \in]-1, 1[$ et déterminer sa somme.
Indication : on pourra étudier d'abord la série $\sum_{n\geq 1} nq^{n-1}$.

Réponse

Soient $q \in]-1,1[$ et $N \in \mathbb{N}$. On a

$$\sum_{n=0}^{N} q^n = \frac{1-q^{N+1}}{1-q}.$$

Les fonctions $q \mapsto \sum_{n=0}^{N} q^n$ et $q \mapsto \frac{1-q^{N+1}}{1-q}$ sont dérivables pour tout $q \in]-1,1[$ et on a donc

$$\sum_{n=1}^{N} nq^{n-1} = \frac{1}{(1-q)^2} + \frac{(N+1)\,q^N - Nq^{N+1}}{(1-q)^2}, \qquad \lim_{N\to+\infty} \frac{(N+1)\,q^N - Nq^{N+1}}{(1-q)^2} = 0,$$

donc $\sum_{n} nq^{n-1}$ converge et

$$\sum_{n=1}^{\infty} nq^{n-1} = \frac{1}{(1-q)^2}.$$

On en déduit que $\sum_{n} nq^n$ converge et

$$\sum_{n=1}^{\infty} nq^n = \frac{q}{(1-q)^2}.$$

$\diamondsuit$

II Séries à termes positifs

Par définition, on ne sait montrer qu'une série converge qu'en calculant explicitement sa somme partielle puis en étudiant sa limite. Ce calcul explicite n'est souvent pas possible en pratique. [4]

Comme pour les intégrales généralisées, un cas très favorable pour étudier la nature d'une série est quand le terme général est positif (ou de signe constant).

1. Somme d'une série à termes positifs

Théorème 2.1

Soit $\sum_{n} u_n$ une série à termes positifs. Notons (S_n) la suite des sommes partielles. Alors

$$\sum_{u} n \text{ converge} \iff \exists M > 0, \forall n \in \mathbb{N}, S_n \leq M.$$

Dans ce cas, on a alors $\sum_{n=0}^{+\infty} u_n = \sup_{n\in\mathbb{N}} S_n$.

4. En pratique, on ne sait pas non plus déterminer une primitive de l'intégrande dans une intégrale généralisée en général.

Démonstration : Pour tout $n \in \mathbb{N}$, $S_{n+1} - S_n = u_{n+1} \geq 0$ donc (S_n) est croissante. D'après le théorème de la limite monotone, (S_n) converge si, et seulement si, elle est majorée. Si c'est le cas, on a

$$\sum_{n=0}^{+\infty} u_n = \lim_{n \to +\infty} S_n = \sup_{n \in \mathbb{N}} S_n.$$

□

Corollaire 2.2

Soient $\sum_n u_n$ et $\sum_n v_n$ deux séries à termes positifs vérifiant $0 \leq u_n \leq v_n$ pour tout $n \in \mathbb{N}$. Si $\sum_n v_n$ converge, alors $\sum_n u_n$ converge et

$$0 \leq \sum_{n=0}^{+\infty} u_n \leq \sum_{n=0}^{+\infty} v_n.$$

2. Comparaison série/intégrale

Ce paragraphe est fondamental. Nous allons voir le lien précis entre intégrale et série, et savoir comment passer de l'une à l'autre. On pourra également déduire la nature de plusieurs séries à l'aide d'intégrales de référence.

L'idée est de comparer une série du type $\sum_{n=n_0}^{N} f(n)$ avec $\int_{n_0}^{N} f(t)\,dt$.

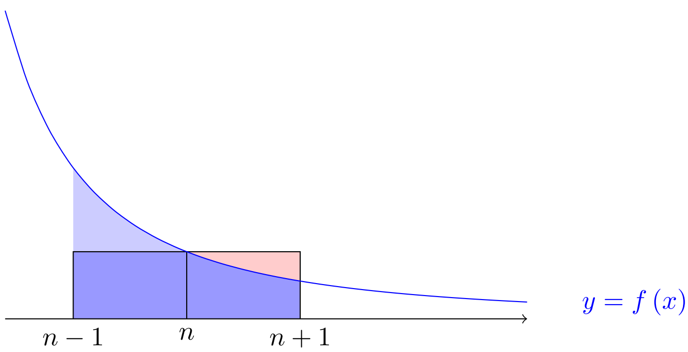
Théorème 2.3 *Comparaison série/intégrale*

Soit $n_0 \in \mathbb{N}$, et soit $f \in \mathcal{C}_m^0([n_0, +\infty[)$. On suppose que f est positive et décroissante. Alors :

(i) $\int_{n_0}^{+\infty} f$ converge si, et seulement si, la série $\sum_n f(n)$ converge.

(ii) Si $\sum_n f(n)$ diverge, alors

$$\sum_{n=n_0}^{N} f(n) \underset{N \to +\infty}{\sim} \int_{n_0}^{N} f(t)\,dt.$$



Démonstration : Soit $n \geq n_0$. Remarquons que $\sum_n f(n)$ est une série à termes positifs. f est décroissante donc, pour tout $n \in [\![n_0+1, N]\!]$,

$$\int_n^{n+1} f(t)\,dt \leq f(n) \leq \int_{n-1}^{n} f(t)\,dt.$$

En sommant, on obtient

$$\int_{n_0}^{N} f(t)\,dt \leq f(N) + \int_{n_0}^{N} f(t)\,dt \leq \sum_{n=n_0}^{N} f(n) \leq f(n_0) + \int_{n_0}^{N} f(t)\,dt.$$

- Si $\displaystyle\int_{n_0}^{+\infty} f(t)\,dt$ converge, alors

  $$\sum_{n=n_0}^{N} f(n) \leq f(n_0) + \int_{n_0}^{+\infty} f(t)\,dt$$

  donc $\sum_n f(n)$ est majorée, cette série converge.
- Si $\displaystyle\int_{n_0}^{+\infty} f(t)\,dt$ diverge, alors $\displaystyle\lim_{N\to+\infty} \int_{n_0}^{N} f(t)\,dt = +\infty$, et

  $$\int_{n_0}^{N} f(t)\,dt \leq \sum_{n=n_0}^{N} f(n)$$

  donc $\displaystyle\lim_{N\to+\infty} \sum_{n=n_0}^{N} f(n) = +\infty$, donc $\sum_n f(n)$ diverge. On a alors

  $$1 \leq \frac{\sum_{n=n_0}^{N} f(n)}{\int_{n_0}^{N} f(t)\,dt} \leq 1 + \frac{f(n_0)}{\int_{n_0}^{N} f(t)\,dt}.$$

  Par le théorème des gendarmes, on a

  $$\lim_{n\to+\infty} \frac{\sum_{n=n_0}^{N} f(n)}{\int_{n_0}^{N} f(t)\,dt} = 1, \quad \sum_{n=n_0}^{N} f(n) \underset{N\to+\infty}{\sim} \int_{n_0}^{N} f(t)\,dt.$$

$\square$

Ce théorème est très utile. Mais surtout, il faut savoir appliquer la méthode. Le point important est de considérer une fonction <u>monotone</u> ! On peut avoir de nombreux renseignements sur une série en étudiant l'intégrale associée : équivalent de la somme partielle, du reste, etc. Par contre, la comparaison série/intégrale ne permet pas, en général, de calculer la somme $\displaystyle\sum_{n=n_0}^{+\infty} f(n)$.

<u>Théorème 2.4</u> *Critère de Riemann*[5]

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

$$\sum_n \frac{1}{n^\alpha} \text{ converge } \iff \alpha > 1.$$

Démonstration :

- Si $\alpha \leq 0$, alors $\sum_n u_n$ diverge grossièrement.
- Si $\alpha > 0$, la fonction $f_\alpha : x \mapsto x^{-\alpha}$ est continue, positive et décroissante sur $[1, +\infty[$. Par le théorème 2.3, et d'après le critère de Riemann (pour les intégrales),

$$\sum_n \frac{1}{n^\alpha} \text{ converge} \iff \int_1^{+\infty} \frac{dx}{x^\alpha} \text{ converge} \iff \alpha > 1.$$

□

Si l'on sait que les séries $\sum_n \frac{1}{n^\alpha}$ sont convergentes pour $\alpha > 1$, c'est une autre histoire de déterminer leur somme. Par exemple,

$$\sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Il s'agit du problème de Bâle, dont la démonstration est l'un des premiers coups d'éclat d'Euler. La démonstration la plus rapide fait intervenir les séries de Fourier.

Exemple 2.5 :
Soit $\alpha \in \mathbb{R}$, on pose pour tout $n \in \mathbb{N}^*, u_n = \frac{1}{n^\alpha}$. Si $\alpha > 1$, on peut donner un équivalent des restes de $\sum_n u_n$. Si $\alpha \leq 1$ on peut donner un équivalent de la suite des sommes partielles de $\sum_n u_n$. Notons

$$f_\alpha : x \mapsto x^{-\alpha}, \quad \forall N \in \mathbb{N}^*, \quad S_N = \sum_{n=1}^{N} \frac{1}{n^\alpha}, \quad R_N = \sum_{n=N+1}^{+\infty} \frac{1}{n^\alpha} \text{ (si } \alpha > 1).$$

1. $\boxed{\alpha > 1}$ f_α est bien continue, positive et décroissante sur $[1, +\infty[$. En reprenant les inégalités obtenues dans la preuve du théorème 2.3, on a, pour tout $N \in \mathbb{N}$,

$$\int_{N+1}^{+\infty} \frac{dx}{x^\alpha} \leq \sum_{n=N+1}^{+\infty} \frac{1}{n^\alpha} \leq (N+1)^{-\alpha} + \int_{N+1}^{+\infty} \frac{dx}{x^\alpha},$$

toutes ces quantités étant convergentes. On a donc

$$\frac{(N+1)^{1-\alpha}}{\alpha - 1} \leq R_N \leq (N+1)^{-\alpha} + \frac{(N+1)^{1-\alpha}}{\alpha - 1}.$$

On a

$$\frac{(N+1)^{1-\alpha}}{\alpha - 1} \underset{N \to +\infty}{\sim} (N+1)^{-\alpha} + \frac{(N+1)^{1-\alpha}}{\alpha - 1} \underset{N \to +\infty}{\sim} \frac{N^{1-\alpha}}{\alpha - 1}.$$

Donc

$$\frac{\frac{(N+1)^{1-\alpha}}{\alpha-1}}{\frac{N^{1-\alpha}}{\alpha-1}} \leq \frac{R_N}{\frac{N^{1-\alpha}}{\alpha-1}} \leq \frac{(N+1)^{-\alpha} + \frac{(N+1)^{1-\alpha}}{\alpha-1}}{\frac{N^{1-\alpha}}{\alpha-1}}.$$

D'après le théorème des gendarmes,

$$\lim_{N \to +\infty} \frac{R_N}{\frac{N^{1-\alpha}}{\alpha-1}} = 1, \quad R_N \underset{N \to +\infty}{\sim} \frac{N^{1-\alpha}}{\alpha - 1}.$$

5. Bernhard Riemann (1826-1866) : Mathématicien allemand.

2. $\boxed{0 \leq \alpha < 1}$ Dans ce cas, $\alpha < 1$ donc $\displaystyle\sum_n \frac{1}{n^\alpha}$ diverge. Puisque f_α est décroissante, on peut utiliser directement le théorème de comparaison série/intégrale énoncé plus haut :

$$\int_1^N \frac{dx}{x^\alpha} = \frac{N^{1-\alpha}}{1-\alpha} - \frac{1}{1-\alpha}, \quad \sum_{n=1}^N \frac{1}{n^\alpha} \underset{N\to+\infty}{\sim} \frac{N^{1-\alpha}}{1-\alpha}.$$

3. $\boxed{\alpha = 1}$ Comme pour le cas 2, mais f_α n'admet pas la même primitive :

$$\sum_{n=1}^N \frac{1}{n} \underset{N\to+\infty}{\sim} \ln N.$$

4. $\boxed{\alpha < 0}$ La fonction f_α est croissante, donc on ne peut pas appliquer tel quel le théorème 2.3. Par contre, on peut refaire la méthode directement. Puisque f_α est croissante on a, pour tous $1 \leq n \leq N$,

$$\int_{n-1}^n f_\alpha \leq \frac{1}{n^\alpha} \leq \int_n^{n+1} f_\alpha, \quad 1 + \int_1^N f_\alpha \leq \sum_{n=1}^N \frac{1}{n^\alpha} \leq \int_1^{N+1} f_\alpha.$$

Donc

$$1 + \frac{N^{1-\alpha}}{1-\alpha} \leq \sum_{n=1}^N \frac{1}{n^\alpha} \leq \frac{(N+1)^{1-\alpha}}{1-\alpha}.$$

Comme dans le cas 1, on peut utiliser le théorème des gendarmes [6] pour montrer que

$$\sum_{n=1}^N \frac{1}{n^\alpha} \underset{N\to+\infty}{\sim} \frac{N^{1-\alpha}}{1-\alpha}.$$

$\diamondsuit$

On remarque donc que le théorème de comparaison série/intégrale est plus qu'un résultat utile, c'est une méthode utile pour obtenir des équivalents de sommes partielles ou de restes. Il faut donc savoir mettre en place la méthode pour conclure au cas par cas.

Exemple 2.6 :
On va montrer que $\displaystyle\sum_n \mathrm{e}^{-n}$ est convergente. Par comparaison série/intégrale, puisque la fonction $x \mapsto \mathrm{e}^{-x}$ est continue, positive et décroissante sur $[1, +\infty[$ et que $\displaystyle\int_1^{+\infty} \mathrm{e}^{-x}\, dx$ converge, alors la série $\displaystyle\sum_n \mathrm{e}^{-n}$ converge. En revanche, on ne peut pas trouver un équivalent de son reste avec cette méthode. En effet, on a

$$\int_{N+1}^{+\infty} \mathrm{e}^{-t}\, dt \leq \sum_{n=N+1}^{+\infty} \mathrm{e}^{-n} \leq \mathrm{e}^{-(N+1)} + \int_{N+1}^{+\infty} \mathrm{e}^{-t}\, dt,$$

donc

$$\mathrm{e}^{-(N+1)} \leq R_N \leq 2\,\mathrm{e}^{-(N+1)}.$$

Le problème vient du fait que $f(N+1)$ est ici du même ordre que $\displaystyle\int_{N+1}^{+\infty} f(t)\, dt$. Pour obtenir un équivalent, on considère cette série comme une série géométrique :

$$\sum_{n=0}^N \mathrm{e}^{-n} = \frac{1-\mathrm{e}^{-(N+1)}}{1-\mathrm{e}^{-1}}, \quad \sum_{n=N+1} \mathrm{e}^{-n} = \frac{\mathrm{e}^{-(N+1)}}{1-\mathrm{e}^{-1}} \underset{N\to+\infty}{\sim} \frac{\mathrm{e}^{-N}}{\mathrm{e}-1}.$$

Or $\dfrac{1}{1-\mathrm{e}^{-1}} \simeq 1,58$, ce qui est cohérent avec l'encadrement trouvé par comparaison série/intégrale. $\diamondsuit$

6. Avec des limites, jamais avec des équivalents !

3. Comparaison de séries à termes positifs

Comme pour les intégrales généralisées, on ne peut pas toujours conclure sur la nature d'une série directement. Par contre, en la comparant à une série à termes positifs dont la nature est connue ou plus facile à déterminer, on va pouvoir conclure.

Théorème 2.7 *Comparaison de séries à termes positifs*

Soient $\sum_n u_n$ et $\sum_n v_n$ deux séries à termes positifs. Alors

(i) Si $u_n \underset{n\to+\infty}{\sim} v_n$ alors

$$\sum_n u_n \text{ converge } \iff \sum_n v_n \text{ converge.}$$

(ii) Si $u_n \underset{n\to+\infty}{=} O(v_n)$ alors

$$\sum_n v_n \text{ converge} \Rightarrow \sum_n u_n \text{ converge.}$$

(iii) Si $u_n \underset{n\to+\infty}{=} o(v_n)$ alors

$$\sum_n v_n \text{ converge} \Rightarrow \sum_n u_n \text{ converge.}$$

C'est exactement le même théorème que pour les comparaisons de fonctions positives ! La preuve est donc un simple copié-collé.

Démonstration : $\boxed{(ii)}$ Par définition, il existe $n_0 \in \mathbb{N}$ et $M > 0$ tels que

$$\forall n \geq n_0, \quad u_n = |u_n| \leq M|v_n| = Mv_n.$$

Donc, pour tout $N \geq n_0$,

$$\sum_{n=0}^{N} u_n = \sum_{n=0}^{n_0-1} u_n + \sum_{n=n_0}^{N} u_n \leq \sum_{n=0}^{n_0-1} u_n + M\sum_{n=n_0}^{N} v_n \leq \sum_{n=0}^{n_0-1} u_n + M\sum_{n=n_0}^{+\infty} v_n.$$

Donc $\sum_n u_n$ est une série à termes positifs bornée, donc convergente.

$\boxed{(i)}$ Si $u_n \underset{n\to+\infty}{\sim} v_n$ alors $u_n = O(v_n)$ et $v_n = O(u_n)$. Les séries ont donc même nature.

$\boxed{(iii)}$ Si $u_n = o(v_n)$ alors $u_n = O(v_n)$. □

Comme pour les intégrales généralisées, ce théorème se généralise facilement :

- aux séries à termes positifs à partir d'un certain rang ;
- aux séries à termes négatifs (éventuellement à partir d'un certain rang).

Exercice 2.8 :
Le théorème de comparaison des séries à termes positifs reste-t-il vrai si on ne sait pas déterminer le signe de (u_n), mais que (v_n) est positive ?

Réponse

Oui pour le point (i) ! En effet, il existe $(h_n) \in \mathbb{K}^{\mathbb{N}}$ telle que

$$\forall n \in \mathbb{N}, \quad u_n = v_n h_n, \quad \lim_{n \to +\infty} h_n = 1.$$

Donc

$$\exists n_0 \in \mathbb{N}, \forall n \geq n_0, \quad h_n \geq 0, \quad u_n \geq 0.$$

Pour les points (ii) et (iii), on aura besoin de la notion de convergence absolue, vue un peu plus loin.

◊

On pourra aussi utiliser les points (ii) et (iii) par contraposée pour montrer qu'une série diverge :

$$\begin{cases} u_n = O\left(v_n\right) \\ \sum_n u_n \text{ diverge} \end{cases} \Rightarrow \sum_n v_n \text{ diverge.}$$

Exemple 2.9 :
Quelle est la nature de la série $\displaystyle\sum_n \left(1 - \cos\frac{1}{n}\right)$? On a

$$\cos\frac{1}{n} \underset{n \to +\infty}{=} 1 - \frac{1}{2n^2} + o\frac{1}{n^2}, \quad \left(1 - \cos\frac{1}{n}\right) \underset{n \to +\infty}{\sim} \frac{1}{2n^2}.$$

De plus, pour tout $n \in \mathbb{N}^*$, $\cos\frac{1}{n} \in]0, 1[$ donc $\displaystyle\sum_n 1 - \cos\frac{1}{n}$ et $\displaystyle\sum_n \frac{1}{2n^2}$ sont des séries à termes positifs. Puisque $\displaystyle\sum_n \frac{1}{2n^2}$ converge par le critère de Riemann, on en déduit que $\displaystyle\sum_n \left(1 - \cos\frac{1}{n}\right)$ converge. ◊

Proposition 2.10 *Développement asymptotique de la série harmonique*
Il existe $\gamma \in \mathbb{R}$ tel que

$$\sum_{n=1}^{N} \frac{1}{n} = \ln N + \gamma + o\left(1\right).$$

γ est appelée *constante d'Euler*, et vaut $\gamma \simeq 0,58$.

Démonstration : Notons $u_n = \dfrac{1}{n}$ et S_N la somme partielle d'indice N de $\displaystyle\sum_n u_n$. On a déjà montré (par comparaison série/intégrale) que $S_N \sim \ln N$. On va pousser le développement asymptotique un cran plus loin. Pour cela on pose $v_N = S_N - \ln N$. On veut montrer que (v_N) converge. On a

$$\begin{aligned} v_{N+1} - v_N = u_{N+1} - \ln\left(N+1\right) + \ln N &= \frac{1}{N+1} - \ln\left(1 + \frac{1}{N}\right) \\ &= \frac{1}{N+1} - \frac{1}{N} + \frac{1}{2N^2} + o\left(\frac{1}{N^2}\right) = -\frac{1}{2N^2} + o\left(\frac{1}{N^2}\right) \\ &\underset{N \to +\infty}{\sim} -\frac{1}{2N^2} \end{aligned}$$

Par comparaison de séries à termes négatifs et critère de Riemann, la série $\sum_n (v_{N+1} - v_N)$ converge. Cette série est télescopique, on en déduit donc que (v_N) converge vers une certaine limite, notée γ. Donc pour tout $N \in \mathbb{N}^*$,

$$v_N \underset{N\to+\infty}{=} \gamma + o(1), \quad \sum_{n=1}^{N} \frac{1}{n} \underset{N\to+\infty}{=} \ln N + \gamma + o(1).$$

□

Théorème 2.11 *Critère de Bertrand*[7]

Soient $\alpha, \beta \in \mathbb{R}$. Alors

$$\sum_n \frac{1}{n^\alpha (\ln n)^\beta} \text{ converge} \iff \alpha > 1 \text{ ou } \begin{cases} \alpha = 1 \\ \beta > 1 \end{cases}.$$

Pas de grosse nouveauté par rapport au critère de Bertrand pour les fonctions. La seule différence est qu'on ne peut plus exhiber une primitive dans le cas $\alpha = 1$...

Démonstration : La fonction $f : x \mapsto \dfrac{1}{x^\alpha \ln^\beta x}$ est positive et dérivable sur $[2, +\infty[$ et

$$\forall x \geq 2, \quad f'(x) = -\frac{\beta + \alpha \ln x}{x^{\alpha+1} \ln^{\beta+1} x}.$$

- Cas 1 : $\alpha > 0$ ou $(\alpha = 0 \text{ et } \beta > 0)$. Posons $n_0 = E\left(\max\left(2, e^{-\beta/\alpha}\right)\right) + 1$. La fonction f est donc continue, décroissante et positive sur $[n_0, +\infty[$, on peut donc appliquer le théorème de comparaison série/intégrale :

$$\sum_n \frac{1}{n^\alpha \ln^\beta n} \text{ converge} \iff \int_{n_0}^{+\infty} \frac{dx}{x^\alpha \ln^\beta x} \text{ converge} \iff \alpha > 1 \text{ ou } (\alpha = 1 \text{ et } \beta > 1).$$

- Cas 2 : $\alpha < 0$ ou $(\alpha = 0, \beta \leq 0)$. Alors, $\sum_n \frac{1}{n^\alpha (\ln n)^\beta}$ diverge grossièrement.

□

4. Critère de D'Alembert

Le théorème suivant ne possède pas d'équivalent pour les intégrales, et s'avère bien pratique dans de nombreux cas que l'on verra ensuite.

Théorème 2.12 *Critère de D'Alembert*[8]

Soit $\sum_n u_n$ une série à termes strictement positifs. On suppose que $\lim_{n\to+\infty} \dfrac{u_{n+1}}{u_n} = \ell \in \mathbb{R}_+ \cup \{+\infty\}$. Alors :

(i) Si $\ell < 1$ alors $\sum_n u_n$ converge.

(ii) Si $\ell > 1$ alors $\sum_n u_n$ diverge.

