Cours de mathématiques (MPSI)

Arnaud Girand

4 juin 2025

Table des matières

Premier semestre

Notions de logique

Ce qui suit a pour vocation d'introduire quelques concepts absolument fondamentaux sans lesquels faire des mathématiques serait bien difficile. Il n'est pas attendu une compréhension fine des théories sous–jacentes.

1.⁻ Propositions

a) C'est quoi ?

Définition 0.1. Une **assertion** est un énoncé, pouvant être vrai ou faux, mettant en relation des objets mathématiques.

➠ **Exemple 0.1.**
- "$2 + 2 = 12$" est une assertion.
- "Toute suite convergente est bornée" également.

Convention. Une assertion est toujours vraie **ou** fausse, et jamais les deux à la fois.

Définition 0.2. Faire des mathématiques, c'est énoncer (et démontrer !) des assertions vraies, appelées **propositions**.

Définition 0.3. Un peu de vocabulaire, en vrac.
- Un **théorème** est une proposition importante.
- Un **lemme** est une proposition qui sert (dans le cadre où elle est énoncée) principalement à démontrer une autre proposition.
- Un **corollaire** est une proposition qui découle immédiatement d'une autre proposition.
- Un **axiome** est une assertion que l'on **décide** vraie.

Définition 0.4. On appelle **prédicat** d'une variable x toute assertion $P(x)$ dépendant de celle–ci.

b) Assertions équivalentes

Définition 0.5. Soient P et Q deux assertions. On dira que P et Q sont équivalentes si elles ont exactement les mêmes valeurs de vérité, c'est à dire si elles sont toutes deux vraies ou toutes deux fausses.

Notation. $P \Leftrightarrow Q$

Exemple 0.2.
- $(1 = 0) \Leftrightarrow 2$ est impair.
- Si n est un entier, (n est pair) $\Leftrightarrow$ ($n + 1$ est impair).

2.⁻ Connecteurs logiques

Les connecteurs jouent un rôle fondamental en logique puisqu'ils permettent de créer de nouvelles assertions à partir de assertions existantes (sans eux, les mathématiques seraient relativement bornées...).

a) Le connecteur "ET"

Définition 0.6. Soient P et Q deux assertions. On définit l'assertion "P et Q" comme étant vraie si et seulement si P et Q sont toutes deux vraies.

Notation. $P \wedge Q$

Exemple 0.3.
- $(1 + 1 = 2) \wedge (2 + 1 = 3)$ est vraie.
- $(1 + 1 = 0) \wedge (2 + 1 = 3)$ est fausse.

Proposition 0.1. Soient P, Q et R des assertions. Alors :
(i) $P \wedge P \Leftrightarrow P$ **[idempotence]** ;
(ii) $P \wedge Q \Leftrightarrow Q \wedge P$ **[commutativité]** ;
(iii) $P \wedge (Q \wedge R) \Leftrightarrow (P \wedge Q) \wedge R$ **[associativité]**.

Remarque 0.1. Le troisième point de cette assertion donne un sens à la notation $P \wedge Q \wedge R$ qui désigne arbitrairement $P \wedge (Q \wedge R)$ ou $(P \wedge Q) \wedge R$.

b) Le connecteur "OU"

Définition 0.7. Soient P et Q deux assertions. On définit l'assertion "P ou Q" comme étant vraie si et seulement si P est vraie et/ou Q est vraie.

Notation. $P \vee Q$.

✌ **Remarque 0.2.** On parle aussi de "OU inclusif", par opposition au "OU exclusif".

➠ **Exemple 0.4.** $(1+1=0) \vee (1+1=2)$ est vraie.

Proposition 0.2. Soient P, Q et R des assertions. Alors on a :

(i) $P \vee P \Leftrightarrow P$;

(ii) $P \vee Q \Leftrightarrow Q \vee P$;

(iii) $P \vee (Q \vee R) \Leftrightarrow (P \vee Q) \vee R$;

(iv) $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$ **[distributivité]** ;

(v) $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$ **[distributivité]**.

✌ **Remarque 0.3.** Le troisième point de cette assertion donne un sens à la notation $P \vee Q \vee R$ qui désigne arbitrairement $P \vee (Q \vee R)$ ou $(P \vee Q) \vee R$.

c) Le connecteur "NON"

Définition 0.8. Soit P une assertion. On définit l'assertion "Non P" comme étant vraie si et seulement si P est fausse.

Notation. $\overline{P}$

Proposition 0.3. Soit P une assertion. Alors :

(i) $\overline{\overline{P}} \Leftrightarrow P$;

(ii) $\overline{(P \wedge \overline{P})}$ est vraie **[non–contradiction]** ;

(iii) $P \vee \overline{P}$ est vraie **[tiers exclus]**.

Le théorème suivant est du à Augustus de Morgan (1806—1871), mathématicien et logicien britannique.