7. Joseph Bertrand (1822-1900) : Economiste et mathématicien français.

Démonstration : (i) Si $\ell < 1$, notons $\varepsilon = \dfrac{1-\ell}{2}$. Alors il existe $n_0 \in \mathbb{N}$ tel que

$$\forall n \geq n_0, \quad \left|\frac{u_{n+1}}{u_n} - \ell\right| \leq \varepsilon, \quad \frac{u_{n+1}}{u_n} \leq \ell + \varepsilon = 1 - \varepsilon.$$

On a donc un produit télescopique : pour tout $n \geq n_0$,

$$\frac{u_n}{u_{n_0}} = \prod_{k=n_0}^{n-1} \frac{u_{k+1}}{u_k} \leq (1-\varepsilon)^{n-n_0}, \quad u_n \leq \frac{u_{n_0}}{(1-\varepsilon)^{n_0}} (1-\varepsilon)^n.$$

Posons $v_n = \dfrac{u_{n_0}}{(1-\varepsilon)^{n_0}} (1-\varepsilon)^n$. Alors les séries $\sum_n u_n$ et $\sum_n v_n$ sont à termes positifs et la série $\sum_n v_n$ converge. En effet, c'est une série géométrique de raison $1 - \varepsilon \in]0,1[$. Donc par comparaison des séries à termes positifs, $\sum_n u_n$ converge.

(ii) Si $\ell > 1$, il existe $n_0 \in \mathbb{N}$ tel que

$$\forall n \in \mathbb{N}, \quad \frac{u_{n+1}}{u_n} \geq 1, \quad u_{n+1} \geq u_n.$$

La suite (u_n) est donc croissante à partir d'un certain rang, et puisqu'elle n'est pas identiquement nulle, elle ne converge pas vers 0. Donc $\sum_n u_n$ diverge grossièrement.

□

Si $\ell = 1$, on ne peut pas conclure. En effet,

$$\lim_{n\to+\infty} \frac{\frac{1}{n+1}}{\frac{1}{n}} = 1, \quad \sum_n \frac{1}{n} \text{ diverge}, \quad \lim_{n\to+\infty} \frac{\frac{1}{(n+1)^2}}{\frac{1}{n^2}} = 1, \quad \sum_n \frac{1}{n^2} \text{ converge.}$$

Exemple 2.13 :
Déterminons la nature de $\sum_n u_n$ avec

$$\forall n \in \mathbb{N}, \quad u_n = \frac{1}{\binom{2n}{n}}.$$

La série $\sum_n u_n$ est à termes strictement positifs. On a, pour tout $n \in \mathbb{N}$,

$$\frac{u_{n+1}}{u_n} = \frac{\binom{2n}{n}}{\binom{2n+2}{n+2}} = \frac{(2n)!\,((n+1)!)^2}{(2n+2)!\,(n!)^2} = \frac{(n+1)^2}{(2n+2)\,(2n+1)} \xrightarrow[n\to+\infty]{} \frac{1}{4}.$$

D'après le critère de D'Alembert, la série $\sum_n u_n$ converge. ♢

Exercice 2.14 :
Soit $a > 0$. Etudier la convergence de la série $\sum_n \binom{n}{3} a^n$.

8. Jean-Baptiste le Rond D'Alembert (1717-1783) : Philosophe et mathématicien français.

Réponse

Posons $u_n = \binom{n}{3} a^n$ pour $n \in \mathbb{N}$. La série $\sum_n u_n$ est à termes strictement positifs et

$$\forall n \in \mathbb{N}, \quad \frac{u_{n+1}}{u_n} = \frac{\binom{n+1}{3} a^{n+1}}{\binom{n}{3} a^n} = \frac{n+1}{n-2} a \xrightarrow[n \to +\infty]{} a.$$

- Si $a > 1$, d'après le critère de D'Alembert, $\sum_n u_n$ diverge.
- Si $a < 1$, d'après le critère de D'Alembert, $\sum_n u_n$ converge.
- Si $a = 1$, on a

$$\forall n \in \mathbb{N}, \quad u_{n+1} = \frac{n+1}{n-2} u_n > u_n.$$

La suite (u_n) est croissante, donc $\sum_n u_n$ diverge grossièrement.

En conclusion, $\sum_n u_n$ converge si, et seulement si, $a < 1$.

◇

Exercice 2.15 :
Soit $a > 0$. On définit

$$\forall n \in \mathbb{N}^*, \quad u_n = a^{\sum_{k=1}^{n} \frac{1}{k}}.$$

Déterminer la nature de la série $\sum_n u_n$.

Réponse

Malgré l'allure de la série, le critère de D'Alembert est en défaut ici, car

$$\lim_{n \to +\infty} \frac{u_{n+1}}{u_n} = \lim_{n \to +\infty} a^{\frac{1}{n+1}} = 1.$$

Qu'à cela ne tienne, on a

$$\sum_{k=1}^{n} \frac{1}{k} = \ln n + \gamma + o(1),$$

d'où

$$u_n = a^{\ln n + \gamma + o(1)} = a^\gamma \, \mathrm{e}^{\ln n \ln a} \, \mathrm{e}^{o(1)} \underset{n \to +\infty}{\sim} \frac{a^\gamma}{n^{-\ln a}}.$$

Les séries $\sum_n u_n$ et $\sum_n \frac{a^\gamma}{n^{-\ln a}}$ sont à termes positifs, donc

$$\sum_n u_n \text{ converge} \iff \sum_n \frac{a^\gamma}{n^{-\ln a}} \text{ converge} \iff -\ln a > 1 \iff a < \mathrm{e}^{-1}.$$

◇

III Étude pratique

Comme pour les intégrales de fonctions dont le signe est variable, si les termes de la série que l'on étudie ne sont pas positifs, le travail est beaucoup plus difficile.

1. Absolue convergence

Comme pour les intégrales, on commencera d'abord par étudier la valeur absolue (ou le module) du terme général de la série.

Théorème 3.1

Soit $\sum_n u_n$ une série à termes réels ou complexes. Alors

$$\sum_n |u_n| \text{ converge} \Longrightarrow \sum_n u_n \text{ converge.}$$

Dans ce cas, on a

$$\left|\sum_{n=0}^{+\infty} u_n\right| \leq \sum_{n=0}^{+\infty} |u_n|.$$

Démonstration : Supposons que $\sum_n |u_n|$ converge.

- Premier cas : u_n est à termes réels. Soit $n \in \mathbb{N}$, on pose

$$u_n^+ = \max(0, u_n), \quad u_n^- = \max(0, -u_n).$$

On a alors

$$u_n = u_n^+ - u_n^-, \quad |u_n| = u_n^+ + u_n^-, \quad 0 \leq u_n^+, u_n^- \leq |u_n|.$$

Donc les séries $\sum_n u_n^+$ et $\sum_n u_n^-$ convergent, et donc $\sum_n u_n$ converge.

- Deuxième cas : u_n est à termes complexes. Pour $n \in \mathbb{N}$, on a

$$u_n = \Re\mathrm{e}(u_n) + i\Im\mathrm{m}(u_n), \quad 0 \leq |\Re\mathrm{e}(u_n)|, |\Im\mathrm{m}(u_n)| \leq |u_n|.$$

Donc les séries $\sum_n |\Re\mathrm{e}(u_n)|$ et $\sum_n |\Im\mathrm{m}(u_n)|$ convergent, donc $\sum_n \Re\mathrm{e}(u_n)$ et $\sum_n \Im\mathrm{m}(u_n)$ convergent, et donc $\sum_n u_n$ converge.

Pour tout $N \in \mathbb{N}$, on a

$$\left|\sum_{n=0}^{N} u_n\right| \leq \sum_{n=0}^{N} |u_n|, \quad \lim_{N\to+\infty}\left|\sum_{n=0}^{N} u_n\right| \leq \lim_{N\to+\infty}\sum_{n=0}^{N} |u_n|, \quad \left|\sum_{n=0}^{+\infty} u_n\right| \leq \sum_{n=0}^{+\infty} |u_n|.$$

$\square$

Définition 3.2 *Convergence absolue et semi-convergence*

Soit $\sum_n u_n$ une série à valeurs dans $\mathbb{K}$. On dit que $\sum_n u_n$ *converge absolument* si $\sum_n |u_n|$ converge. Si la série $\sum_n u_n$ converge mais ne converge pas absolument, on dit que $\sum_n u_n$ est semi-convergente.

On a donc vu, comme dans le cas des intégrales généralisées, que

$$\sum_n u_n \text{ converge absolument} \Rightarrow \sum_n u_n \text{ converge.}$$

Ce critère est très utile en pratique pour étudier la nature d'une série "simple" à termes complexes ou de signe variable. Malheureusement, il existe des intégrales semi-convergentes, comme on va le voir maintenant.

Exemple 3.3 :
La série $\sum_n \mathrm{e}^{(i-1)n}$ converge. En effet,

$$\forall n \in \mathbb{N}, \quad |\,\mathrm{e}^{(i-1)n}\,| = |\,\mathrm{e}^{in}\,\mathrm{e}^{-n}\,| = \mathrm{e}^{-n}\,.$$

C'est une série géométrique, la série $\sum_n \mathrm{e}^{(i-1)n}$ converge absolument, donc converge. ◊

Exercice 3.4 :
Etudier la nature de $\sum_n u_n$ avec $u_n = i + \dfrac{(-1)^n \ln n}{n^{3/2}}$.

Réponse

La série $\sum_n \operatorname{Im}(u_n)$ diverge grossièrement donc $\sum_n u_n$ diverge.

◊

2. Séries alternées

On dispose d'un résultat très puissant pour les séries alternées, c'est-à-dire dont le signe est alterné.

Définition 3.5 *Série alternée*

Soit $\sum_n u_n$ une série à termes réels. On dit que $\sum_n u_n$ est *alternée* si $((-1)^n u_n)_{n\in\mathbb{N}}$ est de signe constant.

Autrement dit, $\sum_n u_n$ est alternée si, et seulement si,

$$\exists \varepsilon \in \{-1, 1\}, \forall n \in \mathbb{N}, \quad u_n = \varepsilon\,(-1)^n\,|u_n|.$$

Théorème 3.6 *Critère spécial des séries alternées*

Soit $\sum_n u_n$ une série alternée. On suppose que la suite $(|u_n|)_{n\in\mathbb{N}}$ est décroissante et converge vers 0. Alors :

(i) La série $\sum_n u_n$ est convergente.

(ii) Pour tout $N \in \mathbb{N}$, $\sum_{n=N}^{+\infty} u_n$ et u_N sont de même signe.

(iii) Pour tout $N \in \mathbb{N}$, $\left|\sum_{n=N}^{+\infty} u_n\right| \leq |u_N|$.

En particulier, $\sum_{n=0}^{\infty} u_n$ est du signe de u_0.

Démonstration : On note, pour tout $N \in \mathbb{N}$, $S_N = \sum_{n=0}^{N} u_n$. Quitte à considérer $(-u_n)$, on peut supposer que $u_0 \geq 0$ (donc u_n est du signe de $(-1)^n$).

$\boxed{(i)}$ On va montrer que les suites (S_{2N}) et (S_{2N+1}) sont adjacentes. Soit $N \in \mathbb{N}$.

$$\begin{aligned} S_{2(N+1)} - S_{2N} &= u_{2N+2} + u_{2N+1} = |u_{2N+2}| - |u_{2N+1}| \leq 0, \\ S_{2(N+1)+1} - S_{2N+1} &= u_{2N+3} + u_{2N+2} = -|u_{2N+3}| + |u_{2N+2}| \geq 0, \\ S_{2N+1} - S_{2N} &= u_{2N+1} \xrightarrow[n\to+\infty]{} 0. \end{aligned}$$

Donc (S_{2N}) est décroissante, (S_{2N+1}) est croissante, et leur différence tend vers 0. Elles sont donc adjacentes, et convergent vers une même limite $\ell \in \mathbb{R}$. On en déduit que (S_N) converge, et donc $\sum_n u_n$ converge (vers ℓ) par définition.

$\boxed{(ii) \text{ et } (iii)}$ On vient de montrer que $\lim_{N\to+\infty}(S_{2N}) = \lim_{N\to+\infty}(S_{2N+1}) = \ell = \sum_{n=0}^{+\infty} u_n$. Posons

$$\forall N \in \mathbb{N}, \quad R_N = \sum_{n=N+1}^{+\infty} u_n = \ell - S_N$$

Puisque (S_{2N}) et (S_{2N+1}) sont adjacentes, on a pour tout $N \in \mathbb{N}$,

$$S_{2N+1} \leq \ell \leq S_{2N}, \quad u_{2N+1} \leq R_{2N} \leq 0.$$

Donc $\sum_{n=2N+1}^{\infty} u_n$ et u_{2N+1} sont de même signe et $\left|\sum_{n=2N+1}^{+\infty} u_n\right| \leq |u_{2N+1}|$. De même, on a

$$S_{2N+1} \leq \ell \leq S_{2N+2}, \quad 0 \leq R_{2N+1} \leq u_{2N+2}.$$

Donc $\sum_{n=2N+2}^{\infty} u_n$ et u_{2N+2} sont de même signe et $\left|\sum_{n=2N+2}^{+\infty} u_n\right| \leq |u_{2N+2}|$. Enfin,

$$0 \leq S_1 \leq \sum_{n=0}^{+\infty} u_n \leq S_0 = u_0,$$

car $S_1 = u_0 + u_1 = |u_0| - |u_1| \geq 0$. Donc $\sum_{n=0}^{\infty} u_n$ et u_0 sont de même signe et $\left|\sum_{n=0}^{+\infty} u_n\right| \leq |u_0|$. $\square$

Ce théorème reste vrai "à partir d'un certain rang".

Exemple 3.7 :
La série $\sum_n \frac{(-1)^n}{n}$ est semi-convergente. En effet, cette série converge d'après le critère spécial des séries alternées, et on sait que $\sum_n \frac{1}{n}$ diverge. Toujours d'après le critère spécial, on sait que $\sum_{n=1}^{\infty} \frac{(-1)^n}{n}$ est négative, mais il ne permet pas de calculer cette somme. On peut par contre reconnaitre le DL de $\ln(1+x)$:

$$\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} + \dots, \qquad -\ln(1+x) = \sum_{n=1}^{N} \frac{(-1)^n x^n}{n} + \dots$$

et conjecturer que $\sum_{n=1}^{\infty} \frac{(-1)^n}{n} = -\ln 2$. Pour cela, on va intégrer la somme de la série géométrique (comme pour trouver le DL de $\ln(1+x)$). On a, pour tout $N \in \mathbb{N}$ et pour tout $x \in]-1,1]$,

$$\sum_{n=0}^{N} \frac{(-x)^n}{n} = \frac{1-(-x)^{N+1}}{1+x},$$
$$\frac{1}{1+x} = \sum_{n=0}^{N} \frac{(-x)^n}{n} + \frac{(-x)^{N+1}}{1+x}.$$

Ces fonctions sont continues sur $[0,1]$, donc on peut intégrer cette égalité :

$$\int_0^1 \frac{dx}{1+x} = \ln 2 = \sum_{n=0}^{N} \int_0^1 \frac{(-x)^n}{n} dx + (-1)^{N+1} \int_0^1 \frac{x^{N+1}dx}{1+x} = \sum_{n=0}^{N} \frac{(-1)^n}{n+1} + (-1)^{N+1} \int_0^1 \frac{x^{N+1}dx}{1+x}$$
$$-\ln 2 = \sum_{n=1}^{N+1} \frac{(-1)^n}{n} + (-1)^N \int_0^1 \frac{x^{N+1}dx}{1+x}.$$

De plus,

$$0 \le \int_0^1 \frac{x^{N+1}dx}{1+x} \le \int_0^1 x^{N+1}dx = \frac{1}{N+2}, \qquad \lim_{N\to+\infty} \int_0^1 \frac{x^{N+1}dx}{1+x} = 0, \qquad -\ln 2 = \sum_{n=1}^{\infty} \frac{(-1)^n}{n}$$

Ici, on fait à peu près la même chose que pour l'exercice 1.22, où l'on a dérivé la série géométrique, et maintenant on l'intègre. ♢

Exercice 3.8 :
Déterminer la nature de $\sum_n \ln\left(1 + \frac{(-1)^n}{\sqrt{n}}\right)$.

Réponse

La série $\sum_n \frac{(-1)^n}{\sqrt{n}}$ n'étant pas de signe constant, il est exclu de raisonner par équivalent. Qu'à cela ne tienne, on fait un développement asymptotique du terme général :

$$\ln\left(1 + \frac{(-1)^n}{\sqrt{n}}\right) \underset{n\to+\infty}{=} \frac{(-1)^n}{\sqrt{n}} + \frac{1}{2n} + o\left(\frac{1}{n}\right).$$

Posons

$$\forall n \in \mathbb{N}, \quad h_n = \ln\left(1 + \frac{(-1)^n}{\sqrt{n}}\right) - \frac{(-1)^n}{\sqrt{n}}, \quad h_n \underset{n\to+\infty}{\sim} \frac{1}{2n}.$$

La série $\sum_n \frac{(-1)^n}{\sqrt{n}}$ converge (en vertu du critère spécial des séries alternées). En revanche, la série $\sum_n \frac{1}{2n}$ est une série à termes positifs divergente (d'après le critère de Riemann), et donc $\sum_n h_n$ diverge par comparaison des séries à termes positifs. Donc $\sum_n \ln\left(1 + \frac{(-1)^n}{\sqrt{n}}\right)$ diverge.

$\diamondsuit$

Au passage, on vient de trouver un contre-exemple au théorème de comparaison de séries à termes positifs lorsque les séries ne sont pas à termes positifs. [9]

Exemple 3.9 :
On considère $\sum_n u_n$ avec

$$\forall n \geq 2, \quad u_n = \frac{(-1)^n}{(-1)^n + \ln n}.$$

La série $\sum_n u_n$ est bien alternée car $\frac{1}{(-1)^n + \ln n} \geq 0$. En revanche, on peut remarquer que la suite $(|u_n|)$ n'est pas décroissante. On a

$$u_n \underset{n\to+\infty}{\sim} \frac{(-1)^n}{\ln n}.$$

Posons pour tout $n \geq 2$,

$$h_n = \frac{(-1)^n}{\ln n} - u_n = \frac{1}{((-1)^n + \ln n)\ln n} \underset{n\to+\infty}{\sim} \frac{1}{\ln^2 n}.$$

Les série $\sum_n h_n$ et $\sum_n \frac{1}{\ln^2 n}$ sont à termes positifs et divergent (d'après le critère de Bertrand et le théorème de comparaison des séries à termes positifs). D'autre part, la série $\sum_n \frac{(-1)^n}{\ln n}$ satisfait bien les hypothèses du critère spécial des séries alternées, donc elle converge. On en déduit que $\sum_n u_n$ diverge. $\diamondsuit$

Aussi puissant que soit le critère spécial des séries alternées, on ne peut pas toujours conclure quant à la nature d'une série dont le terme général est de signe variable.

Proposition 3.10 *Admis*
Soit $\theta \in \mathbb{R}$. Supposons que $\theta \notin \pi\mathbb{Z}$. Alors

(i) La série $\sum_n \frac{\sin(n\theta)}{n^\alpha}$ converge si, et seulement si, $\alpha > 0$.

(ii) La série $\sum_n \frac{\cos(n\theta)}{n^\alpha}$ converge si, et seulement si, $\alpha > 0$.

Un équivalent de ce résultat est d'ailleurs vrai pour les intégrales généralisées, et on l'a prouvé (en partie, du moins). Dans le cadre des séries, on n'a plus accès à l'intégration par parties, ce qui rend le problème beaucoup plus difficile. On ne peut pas non plus utiliser de comparaison série/intégrale, les fonctions trigonométriques n'étant pas monotones.

9. C'est d'ailleurs pour cela que le théorème ne s'appelle pas "comparaison des séries".

Exercice 3.11 :
Etudier la convergence de la série $\sum_n \frac{\sin\left(n\frac{\pi}{2}\right)}{\sqrt{n+1}}$.

Réponse

Posons, pour tout $n \in \mathbb{N}$, $u_n = \frac{\sin\left(n\frac{\pi}{2}\right)}{\sqrt{n+1}}$ et S_n la somme partielle d'indice n de $\sum_n u_n$. On remarque que

$$\forall n \in \mathbb{N}, \quad u_{2p} = 0, \quad u_{2p+1} = \frac{(-1)^p}{\sqrt{2p+2}}.$$

Soit $N \in \mathbb{N}$. On a alors

$$\sum_{n=0}^{2N+1} u_n = \sum_{p=0}^{N} u_{2p} + u_{2p+1} = \sum_{p=0}^{N} \frac{(-1)^p}{\sqrt{2p+2}}.$$

La série $\sum_p \frac{(-1)^p}{\sqrt{2p+2}}$ satisfait le critère spécial des séries alternées, donc elle converge. Donc (S_{2N+1}) converge, vers une limite qu'on note ℓ. De plus

$$S_{2N} = S_{2n+1} - u_{2n+1} = S_{2N+1} - \frac{(-1)^N}{\sqrt{2N+2}} \xrightarrow[N\to+\infty]{} \ell.$$

Donc les suites (S_{2N}) et (S_{2N+1}) convergent vers la même limite ℓ. Donc (S_n) converge, donc $\sum_n u_n$ converge.

$\diamondsuit$

3. Série exponentielle

Proposition 3.12

La série exponentielle $\sum_n \frac{z^n}{n!}$ converge pour tout $z \in \mathbb{C}$, et

$$\sum_{n=0}^{+\infty} \frac{z^n}{n!} = \mathrm{e}^z\,.$$

Démonstration : Posons pour tout $n \in \mathbb{N}, u_n = \frac{z^n}{n!}$. On va appliquer le critère de D'Alembert à la série $\sum_n |u_n|$. En effet,

$$\forall n \in \mathbb{N}, \quad |u_n| \neq 0, \quad \frac{|u_{n+1}|}{|u_n|} = \left|\frac{z^{n+1}n!}{z^n\,(n+1)!}\right| = \frac{|z|}{n+1} \xrightarrow[n\to+\infty]{} 0.$$

Donc $\sum_n u_n$ converge absolument donc converge. Calculons la somme de la série pour $z \in \mathbb{R}$. On sait que $\exp \in \mathcal{C}^\infty(\mathbb{R})$. Soient $I =]0, z[\cup]z, 0[$ et $n \in \mathbb{N}$. Alors

$$\forall x \in I, \quad |\exp^{(n+1)}(x)| = \mathrm{e}^x \leq \mathrm{e}^{|z|}\,.$$

D'après l'inégalité de Taylor-Lagrange appliquée à exp sur I, on a, pour tout $n \in \mathbb{N}^*$

$$\left| \mathrm{e}^z - \sum_{k=0}^{n} \frac{z^k}{k!} \right| \leq \mathrm{e}^{|z|} \frac{|z|^{n+1}}{(n+1)!} \xrightarrow[n\to+\infty]{} 0.$$

Donc $\displaystyle\sum_{n=0}^{+\infty} \frac{z^n}{n!} = \mathrm{e}^z$. On admet que le résultat reste vrai pour $z \in \mathbb{C}$. □

Exercice 3.13 :
Soit $z \in \mathbb{C}$. Montrer que les séries suivantes sont convergentes et calculer leur nature :

$$\sum_n \frac{z^{2n}}{(2n)!}, \quad \sum_n \frac{z^{2n+1}}{(2n+1)!}$$

Réponse

Remarquons que le problème revient à étudier les séries

$$\sum_n \frac{z^n}{n!} \mathbb{1}_{\{n \text{ pair}\}}, \quad \sum_n \frac{z^n}{n!} \mathbb{1}_{\{n \text{ impair}\}}$$

Ces séries sont absolument convergentes, car

$$\forall n \in \mathbb{N}, \quad \left| \frac{z^n}{n!} \mathbb{1}_{\{n \text{ pair}\}} \right| \leq \frac{|z|^n}{n!}, \quad \left| \frac{z^n}{n!} \mathbb{1}_{\{n \text{ impair}\}} \right| \leq \frac{|z|^n}{n!}, \quad \sum_n \frac{|z|^n}{n!} \text{ converge.}$$

Les sommes ressemblent aux développements limités respectifs de $\operatorname{ch} z$ et $\operatorname{sh} z$. On a, en effet,

$$\begin{aligned}\operatorname{ch} z = \frac{\mathrm{e}^z + \mathrm{e}^{-z}}{2} &= \frac{1}{2}\left(\sum_{k=0}^{\infty} \frac{z^n}{n!} + \sum_{k=0}^{\infty} \frac{(-z)^n}{n!} \right) = \frac{1}{2}\left(\sum_{k=0}^{\infty} \frac{z^n}{n!} + \frac{(-z)^n}{n!} \right) \\ &= \frac{1}{2} \sum_{k=0}^{\infty} \frac{2z^n}{n!} \mathbb{1}_{\{n \text{ pair}\}} = \sum_{n=0}^{\infty} \frac{z^{2n}}{(2n)!}\end{aligned}$$

De plus, on a

$$\operatorname{sh} z = \mathrm{e}^z - \operatorname{ch} z = \sum_{k=0}^{\infty} \frac{2z^n}{n!} - \sum_{k=0}^{\infty} \frac{2z^n}{n!} \mathbb{1}_{\{n \text{ pair}\}} = \sum_{k=0}^{\infty} \frac{2z^n}{n!} \mathbb{1}_{\{n \text{ impair}\}} \sum_{n=0}^{\infty} \frac{z^{2n+1}}{(2n+1)!}.$$

♢

4. Formule de Stirling

Dans le monde discret, on peut définir des séries avec des produits, et un cas particulier de produit est la factorielle. On donne ici une formule permettant d'obtenir un équivalent de la factorielle.

Théorème 3.14 *Formule de Stirling*[10]*- Admis*
On a

$$n! \underset{n\to+\infty}{\sim} \sqrt{2\pi n} \left(\frac{n}{\mathrm{e}}\right)^n.$$

Cette formule est difficile à démontrer sans tricher (lorsqu'on ne connait pas la forme de l'équivalent, comme c'était le cas pour les premiers mathématiciens qui se sont attaqués au problème). Et encore, il est difficile de trouver la bonne constante, c'est-à-dire le facteur $\sqrt{2\pi}$. On peut en donner un encadrement grossier de manière très simple, par contre.

Exercice 3.15 :
Montrer que, pour tout $n \in \mathbb{N}^*$,

$$\mathrm{e}\left(\frac{n}{\mathrm{e}}\right)^n \leq n! \leq \mathrm{e}\left(\frac{n}{\mathrm{e}}\right)^n n.$$

Indication : On pourra utiliser une comparaison série/intégrale.

Réponse

Notons pour $n \in \mathbb{N}^*$,

$$S_n = \ln(n!) = \ln\left(\prod_{k=1}^{n} k\right) = \sum_{k=1}^{n} \ln k.$$

La fonction ln étant croissante et positive sur $[1, +\infty[$, on a, pour tout $n \in \mathbb{N}$,

$$\int_{n-1}^{n} \ln t dt \leq \ln n \leq \int_{n}^{n+1} \ln t dt, \quad \int_{1}^{n} \ln t dt \leq \sum_{k=1}^{n} \ln k \leq \int_{1}^{n} \ln t dt + \ln n$$

On a alors

$$\int_{1}^{n} \ln t dt = [t \ln t - t]_{t=1}^{n} = n \ln n - n + 1, \quad \exp\left(\int_{1}^{n} \ln t dt\right) = \mathrm{e}\left(\frac{n}{\mathrm{e}}\right)^n.$$

Par croissance de l'exponentielle, on en déduit que

$$\mathrm{e}\left(\frac{n}{\mathrm{e}}\right)^n \leq \mathrm{e}^{S_n} \leq \mathrm{e}\left(\frac{n}{\mathrm{e}}\right)^n n.$$

◊

IV Familles sommables et dénombrabilité

Dans tout ce chapitre, on a sommé des familles indexées par $\mathbb{N}$. Il y a donc un ordre et un point de départ évidents pour sommer les termes. La nouvelle question qu'on se pose est "peut-on faire la même chose si les termes sont indexés par $\mathbb{Z}$, ou par $\mathbb{N}^2$, ou par $\mathbb{R}$?" Pour répondre à cette question, on aura besoin de définir la notion d'ensemble dénombrable, puis la notion de famille sommable.

1. Ensembles dénombrables

Définition 4.1 *Ensemble dénombrable*
Soit I un ensemble non-vide. On dit que I est *dénombrable* s'il existe une bijection de I vers un sous-ensemble non-vide de $\mathbb{N}$.

10. James Stirling (1692-1770) : Mathématicien écossais.

Dire que I est dénombrable revient à dire que l'on peut "compter ses éléments", la bijection servant à "numéroter" les éléments de I. De manière équivalente, I est dénombrable s'il existe une injection de I vers $\mathbb{N}$ ou une surjection de $\mathbb{N}$ vers I.

Cette notion est plutôt théorique et on ne l'utilisera pas en pratique. On devra juste savoir quels sont les ensembles dénombrables classiques.

Définition 4.2 *Suite exhaustive*

Soit I un ensemble non-vide et soit $(J_n)_{n\in\mathbb{N}}$ une suite de sous-ensembles de I. On dit que (J_n) *est une suite exhaustivede* I si

(i) $I = \bigcup_{n=0}^{+\infty} J_n$.

(ii) Pour tout $n \in \mathbb{N}$, $J_n \subseteq J_{n+1}$.

Exemple 4.3 :

- La suite $([-n, n])_{n\in\mathbb{N}}$ est une suite exhaustive de $\mathbb{R}$.
- La suite $\left([\![0, n]\!]^2\right)_{n\in\mathbb{N}}$ est une suite exhaustive de $\mathbb{N}^2$.

$\diamondsuit$

Théorème 4.4

Soit I un ensemble non-vide. Alors on a équivalence entre :

(i) I est dénombrable

(ii) I admet une suite exhaustive de parties finies.

Démonstration : $\boxed{(i) \Rightarrow (ii)}$ Il existe $A \subseteq \mathbb{N}$ une partie non-vide et une bijection $\varphi : A \to I$. On pose $A_n = A \cap [\![0, n]\!]$ et $J_n = f(A_n)$. La suite (A_n) est croissante (pour l'inclusion), donc (J_n) est une suite de parties finies croissante. De plus,

$$A = A \cap \left(\bigcup_{n=0}^{+\infty} [\![0, n]\!]\right) = \bigcup_{n=0}^{+\infty} A_n.$$

Donc pour tout $y \in I$, il existe $x \in A$ tel que $f(x) = y$. Or il existe $n \in \mathbb{N}$ tel que $x \in A_n$ et donc $y \in f(A_n) = J_n$. Donc $I = \cup_{n=0}^{+\infty} J_n$ et donc (J_n) est une suite exhaustive de parties finies.

$\boxed{(ii) \Rightarrow (i)}$ Soit (J_n) une suite exhaustive de parties finies. Si (J_n) est stationnaire, alors l'ensemble I est fini et non-vide, donc dénombrable. Sinon, quitte à extraire une sous-suite, on peut supposer sans perte de généralité que $J_0 \neq \emptyset$ et que la suite (J_n) est strictement croissante. On définit alors $\varphi : \mathbb{N} \to I$ comme dans l'exemple 4.7. On pose

$$H_1 = J_0, \quad \forall n \in \mathbb{N}, \quad H_n = J_{n+1} \setminus J_n.$$

Par hypothèse, les ensembles H_n qu'on vient de définir ne sont pas vides. Alors,

$$I = \bigsqcup_{n=1}^{+\infty} H_n, \quad \forall y \in I, \exists! n \in \mathbb{N}, \quad y \in H_n.$$

On dit que (H_n) est une partition de l'ensemble I. On définit, pour tout $n \in \mathbb{N}^*$,

$$|H_n| = h_n, \quad H_n = \{y_1^{(n)}, \dots, y_{h_n}^{(n)}\}.$$

On pose, pour tout $k \in \mathbb{N}^*$,

$$\varphi(k) = \sum_{n=1}^{+\infty} y_k^{(n)} \mathbb{1}_{\{\sum_{p=1}^{n-1} h_p < k \leq \sum_{p=1}^{n} h_p\}} = \begin{cases} y_k^{(1)} & \text{si } k \leq h_1 \\ y_k^{(n)} & \text{si } \sum_{p=1}^{n-1} h_p < k \leq \sum_{p=1}^{n} h_p \end{cases}.$$

φ est bien définie car la somme est finie (elle ne contient qu'un terme). De plus, elle est bijective car les applications

$$\varphi_n : [\![\sum_{p=1}^{n-1} h_p + 1, \sum_{p=1}^{n} h_p]\!] \to H_n, \quad \varphi_n(k) = \varphi(k)$$

sont bijectives et $\displaystyle\bigsqcup_{n=1}^{+\infty} \mathrm{Im}(\varphi_n) = \bigsqcup_{n=1}^{+\infty} H_n = I$. Donc φ est bijective. □

Proposition 4.5

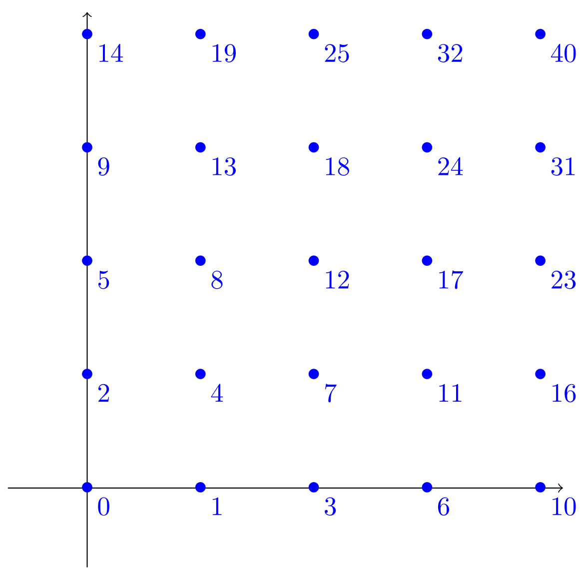
(i) Un ensemble fini est dénombrable.
(ii) $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$ sont dénombrables.
(iii) $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{R} \setminus \mathbb{Q}$ ne sont pas dénombrables.
(iv) Tout ensemble dénombrable est soit fini, soit en bijection avec $\mathbb{N}$.
(v) Un sous-ensemble non-vide d'un ensemble dénombrable est dénombrable.
(vi) Un produit cartésien fini d'ensembles dénombrables est dénombrable.
(vii) La réunion de deux ensembles dénombrables est dénombrable.

Exemple 4.6 :
Montrons que $\mathbb{Z}$ est dénombrable. On pose

$$\begin{array}{rccl} \varphi : & \mathbb{Z} & \to & \mathbb{N} \\ & p & \mapsto & \begin{cases} 2p & \text{si } p \geq 0 \\ -2p+1 & \text{si } p < 0 \end{cases} \end{array}.$$

φ est surjective car $\varphi(\mathbb{Z}) = \{2p / p \in \mathbb{N}\} \cup \{2p+1 / p \in \mathbb{N}^*\} = \mathbb{N}$. φ est injective car, si $\varphi(p) = \varphi(q)$ alors p et q sont de même signe, et φ est strictement croissante sur $\mathbb{N}$ et strictement décroissante sur $\mathbb{Z} \setminus \mathbb{N}$. Donc $p = q$. ♢

Exemple 4.7 :
On a déjà vu que $\mathbb{N}^2$ était dénombrable, car la famille de parties $\left([\![0, n]\!]^2\right)_{n\in\mathbb{N}}$ est une suite exhaustive de parties finies. On peut aussi le voir à l'aide d'une bijection : on peut lister les éléments de $\mathbb{N}^2$.



On peut écrire la bijection de la forme suivante : en notant pour $p \in \mathbb{N}, S_p = \sum_{k=0}^{p} k$, soit $\varphi : \mathbb{N} \to \mathbb{N}^2$ telle que :

$$\forall n \in \mathbb{N}, \quad \varphi(n) = \sum_{p=0}^{+\infty} (S_{p+1} - n - 1, n - S_p) \mathbb{1}_{\{S_p \leq n < S_{p+1}\}}.$$

$\diamondsuit$

Si on veut l'écrire proprement, on remarque qu'en général la bijection est plus difficile à écrire que la suite exhaustive de parties finies. On privilégie donc le second critère dans la suite (même si on n'aura jamais à démontrer que tel ou tel ensemble est dénombrable).

2. Familles sommables

Dans la suite, on définit I un ensemble dénombrable. On considèrera des familles du type $(u_i)_{i \in I}$ dont les termes sont des éléments de $\mathbb{K}$ indexés par I. Par exemple :

$$\left((1+i)^{p+q}\right)_{(p,q)\in\mathbb{N}^2}, \quad \left(\frac{2}{n}\right)_{n\in\mathbb{Z}^*}.$$

Dans les applications, on choisira toujours $I = \mathbb{Z}$ ou $I = \mathbb{N}^2$ (ou des sous-parties de ces ensembles).

Il faut comprendre que pour faire la somme des termes de ces familles, on n'a pas d'ordre "naturel" comme pour les familles indexées par $\mathbb{N}$ ou $\mathbb{N}^*$. On commence par un exemple fondamental, pour comprendre les notions à venir.

Exemple 4.8 :
On sait que

$$\sum_{n=1}^{+\infty} \frac{(-1)^{n+1}}{n} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \cdots = \ln 2.$$

On s'intéresse à la somme de cette série obtenue en changeant l'ordre des termes et en prenant deux termes positifs puis un terme négatif :

$$S = 1 + \frac{1}{3} - \frac{1}{2} + \frac{1}{5} + \frac{1}{7} - \frac{1}{4} + \frac{1}{9} + \frac{1}{11} + \ldots$$

Posons donc, pour tout $p \in \mathbb{N}$,

$$u_{3p+1} = \frac{1}{4p+1}, \quad u_{3p+2} = \frac{1}{4p+3}, \quad u_{3p+3} = -\frac{1}{2p+2}.$$

Posons, pour tout $N \in \mathbb{N}^*$,

$$S_N = \sum_{n=1}^{N} u_n, \quad T_n = \sum_{k=1}^{N} \frac{1}{n} \underset{N\to+\infty}{=\!=} \ln N + \gamma + o(1).$$

On a alors

$$\begin{aligned}
S_{3N} &= \sum_{p=0}^{N-1} \frac{1}{4p+1} + \frac{1}{4p+3} - \frac{1}{2p+2} = \sum_{k=1}^{2N} \frac{1}{2k+1} - \frac{T_N}{2} = \sum_{k=1}^{4N} \frac{\mathbb{1}_{\{k \text{ impair}\}}}{k} - \frac{T_N}{2} \\
&= \sum_{k=1}^{4N} \frac{1}{k} - \sum_{k=1}^{4N} \frac{\mathbb{1}_{\{k \text{ pair}\}}}{k} - \frac{T_N}{2} = T_{4N} - \sum_{p=1}^{2N} \frac{1}{2p} - \frac{T_N}{2} = T_{4N} - \frac{T_{2N}}{2} - \frac{T_N}{2} \\
&\underset{N\to+\infty}{=\!=} \ln(4N) + \gamma - \frac{\ln(2N)}{2} - \frac{\gamma}{2} - \frac{\ln N}{2} - \frac{\gamma}{2} + o(1) = \ln\left(\frac{4N}{\sqrt{2N}\sqrt{N}}\right) + o(1) \\
&\xrightarrow[N\to+\infty]{} \frac{3}{2} \ln 2.
\end{aligned}$$

De même, $S_{3N+1} = S_{3N} + u_{3N+1}$ et $S_{3N+1} = S_{3N+1} + u_{3N+2}$ donc les suites $(S_{3N}), (S_{3N+1})$ et (S_{3N+2}) convergent vers la même limite $\frac{3}{2}\ln 2$. Donc $\sum_n u_n$ converge et

$$S = \sum_{n=1}^{+\infty} u_n = \frac{3}{2}\ln 2.$$

$\diamondsuit$

On voit donc que si la série ne converge pas absolument, l'ordre des termes est très important : si l'on somme les termes dans un ordre différent, on obtient potentiellement une autre limite.

Définition 4.9 *Famille sommable*
Soit $(u_i)_{i\in I}$ une famille à termes quelconques (réels ou complexes). On dit que $(u_i)_{i\in I}$ est *sommable* si

$$\exists M > 0, \quad \forall J \subseteq I, \quad \left(|J| < +\infty \Rightarrow \sum_{i\in J} |u_i| \leq M\right).$$

Définition/Proposition 4.10 *Admise*
Soit $(u_i)_{i\in I}$ une famille à termes quelconques sommable. Alors pour tout suite exhaustive (J_n) de parties finies de I, la suite $\left(\sum_{i\in J_n} u_i\right)_{n\in\mathbb{N}}$ est convergente. De plus, sa limite ne dépend pas de la suite (J_n). On note

$$\sum_{i\in I} u_i = \lim_{n\to+\infty} \sum_{i\in J_n} u_i.$$

La notion de "famille sommable" signifie qu'on peut sommer tous les termes de la famille, sans ordre. Sinon, la somme de la famille (quand elle existe) dépendrait de la suite (J_n), comme à l'exemple 4.8. Pour une famille $(u_i)_{i\in I}$ à termes positifs, on n'a pas tout à fait le même problème de mauvaise définition de la somme $\sum_{i\in I} u_i$: soit celle-ci existe, soit "elle est infinie".

On remarquera qu'une famille $(u_n)_{n\in\mathbb{N}}$ est sommable si, et seulement si, la série $\sum_n u_n$ est absolument convergente, et qu'alors on a

$$\sum_{n\in\mathbb{N}} u_n = \sum_{n=0}^{+\infty} u_n.$$

La définition de somme d'une série semi-convergente fait quant à elle intervenir l'ordre usuel sur $\mathbb{N}$ dans le passage à la limite quand "n est de plus en plus grand".

3. Familles indexées par $\mathbb{Z}$

Théorème 4.11
Soit $(u_n)_{n\in\mathbb{Z}}$ une famille à termes quelconques. Alors on a l'équivalence

(i) $(u_n)_{n\in\mathbb{N}}$ est sommable.

(ii) La suite $\left(\sum_{n=-N}^{N} |u_n|\right)_{N\in\mathbb{N}}$ converge.

(iii) Les séries $\sum_n |u_n|$ et $\sum_n |u_{-n}|$ convergent.

Dans ce cas, on a

$$\sum_{n\in\mathbb{Z}} u_n = \lim_{N\to+\infty} \sum_{n=-N}^{N} u_n = \sum_{n=0}^{+\infty} u_n + \sum_{n=1}^{+\infty} u_{-n}.$$

On ne manquera pas de remarquer le lien avec les suites exhaustives utilisées pour montrer que $\mathbb{Z}$ est dénombrable.

4. Séries doubles

Le cas particulier de famille dénombrable qui nous intéresse pour finir est le cas des familles indexées sur $\mathbb{N}^2$, c'est-à-dire de la forme $(u_{p,q})_{(p,q)\in\mathbb{N}^2}$.

Théorème 4.12 *Fubini*[11] *- Admis*

Soit $(u_{p,q})_{(p,q)\in\mathbb{N}^2}$ une famille à termes quelconques indexée par $\mathbb{N}^2$. Alors on a équivalence entre :

(i) La famille $(u_{p,q})_{(p,q)\in\mathbb{N}}$ est sommable.

(ii) Pour tout $p \in \mathbb{N}$, la série $\sum_q |u_{p,q}|$ converge et la série $\sum_p \left(\sum_{q=0}^{\infty} |u_{p,q}|\right)$ converge.

(iii) Pour tout $q \in \mathbb{N}$, la série $\sum_p |u_{p,q}|$ converge et la série $\sum_q \left(\sum_{p=0}^{\infty} |u_{p,q}|\right)$ converge.

Dans ce cas, on a alors

$$\sum_{(p,q)\in\mathbb{N}^2} u_{p,q} = \sum_{p=0}^{+\infty} \left(\sum_{q=0}^{\infty} u_{p,q}\right) = \sum_{q=0}^{+\infty} \left(\sum_{p=0}^{\infty} u_{p,q}\right).$$

Autrement dit, on peut échanger les symboles $\sum$ si la famille $(u_{p,q})_{(p,q)\in\mathbb{N}}$ est sommable. Attention, ici le résultat est faux si la famille n'est pas sommable car les limites n'existent pas forcément.

L'idée de la preuve est la suivante : on peut toujours échanger des sommes finies sur $[\![1, N]\!]^2$, et on peut passer à la limite (dans $\mathbb{R}_+$) uniquement si la famille est sommable.

En fait, si la famille $(u_{p,q})_{(p,q)\in\mathbb{N}}$ est à termes positifs, on a toujours l'égalité

$$\sum_{(p,q)\in\mathbb{N}^2} u_{p,q} = \sum_{p=0}^{+\infty} \left(\sum_{q=0}^{\infty} u_{p,q}\right) = \sum_{q=0}^{+\infty} \left(\sum_{p=0}^{\infty} u_{p,q}\right).$$

Simplement, elle est valable dans $\mathbb{R}_+ \cup \{+\infty\}$.

Exemple 4.13 :
Soient $a \in]-1, 1[, b \in \mathbb{R}$. On définit la famille $(u_{p,q})_{p,q\in\mathbb{N}}$ par

$$\forall p, q \in \mathbb{N}, \quad u_{p,q} = \frac{(-1)^p\, a^q b^{2p+1}}{(2p+1)!}.$$

11. Guido Fubini (1879-1943) : Mathématicien italien.

Montrons que la famille est sommable. On a

$$\forall q \in \mathbb{N}, \quad \sum_{p=0}^{+\infty} |u_{p,q}| = a^q \operatorname{sh} b, \quad \sum_{q=0}^{+\infty} \left(\sum_{p=0}^{+\infty} |u_{p,q}| \right) = \frac{\operatorname{sh} b}{1-a}.$$

D'après le théorème de Fubini, on en déduit que la famille $(u_{p,q})_{p,q\in\mathbb{N}}$ est sommable. On a alors

$$\forall q \in \mathbb{N}, \quad \sum_{p=0}^{+\infty} u_{p,q} = a^q \sin b, \quad \sum_{q=0}^{+\infty} \left(\sum_{p=0}^{+\infty} u_{p,q} \right) = \frac{\sin b}{1-a}.$$

Donc, toujours d'après le théorème de Fubini,

$$\sum_{(p,q)\in\mathbb{N}^2} u_{p,q} = \frac{\sin b}{1-a}.$$

◇

Exemple 4.14 :
On étudie la sommabilité de la famille $(u_{p,q})_{(p,q)\in\mathbb{N}^2}$, avec

$$\forall p, q \in \mathbb{N}, \quad u_{p,q} = \frac{(-q)^p}{p!}.$$

On a

$$\forall q \in \mathbb{N}, \quad \sum_{p=0}^{+\infty} |u_{p,q}| = \sum_{p=0}^{+\infty} \frac{q^p}{p!} = \mathrm{e}^q, \quad \sum_q \mathrm{e}^q \text{ diverge.}$$

D'après le théorème de Fubini, la famille $(u_{p,q})$ n'est pas sommable. Par contre,

$$\forall q \in \mathbb{N}, \quad \sum_{p=0}^{+\infty} u_{p,q} = \mathrm{e}^{-q}, \quad \sum_{q=0}^{+\infty} \left(\sum_{p=0}^{+\infty} u_{p,q} \right) = \frac{\mathrm{e}}{\mathrm{e}-1}.$$

En revanche, pour tout $p \in \mathbb{N}$, la série $\displaystyle\sum_q \frac{(-q)^p}{p!}$ diverge grossièrement. ◇

⚠ Pour les familles doubles sommables, il y a toujours un ordre de sommation dans lequel les calculs sont simples, et un ordre plus compliqué.