Théorème 0.4 (De Morgan)**.**
Soient P et Q deux assertions. Alors :

(i) $\overline{P \vee Q} = \overline{P} \wedge \overline{Q}$

(ii) $\overline{P \wedge Q} = \overline{P} \vee \overline{Q}$

✍ **Exercice .1.** Soient P et Q deux assertions. On définit l'assertion $P \otimes Q = (P \wedge \overline{Q}) \vee (\overline{P} \wedge Q)$ (ce nouveau connecteur est appelé "**OU exclusif**"). Dresser la table de vérité de $\otimes$.

d) Le connecteur "IMPLIQUE"

Définition 0.9. Soient P et Q deux assertions. On définit l'assertion "P implique Q" comme étant fausse si et seulement si P est vraie alors que Q est fausse.

Notation. $P \Rightarrow Q$

✌ **Remarque 0.4.** On notera que "faux" implique tout ce que l'on veut...

➠ **Exemple 0.5.**
— $(1 = 0) \Rightarrow$ (J'ai mangé une pomme hier à 21h)
— (3 est pair) $\Rightarrow$ (2 est pair)
— Si f est une fonction de $\mathbb{R}$ dans $\mathbb{R}$, (f est dérivable) $\Rightarrow$ (f est continue)

Proposition 0.5. Soient P, Q et R des assertions. Alors on a :
(i) $(P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$ [Transitivité]
(ii) $(P \Leftrightarrow Q) \Leftrightarrow ((P \Rightarrow Q) \wedge (Q \Rightarrow P))$
(iii) $(P \Rightarrow Q) \Leftrightarrow \overline{P} \vee Q$
(iv) $(P \vee Q) \Leftrightarrow (\overline{P} \Rightarrow Q)$
(v) $\overline{(P \Rightarrow Q)} \Leftrightarrow P \wedge \overline{Q}$
(vi) $(P \Rightarrow Q) \Leftrightarrow (\overline{Q} \Rightarrow \overline{P})$ [Contraposée]
(vii) $(\overline{P} \Rightarrow (Q \wedge \overline{Q})) \Rightarrow P$ [Démonstration par l'absurde]

3.⁻ Méthodes de démonstration

Énoncer des assertions, c'est bien. Les démontrer c'est mieux. Les démontrer proprement, c'est encore mieux ! Voici une sélection de quelques-unes des méthodes les plus usitées dans tous les domaines des mathématiques...

a) Comment démontrer que $P \Rightarrow Q$?

Cette méthode de démonstration est absolument primordiale. On voit trop souvent des rédactions du genre "$P \Rightarrow R \Rightarrow S \Rightarrow Q \Rightarrow$ ok"... La première règle à respecter lorsque l'on veut démontrer une implication est de **ne pas utiliser le symbole "$\Rightarrow$"** ! En effet, comme l'on vient de le voir, **celui-ci est un connecteur logique qui n'a absolument rien à voir avec le mot "donc"**. Pour montrer que $P \Rightarrow Q$, le mieux est de suivre la méthode suivante :

1. Supposer que P est vraie.
2. Démontrer qu'alors Q est vraie.

Cette approche est en règle générale la seule valable...

Exemple "idiot" :
On veut démontrer "$(2 + 3 = 6) \Rightarrow$ (16 est un carré parfait)".

1. Supposons que $2{+}3 = 6$.

2. $16 = 4 \times 4$ donc 16 est un carré parfait. D'où le résultat.

Cet exemple n'a aucun intérêt mathématique étant donné que l'on a pas fait usage de l'hypothèse (qui par ailleurs à la facheuse propriété d'être fausse...) ! Lorsque l'on arrive à démontrer que $P \Rightarrow Q$ sans avoir utilisé la véracité de P, c'est que l'on a fort vraisemblablement commis une erreur...

b) Comment démontrer que $P \Leftrightarrow Q$?

Pour démontrer une équivalence, il faut et il suffit de montrer deux implications. Ainsi, on procède en 2 temps :

1. On montre que $P \Rightarrow Q$.
2. On montre que $Q \Rightarrow P$.

Ce type de rédaction à l'immense avantage d'être bien moins "casse-gueule" que les suites (plus ou moins logiques, hélas...) de symboles " $\Leftrightarrow$ "...

c) Comment démontrer que $P \vee Q$?

Sur le papier, ce genre de choses est excessivement simple. En pratique, il donne lieu à des raisonnements souvent assez brouillons. La meilleure méthode pour démontrer ce genre d'assertion est de procéder de la façon suivante : comme on a vu que $(P \vee Q) \Leftrightarrow (\overline{P} \Rightarrow Q)$, démontrer une assertion du type "soit P, soit Q" peut se faire en suivant ce plan :

1. Supposer que P est fausse.
2. Montrer qu'alors Q est vraie.

✍ **Exercice .2.** Soit $x \in [0, 1[$ démontrer que :

$$(x = 0) \vee ((x > 0) \wedge (x < 1)) .$$

d) Comment démontrer que $P \wedge Q$?