Exemple 4.15 :
Montrons que la famille $(u_{p,q})_{p,q\in\mathbb{N}^*}$ est sommable, avec

$$\forall p, q \in \mathbb{N}^*, \quad u_{p,q} = \frac{q^2}{p^3\,(2p^2+3p+1)} \mathbb{1}\{p \geq q\}.$$

Remarquons que la famille est positive. On choisit de sommer d'abord sur q :

$$\forall p \in \mathbb{N}^*, \quad \sum_{q=1}^{+\infty} u_{p,q} = \sum_{q=1}^{p} \frac{q^2}{p^3\,(2p^2+3p+1)} = \frac{1}{p^3\,(2p^2+3p+1)} \times \frac{p\,(p+1)\,(2p+1)}{6} = \frac{1}{6p^2}.$$

Puisque $\displaystyle\sum_p \frac{1}{2p^2}$ converge, d'après le théorème de Fubini (pour les familles positives), on en déduit que la famille $(u_{p,q})$ est sommable et que

$$\sum_{p,q\in\mathbb{N}^*} u_{p,q} = \sum_{p=1}^{+\infty} \left(\sum_{q=1}^{+\infty} u_{p,q} \right) = \sum_{p=1}^{+\infty} \frac{1}{6p^2} = \frac{\pi^2}{36}.$$

◇

À connaître à la fin du chapitre

Séries de référence

- Savoir reconnaître les séries exponentielles, géométriques et télescopiques (entre autres).
- Connaître les résultats propres aux séries : critère spécial des séries alternées, critère de D'Alembert, formule de Stirling...

Séries à termes positifs

- Déterminer la convergence (ou l'absolue convergence) d'une série à l'aide d'un équivalent, d'une majoration, ou de relations de comparaison.

Vrai/Faux

☐ Si $\sum_n u_n$ converge, alors $\sum_n u_n^2$ converge.

☐ Si $\sum_n u_n$ converge absolument, alors $\sum_n u_n^2$ converge.

☐ Si $\sum_n u_n$ converge, alors $\sum_n n u_n$ converge.

☐ Si $\sum_n u_n$ converge, alors $\sum_n \frac{1}{n} u_n$ converge.

☐ Si $\sum_n u_n$ et $\sum_n v_n$ divergent, alors $\sum_n (u_n + v_n)$ diverge.

☐ Si $\sum_n u_n$ converge, alors $\sum_n \frac{1}{u_n}$ diverge.

☐ $\sum_n u_n$ converge si, et seulement si, $\sum_n u_{2n}$ et $\sum_n u_{2n+1}$ convergent.

Pour aller plus loin

- Théorème de réarrangement de Riemann.
- Séries géométriques dérivées et intégrées.
- Séries entières.

CHAPITRE 14

PROBABILITÉS DISCRÈTES

CHAPITRE 15

ALGÈBRE LINÉAIRE – DÉTERMINANT

On l'a vu dans les chapitres précédents, en dimension finie, les problèmes suivants se ramènent au mêmes calculs :

- déterminer si une matrice est inversible
- résoudre un système linéaire
- déterminer si une application linéaire est bijective
- déterminer si une famille est une base d'un espace vectoriel

On va donc introduire un outil unifié pour faire cette étude : il s'agit du déterminant. il faudra donc être à l'aise avec les deux chapitres suivants :

- Espaces vectoriels de dimension finie
- Matrices

Dans tout ce chapitre, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

I Définitions et premières propriétés

Dans toute cette partie, E et F sont des $\mathbb{K}$-espace vectoriels.

1. Formes multilinéaires alternées

On rappelle qu'une forme linéaire est une application linéaire de E dans $\mathbb{K}$.

Définition 1.1 *Application et forme multilinéaire*

Soit $p \in \mathbb{N}^*$ et soit $f : E^p \to F$. On dit que f est une *application multilinéaire* (ou *p-linéaire*) sur E si, pour tout $i \in [\![1, p]\!]$ et pour tous $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_p \in E$, l'application

$$\begin{array}{ccc} E & \to & F \\ x & \mapsto & f(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_p) \end{array}$$

est linéaire. On note $\mathcal{L}_p(E, F)$ l'ensemble des applications p-linéaires de E dans F.

On dit que f est une *forme multilinéaire* si $F = \mathbb{K}$.

Une application multilinéaire est une application de E^p dans F qui est linéaire par rapport à chacune de ses variables $x_1, \ldots, x_p$.

- si $p = 1$, cela correspond à la définition d'application linéaire.
- si $p = 2$, on parle d'application bilinéaire.
- si $p = 3$, on parle d'application trilinéaire.

⚠ Il faut bien sûr vérifier que E et F sont des espaces vectoriels avant de parler d'application (multi)linéaire.

Exemple 1.2 :

1. L'application $\Phi : \begin{array}{ccc} \mathcal{C}^0_m([0,1],\mathbb{R})^2 & \to & \mathbb{R} \\ (f,g) & \mapsto & \displaystyle\int_0^1 f(t)\,g(t)\,dt \end{array}$ est une forme bilinéaire sur $\mathcal{C}^0_m([0,1],\mathbb{R})$.
2. Le produit scalaire $f : \begin{array}{ccc} (\mathbb{C}^n)^2 & \to & \mathbb{C} \\ (x,y) & \mapsto & \displaystyle\sum_{i=1}^n x_i y_i \end{array}$ est une forme bilinéaire sur $\mathbb{C}^n$.
3. Le produit matriciel $f : \begin{array}{ccc} (\mathcal{M}_n(\mathbb{K}))^2 & \to & \mathcal{M}_n(\mathbb{K}) \\ (A,B) & \mapsto & AB \end{array}$ est une application bilinéaire sur $\mathcal{M}_n(\mathbb{K})$.
4. Le produit vectoriel $f : \begin{array}{ccc} (\mathbb{R}^3)^2 & \to & \mathbb{R}^3 \\ (\vec{u},\vec{v}) & \mapsto & \vec{u}\wedge\vec{v} \end{array}$ est une application bilinéaire sur $\mathbb{R}^3$.
5. L'application $f : \begin{array}{ccc} \mathbb{K}^n & \to & \mathbb{K} \\ (x_1,\ldots,x_n) & \mapsto & \displaystyle\prod_{i=1}^n x_i \end{array}$ est une forme n-linéaire sur $\mathbb{K}$. Attention, ce n'est pas une forme linéaire sur $\mathbb{K}^n$.

♢

Remarque 1.3 : Attention, une application p-linéaire sur E n'est pas une application linéaire sur E^p :

- si $f \in \mathcal{L}(E^p, F)$, si $\lambda \in \mathbb{K}$ et $(x_1, \ldots, x_p) \in E^p$ alors
$$f(\lambda x_1, \ldots, \lambda x_p) = \lambda(x_1, \ldots, x_p).$$
- si $f \in \mathcal{L}_p(E, F)$, si $\lambda \in \mathbb{K}$ et $(x_1, \ldots, x_p) \in E^p$ alors
$$f(\lambda x_1, \ldots, \lambda x_p) = \lambda^p(x_1, \ldots, x_p).$$

Pour les applications multilinéaires, l'espace d'intérêt est E, dont on prend p vecteurs (et pas E^p).

- Le produit $\begin{array}{ccc} \mathbb{K}^2 & \to & \mathbb{K} \\ (x_1,x_2) & \mapsto & x_1x_2 \end{array}$ est bilinéaire sur $\mathbb{K}$ mais pas linéaire sur $\mathbb{K}^2$.
- La projection $\begin{array}{ccc} \mathbb{K}^2 & \to & \mathbb{K} \\ (x_1,x_2) & \mapsto & x_1 \end{array}$ est linéaire mais pas bilinéaire.

♢

Théorème 1.4 *Structure de l'ensemble des formes p-linéaires*

Soit $p \in \mathbb{N}^*$. L'ensemble $\mathcal{L}_p(E,F)$ est un espace vectoriel. De plus, si E et F sont de dimension finie non-nulles, alors $\mathcal{L}_p(E,F)$ est de dimension finie et
$$\dim(\mathcal{L}_p(E,F)) = (\dim(E))^p \times \dim(F).$$

Démonstration : On montre sans problème que $\mathcal{L}_p(E,F)$ est un sous-espace de $\mathscr{F}(E^p,F)$. Supposons que E et F soient de dimensions finies non-nulles et notons $n = \dim E$ et $m = \dim F$. [1] On va faire le cas particulier dans le cas $F = \mathbb{K}$ et $p = 2$. Soit $B = (e_1, \dots, e_n)$ une base de E et soient $x, y \in E$ de coordonnées respectives (dans la base B) $(x_1, \dots, x_n)$ et $(y_1, \dots, y_n)$. Soient $\varphi_{i,j}(x,y) = x_i y_j$ et $f \in \mathcal{L}_2(E,F)$. On a

$$f(x,y) = \sum_{i,j=1}^{n} x_i y_j f(e_i, e_j) = \sum_{i,j=1}^{n} f(e_i, e_j)\, \varphi_{i,j}(x,y).$$

Les $\varphi_{i,j}$ sont des applications de $\mathcal{L}_2(E,\mathbb{K})$ et d'après le calcul précédent, $(\varphi_{i,j})_{1\le i,j\le n}$ est une famille génératrice de $\mathcal{L}_2(E,\mathbb{K})$. Soient $(\lambda_{i,j})_{1\le i,j\le n}$ tels que $\displaystyle\sum_{i,j=1}^{n} \lambda_{i,j}\varphi_{i,j} = 0$. Alors, pour tout $(k,l) \in [\![1,n]\!]^2$, on a

$$\sum_{i,j=1}^{n} \lambda_{i,j}\varphi_{i,j}(e_k, e_l) = 0 + \lambda_{k,l}\varphi_{k,l}(e_k,e_l) = \lambda_{k,l} = 0.$$

Donc les $\lambda_{i,j}$ sont tous nuls et $(\varphi_{i,j})_{1\le i,j\le n}$ est libre, c'est donc une base de $\mathcal{L}_2(E,\mathbb{K})$. De plus,

$$\dim(\mathcal{L}_2(E,\mathbb{K})) = |\,(\varphi_{i,j})_{1\le i,j\le n}\,| = n^2.$$

Pour généraliser ce résultat à $p \ge 2$ et $m \ge 1$, il faudra effectuer la même manœuvre sur chaque composante d'une base $C = (\varepsilon_1, \dots, \varepsilon_m)$ de F. On prendra la base composée des applications :

$$\forall i_1, \dots, i_p \in [\![1,n]\!], \forall k \in [\![1,m]\!], \quad \varphi_{i_1,\dots,i_p,k}(x_1, \dots, x_p) = x_{i_1} \dots x_{i_p} \varepsilon_k.$$

□

Définition 1.5

Soient $p \in \mathbb{N}^*$ et $f \in \mathcal{L}_p(E,F)$. On dit que f est *symétrique* si, pour tous $x_1, \dots, x_p \in E$ et pour tous $i, j \in [\![1,p]\!]$,

$$f(x_1, \dots, x_{i-1}, x_j, x_{i+1}, \dots, x_{j-1}, x_i, x_{j+1}, \dots, x_p) = f(x_1, \dots, x_p).$$

On dit que f est *antisymétrique* si, pour tous $x_1, \dots, x_p \in E$ et pour tous $i \ne j \in [\![1,p]\!]$,

$$f(x_1, \dots, x_{i-1}, x_j, x_{i+1}, \dots, x_{j-1}, x_i, x_{j+1}, \dots, x_p) = -f(x_1, \dots, x_p).$$

On dit que f est *alternée* si, pour tous $x_1, \dots, x_p \in E$

$$\exists i \ne j \in [\![1,p]\!], \quad x_i = x_j \Rightarrow f(x_1, \dots, x_p) = 0.$$

On retiendra que, quand on échange deux variables

- si f est symétrique, cela ne change pas la valeur ;
- si f est antisymétrique, on prend la valeur opposée.

Si f est alternée, alors elle vaut 0 dès que deux variables sont égales.

Exemple 1.6 :
Quelles sont les applications mentionnées à l'exemple précédent qui sont symétriques ? Antisymétriques ? Alternées ?

On remarque que la seule application bilinéaire antisymétrique est le produit vectoriel, et qu'elle est aussi alternée. C'est normal. ♢

1. On remarque que $\mathscr{F}(E^p,F)$ n'est pas de dimension finie, sans quoi la fin de la preuve serait évidente.

Proposition 1.7

Soient $p \in \mathbb{N}^*$ et $f \in \mathcal{L}_p(E,F)$. Alors f est alternée si, et seulement si, f est antisymétrique.

Démonstration : Supposons que f soit antisymétrique. Soient $x_1,\dots,x_p \in E$, supposons que il existe $i < j \in [\![1,n]\!]$ tels que $x_i = x_j$. Alors

$$f(x_1,\dots,x_i,\dots,x_j,\dots,x_n) = f(x_1,\dots,x_j,\dots,x_i,\dots,x_n) = -f(x_1,\dots,x_i,\dots,x_j,\dots,x_n).$$

Donc $f(x_1,\dots,x_i,\dots,x_j,\dots,x_n) = 0$ donc f est alternée.

Réciproquement, supposons que f soit alternée, et soient $x_1,\dots,x_p \in E$. Alors, pour tout $i \neq j \in [\![1,p]\!]$, par linéarité en les variables x_i et x_j,

$$\begin{aligned}0 &= f(x_1,\dots,x_i+x_j,\dots,x_i+x_j,\dots,x_n)\\ &= f(x_1,\dots,x_i,\dots,x_i+x_j,\dots,x_n) + f(x_1,\dots,x_j,\dots,x_i+x_j,\dots,x_n)\\ &= f(x_1,\dots,x_i,\dots,x_i,\dots,x_n) + f(x_1,\dots,x_i,\dots,x_j,\dots,x_n)\\ &\quad + f(x_1,\dots,x_j,\dots,x_i,\dots,x_n) + f(x_1,\dots,x_j,\dots,x_j,\dots,x_n)\\ &= f(x_1,\dots,x_i,\dots,x_j,\dots,x_n)\\ &\quad + f(x_1,\dots,x_j,\dots,x_i,\dots,x_n).\end{aligned}$$

Donc f est antisymétrique. □

Attention, cette équivalence n'est vraie que pour les applications linéaires.

Exercice 1.8 :
Soient $p \in \mathbb{N}^*$ et $f \in \mathcal{L}_p(E,F)$. Soit $A = (x_1,\dots,x_p)$ une famille de vecteurs de E. Montrer que si f est alternée et A est liée, alors $f(x_1,\dots,x_p) = 0$.

Réponse

Puisque la famille $(x_1,\dots,x_p)$ est liée, l'un de ses vecteurs est combinaison linéaire des autres. Quitte à réordonner la famille, supposons que x_p est combinaison linéaire des autres vecteurs. Alors il existe $\lambda_1,\dots,\lambda_{p-1} \in \mathbb{K}$ tels que

$$x_p = \sum_{k=1}^{p-1} \lambda_k x_k.$$

Puisque f est alternée, on a bien

$$f(x_1,\dots,x_p) = \sum_{k=1}^{p-1} \lambda_k f(x_1,\dots,x_{p-1},x_k) = 0.$$

◇

Théorème 1.9 *Structure de l'ensemble des formes n-linéaires alternées - Admis*

Supposons que E soit un espace vectoriel de dimension finie $n \in \mathbb{N}^*$ muni d'une base B. Notons

$$\mathcal{L}_n^{\mathrm{alt}}(E,\mathbb{K}) = \{f \in \mathcal{L}_n(E,\mathbb{K}) / f \text{ est alternée}\}.$$

Alors l'application $\begin{array}{ccc}\mathcal{L}_n^{\mathrm{alt}}(E,\mathbb{K}) & \to & \mathbb{K}\\ f & \mapsto & f(B)\end{array}$ est un isomorphisme d'espaces vectoriels. En particulier, $\mathcal{L}_n^{\mathrm{alt}}(E,\mathbb{K})$

est un espace vectoriel de dimension 1.

La démonstration est compliquée, et fait habituellement appel à la théorie des bases duales et des signatures de permutation.

2. Déterminant d'une famille dans une base

Dans toute cette partie, E est une espace vectoriel de dimension $n \in \mathbb{N}^*$.

Définition 1.10 *Déterminant dans la base B*

Soit B une base de E. On appelle déterminant dans la base B l'unique forme n-linéaire alternée $f \in \mathcal{L}_n^{\text{alt}}(E, \mathbb{K})$ vérifiant $f(B) = 1$. On la note $\det_B$.

A retenir pour la suite :

- $\det_B$ est défini comme étant la seule forme n-linéaire alternée vérifiant $\det_B(B) = 1$.
- Le déterminant est p-linéaire pour $p = n$. Cela signifie qu'on regardera le déterminant de n vecteurs $x_1, \ldots, x_n$ (ou, par un léger abus de notation, d'une famille de n vecteurs $(x_1, \ldots, x_n)$).

Théorème 1.11 *Changement de base pour le déterminant*

Soient B et B' deux bases de E. Alors

$$\det_{B'} = \det_{B'}(B) \det_B .$$

De plus, $\det_{B'}(B) \neq 0$, $\det_B(B') \neq 0$ et $\det_B(B') = \dfrac{1}{\det_{B'}(B)}$.

Démonstration : Les applications $\det_B$ et $\det_{B'}$ sont deux formes n-linéaires alternées non-nulles sur E. En particulier, $\det_B$ est une base de $\mathcal{L}_n^{\text{alt}}(E, \mathbb{K})$ (qui est un espace vectoriel de dimension 1). Donc il existe un unique $\lambda \in \mathbb{K}^*$ tel que $\det_{B'} = \lambda \det_B$. En évaluant cette égalité sur la famille B, on a

$$\det_{B'}(B) = \lambda \det_B(B) = \lambda, \quad \det_{B'} = \det_{B'}(B) \det_B .$$

Puisque $\lambda \in \mathbb{K}^*$, on en déduit que $\det_{B'}(B) \neq 0$. En appliquant évaluant la relation $\det_{B'} = \lambda \det_B$ en B', on obtient alors

$$\det_{B'}(B') = 1 = \det_{B'}(B) \det_B(B') , \quad \det_B(B') = \frac{1}{\det_{B'}(B)}.$$

□

Proposition 1.12 *Propriétés du déterminant dans une base*

Soit B une base de E, et soient $x_1, \ldots, x_n \in E$. Alors on a :

(i) Pour tout $i \in [\![1, n]\!]$ et $\lambda \in \mathbb{K}$,

$$\det_B(x_1, \ldots, \lambda x_i, \ldots, x_n) = \lambda (x_1, \ldots, x_n) .$$

(ii) Pour tout $\lambda \in \mathbb{K}$,

$$\det_B(\lambda x_1, \ldots, \lambda x_n) = \lambda^n \det_B(x_1, \ldots, x_n) .$$

(iii) Pour tous $i \neq j \in [\![1,n]\!]$,

$$\det_B(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_n) = -\det_B(x_1,\ldots,x_i,\ldots,x_j\ldots,x_n).$$

(iv) S'il existe $i \neq j \in [\![1,n]\!]$ tels que $x_i = x_j$, alors

$$\det_B(x_1,\ldots,x_n) = 0.$$

(v) La famille $(x_1,\ldots,x_n)$ est une base de E si, et seulement si, $\det_B(x_1,\ldots,x_n) \neq 0$.
(vi) On a $\det_B(B) = 1$.

Démonstration : A part le point (v), tout est évident (soit par définition du déterminant, soit par le fait que ce soit une forme n-linéaire alternée et antisymétrique). Notons $B' = (x_1,\ldots,x_n)$.

$\boxed{\Rightarrow}$ Supposons que B' soit une base de E. Alors $\det_B(B') \neq 0$ d'après le théorème 1.11.

$\boxed{\Leftarrow}$ Supposons que B' soit liée. Alors l'un des x_i est combinaison linéaire des autres. Quitte à réordonner la famille, supposons qu'il s'agit de x_n : il existe $\lambda_1,\ldots,\lambda_{n-1} \in \mathbb{K}$ tels que

$$x_n = \sum_{k=1}^{n-1} \lambda_k x_k.$$

Puisque $\det_B$ est alternée, on a

$$\det_B(x_1,\ldots,x_n) = \sum_{k=1}^{n-1} \lambda_k \det_B(x_1,\ldots,x_{n-1},x_k) = 0.$$

□

Notons que le dernier point de la preuve est le sujet de l'exercice 1.8.

Remarque 1.13 :

(i) Si $E = \mathbb{R}^2$ et B est la base canonique de $\mathbb{R}^2$, alors $\det_B(x,y)$ est l'aire algébrique du parallélogramme engendré par x et y. En particulier, (x,y) est libre si, et seulement si, ces deux vecteurs ne sont pas colinéaires, i.e. le parallélogramme n'est pas dégénéré.
(ii) Si $E = \mathbb{R}^3$ et B est la base canonique de $\mathbb{R}^3$, alors $\det_B(x,y,z)$ est l'aire algébrique du parallélépipède engendré par x,y et z. En particulier, (x,y,z) est libre si, et seulement si, ces trois vecteurs ne sont pas coplanaires, i.e. le parallélépipède n'est pas plat.

♢

Exemple 1.14 :
Soit $E = \mathbb{R}^3$ et posons $x_1 = (2,0,2), x_2 = (2,1,0), x_3 = (-1,0,0)$. On va montrer que la famille $A = (x_1,x_2,x_3)$ est une base de E en calculant son déterminant dans la base canonique $B = (e_1,e_2,e_3)$. On a alors

$$\begin{aligned}
\det_B(A) &= 2\det_B(e_1+e_3, 2e_1+e_2, -e_1) \\
&= 2\det_B(e_1, 2e_1+e_2, -e_1) + 2\det_B(e_3, 2e_1+e_2, -e_1) \\
&= -2\det_B(e_1, 2e_1+e_2, e_1) - 2\det_B(e_3, 2e_1+e_2, e_1) \\
&= 0 - 2\det_B(e_3, 2e_1, e_1) - 2\det_B(e_3, e_2, e_1) = 0 + 2\det_B(e_1,e_2,e_3) \\
&= 2.
\end{aligned}$$

♢

Ces calculs ne sont pas forcément très pratiques en l'état, mais on verra que le calcul du déterminant est un excellent outil pour étudier si une famille est une base ou pas (dès qu'on fera ces calculs sous formes de matrices).

3. Déterminant d'un endomorphisme

Dans toute cette partie, E est une espace vectoriel de dimension $n \in \mathbb{N}^*$.

Définition/Proposition 1.15 *Déterminant d'un endomorphisme*

Soit $f \in \mathcal{L}(E)$. Il existe un unique scalaire $\lambda \in \mathbb{K}$ tel que, pour toute base B de E,

$$\forall x_1, \ldots, x_n \in E, \quad \det_B (f(x_1), \ldots, f(x_n)) = \lambda \det_B (x_1, \ldots, x_n).$$

Ce scalaire est appelé déterminant de f et on note $\lambda = \det(f)$. Pour toute base B de E, on a alors

$$\det(f) = \det_B(f(B)).$$

Le déterminant d'un endomorphisme ne dépend pas de la base choisie.

Démonstration : Soit B une base de E. Posons $\varphi : \begin{array}{ccc} E^n & \to & \mathbb{K} \\ (x_1, \ldots, x_n) & \mapsto & \det_B(f(x_1), \ldots, f(x_n)) \end{array}$. Puisque f est linéaire et que $\det_B$ est n-linéaire alternée, l'application φ est une forme n-linéaire alternée. Puisque $\det_B$ est non-nulle, $\det_B$ forme une base de $\mathcal{L}_n^{\text{alt}}(E, \mathbb{K})$, et donc il existe $\lambda \in \mathbb{K}$ tel que $\varphi = \lambda \det_B$. On a donc montré que

$$\forall x_1, \ldots, x_n \in E, \quad \det_B (f(x_1), \ldots, f(x_n)) = \lambda \det_B (x_1, \ldots, x_n).$$

Il reste à montrer que λ ne dépend pas de B. Soient $x_1, \ldots, x_n \in E$. Alors

$$\begin{aligned} \det_{B'}(f(x_1), \ldots, f(x_n)) &= \det_{B'}(B) \times \det_B(f(x_1), \ldots, f(x_n)) \\ &= \lambda \det_{B'}(B) \times \det_B(x_1, \ldots, x_n) \\ &= \lambda \det_{B'}(B) \times \det_B(B') \times \det_{B'}(x_1, \ldots, x_n) \\ &= \lambda \det_{B'}(x_1, \ldots, x_n). \end{aligned}$$

Donc λ ne dépend pas de B. En prenant $(x_1, \ldots, x_n) = B$, on a $\lambda = \det_B(f(B))$. $\square$

Proposition 1.16

Pour tout $f \in \mathcal{L}(E)$ et pour tout $\lambda \in \mathbb{K}$, on a

$$\det(\lambda f) = \lambda^n \det(f).$$

De plus, $\det(\mathrm{Id}_E) = 1$ et $\det\left(0_{\mathcal{L}(E)}\right) = 0$.

⚠ Le déterminant n'est pas linéaire. Dès que $n \geq 2$, on a

$$\det(2\,\mathrm{Id}_E) = \det(\mathrm{Id}_E + \mathrm{Id}_E) \neq \det(\mathrm{Id}_E) + \det(\mathrm{Id}_E) = 2\det(\mathrm{Id}_E).$$

Théorème 1.17

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

$$\det(f \circ g) = \det(f)\det(g).$$

Démonstration : Soit $B = (e_1, \dots, e_n)$ une base de E. On a alors

$$\begin{aligned}\det(f \circ g) &= \det_B(f(g(e_1)), \dots, f(g(e_n))) = \det(f)\det_B(g(e_1), \dots, g(e_n)) \\ &= \det(f)\det(g)\det_B(e_1, \dots, e_n) = \det(f)\det(g).\end{aligned}$$

□

Théorème 1.18

Soit $f \in \mathcal{L}(E)$ Alors on a équivalence entre :

(i) f est bijective.
(ii) $\det(f) \neq 0$.

De plus dans ce cas, on a

$$\det\left(f^{-1}\right) = \frac{1}{\det(f)}.$$

Démonstration : Soit B une base de E. Alors

$$f \text{ est bijective} \iff f(B) \text{ est une base de } E \iff \det_B(f(B)) \neq 0 \iff \det(f) \neq 0.$$

De plus, si f est bijective, alors

$$\det(f)\det\left(f^{-1}\right) = \det\left(f \circ f^{-1}\right) = \det(\mathrm{Id}_E) = 1, \quad \det\left(f^{-1}\right) = \frac{1}{\det(f)}.$$

□

Exercice 1.19 :

Montrer que l'application $f : \begin{array}{ccc} \mathbb{C}^3 & \to & \mathbb{C}^3 \\ (x, y, z) & \mapsto & (2x + 2y - z, y, 2x, 0, 0) \end{array}$ est un automorphisme de $\mathbb{C}^3$.

Réponse

En l'absence de bonne idée, on calcule bêtement le déterminant de f en s'aidant de la base canonique $B = (e_1, e_2, e_3)$ de $\mathbb{C}^3$:

$$\det f = \det_B(f(e_1), f(e_2), f(e_3)) = \det_B((2, 0, 2), (2, 1, 0), (-1, 0, 0)) = 2.$$

En effet, on a déjà fait ce calcul auparavant. Donc $\det f \neq 0$ donc f est bijective.

◊

Exercice 1.20 :

Dans cet exercice, on considère $\mathbb{C}$ en tant que $\mathbb{R}$-espace vectoriel. Soit $f \in \mathcal{L}_{\mathbb{R}}(\mathbb{C})$.

1. Montrer qu'il existe un unique couple $(a, b) \in \mathbb{C}$ tel que

$$\forall z \in \mathbb{C}, \quad f(z) = az + b\overline{z}.$$

2. Déterminer le déterminant de f en fonction de a et b.

Réponse

1. $\boxed{\text{Analyse}}$ Supposons qu'il existe un couple $(a,b) \in \mathbb{C}^2$ tel que, pour tout $z \in \mathbb{C}$, $f(z) = az + b\overline{z}$. On a alors

$$f(1) = a + b, \quad f(i) = ia - ib, \quad a = \frac{f(1) - if(i)}{2}, \quad b = \frac{f(1) + if(i)}{2}.$$

$\boxed{\text{Synthèse}}$ Posons $a = \dfrac{f(1) - if(i)}{2}$ et $b = \dfrac{f(1) + if(i)}{2}$. Soit $z \in \mathbb{C}$. En notant $\Re(z) = z_1$ et $\mathrm{Im}(z) = z_2$, on a

$$\begin{aligned} az + b\overline{z} = \frac{f(1) - if(i)}{2}(z_1 + iz_2) + \frac{f(1) + if(i)}{2}(z_1 - iz_2) = f(1) z_1 - i^2 f(i) z_2 \\ f(z_1 + iz_2) = f(z). \end{aligned}$$

On a donc prouvé l'existence, et l'unicité découle de l'analyse.

2. Notons $B = (1, i)$ la base canonique de $\mathbb{C}$, et

$$\Re(a) = a_1, \quad \mathrm{Im}(a) = a_2, \quad \Re(b) = b_1, \quad \mathrm{Im}(b) = b_2.$$

On a alors

$$\begin{aligned} \det(f) &= \det_B(f(1), f(i)) = \det_B(a + b, ia - ib) \\ &= (a_1 + b_1)\det_B(1, ia - ib) + (a_2 + b_2)\det_B(i, ia - ib) \\ &= (a_1 + b_1)(a_1 - b_1)\det_B(1, i) - (a_2 + b_2)(a_2 - b_2)\det_B(i, 1) \\ &= a_1^2 + a_2^2 - b_1^2 - b_2^2 = |a|^2 - |b|^2. \end{aligned}$$

♢

II Déterminant matriciel

Dans toute cette section, on considère un entier naturel non-nul $n \in \mathbb{N}^*$.

1. Définition et lien avec les autres déterminants

On va voir que les déterminants précédemment définis (d'une famille ou d'un endomorphisme) peuvent s'interpréter en termes de calcul matriciel. Surtout, c'est de cette manière qu'on fera les calculs en général, car ils seront plus rapides.

Définition 2.1 *Déterminant matriciel*

Soit $A = [a_{i,j}]_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{K})$. Notons $C_1, \ldots, C_n \in \mathcal{M}_{n,1}(\mathbb{K})$ les colonnes de A et B la base canonique de $\mathcal{M}_{n,1}(\mathbb{K})$. On définit

$$\det(A) = \det_B(C_1, \ldots, C_n).$$

On note :

$$\det(A) = \begin{vmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & & a_{2,n} \\ \vdots & & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{vmatrix}$$

Calculer le déterminant d'une matrice non-carrée n'a aucun sens ![2]

Proposition 2.2 *Règle de Sarrus*[3]

(i) Soit $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathcal{M}_2(\mathbb{K})$. Alors

$$\det(A) = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

(ii) Soit $A = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix} \in \mathcal{M}_3(\mathbb{K})$. Alors

$$\begin{aligned} \det(A) = \begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix} &= a_{1,1}a_{2,2}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} \\ &\quad - a_{3,1}a_{2,2}a_{1,3} - a_{2,1}a_{1,2}a_{3,3} - a_{1,1}a_{3,2}a_{2,3}. \end{aligned}$$

Autrement dit : on fait la somme des diagonales descendantes ($\searrow$) avec la différence des diagonales montantes ($\nearrow$).

La règle de Sarrus ne fonctionne pas en dimension $n \geq 4$.

Démonstration : (i) Ce premier point est facile, on a déjà fait ce calcul plusieurs fois sans le dire. Posons $B = (E_{1,1}, E_{2,1})$ la base canonique de $\mathcal{M}_{2,1}(\mathbb{R})$. On a

$$\begin{aligned} \det A &= \det_B(aE_{1,1} + cE_{1,2}, bE_{1,1} + dE_{1,2}) \\ &= a\det_B(E_{1,1}, bE_{1,1} + dE_{1,2}) + c\det_B(E_{1,2}, bE_{1,1} + dE_{1,2}) \\ &= ad\det_B(E_{1,1}, E_{1,2}) + bc\det_B(E_{1,2}, E_{1,1}) = ad - bc \end{aligned}$$

(ii) Comme pour le point (i), mais en plus long : il suffit de développer brutalement.

$\square$

Tout problème de calcul de déterminant d'une famille ou d'un endomorphisme peut se ramener à un calcul de déterminant matriciel.

2. C'est lié au fait que le déterminant est une forme n-linéaire sur un espace de dimension n.
3. Pierre Frédéric Sarrus (1798-1861) : Mathématicien français.

Proposition 2.3

Soit E un $\mathbb{K}$-espace vectoriel de dimension n muni d'une base B.

(i) Soient $x_1, \dots, x_n \in E$ et $A \in \mathcal{M}_n(\mathbb{K})$ tels que $A = \mathrm{mat}_B(x_1, \dots, x_n)$. Alors

$$\det_B(x_1, \dots, x_n) = \det A.$$

(ii) Soit $f \in \mathcal{L}(E)$ et $A \in \mathcal{M}_n(\mathbb{K})$ tels que $\mathrm{mat}_B(f) = A$. Alors

$$\det f = \det A.$$

Démonstration : (i) Par définition, en notant $B = (e_1, \dots, e_n)$ et $B_M = (E_{1,1}, \dots, E_{n,1})$ la base canonique de $\mathcal{M}_n(\mathbb{K})$,

$$\det_B(x_1, \dots, x_n) = \det_{B_M}\left(\sum_{i=1}^{n} A_{i,1}E_{i,1}, \dots, \sum_{i=1}^{n} A_{i,n}E_{i,1}\right) = \det A.$$

(ii) Par définition, $A = \mathrm{mat}_B(f(B))$ donc d'après (i),

$$\det f = \det_B(f(B)) = \det A.$$

□

A noter : le déterminant d'un endomorphisme est égal à celui de sa matrice dans une base donnée. En particulier, il ne dépend pas de la base. Lorsque l'on souhaitera déterminer le déterminant d'une matrice (ou d'un endomorphisme), on fera les calculs dans une base bien choisie. D'un point de vue matriciel, cela revient à calculer le déterminant d'une matrice équivalente à A.

Exemple 2.4 :
Montrons que la famille $B' = \left(1 + 2X + 3X^2, -1 + 4X + 6X^2, 5X + 7X^2\right)$ est une base de $\mathbb{R}_2[X]$. En notant $B = \left(1, X, X^2\right)$ la base canonique de $\mathbb{R}_2[X]$, on définit

$$A = \mathrm{mat}_B(B') = \begin{bmatrix} 1 & -1 & 0 \\ 2 & 4 & 5 \\ 3 & 6 & 7 \end{bmatrix}.$$

D'après la règle de Sarrus,

$$\begin{vmatrix} 1 & 0 & 0 \\ 2 & 4 & 5 \\ 3 & 6 & 7 \end{vmatrix} = 4 \times 7 - 5 \times 6 = -3 \neq 0.$$

Donc B' est une base de $\mathbb{R}_2[X]$. ♢

Proposition 2.5 *Propriétés du déterminant matriciel*

Soient $A \in \mathcal{M}_n(\mathbb{K})$. Notons $C_1, \dots, C_n$ les colonnes de A. Alors :

(i) Pour tout $i \in [\![1, n]\!]$ et $\lambda \in \mathbb{K}$,

$$\det[C_1, \dots, \lambda C_i, \dots, C_n] = \lambda \det A.$$

(ii) $\det(\lambda A) = \lambda^n \det(A)$.

(iii) Pour tous $i \neq j \in [\![1, n]\!]$,

$$\det[C_1, \dots, C_j, \dots, C_i, \dots, C_n] = -\det(A).$$

(iv) S'il existe $i \neq j \in [\![1, n]\!]$ tels que $C_i = C_j$, alors $\det(A) = 0$.

(v) Pour tout $B \in \mathcal{M}_n(\mathbb{K})$ on a

$$\det(AB) = \det(A)\det(B).$$

(vi) Pour tout $p \in \mathbb{N}$, on a

$$\det(A^p) = \det(A)^p.$$

(vii) La matrice A est inversible si, et seulement si, $\det A \neq 0$. Dans ce cas on a

$$\det\left(A^{-1}\right) = \frac{1}{\det(A)}.$$

Démonstration : On a déjà tout montré, soit par définition du déterminant comme forme n-linéaire alternée, soit pour les endomorphismes. Auquel cas, on posera f et g les endomorphismes de $\mathbb{K}^n$ canoniquement associés à A et B. □

En particulier, si A et A' sont équivalentes, alors elles représentent la matrice d'un endomorphisme $f \in \mathcal{L}(E)$ dans deux bases B et B'. Alors, en notant $P = \mathrm{Pass}(B, B')$,

$$\det A' = \det\left(P^{-1}AP\right) = \frac{1}{\det P}\det A \det P = \det A.$$

C'est cohérent : le déterminant d'un endomorphisme ne dépend pas de la base considérée, et donc deux matrices équivalentes ont même déterminant.

Définition/Proposition 2.6 *Groupe spécial linéaire*

L'application det : $\begin{array}{ccc} (\mathrm{GL}_n(\mathbb{K}), \times) & \to & (\mathbb{K}^*, \times) \\ A & \mapsto & \det(A) \end{array}$ est un morphisme de groupes.

On appelle *groupe spécial linéaire* l'ensemble

$$\mathrm{SL}_n(\mathbb{K}) = \{A \in \mathcal{M}_n(\mathbb{K}) \,/\, \det(A) = 1\}.$$

Comme son nom l'indique, $(\mathrm{SL}_n(\mathbb{K}), \times)$ est un sous-groupe de $(\mathrm{GL}_n(\mathbb{K}), \times)$.

Démonstration : On a déjà tout montré. En effet, les ensembles $(\mathrm{GL}_n(\mathbb{K}), \times)$ et $(\mathbb{K}^*, \times)$ sont bien des groupes, et

$$\forall A, B \in \mathrm{GL}_n(\mathbb{K}), \quad \det(AB) = \det(A)\det(B), \quad \det\left(A^{-1}\right) = \det(A)^{-1}.$$

Par définition, $\mathrm{SL}_n(\mathbb{K}) = \{A \in \mathrm{GL}_n(\mathbb{K}) \,/\, \det(A) = 1\} = \ker(\det)$, c'est donc un sous-groupe de $\mathrm{GL}_n(\mathbb{K})$. □

2. Déterminant et opérations matricielles

Dans cette partie, on s'intéresse au comportement du déterminant lorsqu'on effectue des opérations élémentaires sur une matrice. Cela permet parfois de simplifier le calcul d'un déterminant. Commençons par un lemme sur le déterminant des matrices élémentaires.

Soient $\lambda \in \mathbb{K}$, et $i \neq j \in [\![1, n]\!]$. On rappelle que les matrices d'opérations élémentaires sur les colonnes sont :

$$\begin{aligned} E'_{C_i \leftarrow \lambda C_i} &= I_n + (\lambda - 1) E_{i,i}, \\ E'_{C_i \leftarrow C_i + \lambda C_j} &= I_n + \lambda E_{j,i}, \\ E'_{C_i \leftrightarrow C_j} &= I_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}. \end{aligned}$$

De plus, les matrices d'opérations élémentaires sur les lignes sont :

$$\begin{aligned} E'_{L_i \leftarrow \lambda L_i} &= \left(E'_{C_i \leftarrow \lambda C_i}\right)^\intercal, \\ E'_{L_i \leftarrow L_i + \lambda L_j} &= \left(E'_{C_i \leftarrow C_i + \lambda C_j}\right)^\intercal, \\ E'_{L_i \leftrightarrow L_j} &= \left(E'_{C_i \leftrightarrow C_j}\right)^\intercal. \end{aligned}$$

Lemme 2.7

Pour tous $\lambda \in \mathbb{K}$, et $i \neq j \in [\![1, n]\!]$, on a

(i) $\det\left(E'_{C_i \leftarrow \lambda C_i}\right) = \det\left(E'_{L_i \leftarrow \lambda L_i}\right) = \lambda$.
(ii) $\det\left(E'_{C_i \leftarrow C_i + \lambda C_j}\right) = \det\left(E'_{L_i \leftarrow L_i + \lambda L_j}\right) = 1$.
(iii) $\det\left(E'_{C_i \leftrightarrow C_j}\right) = \det\left(E'_{L_i \leftrightarrow L_j}\right) = -1$.

On remarque au passage que le déterminant des matrices d'opérations élémentaires est égal à celui de leur transposée.

Démonstration : Les points (i) et (iii) sont des conséquences immédiates de la linéarité (en les colonnes) et du caractère antisymétrique du déterminant, il reste donc à montrer le point (ii). Alors, puisque le déterminant est linéaire (sur la i-ème colonne) et alterné,

$$\det\left(E'_{C_i \leftarrow C_i + \lambda C_j}\right) = \det\left(E_1, \ldots, E_i + \lambda E_j, \ldots, E_n\right) = \det I_n + \lambda \det\left(E_1, \ldots, \lambda E_j, \ldots, E_n\right) = 1.$$

On fait la même chose sur la j-ème colonne pour montrer que $\det\left(E'_{L_i \leftarrow L_i + \lambda L_j}\right) = 1$. $\square$

Proposition 2.8 *Déterminant et opérations élémentaires*

Soit $A \in \mathcal{M}_n(\mathbb{K})$. Soient $\lambda \in \mathbb{K}$, et $i \neq j \in [\![1, n]\!]$. On note A' la matrice obtenue par l'une opération élémentaire (sur les colonnes ou sur les lignes) suivantes :

(i) $A \overset{C_i \leftarrow \lambda C_i}{\longrightarrow} A'$ ou $A \overset{L_i \leftarrow \lambda L_i}{\longrightarrow} A'$. Alors $\det A' = \lambda \det A$.
(ii) $A \overset{C_i \leftarrow C_i + \lambda C_j}{\longrightarrow} A'$ ou $A \overset{L_i \leftarrow L_i + \lambda L_j}{\longrightarrow} A'$. Alors $\det A' = \det A$.
(iii) $A \overset{C_i \leftrightarrow C_j}{\longrightarrow} A'$ ou $A \overset{L_i \leftrightarrow L_j}{\longrightarrow} A'$. Alors $\det A' = -\det A$.

C'est une conséquence directe du lemme 2.7. On retiendra qu'ajouter à une colonne (ou à une ligne) une combinaison linéaire des autres ne change pas le déterminant de la matrice.

Théorème 2.9 *Déterminant et transposée*

Soit $A \in \mathcal{M}_n(\mathbb{K})$. Alors $\det\left(A^\intercal\right) = \det A$.

Démonstration : $\boxed{\text{Cas 1 : } A \text{ n'est pas inversible}}$ Alors $A^\intercal$ n'est pas inversible non plus, donc

$$\det\left(A^\intercal\right) = 0 = \det A.$$

$\boxed{\text{Cas 2 : } A \text{ est inversible}}$ Alors d'après le pivot de Gauss, il existe $p \in \mathbb{N}$ et des matrices d'opérations élémentaires sur les lignes $M_1, \ldots, M_p \in \mathrm{GL}_n(\mathbb{K})$ tels que

$$M_p \times \cdots \times M_1 \times A = I_n, \quad A^\intercal \times M_1^\intercal \times \cdots \times M_p^\intercal = I_n.$$

Puisque, pour tout $i \in [\![1, p]\!]$, $\det(M_i) = \det(M_i^\intercal)$, on en déduit que

$$\det(A^\intercal) = \frac{1}{\prod_{i=1}^{p} \det(M_i^\intercal)} = \frac{1}{\prod_{i=1}^{p} \det(M_i)} = \det A.$$

$\square$

Remarque 2.10 : D'après ce dernier théorème, tout ce que l'on a dit pour le déterminant matriciel concernant les colonnes reste vrai pour les lignes. Par exemple, le déterminant est multilinéaire, alterné et antisymétrique pour les lignes de la matrice, etc. $\diamondsuit$

3. Développement par rapport à une ligne ou à une colonne

On arrive à la partie la plus importante concernant le déterminant matriciel. On va voir que pour calculer un déterminant de taille $n+1$, on peut se ramener à calculer des déterminants de taille n. En pratique, c'est très utile si la matrice de départ a beaucoup de zéros.

Définition 2.11 *Mineur et comatrice*
Supposons que $n \geq 2$. Soit $A \in \mathcal{M}_n(\mathbb{K})$ et soient $i, j \in [\![1, n]\!]$. On appelle *mineur d'ordre (i,j) de la matrice* A le nombre

$$\Delta_{i,j}(A) = \det\left(\widetilde{A}_{i,j}\right), \quad \text{avec } \widetilde{A}_{i,j} = \begin{bmatrix} A_{1,1} & \cdots & A_{1,j-1} & A_{1,j+1} & \cdots & A_{1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ A_{i-1,1} & \cdots & A_{i-1,j-1} & A_{i-1,j+1} & \cdots & A_{i-1,n} \\ A_{i+1,1} & \cdots & A_{i+1,j-1} & A_{i+1,j+1} & \cdots & A_{i+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ A_{n,1} & \cdots & A_{n,j-1} & A_{n,j+1} & \cdots & A_{n,n} \end{bmatrix}.$$

On appelle *cofacteur d'ordre (i,j)* A le nombre $(-1)^{i+j}\Delta_{i,j}(A)$. On appelle *comatrice de A* la matrice des cofacteurs de A, définie par

$$\mathrm{Com}(A) = \left[(-1)^{i+j}\Delta_{i,j}(A)\right]_{i,j\in[\![1,n]\!]} \in \mathcal{M}_n(\mathbb{K}).$$

$\widetilde{A}_{i,j}$ est ici la matrice carrée de taille $n-1$ à laquelle on a retiré la ligne i et la colonne j. Pour retenir le signe devant le cofacteur, il suffit de retenir le schéma suivant :

$$\begin{bmatrix} + & - & + & - & \cdots \\ - & + & - & + & \cdots \\ + & - & + & - & \cdots \\ - & + & - & + & \cdots \\ \vdots & \vdots & \vdots & \vdots & \end{bmatrix}$$

Théorème 2.12 *Développement du déterminant par rapport à une ligne ou une colonne - Admis*
Soit $A \in \mathcal{M}_n(\mathbb{K})$. Notons $C_1, \ldots, C_n$ et $L_1, \ldots, L_n$ les colonnes et lignes respectives de A.

(i) Soit $j \in [\![1, n]\!]$. On peut développer par rapport à la j-ème colonne :

$$\det A = \sum_{i=1}^{n} (-1)^{i+j} A_{i,j}\Delta_{i,j}(A).$$

(ii) Soit $i \in [\![1, n]\!]$. On peut développer par rapport à la i-ème ligne :

$$\det A = \sum_{j=1}^{n} (-1)^{i+j} A_{i,j} \Delta_{i,j}(A).$$

Idée de démonstration : (i) Soit $j \in [\![1, n]\!]$. Posons

$$\Phi_j : A \mapsto \sum_{i=1}^{n} (-1)^{i+j} A_{i,j} \Delta_{i,j}(A).$$

Il suffit de montrer que Φ_j, en tant qu'application de $(\mathcal{M}_{n,1}(\mathbb{K}))^n$ dans $\mathbb{K}$, est n-linéaire (par rapport aux colonnes) et alternée. Φ_j est donc une forme n-linéaire alternée sur $\mathcal{M}_{n,1}(\mathbb{K})$, et donc il existe $\lambda \in \mathbb{K}$ tel que $\Phi_j = \lambda \det$. Ensuite, on a

$$\Phi_j(I_n) = \sum_{i=1}^{n} (-1)^{i+j} \delta_{i,j} \Delta_{i,j}(I_n) = (-1)^{2j} \Delta_{j,j}(I_n) = 1 = \det(I_n).$$

Donc $\lambda = 1$ donc $\Phi_j = \det$.

(ii) Par définition, il est clair que $\Delta_{i,j}(A) = \Delta_{j,i}(A^\intercal)$. On a alors, pour tout $i \in [\![1, n]\!]$

$$\det A = \det A^\intercal = \varphi_i(A^\intercal) = \sum_{j=1}^{n} (-1)^{j+i} A^\intercal_{j,i} \Delta_{j,i}(A^\intercal) = \sum_{j=1}^{n} (-1)^{i+j} A_{i,j} \Delta_{i,j}(A).$$

□

Corollaire 2.13

Soit $A \in \mathcal{M}_n(\mathbb{K})$. Si A est triangulaire, alors

$$\det A = \prod_{i=1}^{n} A_{i,i}.$$

Ce résultat est vrai en particulier pour les matrices diagonales.

On en déduit qu'une méthode pour calculer un déterminant consiste à transformer la matrice associée en matrice triangulaire supérieure par opérations élémentaires (méthode du pivot de Gauss) puis de faire le produit des termes diagonaux.

Exemple 2.14 :
En développant par rapport à la seconde colonne puis en utilisant les formules de Sarrus, on a

$$\begin{vmatrix} 2 & 2 & 3 & 1 \\ 1 & 0 & 1 & 0 \\ 3 & 1 & 2 & -1 \\ 0 & 0 & 4 & 1 \end{vmatrix} = -2 \begin{vmatrix} 1 & 1 & 0 \\ 3 & 2 & -2 \\ 0 & 4 & 1 \end{vmatrix} - \begin{vmatrix} 2 & 3 & 1 \\ 1 & 1 & 0 \\ 0 & 4 & 1 \end{vmatrix} = -2(2+8-3) - (2+4-3) = -17$$

♢

Exemple 2.15 :
En effectuant les opérations élémentaires successives $L_i \leftarrow L_i - L_1$ pour $i \in [\![2, 4]\!]$,

$$\begin{vmatrix} 2 & 1 & -1 & 2 \\ 2 & 1 & 2 & 1 \\ 2 & -1 & 3 & 4 \\ 2 & 4 & -2 & 1 \end{vmatrix} = \begin{vmatrix} 2 & 1 & -1 & 2 \\ 0 & 0 & 3 & -1 \\ 0 & -2 & 5 & 2 \\ 0 & 3 & -1 & -1 \end{vmatrix} = 2 \begin{vmatrix} 0 & 3 & -1 \\ -2 & 4 & 2 \\ 3 & -1 & -1 \end{vmatrix} = 2 \times (18 - 2 - 6 + 12) = 44.$$

◇

Le déterminant fournit une formule explicite pour trouver l'inverse d'une matrice inversible.

Théorème 2.16

Si A est inversible, alors

$$A^{-1} = \frac{1}{\det A} \operatorname{Com}(A)^{\intercal}.$$

Le théorème 2.16 est une conséquence directe du lemme suivant.

Lemme 2.17

Soit $A \in \mathcal{M}_n(\mathbb{K})$. Alors

$$A \operatorname{Com}(A)^{\intercal} = \det(A)\, I_n.$$

Démonstration : Notons $M = A \operatorname{Com}(A)^{\intercal}$. Alors, pour tous $i, j \in [\![1, n]\!]$,

$$M_{i,j} = \sum_{k=1}^{n} A_{i,k} \operatorname{Com}(A)^{\intercal}_{k,j} = \sum_{k=1}^{n} A_{i,k} \operatorname{Com}(A)_{j,k} = \sum_{k=1}^{n} (-1)^{j+k} A_{i,k} \Delta_{j,k}(A).$$

- Cas 1 : si $i = j$. Alors

$$M_{i,i} = \sum_{k=1}^{n} (-1)^{i+k} A_{i,k} \Delta_{i,k}(A) = \det A,$$

où l'on a reconnu le développement du déterminant par rapport à la i-ème ligne.

- Cas 2 : si $i \neq j$. Soit A' la matrice obtenue à partir de A en remplaçant sa j-ème ligne par sa i-ème ligne. Puisque A' a deux lignes égales, elle n'est pas inversible. En développant par rapport à la j-ème ligne, on obtient

$$\det A' = \sum_{k=1}^{n} (-1)^{j+k} A'_{j,k} \Delta_{j,k}(A') = \sum_{k=1}^{n} (-1)^{j+k} A_{i,k} \Delta_{j,k}(A') = 0$$

Enfin, on remarque que

$$\Delta_{j,k}(A') = \begin{vmatrix} A_{1,1} & \cdots & A_{1,k-1} & A_{1,k+1} & \cdots & A_{1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ A_{j-1,1} & \cdots & A_{j-1,k-1} & A_{j-1,k+1} & \cdots & A_{j-1,n} \\ A_{j+1,1} & \cdots & A_{j+1,k-1} & A_{j+1,k+1} & \cdots & A_{j+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ A_{n,1} & \cdots & A_{n,k-1} & A_{n,k+1} & \cdots & A_{n,n} \end{vmatrix} = \Delta_{j,k}(A).$$

On en déduit que $\displaystyle\sum_{k=1}^{n} (-1)^{j+k} A_{i,k} \Delta_{j,k}(A) = 0$.

En conclusion, $M_{i,j} = \det(A)\, \delta_{i,j}$ donc $M = \det(A)\, I_n$. □

Exemple 2.18 :

Grâce à la formule de l'inverse par le déterminant, on peut calculer facilement l'inverse suivant :

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 9 \end{bmatrix}^{-1} = \frac{1}{2} \begin{bmatrix} 6 & -5 & 1 \\ -6 & 8 & -2 \\ 2 & -3 & 1 \end{bmatrix}.$$

◇

4. Calculs de déterminants

4.1. Déterminant de Vandermonde

Définition 2.19 *Matrice et déterminant de Vandermonde*[4]
Soient $(a_1, \dots, a_n) \in \mathbb{K}^n$. On appelle *matrice de Vandermonde associée à* $(a_1, \dots, a_n)$ la matrice

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{bmatrix} = \left[a_j^{i-1}\right]_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{K}).$$

On appelle *déterminant de Vandermonde associé à* $(a_1, \dots, a_n)$ le déterminant de cette matrice.

Proposition 2.20
Soient $(a_1, \dots, a_n) \in \mathbb{K}^n$. La matrice de Vandermonde associée à $(a_1, \dots, a_n)$ est inversible si, et seulement si, les a_i sont distincts. De plus,

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{vmatrix} = \prod_{i<j} (a_j - a_i).$$

⚠ On trouve aussi comme définition la matrice transposée de la matrice donnée en définition. Cela n'influe évidemment pas sur le calcul du déterminant ni sur la condition d'inversibilité.

Démonstration : Notons $d_n(a_1, \dots, a_n)$ le déterminant de Vandermonde de taille n associée à $a_1, \dots, a_n$. En effectuant successivement les opérations élémentaires $L_n \leftarrow L_n - x_1 L_{n-1}, \dots, L_2 \leftarrow L_2 - x_1 L_1$, puis en développant par rapport à la première colonne, on obtient

$$\begin{aligned}
\begin{vmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{vmatrix} &= \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 0 & a_2 - a_1 & \cdots & a_n - a_1 \\ 0 & a_2^2 - a_1 a_2 & \cdots & a_n^2 - a_1 a_n \\ \vdots & \vdots & \cdots & \vdots \\ 0 & a_2^{n-1} - a_1 a_2^{n-2} & \cdots & a_n^{n-1} - a_1 a_n^{n-2} \end{vmatrix} \\
&= \begin{vmatrix} a_2 - a_1 & \cdots & a_n - a_1 \\ a_2^2 - a_1 a_2 & \cdots & a_n^2 - a_1 a_n \\ \vdots & \cdots & \vdots \\ a_2^{n-1} - a_1 a_2^{n-2} & \cdots & a_n^{n-1} - a_1 a_n^{n-2} \end{vmatrix} \\
&= (a_2 - a_1) \dots (a_n - a_1) \begin{vmatrix} 1 & \cdots & 1 \\ a_2 & \cdots & a_n \\ \vdots & \cdots & \vdots \\ a_2^{n-2} & \cdots & a_n^{n-2} \end{vmatrix}
\end{aligned}$$

$$d_n(a_1, \dots, a_n) = d_{n-1}(a_2, \dots, a_n) \prod_{i=2}^{n} (a_i - a_1)$$

4. Alexandre-Théophile VANDERMONDE (1735-1796) : Mathématicien et chimiste français.

Par une récurrence immédiate, on en déduit que $d_n(a_1,\dots,a_n)=\prod_{i<j}(a_j-a_i)$. Et donc, la matrice associée est inversible si, et seulement si, $d_n(a_1,\dots,a_n)\neq 0$, i.e. les a_i sont distincts. □

4.2. Déterminant tridiagonal

Exercice 2.21 :
Soient $a,b\in\mathbb{C}$. Calculer le déterminant de taille n défini par

$$d_n=\begin{vmatrix} a+b & b & & (0) \\ a & \ddots & \ddots & \\ & \ddots & \ddots & b \\ (0) & & a & a+b \end{vmatrix}.$$

Réponse
En développant par rapport à la première colonne, on a, pour tout $n\geq 3$,

$$d_n=(a+b)\,d_{n-1}-a\begin{vmatrix} b & 0 & \cdots & \cdots & 0 \\ 0 & a+b & b & & (0) \\ \vdots & a & \ddots & \ddots & \\ \vdots & & \ddots & \ddots & b \\ 0 & (0) & & a & a+b \end{vmatrix}=(a+b)\,d_{n-1}-abd_{n-2}.$$

On en déduit que la suite (d_n) est définie par une relation de récurrence d'ordre 2 dont le polynôme caractéristique est $X^2-(a+b)\,X+ab=(X-a)\,(X-b)$.

- Si $a\neq b$, alors

  $$\exists A,B\in\mathbb{C},\forall n\in\mathbb{N}\quad d_n=Aa^n+Bb^n.$$

  De plus,

  $$d_1=a+b=(A+B)\,a,\quad d_2=Aa^2+Bb^2=a^2+b^2+ab,\quad A=\frac{a}{a-b},\quad B=\frac{b}{b-a}.$$

  On en déduit que $d_n=\dfrac{a^{n+1}-b^{n+1}}{a-b}$.
- Si $a=b$ alors

  $$\exists A,B\in\mathbb{C},\forall n\in\mathbb{N}\quad d_n=(A+Bn)\,a^n.$$

  De plus,

  $$d_1=2a=(A+B)\,a,\quad d_2=(A+2B)\,a^2=3a^2,\quad A=B=1.$$

  On en déduit que $d_n=(n+1)\,a^n$.

♢

4.3. Déterminant imbriqué

Exercice 2.22 :
Soient $a,b,c,d\in\mathbb{C}$. Déterminer une condition nécessaire et suffisante sur a,b,c et d pour que la matrice

$$M = \begin{bmatrix} a & a & a & a \\ a & b & b & b \\ a & b & c & c \\ a & b & c & d \end{bmatrix}$$ soit inversible.

Réponse

On effectue des opérations élémentaires pour se ramener à une matrice triangulaire supérieure.

$$\begin{aligned}
\begin{vmatrix} a & a & a & a \\ a & b & b & b \\ a & b & c & c \\ a & b & c & d \end{vmatrix} \underset{L_4 \leftarrow L_4 - L_3}{=} \begin{vmatrix} a & a & a & a \\ a & b & b & b \\ a & b & c & c \\ 0 & 0 & 0 & d-c \end{vmatrix} \underset{L_3 \leftarrow L_3 - L_2}{=} \begin{vmatrix} a & a & a & a \\ a & b & b & b \\ 0 & 0 & c-b & c-b \\ 0 & 0 & 0 & d-c \end{vmatrix} \\
\underset{L_2 \leftarrow L_2 - L_1}{=} \begin{vmatrix} a & a & a & a \\ 0 & b-a & b-a & b-a \\ 0 & 0 & c-b & c-b \\ 0 & 0 & 0 & d-c \end{vmatrix} \\
= a\,(b-a)\,(c-b)\,(d-c)\,.
\end{aligned}$$

On en déduit que la matrice M est inversible si, et seulement si $a \neq 0, a \neq b, b \neq c$ et $c \neq d$

$\diamondsuit$

4.4. Fonction définie par un déterminant

Exercice 2.23 :
Soient $n \in \mathbb{N}^*$ et $a, b, c \in \mathbb{R}$ distincts. On définit $f : x \mapsto \det(A + xB)$, avec $A, B \in \mathcal{M}_n(\mathbb{K})$ définies par :

$$A = \begin{bmatrix} a & & (b) \\ & \ddots & \\ (c) & & a \end{bmatrix}, \quad B = \begin{bmatrix} & & \\ & (1) & \\ & & \end{bmatrix}.$$

Déterminer une expression simple pour f.

Réponse

Pour tout $x \in \mathbb{R}$, on effectue les opérations élémentaires $C_i \leftarrow C_i - C_1$ pour $i \in [\![2, n]\!]$. On obtient alors

$$\begin{aligned}
f(x) &= \begin{vmatrix} a+x & b+x & b+x & \cdots & b+x \\ c+x & a+x & b+x & \cdots & b+x \\ \vdots & c+x & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & b+x \\ c+x & c+x & \cdots & c+x & a+x \end{vmatrix} = \begin{vmatrix} a+x & b-a & b-a & \cdots & b-a \\ c+x & a-c & b-c & \cdots & b-c \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & b-c \\ c+x & 0 & \cdots & 0 & a-c \end{vmatrix} \\
&= x \begin{vmatrix} 1 & b-a & b-a & \cdots & b-a \\ 1 & a-c & b-c & \cdots & b-c \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & b-c \\ 1 & 0 & \cdots & 0 & a-c \end{vmatrix} + \begin{vmatrix} a & b-a & b-a & \cdots & b-a \\ c & a-c & b-c & \cdots & b-c \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & b-c \\ c & 0 & \cdots & 0 & a-c \end{vmatrix}
\end{aligned}$$

La fonction f est donc un fonction polynomiale de degré inférieur à 1, donc il existe $\alpha, \beta \in \mathbb{R}$ tels que $f : x \mapsto \alpha x + \beta$. On pourrait alors calculer les deux déterminants obtenus précédemment. Une autre méthode est d'évaluer f en $-b$ et $-c$:

$$f(-b) = \begin{vmatrix} a-b & 0 & \cdots & 0 \\ c-b & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ c-b & \cdots & c-b & a-b \end{vmatrix} = (a-b)^n, \quad f(-c) = (a-c)^n.$$

On en déduit que

$$\begin{cases} -\alpha b + \beta = (a-b)^n \\ -\alpha c + \beta = (a-c)^n \end{cases}, \quad \alpha(b-c) = (a-c)^n - (a-b)^n, \quad \beta(b-c) = b(a-c)^n - c(a-b)^n,$$

Donc

$$\begin{aligned} \forall x \in \mathbb{R}, \quad f(x) &= \frac{(a-c)^n - (a-b)^n}{b-c} x + \frac{b(a-c)^n - c(a-b)^n}{b-c} \\ &= \frac{(a-c)^n}{b-c}(x+b) + \frac{(a-b)^n}{c-b}(x+c). \end{aligned}$$

On remarque que f est bien symétrique en b et c, car $\det(A + xB) = \det((A + xB)^\intercal)$.

◊

4.5. Matrice compagnon

Exercice 2.24 :
Soient $a, b, c, d, e \in \mathbb{C}$. On pose

$$M = \begin{bmatrix} 0 & 0 & 0 & 0 & -a \\ 1 & 0 & 0 & 0 & -b \\ 0 & 1 & 0 & 0 & -c \\ 0 & 0 & 1 & 0 & -d \\ 0 & 0 & 0 & 1 & -e \end{bmatrix}.$$

Pour tout $\lambda \in \mathbb{C}$, calculer $-\det(M - \lambda I_n)$.

Réponse

En développant par rapport à la dernière colonne, on a

$$
\begin{aligned}
-\det\left(M-\lambda I_n\right) &= -\begin{vmatrix} -\lambda & 0 & 0 & 0 & -a \\ 1 & -\lambda & 0 & 0 & -b \\ 0 & 1 & -\lambda & 0 & -c \\ 0 & 0 & 1 & -\lambda & -d \\ 0 & 0 & 0 & 1 & -e-\lambda \end{vmatrix} \\
&= a\begin{vmatrix} 1 & -\lambda & & (0) \\ 0 & 1 & -\lambda & \\ & 0 & 1 & -\lambda \\ (0) & & 0 & 1 \end{vmatrix} - b\begin{vmatrix} -\lambda & 0 & & (0) \\ 0 & 1 & -\lambda & \\ & 0 & 1 & -\lambda \\ (0) & & 0 & 1 \end{vmatrix} + c\begin{vmatrix} -\lambda & 0 & & (0) \\ 1 & -\lambda & 0 & \\ & 0 & 1 & -\lambda \\ (0) & & 0 & 1 \end{vmatrix} \\
&\quad - d\begin{vmatrix} -\lambda & 0 & & (0) \\ 1 & -\lambda & 0 & \\ & 1 & -\lambda & 0 \\ (0) & & 0 & 1 \end{vmatrix} + (e+\lambda)\begin{vmatrix} -\lambda & 0 & & (0) \\ 1 & -\lambda & 0 & \\ & 1 & -\lambda & 0 \\ (0) & & 1 & -\lambda \end{vmatrix} \\
&= a + b\lambda - c\lambda\begin{vmatrix} -\lambda & 0 & 0 \\ 0 & 1 & -\lambda \\ 0 & 0 & 1 \end{vmatrix} + d\lambda\begin{vmatrix} -\lambda & 0 & 0 \\ 1 & -\lambda & 0 \\ 0 & 0 & 1 \end{vmatrix} + e\lambda^4 + \lambda^5 \\
&= a + b\lambda + c\lambda^2 + d\lambda^3 + e\lambda^4 + \lambda^5.
\end{aligned}
$$

♢

On dit que la matrice M est la matrice compagnon du polynôme $a+bX+cX^2+dX^3+eX^4+X^5$. On reverra cette notion très importante dans le chapitre de réduction des endomorphismes et des matrices.

III Déterminant et systèmes linéaires

Dans toute cette section, n et p sont deux entiers naturels non-nuls.

1. Solutions d'un système linéaire

Définition 3.1 *Système linéaire*

On appelle *système linéaire à n équations et p inconnues* toute équation vectorielle (d'inconnue X) de la forme

$$(S) \quad : \quad AX = B, \quad X \in \mathcal{M}_{p,1}(\mathbb{K}), A \in \mathcal{M}_{n,p}(\mathbb{K}), B \in \mathcal{M}_{n,1}(\mathbb{K})$$

A est appelée *matrice du système linéaire* (S) et B est appelé *second membre*. On appelle *système homogène associé à* (S) le système

$$(S_0) \quad : \quad AX = O_{n,1}$$

Une unique équation vectorielle (d'inconnue X) est équivalente à n équations scalaires (d'inconnues $X_1, \ldots, X_n$) :

$$AX = B \iff \begin{cases} A_{1,1}X_1 + \cdots + A_{1,p}X_p = B_1 \\ A_{2,1}X_1 + \cdots + A_{2,p}X_p = B_2 \\ \ldots \\ A_{n,1}X_1 + \cdots + A_{n,p}X_p = B_n \end{cases}.$$

Définition 3.2

Soit (S) un système linéaire dont la matrice associée est A. On définit alors le *rang du système* par $\operatorname{rg}(S) = \operatorname{rg}(A)$.

Proposition 3.3 *Structure des solutions du système homogène*

Soit (S) un système linéaire à n équations et p inconnues. L'ensemble des solutions de (S_0) est un espace vectoriel de dimension finie. Sa dimension est $p - \operatorname{rg}(S)$.

Démonstration : Soit A la matrice associée à (S), et soit $X \in \mathbb{K}^n$. Alors, par définition,

$$X \text{ est solution de } (S_0) \iff AX = O_{n,1} \iff X \in \ker A.$$

En conséquence, l'ensemble des solutions de (S_0) est $\ker A$, qui est un espace vectoriel de dimension finie, et d'après le théorème du rang,

$$\dim \ker A = \dim \mathcal{M}_p(\mathbb{K}) - \operatorname{rg}(A) = p - \operatorname{rg}(S).$$

$\square$

Proposition 3.4 *Structure des solutions du système homogène*

Soit $(S) : AX = B$ un système linéaire à n équations et p inconnues. Alors

(i) Si $B \notin \operatorname{Im} A$, (S) n'admet pas de solutions.
(ii) Si $B \in \operatorname{Im} A$, alors (S) admet au moins une solution X_p, et l'ensemble des solutions de (S) est

$$X_p + \ker A = \{X_p + X_0 / X_0 \in \ker A\}.$$

C'est un type de structure qu'on appelle un *espace affine*.

Démonstration : Le point (i) étant évident, on suppose que $B \in \operatorname{Im} A$. Par définition, il existe $X_p \in \mathcal{M}_{n,1}(\mathbb{K})$ tel que $AX_p = B$, donc X_p est une solution. Soit $X \in \mathcal{M}_{n,1}(\mathbb{K})$, alors

$$\begin{aligned} AX = B &\iff AX = AX_p \iff A(X - X_p) = O_{n,1} \iff X - X_p \in \ker A \\ &\iff \exists X_0 \in \ker A, X = X_p + X_0. \end{aligned}$$

$\square$

2. Systèmes de Cramer

Maintenant qu'on a vu l'existence de solutions de (S) et la forme de leur ensemble, lorsqu'il n'est pas vide, on s'intéresse à l'unicité des solutions et à leur calcul effectif. Pour $A \in \mathcal{M}_{n,p}(\mathbb{K})$, remarquons que l'application $X \mapsto AX$

- n'est pas surjective si $n > p$ (car $\operatorname{rg} A \leq p < n$) ;
- n'est pas injective si $n > p$ (car $\operatorname{rg} A \leq n < p$).

On en déduit que pour avoir existence et unicité des solutions, une condition nécessaire est $n = p$.

Définition 3.5 *Système de Cramer*[5]

Soit (S) un système à n équations et n inconnues. On dit que (S) est un *système de Cramer* si $\operatorname{rg}(S) = n$.

Pour déterminer si un système est de Cramer, le plus simple est souvent de calculer un déterminant : (S) est de Cramer si, et seulement si, la matrice associée est de déterminant non-nul.

Théorème 3.6 *Formule de Cramer*

Soit $(S) : AX = B$ un système linéaire à n équations et n inconnues. Si (S) est un système de Cramer, alors A est inversible, et (S) admet une unique solution X définie par

$$\forall i \in [\![1, n]\!], \quad X_i = \frac{1}{\det A} \det[C_1, \ldots, C_{i-1}, B, C_{i+1}, \ldots, C_n].$$

où $C_1, \ldots, C_n$ sont les colonnes de A.

Démonstration : Si $n = \operatorname{rg} S = \operatorname{rg} A$ alors $A \in \mathrm{GL}_n(\mathbb{K})$. Alors on sait qu'il existe un unique $X \in \mathcal{M}_{n,1}(\mathbb{K})$ tel que $AX = B$. Donc (S) admet une unique solution $X = A^{-1}B = \dfrac{1}{\det A} \operatorname{Com}(A)^{\intercal} B$. Alors, pour tout $i \in [\![1, n]\!]$,

$$X_i = \frac{1}{\det A} \sum_{j=1}^{n} (-1)^{i+j} B_i \Delta_{i,j} = \frac{1}{\det A} \det[C_1, \ldots, C_{i-1}, B, C_{i+1}, \ldots, C_n],$$

car on a reconnu le développement du déterminant par rapport à la i-ème colonne de la matrice $[C_1, \ldots, C_{i-1}, B, C_{i+1}, \ldots, C_n]$.
□

Pour résoudre un système linéaire $AX = B$, on pourra utiliser la méthode que l'on souhaite : le résoudre directement, calculer A^{-1} par la méthode de son choix, ou utiliser la formule de Cramer. Cette dernière convient particulièrement

- aux système de 2 équations à 2 inconnues ;
- aux systèmes à paramètres ;
- aux systèmes dont on sait calculer facilement le déterminant de la matrice associée.

Attention, la formule de Cramer n'est valable que pour les systèmes de Cramer, ce qui exclut tous les systèmes à n équations et p inconnues quand $n \neq p$.

Exercice 3.7 :
Soient $a, b, c, d \in \mathbb{R}^*$ et soient $\alpha, \beta \in \mathbb{R}$. Résoudre le système $\begin{cases} ax + by = \alpha \\ cx + dy = \beta \end{cases}$.

Réponse

$\boxed{\text{Cas 1 : } ad - bc \neq 0}$ Le système est de Cramer et possède une unique solution

$$x = \frac{\alpha d - \beta b}{ad - bc}, \quad y = \frac{\alpha a - \beta c}{ad - bc}.$$

$\boxed{\text{Cas 2 : } ad - bc = 0}$ Le système n'est pas de Cramer. Donc il existe $\lambda \in \mathbb{R}^*$ tel que

$$ad = bc, \quad \frac{a}{c} = \lambda = \frac{b}{d}, \quad c = \lambda a \quad d = \lambda b.$$

5. Gabriel Cramer (1707-1752) : Mathématicien suisse.

Donc

$$\begin{cases} ax+by=\alpha \\ cx+dy=\beta \end{cases} \iff \begin{cases} ax+by=\alpha \\ \lambda ax+\lambda by=\beta \end{cases} \iff \begin{cases} ax+by=\alpha \\ ax+by=\frac{\beta}{\lambda} \end{cases}.$$

$\boxed{\text{Cas 2a : } \beta \neq \lambda a}$ Le système $\begin{cases} ax+by=\alpha \\ cx+dy=\beta \end{cases}$ n'a pas de solutions.

$\boxed{\text{Cas 2b : } \beta = \lambda a}$ On a

$$\begin{cases} ax+by=\alpha \\ cx+dy=\beta \end{cases} \iff ax+by=\alpha \iff (x,y)\in\left(\frac{\alpha}{a},0\right)+\operatorname{Vect}(-b,a).$$

◊

Exercice 3.8 :

Soient $a,b,c,d\in\mathbb{K}$ avec a,b,c distincts. Résoudre le système $\begin{cases} x+y+z=1 \\ ax+by+cz=d \\ a^2x+b^2y+c^2z=d^2 \end{cases}$.

Réponse

Le système est de Cramer car le déterminant de la matrice associée est un déterminant de Vandermonde non-nul : il vaut $\delta=(c-b)(c-a)(b-a)$. D'après la formule de Cramer, on a

$$x=\frac{1}{\delta}\begin{vmatrix} 1 & 1 & 1 \\ d & b & c \\ d^2 & b^2 & c^2 \end{vmatrix}=\frac{(c-d)(b-d)(c-b)}{(c-a)(b-a)(c-b)}=\frac{(c-d)(b-d)}{(c-a)(b-a)}.$$

De même,

$$b=\frac{(c-d)(d-a)}{(c-b)(b-a)},\quad c=\frac{(d-b)(d-a)}{(c-b)(c-a)}.$$

◊

À connaître à la fin du chapitre

Déterminants

- Connaître la définition du déterminant dans une base et le lien entre base et déterminant.
- Connaître la définition du déterminant d'un endomorphisme et le lien entre bijectivité et déterminant.
- Connaître la définition du déterminant d'une matrice et le lien entre inversibilité et déterminant.

Opérations matricielles

- Savoir calculer en pratique un déterminant en dimensions 2,3,4 et 5.
- Utiliser les opérations matricielles en théorie pour calculer des déterminants en dimension n.
- Connaître la formule de l'inverse par le déterminant, et savoir dans quels cas il est utile de l'utiliser.
- Appliquer les formules de Cramer.

CHAPITRE 16

ESPACES PRÉHILBERTIENS

Pré-requis :

- Espaces vectoriels.
- Matrices.

Dans tout le chapitre, sauf mention contraire, E et F sont des $\mathbb{R}$-espaces vectoriels.

I Produit scalaire et norme

1. Produit scalaire

Définition 1.1 *Produit scalaire*

Soit $\varphi \in \mathcal{F}\left(E^2, \mathbb{R}\right)$. On dit que φ est un *produit scalaire sur* E si :

(i) φ est bilinéaire.

(ii) φ est symétrique :

$$\forall x, y \in E, \quad \varphi(x, y) = \varphi(y, x).$$

(iii) φ est positive :

$$\forall x \in E, \quad \varphi(x, x) \geq 0.$$

(iv) φ est définie :

$$\forall x \in E, \quad \varphi(x, x) = 0 \iff x = 0.$$

Dans la suite, on notera généralement les produits scalaires $< x, y >$. Il existe d'autres notations possibles : $x \cdot y$ ou $(x|y)$ parmi les plus courantes.

Exemple 1.2 :

On a vu dans le cours d'intégration que l'application $(f, g) \mapsto \displaystyle\int_0^1 f(t)\, g(t)\, dt$ est un produit scalaire sur $\mathcal{C}^0([0,1], \mathbb{R})$. Ce n'est pas un produit scalaire sur $\mathcal{C}^0_m([0,1], \mathbb{R})$. ♢

Remarque 1.3 : Une conséquence directe : pour tout $x \in E$, on a $< x, 0 >=< 0, x >= 0$. En effet,

$$< x, 0 >=< x, -0_E >= - < x, 0 >, \quad < x, 0 >= 0.$$

$\diamondsuit$

Définition/Proposition 1.4

Soit $n \in \mathbb{N}^*$. L'application définie pour tous $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{R}^n$ par

$$< x, y >= \sum_{i=1}^{n} x_i y_i$$

est un un produit scalaire sur $\mathbb{R}^n$. On l'appelle produit scalaire *usuel* (ou *canonique*).

Démonstration : Soient $x, x', y \in \mathbb{R}^n$, $\lambda, \lambda' \in \mathbb{R}$.

- On a

$$< \lambda x + \lambda' x', y >= \sum_{i=1}^{n} (\lambda x_i + \lambda' x'_i) y_i = \lambda \sum_{i=1}^{n} x_i + \lambda' \sum_{i=1}^{n} x'_i y_i = \lambda < x, y > +\lambda' < x', y >,$$

alors $< \cdot, \cdot >$ est linéaire à gauche. De même, on montre que $< \cdot, \cdot >$ est linéaire à droite.
- Par définition, $< x, y >= \sum_{i=1}^{n} x_i y_i \sum_{i=1}^{n} y_i x_i =< y, x >$. Donc $< \cdot, \cdot >$ est symétrique.
- On a $< x, x >= \sum_{i=1}^{n} x_i^2 \geq 0$. Donc $< \cdot, \cdot >$ est positive.
- Remarquons que, pour tout $i \in [\![1, n]\!]$, $x_i^2 \geq 0$. Donc

$$< x, x >= 0 \iff \sum_{i=1}^{n} x_i = 0 \iff \forall i \in [\![1, n]\!], x_i^2 = 0 \iff x = 0.$$

Donc $< \cdot, \cdot >$ est définie.

$\square$

Le produit scalaire usuel sur $\mathbb{R}^2$ ou $\mathbb{R}^3$ est déjà bien connu, même si on le note plutôt $u \cdot v$:

$$(u_1, u_2) \cdot (v_1, v_2) = u_1 v_1 + u_2 v_2.$$

Exemple 1.5 :
L'application définie pour tous $P, Q \in \mathbb{R}[X]$ par

$$< P, Q >= \int_0^{+\infty} P(t) Q(t) \mathrm{e}^{-t} \, dt$$

est un produit scalaire sur $\mathbb{R}[X]$. $\diamondsuit$

Exercice 1.6 :
Soit $n \in \mathbb{N}^*$. Montrer que l'application définie pour tous $A, B \in \mathcal{M}_n(\mathbb{R})$ par

$$< A, B >= \mathrm{Tr}(A^{\intercal} B)$$

est un produit scalaire sur $\mathcal{M}_n(\mathbb{R})$.

Réponse

Par le calcul, on montre facilement que, pour tous $A = [a_{i,j}], B = [b_{i,j}] \in \mathcal{M}_n(\mathbb{R})$,

$$< A, B >= \operatorname{Tr}(A^\intercal B) = \sum_{1 \leq i,j \leq n} a_{i,j} b_{i,j}.$$

C'est donc le produit scalaire usuel dans $\mathcal{M}_n(\mathbb{R}) \simeq \mathbb{R}^{n^2}$.

◊

Définition 1.7 *Espace préhilbertien et espace euclidien*

Soit E un $\mathbb{R}$-espace vectoriel. On dit que E *est un espace préhilbertien réel* si E admet un produit scalaire. On dit que E *est euclidien* si E est un espace préhilbertien réel de dimension finie.

Théorème 1.8 *Inégalité de Cauchy*[1]*-Schwarz*[2]

Soit E un espace préhilbertien réel. Alors, pour tous $x, y \in E$, on a

$$| < x, y > | \leq \sqrt{< x, x >}\sqrt{< y, y >}.$$

De plus, il y a égalité si, et seulement si, la famille (x, y) est liée.

Démonstration : Pour $\lambda \in \mathbb{R}$, on pose

$$\begin{aligned} P(\lambda) &=< \lambda x + y, \lambda x + y > && (\star) \\ &= \lambda < x, \lambda x + y > + < y, \lambda x + y >= \lambda^2 < x, x > +\lambda < x, y > +\lambda < y, x > + < y, y > \\ &= \lambda^2 < x, x > +2\lambda < x, y > + < y, y > . && (\star\star) \end{aligned}$$

Ces égalités sont vraies par linéarité et symétrie du produit scalaire. D''après $(\star\star)$, P est un polynôme de degré inférieur ou égal à 2.

$\boxed{\text{Cas 1 : } x = 0}$ Si $x = 0$, alors $| < x, y > | = 0 = \sqrt{< x, x >}\sqrt{< y, y >}$. L'inégalité de Cauchy-Schwarz est vérifiée, et c'est une égalité (et (x, y) est liée).

$\boxed{\text{Cas 2 : } x \neq 0}$ Alors $< x, x >\neq 0$ car le produit scalaire est défini, et donc P est un polynôme de degré 2. D'après $(\star)$ et par positivité du produit scalaire, on a

$$\forall \lambda \in \mathbb{R}, \quad P(\lambda) \geq 0.$$

Le discriminant Δ de P est donc négatif. On a

$$\Delta = 4 < x, y >^2 -4 < x, x >< y, y >\leq 0,$$

$$\begin{aligned} &4 < x, y >^2 \leq 4 < x, x >< y, y > \\ &| < x, y > | \leq \sqrt{< x, x >}\sqrt{< y, y >}. \end{aligned}$$

L'inégalité de Cauchy-Schwarz est bien vérifiée. De plus,

$$\begin{aligned} | < x, y > | = \sqrt{< x, x >}\sqrt{< y, y >} &\iff \Delta = 0 \\ &\iff \exists \lambda \in \mathbb{R}, \quad P(\lambda) = 0 \\ &\iff \exists \lambda \in \mathbb{R}, \quad < \lambda x + y, \lambda x + y >= 0 \\ &\iff \exists \lambda \in \mathbb{R}, \quad \lambda x + y = 0 \\ &\iff (x, y) \text{ est liée.} \end{aligned}$$

1. Augustin Cauchy (1789-1857) : Mathématicien français.
2. Hermann Schwarz (1843-1921) : Mathématicien allemand.

Attention, la réciproque de la dernière équivalence est vraie uniquement car $x \neq 0$. □

2. Norme

Définition 1.9 *Norme*

Soit $N \in \mathcal{F}(E, \mathbb{R})$. On dit que N est une *norme* si :

(i) N est définie :

$$\forall x \in E, \quad N(x) \geq 0.$$

(ii) N est positive :

$$\forall x \in E, \quad N(x) = 0 \iff x = 0.$$

(iii) N est homogène :

$$\forall x \in E, \lambda \in \mathbb{R}, \quad N(\lambda x) = |\lambda| N(x).$$

(iv) N vérifie l'inégalité triangulaire :

$$\forall x, y \in E, \quad N(x+y) \leq N(x) + N(y).$$

Dans la suite, on note généralement les normes $\|x\|$.

Définition/Proposition 1.10 *Espce préhilbertien*[3]

Soit E un espace préhilbertien réel. Alors l'application définie pour tout $x \in E$ par

$$\|x\| = \sqrt{< x, x >}$$

est une norme sur E. On l'appelle *norme euclidienne*.

Démonstration : D'abord, l'application $\|\cdot\|$ est bien définie, car $< \cdot, \cdot >$ est positif par définition. Soient $x, y \in E$ et $\lambda \in \mathbb{R}$.

- Puisque $x \mapsto \sqrt{x}$ est positive, il est clair que $\|x\| \geq 0$. Donc $\|\cdot\|$ est bien définie.
- Puisque $< \cdot, \cdot >$ est défini, on a
$$\|x\| = 0 \iff \sqrt{< x, x >} = 0 \iff < x, x >= 0 \iff x = 0.$$
Donc $\|\cdot\|$ est bien positive.
- Puisque $< \cdot, \cdot >$ est bilinéaire, on a
$$\|\lambda x\| = \sqrt{< \lambda x, \lambda x >} = \sqrt{\lambda^2 < x, x >} = |\lambda| \sqrt{< x, x >} = |\lambda| \|x\|.$$
Donc $\|\cdot\|$ est bien homogène.
- Par linéarité et symétrie de $< \cdot, \cdot >$, on a
$$\begin{aligned} \|x+y\|^2 &=< x+y, x+y >=< x+y, x > + < x+y, y > \\ &=< x, x > + < x, y > + < y, x > + < y, y >=< x, x > +2 < x, y > + < y, y > \\ &= \|x\|^2 + 2 < x, y > + \|y\|^2, \\ (\|x\| + \|y\|)^2 &= \|x\|^2 + 2\|x\|.\|y\| + \|y\|^2. \end{aligned}$$

3. David Hilbert (1862-1943) : Mathématicien allemand. La structure préhilbertienne est un pré-requis pour parler d'espaces de Hilbert.

D'après l'inégalité de Cauchy-Schwarz, $< x, y > \leq | < x, y > | \leq \|x\|.\|y\|$, donc $\| \cdot \|$ vérifie bien l'inégalité triangulaire.

□

Remarque 1.11 (*Distance*) : Une norme permet de définir une *distance* par

$$\forall x, y \in E, \quad d(x, y) = \|y - x\|.$$

Une distance vérifie les trois axiomes suivants :

- $\forall x, y \in E,\ d(x, y) = d(y, x)$.
- $\forall x, y \in E,\ d(x, y) = 0 \iff x = y$.
- $\forall x, y, z \in E,\ d(x, z) \leq d(x, y) + d(y, z)$.

C'est avec cette notion que l'on peut définir les notions de suites et de convergence dans des espaces plus généraux que $\mathbb{R}$ ou $\mathbb{C}$ (les espaces normés, ou les espaces métriques). ◇

Proposition 1.12 *Identités remarquables*

Soient E un espace préhilbertien réel muni d'un produit scalaire $< \cdot, \cdot >$. On note $\| \cdot \|$ la norme associée. Alors, pour tous $x, y \in E$,

(i) $\|x + y\|^2 = \|x\|^2 + 2 < x, y > + \|y\|^2$.
(ii) $\|x - y\|^2 = \|x\|^2 - 2 < x, y > + \|y\|^2$.
(iii) $< x + y, x - y > = \|x\|^2 - \|y\|^2$.

Démonstration : Pour tous $x, y \in E$, on a

$$\begin{aligned}\|x + y\|^2 &= < x + y, x + y > = < x + y, x > + < x + y, y > \\ &= < x, x > + < x, y > + < y, x > + < y, y > = < x, x > + 2 < x, y > + < y, y > \\ &= \|x\|^2 + 2 < x, y > + \|y\|^2.\end{aligned}$$

D'après la formule (i), on a alors

$$\|x - y\|^2 = \|x\|^2 + 2 < x, -y > + \| - y\|^2 = \|x\|^2 - 2 < x, y > + \|y\|^2.$$

Enfin, en développant de la même manière, on a $< x + y, x - y > = \|x\|^2 - \|y\|^2$. □

Proposition 1.13 *Identité du paralélogramme*

Soient E un espace préhilbertien réel muni d'un produit scalaire $< \cdot, \cdot >$. On note $\| \cdot \|$ la norme associée. Alors, pour tous $x, y \in E$,

$$\|x + y\|^2 + \|x - y\|^2 = 2\left(\|x\|^2 + \|y\|^2\right).$$

Démonstration : D'après les identités remarquables, on a, pour tous $x, y \in E$,

$$\|x + y\|^2 + \|x - y\|^2 = \|x\|^2 + 2 < x, y > + \|y\|^2 + \|x\|^2 - 2 < x, y > + \|y\|^2 = 2\left(\|x\|^2 + \|y\|^2\right).$$

□

Proposition 1.14 *Identité de polarisation*

Soient E un espace préhilbertien réel muni d'un produit scalaire $< \cdot,\cdot >$. On note $\|\cdot\|$ la norme associée. Alors, pour tous $x, y \in E$,

(i) $< x, y >= \frac{1}{4}\left(\|x+y\|^2 - \|x-y\|^2\right).$

(ii) $< x, y >= \frac{1}{2}\left(\|x+y\|^2 - \|x\|^2 - \|y\|^2\right).$

Démonstration : D'après les identités remarquables, on a, pour tous $x, y \in E$,

$$\|x+y\|^2 - \|x-y\|^2 = \|x\|^2 + 2 < x, y > + \|y\|^2 - \|x\|^2 + 2 < x, y > - \|y\|^2 = 4 < x, y > .$$

□

Exercice 1.15 :
Soient $a < b$ et $E = \mathcal{C}^0([a,b], \mathbb{R})$. Pour $f \in E$, on définit

$$N(f) = \max_{[a,b]} |f|.$$

1. Montrer que N est une norme sur E.
2. Montrer que N ne satisfait pas l'identité du parallélogramme. Que peut-on en conclure ?

Réponse

1. N est bien définie, car si $f \in E$ alors $|f| \in \mathcal{C}^0([a,b])$. Puisque $[a,b]$ est un segment, $|f|$ est bornée et atteint ses bornes, donc $\max_{[a,b]} |f|$ existe. Soient $f, g \in E$ et $\lambda \in \mathbb{R}$.
   - N est clairement positive par définition.
   - Il est clair que $f = 0 \Rightarrow N(f) = 0$. De plus
   $$N(f) = 0 \Rightarrow \max_{[a,b]} |f| = 0, \Rightarrow \forall x \in [a,b], |f(x)| \leq 0 \Rightarrow \forall x \in [a,b], f(x) = 0 \Rightarrow f = 0.$$
   - Il existe $c \in [a,b]$ tel que $|f(c)| = \max_{[a,b]} |f|$. Pour tout $x \in [a,b]$, on a
   $$|\lambda f(x)| \leq |\lambda|.|f(c)| = |\lambda| N(f), \quad \max_{[a,b]} |\lambda f| \leq |\lambda| N(f), \quad N(\lambda f) \leq |\lambda| N(f).$$
   De plus
   $$|\lambda f(c)| = |\lambda| N(f), \quad \max_{[a,b]} |\lambda f| = |\lambda| N(f), \quad N(\lambda f) = |\lambda| N(f).$$
   - Il existe $c, d \in [a,b]$ tels que $|f(c)| = \max_{[a,b]} |f|$ et $|g(d)| = \max_{[a,b]} |g|$. Alors, pour tout $x \in [a,b]$,
   $$|f(x) + g(x)| \leq |f(x)| + |g(x)| \leq |f(c)| + |g(d)| = \max_{[a,b]} |f| + \max_{[a,b]} |g|,$$
   donc $\max_{[a,b]} |f+g| \leq \max_{[a,b]} |f| + \max_{[a,b]} |g|$.
2. Posons $f : x \mapsto \dfrac{x-a}{b-a}$ et $g = 1 - f$. Les fonctions f et g sont continues sur $[a,b]$ on a
   $$N(f) = 1, \quad N(g) = 1, \quad N(f+g) = 1, \quad N(f-g) = 1.$$
   Alors
   $$N(f)^2 + N(g)^2 = 2, \quad 2\left(N(f)^2 + N(g)^2\right) = 4.$$

Donc N ne vérifie pas l'identité du parallélogramme. On en déduit que N n'est pas une norme euclidienne.

◇

3. Structure complexe et produit hermitien

Pourquoi choisit-on de travailler seulement dans le cas réel ? Une fois n'est pas coutume, il existe une grosse différence entre le cas réel et le cas complexe en ce qui concerne les produits scalaires.

Dans le cas complexe, on remarque que le "produit scalaire usuel" n'est pas un produit scalaire. En effet, l'application

$$\varphi \begin{array}{ccc} \left(\mathbb{C}^2\right)^2 & \to & \mathbb{C} \\ \left((z_1, z_2), (z_1', z_2')\right) & \mapsto & z_1 z_1' + z_2 z_2' \end{array}$$

n'est pas positive : $\varphi\left((i,i),(i,i)\right) = 2i^2 = -2$. Toute la théorie bâtie jusqu'alors ne fonctionne plus. Dans le cas complexe, il faut parler de produit hermitien.

Définition 1.16 *Produit hermitien*[4]

Soit E un $\mathbb{C}$-espace vectoriel, et soit $\varphi \in \mathcal{F}\left(E^2, \mathbb{C}\right)$. On dit que φ est un *produit hermitien sur E* si :

(i) φ est sesquilinéaire :

$$\forall x, y, z \in E, \forall \lambda, \mu \in \mathbb{C}, \quad \begin{cases} \varphi\left(\lambda x + \mu y, z\right) = \overline{\lambda}\varphi\left(x, z\right) + \overline{\mu}\varphi\left(y, z\right) \\ \varphi\left(x, \lambda y + \mu z\right) = \lambda\varphi\left(x, y\right) + \mu\varphi\left(x, z\right) \end{cases}.$$

(ii) φ est hermitienne :

$$\forall x, y \in E, \quad \varphi\left(x, y\right) = \overline{\varphi\left(y, x\right)}.$$

(iii) φ est positive :

$$\forall x \in E, \quad \varphi\left(x, x\right) \geq 0.$$

(iv) φ est définie :

$$\forall x \in E, \quad \varphi\left(x, x\right) = 0 \iff x = 0.$$

Sans rentrer dans les détails, c'est avec une structure hermitienne complexe qu'on aura les mêmes résultats qu'un produit scalaire réel. on dira alors que E est un espace préhilbertien complexe si E est muni d'un produit hermitien.

Exemple 1.17 :
Le produit hermitien usuel sur $\mathbb{C}^n$ est

$$\varphi\left((z_1, \ldots, z_n), (z_1', \ldots, z_n')\right) = \sum_{i=1}^{n} \overline{z_i}.z_i'.$$

◇

4. Charles Hermite (1822-1901) : Mathématicien français.

II Orthogonalité

Les notions de produit scalaire et de norme sont le bon cadre pour parler d'angles et d'orthogonalité. C'est ce dernier concept auquel on s'intéresse maintenant.

Dans toute cette partie, E est un espace préhilbertien réel muni d'un produit scalaire $< \cdot, \cdot >$. On note $\| \cdot \|$ la norme euclidienne associée.

Tout ce qu'on raconte dans la suite dépend fortement du produit scalaire choisi au départ.

1. Familles orthogonales ou orthonormées

Définition 2.1 *Orthogonalité*

Deux vecteurs $x, y \in E$ sont dits *orthogonaux* si $< x, y >= 0$.

Une famille (ou un ensemble) A de vecteurs de E est dite *orthogonale* si, pour tous $x, y \in A$, $< x, y >= 0$.

Deux sous-espaces vectoriels F et G de E sont dits *orthogonaux* si, pour tous $x \in F, y \in G$, $< x, y >= 0$.

Définition 2.2 *Vecteur unitaire et famille orthonormée*

Un vecteur $x \in E$ est dit *unitaire* si $\|x\| = 1$.

Une famille (ou un ensemble) A de vecteurs de E est dite *orthonormée* si

$$\forall x, y \in A, \quad < x, y >= \begin{cases} 1 & \text{si } x = y \\ 0 & \text{sinon} \end{cases}.$$

Autrement dit, une famille orthonormée est une famille orthogonale dont tous les vecteurs sont unitaires.

Exemple 2.3 :
La base canonique de $\mathbb{R}^n$ est orthonormée pour le produit scalaire usuel. ◇

Proposition 2.4

Toute famille orthogonale dont les vecteurs sont non-nuls est libre. En particulier, toute famille orthonormée est libre.

Démonstration : Soit $A = (x_i)_{i \in I}$ une famille orthogonale (non-vide) dont les vecteurs sont non-nuls. Soit J une partie finie de I et soit $(\lambda_i)_{i \in J} \in \mathbb{R}^J$ tel que

$$x = \sum_{i \in J} \lambda_i x_i = 0.$$

Alors, pour tout $k \in J$, on a

$$< x, x_k >= \sum_{i \in J} \lambda_i < x_i, x_k >= \lambda_k \|x_k\| = 0.$$

Or $x_k \neq 0$ donc $\lambda_k = 0$. Ceci étant vrai pour tout $k \in J$, on en déduit que $(x_i)_{i \in J}$ est libre, et donc $(x_i)_{i \in I}$ est libre par définition.

Une famille orthonormée étant une famille orthogonale dont les vecteurs sont unitaires, ils sont en particulier non-nuls. $\square$

Proposition 2.5 *Méthode d'orthonormalisation de Gram*[5]*-Schmidt*[6]

Soient $p \in \mathbb{N}^*$ et $A = (x_1, \dots, x_p)$ une famille libre de E. Alors il existe une famille orthonormée $A' = (u_1, \dots, u_p)$ telle que

$$\forall k \in [\![1, p]\!], \quad \text{Vect}\,(x_1, \dots, x_k) = \text{Vect}\,(u_1, \dots, u_k)\,.$$

Démonstration : Remarquons que les x_i ne sont pas nuls car A est libre. On raisonne par récurrence finie en construisant la famille A' au fur et à mesure.

$\boxed{\text{Initialisation}}$ Posons $u_1 = \dfrac{x_1}{\|x_1\|}$. Alors la famille (u_1) est bien orthonormée et on a $\text{Vect}\,(x_1) = \text{Vect}\,(u_a)$.

$\boxed{\text{Hérédité}}$ Soit $k \in [\![1, p-1]\!]$. Supposons que $(u_1, \dots, u_k)$ soit orthonormée et vérifie

$$\forall i \in [\![1, k]\!], \quad \text{Vect}\,(x_1, \dots, x_i) = \text{Vect}\,(u_1, \dots, u_i)\,.$$

On va donc construire u_{k+1}. Posons $F = \text{Vect}\,(x_1, \dots, x_k) = \text{Vect}\,(u_1, \dots, u_k)$ et

$$p = \sum_{i=1}^{k} < x_{k+1}, u_i > u_i, \quad x' = x_{k+1} - p, \quad u_{k+1} = \frac{x'}{\|x'\|}.$$

Puisque $(x_1, \dots, x_{k+1})$ est libre, $x_{k+1} \notin F$, mais $p \in F$, donc $x' \neq 0$ et donc u_{k+1} est bien défini. Alors, pour tout $i \in [\![1, k]\!]$,

$$\begin{aligned}
< x', u_i > &=< x_{k+1}, u_i > - \left\langle \sum_{j=1}^{k} < x_{k+1}, u_j > u_j, u_i \right\rangle =< x_{k+1}, u_i > - \sum_{j=1}^{k} < x_{k+1}, u_j >< u_j, u_i > \\
&=< x_{k+1}, u_i > - < x_{k+1}, u_i > \|u_i\|^2 = 0, \\
< u_{k+1}, u_i > &= \frac{1}{\|x'\|} < x', u_i >= 0, \\
\|u_{k+1}\| &= \left\| \frac{x'}{\|x'\|} \right\| = \frac{\|x'\|}{\|x'\|} = 1.
\end{aligned}$$

La famille $(u_1, \dots, u_{k+1})$ est donc orthonormée. Puisque $p \in F$, $u_{k+1} \in \text{Vect}\,(x_1, \dots, x_{k+1})$ donc

$$\text{Vect}\,(u_1, \dots, u_{k+1}) \subseteq \text{Vect}\,(x_1, \dots, x_{k+1})\,.$$

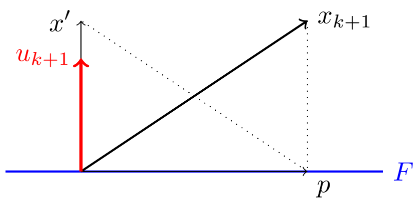
De même, $x_{k+1} \in \text{Vect}\,(u_1, \dots, u_{k+1})$ donc

$$\text{Vect}\,(x_1, \dots, x_{k+1}) \subseteq \text{Vect}\,(u_1, \dots, u_{k+1})\,, \quad \text{Vect}\,(u_1, \dots, u_{k+1}) = \text{Vect}\,(x_1, \dots, x_{k+1})\,.$$

$\square$

Remarque 2.6 : Hors son aspect théorique important, il convient de savoir mettre en place cet algorithme en pratique pour transformer une famille libre donnée en famille orthonormée. Le choix du vecteur p dans la preuve n'est pas anodin. On verra plus tard qu'il s'agit de la projection orthogonale du vecteur x_{k+1} sur F. Le vecteur x' est alors orthogonal à F, et u_{k+1} est une simple renormalisation de x'.

6. ? ? ? ? ?



◊

La famille orthonormée n'est pas unique (on peut l'assurer sous certaines conditions). C'est simple à comprendre : à chaque étape, on peut choisir u_{k+1} ou $-u_{k+1}$.

Théorème 2.7 *Théorème de Pythagore*[7]
Soit $A = (x_1, \ldots, x_p)$ une famille orthogonale. Alors

$$\left\| \sum_{k=1}^{p} x_k \right\|^2 = \sum_{k=1}^{p} \|x_k\|^2.$$

Démonstration : On a :

$$\left\| \sum_{k=1}^{p} x_k \right\|^2 = \left\langle \sum_{i=1}^{p} x_i, \sum_{j=1}^{p} x_j \right\rangle = \sum_{i=1}^{p} \left\langle x_i, \sum_{j=1}^{p} x_j \right\rangle = \sum_{1 \leq i,j \leq p} < x_i, x_j >$$
$$= \sum_{k=1}^{p} < x_k, x_k >= \sum_{k=1}^{p} \|x_k\|^2$$

□

2. Orthogonal d'une partie

Définition/Proposition 2.8 *Orthogonal d'une partie*
Soit A une partie de E. On appelle orthogonal de A l'ensemble

$$A^\perp = \{x \in E / \forall a \in A, < x, a >= 0\}.$$

Alors $A^\perp$ est un sous-espace vectoriel de E.

Démonstration : D'abord, $A^\perp \subseteq E$ par définition, et E est bien un espace vectoriel. Ensuite, $0 \in A^\perp$ de manière évidente. Enfin, pour tous $x, y \in A^\perp$ et $\lambda, \mu \in \mathbb{R}$,

$$\forall a \in A, \quad < \lambda x + \mu y, a >= \lambda < x, a > +\mu < y, a >= 0,$$

donc $\lambda x + \mu y \in A^\perp$. Donc $A^\perp$ est un sous-espace vectoriel de E. □

7. Pythagore (vers 500 av. J.C.) : Mathématicien grec.

Proposition 2.9

Soit A une partie de E. Alors $A^{\perp} = (\text{Vect } A)^{\perp}$.

Démonstration : Puisque $A \subseteq \text{Vect } A$, on en déduit directement par la définition que $(\text{Vect } A)^{\perp} \subseteq A^{\perp}$. Soit $x \in A^{\perp}$, soit $a \in \text{Vect } A$. Alors il existe $a_1, \ldots, a_p \in A$ et $\lambda_1, \ldots, \lambda_p \in \mathbb{R}$ tels que

$$a = \sum_{k=1}^{p} \lambda_k a_k, \quad < x, a >= \left\langle x, \sum_{k=1}^{p} \lambda_k a_k \right\rangle = \sum_{k=1}^{p} \lambda_k < x, a_k >= 0.$$

Donc $x \in (\text{Vect } A)^{\perp}$, donc $A^{\perp} = (\text{Vect } A)^{\perp}$. $\square$

Exercice 2.10 :

Soit $E = \mathcal{C}^0([0,1], \mathbb{R})$ muni du produit scalaire défini par

$$\forall f, g \in E, \quad < f, g >= \int_0^1 f(t)\, g(t)\, dt.$$

Soit $F = \{f \in F / f(0) = 0\}$.

1. Montrer que F est un hyperplan de E.
2. Montrer que $F^{\perp} = \{0\}$.

Réponse

1. $F = \ker \varphi$ avec $\varphi : f \mapsto f(0)$. L'évaluation d'une fonction est classiquement une forme linéaire. De plus $\varphi\left(\widetilde{1}\right) = 1 \neq 0$ donc $\varphi \neq 0$; on en déduit que F est un hyperplan de E.
2. Soit $f \in F^{\perp}$. Alors on remarque que $\widetilde{f} : x \mapsto x f(x) \in F$. En particulier

$$< \widetilde{f}, f >= \int_0^1 x f(x)^2\, dx = 0.$$

Or la fonction $x \mapsto x f(x)^2$ est continue, positive et d'intégrale nulle sur $[0,1]$, on en déduit qu'elle est identiquement nulle. Donc

$$\forall x > 0, \quad f(x)^2 = 0, \quad f(x) = 0.$$

Par continuité, on a aussi $f(0) = 0$ et donc $f = 0$. D'où $F^{\perp} = \{0\}$.

$\diamondsuit$

3. Espaces euclidiens

Définition 2.11 *Espace euclidien*[8]

Soit E un $\mathbb{R}$-espace vectoriel. On dit que E est un *espace euclidien* si E est muni d'un produit scalaire et si E est de dimension finie. Autrement dit, c'est un espace préhilbertien réel de dimension finie.

Remarque 2.12 : Tout $\mathbb{R}$-espace vectoriel de dimension finie E est un espace euclidien . La notion d'orthogonalité dans E dépendra alors de la base choisie au départ. En effet, il faut montrer que E admet un produit scalaire. E possède une base $B = (e_1, \dots, e_n)$. Pour tous $x, y \in E$ de coordonnées respectives dans la base B (x_1, x_2) et (y_1, y_2), on définit

$$f(x, y) = \sum_{i=1}^{n} x_i y_i.$$

Alors $f \in \mathcal{F}(E^2, \mathbb{R})$ et on peut montrer sans problème que f est un produit scalaire : il suffit de copier la preuve de la proposition 1.4. ♢

Proposition 2.13

Tout espace euclidien admet une base orthonormée.

Démonstration : Si E est un espace euclidien, alors E possède une base B. En appliquant l'algorithme de Gram-Schmidt à B (qui est libre), on obtient une famille B' orthonormée (donc libre). De plus $E = \operatorname{Vect} B = \operatorname{Vect} B'$ donc B' est génératrice, c'est donc une base orthonormée de E. □

Proposition 2.14

Soit F un sous-espace vectoriel d'un espace euclidien E. Alors :

(i) $F \oplus F^{\perp} = E$.
(ii) $\dim(F^{\perp}) = \dim E - \dim F$.
(iii) $(F^{\perp})^{\perp} = F$.

Démonstration : (i) F étant lui aussi un espace euclidien, il possède donc une base orthonormée $B_F = (u_1, \dots, u_p)$.

$\boxed{F \oplus G = E}$ Soit $x \in E$. Guidés par la méthode d'orthonormalisation de Gram-Schmidt, on pose

$$p = \sum_{k=1}^{p} < x, u_k > u_k, \quad x' = x - p.$$

Alors il est évident que $x = x' + p$ et que $p \in \operatorname{Vect}(u_1, \dots, u_k) = F$. D'autre part, pour tout $i \in [\![1, p]\!]$,

$$< x', u_i > = < x, u_i > - \left\langle \sum_{j=1}^{p} < x, u_j > u_j, u_i \right\rangle = < x, u_i > - \sum_{j=1}^{p} < x, u_j > < u_j, u_i > = 0.$$

Donc $x' \in (u_1, \dots, u_p)^{\perp} = (\operatorname{Vect}(u_1, \dots, u_p))^{\perp} = F^{\perp}$. On en déduit que $x \in F + F^{\perp}$ et donc $F + F^{\perp} = E$.

$\boxed{F \cap F^{\perp} = \{0\}}$ Soit $x \in F \cap F^{\perp}$. Alors $< x, x > = 0$ (car $x \in F$ et $x \in F^{\perp}$) et donc $x = 0$, donc $F \cap F^{\perp} = \{0\}$.

(ii) C'est une conséquence directe du point (i).

(iii) Soit $x \in F$. Alors, pour tout $y \in F^{\perp}$, $< x, y > = 0$ donc $x \in (F^{\perp})^{\perp}$. Donc $F \subseteq (F^{\perp})^{\perp}$. D'après le point (ii), on a

$$\dim (F^{\perp})^{\perp} = \dim E - \dim F^{\perp} = \dim F, \quad F = (F^{\perp})^{\perp}$$

□

8. Euclide (vers 300 av. J.C.) : Mathématicien grec.

Ces propriétés ne sont pas vraies en dimension infinie (c'est-à-dire pour un espace préhilbertien non-euclidien). On s'en convaincra à l'aide l'exercice 2.10.

Exercice 2.15 :
Soient F et G des sous-espaces vectoriels d'un espace euclidien E.

1. Montrer que si $F \subseteq G$ alors $G^\perp \subseteq F^\perp$.
2. (a) Montrer que $(F+G)^\perp = F^\perp \cap G^\perp$.
   (b) Montrer que $(F \cap G)^\perp = F^\perp + G^\perp$.

Réponse

1. Supposons que $F \subseteq G$. Alors soit $x \in G^\perp$. Donc pour tout $y \in G$, $< x, y >= 0$. En particulier, pour tout $y \in F$, $< x, y >= 0$, et donc $x \in F^\perp$. D'où $G^\perp \subseteq F^\perp$.
2. (a) $F \subseteq F + G$ donc d'après la question 1, $(F+G)^\perp \subseteq F^\perp$. De même, $(F+G)^\perp \subseteq G^\perp$. On en déduit que $(F+G)^\perp \subseteq F^\perp \cap G^\perp$. Soit $x \in F^\perp \cap G^\perp$. Pour tout $y \in F+G$, il existe $(y_F, y_G) \in F \times G$ tel que $y = y_F + y_G$. Alors
$$< x, y >=< x, y_F + y_G >=< x, y_F > + < x, y_G >= 0 + 0 = 0.$$
Donc $x \in (F+G)^\perp$ et donc $(F+G)^\perp = F^\perp \cap G^\perp$.
   (b) D'après la question précédente, et puisque $\left(F^\perp\right)^\perp = F$ et $\left(G^\perp\right)^\perp = G$,
$$(F \cap G)^\perp = \left(\left(F^\perp\right)^\perp \cap \left(G^\perp\right)^\perp\right)^\perp = \left(\left(F^\perp + G^\perp\right)^\perp\right)^\perp = F^\perp + G^\perp.$$

♢

Définition 2.16 *Projecteur et symétrie orthogonale*
Soit F un sous-espace vectoriel d'un espace euclidien E. On appelle *projecteur orthogonale* (resp. *symétrie orthogonale*) le projecteur (resp. la symétrie) sur F parallèlement à $F^\perp$.

Ces deux applications sont bien définies car, si E est un espace euclidien, on a bien $F \oplus F^\perp = E$.

Proposition 2.17
Soit F un sous-espace vectoriel d'un espace euclidien E. On définit respectivement p et s le projecteur et la symétrie orthogonaux sur F. Soit $B = (e_1, \ldots, e_p)$ une base orthonormée de F. Alors, pour tout $x \in E$,
$$p(x) = \sum_{k=1}^{p} < x, e_k > e_k, \quad s(x) = 2\sum_{k=1}^{p} < x, e_k > e_k - x.$$

Démonstration : Soit $f : x \mapsto \sum_{k=1}^{p} < x, e_k > e_k$. On va montrer que f est le projecteur orthogonal sur F. Il est clair que $\operatorname{Im} f \subseteq \operatorname{Vect}(e_k) = F$ et, pour tout $k \in [\![1, p]\!]$, on a
$$f(e_k) = \sum_{i=1}^{p} < e_k, e_i > e_i = e_k, \quad f_{\|F} = \mathrm{Id}_F\,.$$

Donc $f^2 = f$, donc f est un projecteur. On a $\operatorname{Im} f \subseteq F$ et, pour tout $k \in [\![1,p]\!]$, $f(e_k) = e_k$ donc $e_k \in \operatorname{Im} f$ donc $F \subseteq \operatorname{Im} f$. D'où $\operatorname{Im} f = F$. Soit $x \in E$. Alors

$$\begin{aligned} x \in \ker F &\iff \sum_{k=1}^{p} < x, e_k > e_k = 0 \iff \forall j \in [\![1,p]\!], < x, e_k >= 0 \qquad \text{(car } B \text{ est libre)} \\ &\iff x \in B^{\perp} \iff x \in \operatorname{Vect}(B)^{\perp} \\ &\iff x \in F^{\perp}. \end{aligned}$$

Donc $\ker f = F^{\perp}$. Donc f est la projection sur F parallèlement à $F^{\perp}$. On en déduit que $f = p$. Puisque $s = 2p - \operatorname{Id}$, la formule pour s est alors évidente. □

Exercice 2.18 :
On considère $E = \mathbb{R}_4[X]$.

1. Pour $P, Q \in E$, tels que $P = \sum_{k=0}^{4} a_k X^k$ et $Q = \sum_{k=0}^{4} b_k X^k$, on note $< P, Q >= \sum_{k=0}^{n} 2^k a_k b_k$.
   (a) Montrer que $< \cdot, \cdot >$ est un produit scalaire sur E.
   (b) Déterminer $\mathbb{R}_0[X]^{\perp}$.
   (c) Déterminer l'expression du projecteur orthogonal sur $\mathbb{R}_2[X]$.
2. Mêmes questions avec $< P, Q >= \int_{-1}^{1} P(t)\, Q(t)\, dt$.

Réponse

1. (a) Exactement comme pour le produit scalaire usuel.

   (b) Soit $P = \sum_{k=0}^{4} a_k X^k \in E$. Alors

   $$P \in \mathbb{R}_0[X]^{\perp} \iff \forall \lambda \in \mathbb{K}, \quad \lambda a_0 = 0 \iff a_0 = 0.$$

   On en déduit que $\mathbb{R}_0[X]^{\perp} = \operatorname{Vect}\left(X, X^2, X^3, X^4\right)$.

   (c) Notons π la projection orthogonale sur $\mathbb{R}_1[X]$. Il faut d'abord trouver une base orthonormée de $\mathbb{R}_1[X]$. Notons $B = (1, X)$. Alors, en appliquant le procédé d'orthonormalisation de Gram-Schmidt à B, on trouve une nouvelle base orthonormée $B' = \left(1, \frac{X}{\sqrt{2}}, \frac{X^2}{2}\right)$. On en déduit que, pour tout $P = \sum_{k=0}^{4} a_k X^k \in E$,

   $$\pi(P) =< P, 1 > 1 + \left\langle P, \frac{X}{\sqrt{2}} \right\rangle \frac{X}{\sqrt{2}} + \left\langle P, \frac{X^2}{2} \right\rangle \frac{X^2}{2} = a_0 + a_1 X + a_2 X^2.$$

2. (a) On sait que $(f, g) \mapsto \int_{-1}^{1} fg$ est un produit scalaire sur $\mathcal{C}^0([-1,1], \mathbb{R})$. Puisque E est un sous-espace vectoriel de $\mathcal{C}^0([-1,1], \mathbb{R})$, $< \cdot, \cdot >$ est un produit scalaire sur E.

   (b) Soit $P = \sum_{k=0}^{4} a_k X^k \in E$. Alors

   $$\begin{aligned} P \in \mathbb{R}_0[X]^{\perp} &\iff < P, 1 >= 0 \iff \int_{-1}^{1} P(t)\, dt = 0 \\ &\iff 2a_0 + \frac{2}{3} a_2 + \frac{2}{5} a_4 = 0 \\ &\iff P \in \operatorname{Vect}\left(3X^2 - 1, 5X^4 - 1, X, X^3\right) \end{aligned}$$

D'où $\mathbb{R}_0[X]^\perp = \text{Vect}\left(3X^2-1, 5X^4-1, X, X^3\right)$.

(c) Notons π la projection orthogonale sur $\mathbb{R}_1[X]$. Il faut d'abord trouver une base orthonormée de $\mathbb{R}_1[X]$. Notons $B=(1,X)$. Alors, en appliquant le procédé d'orthonormalisation de Gram-Schmidt à B, on trouve une nouvelle base orthonormée $B' = \left(\frac{1}{\sqrt{2}}, \sqrt{\frac{3}{2}}X, \sqrt{\frac{2}{2}}X^2\right)$. On en déduit que, pour tout $P = \sum_{k=0}^{4} a_k X^k \in E$,

$$\pi(P) =< P, \frac{1}{\sqrt{2}} > \frac{1}{\sqrt{2}} + \left\langle P, \sqrt{\frac{3}{2}}X \right\rangle \sqrt{\frac{3}{2}}X + \left\langle P, \sqrt{\frac{2}{2}}X^2 \right\rangle \sqrt{\frac{2}{2}}X^2 = .$$

◊

Pour aller plus loin

- Espaces normés, espaces métriques