Lorsque l'on doit démontrer "P et Q", le mieux reste encore... de démontrer P **et** de démontrer Q ! Attention cependant à bien séparer les deux démonstrations, il ne s'agit pas de montrer $P \Rightarrow Q$...

e) Contraposée

Comme $(P \Rightarrow Q) \Leftrightarrow (\overline{Q} \Rightarrow \overline{P})$, il est possible de démontrer $P \Rightarrow Q$ en démontrant $\overline{Q} \Rightarrow \overline{P}$.

✍ **Exercice .3.** Démontrer que si a est un nombre réel tel que

$$\forall \varepsilon > 0, \quad |a| \leq \varepsilon$$

alors a est nécessairement nul.

f) Démonstration par l'absurde

On a vu que $(\overline{P} \Rightarrow (Q \wedge \overline{Q})) \Rightarrow P$. Ainsi, si on suppose "Non P" et que l'on aboutit à une contradiction, alors P est vraie. Il est recommandé de ne pas abuser de cette méthode.

✍ **Exercice .4.** Démontrer qu'un nombre entier ne peut être à la fois pair et impair.

g) Démonstration par analyse–synthèse

Lorsque l'on se retrouve face à une question ouverte, il peut être intéressant de supposer trouvée une solution au problème pour en déduire des conditions nécessaires dessus (l'analyse), avant de vérifier qu'elles sont suffisantes (la synthèse).

La partie analyse assure l'unicité du ou des objets étudiés, la synthèse en démontre (ou pas, auquel cas on peut basculer sur une démonstration par l'absurde à peu de frais) l'existence.

✍ **Exercice .5.** Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction. Démontrer qu'il existe une unique écriture de f comme somme d'une fonction paire et d'une fonction impaire.

Chapitre I

Ensembles

1.⁻ C'est quoi ?

a) Ensembles, quantificateurs

Définition I.1. On appelle **ensemble** toute collection (non ordonnée) d'objets distincts, appelés éléments.

Notation. $a \in E$ signifie que l'objet a est un élément de l'ensemble E.

La question qui va nous occuper dans un premier temps est la suivante : **comment décrire un ensemble ?** De prime abord, deux choix s'offrent à nous.

1. **Lister les éléments de l'ensemble.**

$$E = \{\clubsuit, \nabla, 4\}.$$

2. **Caractériser l'ensemble par une propriété.**

$$E = \{\underbrace{x \in \mathbb{R}}_{\text{cas de base}} \mid \underbrace{x > 0}_{\text{prédicat}}\}.$$

3. **Comme image d'une application.**

$$E = \{x^2 + 1 \mid x \in [0, 1]\}.$$

Vocabulaire. Un ensemble ne contenant qu'un seul élément est appelé **singleton.**

◇ Quantificateurs

Définition I.2. On définit les deux **quantificateurs suivants** :

1. le **quantificateur universel**, noté "$\forall$"
2. le **quantificateur existentiel**, noté "$\exists$"

On appelle **phrase** (ou expression) **quantifiée** toute propriété faisant intervenir des quantificateurs.

Signification des quantificateurs :
Soit P une assertion portant sur les éléments d'un ensemble $\mathbb{E}$. On définit alors de nouvelles assertions :

1. $\forall x \in \mathbb{E}, P(x)$, qui signifie que tous les éléments de $\mathbb{E}$ vérifient la propriété P.
2. $\exists x \in \mathbb{E}, P(x)$, qui signifie qu'il existe un élément de $\mathbb{E}$ qui vérifie la propriété P.

De plus, si un **unique** élément de $\mathbb{E}$ vérifie P, on note : $\exists! x \in \mathbb{E}, P(x)$.

➠ **Exemple I.1.**

$$F = \{n \in \mathbb{N} \,|\, \exists p \in \mathbb{N},\ n = 2p\}$$

décrit l'ensemble des entiers naturels pairs.

◇ Échange de quantificateurs

Soit P une propriété dépendant de deux paramètres $x \in \mathbb{E}$ et $y \in \mathbb{F}$. Alors les deux propriétés suivantes sont équivalentes :

1. $\exists x \in \mathbb{E}, \exists y \in \mathbb{F}, P(x, y)$
2. $\exists y \in \mathbb{F}, \exists x \in \mathbb{E}, P(x, y)$

Il est ainsi possible au sein d'une phrase quantifiée d'intervertir deux quantificateurs existentiels sans en changer le sens. De la même façon, sont équivalents :

1. $\forall x \in \mathbb{E}, \forall y \in \mathbb{F}, P(x, y)$
2. $\forall y \in \mathbb{F}, \forall x \in \mathbb{E}, P(x, y)$

➠ **Exemple I.2.** Pour $x, y \in \mathbb{Z}$, on définit $P(x, y) = x|y$.

En revanche, il est **impossible** d'échanger la place d'un quantificateur universel et d'un quantificateur existentiel, comme nous le verrons ci-après. Les deux équivalences ci dessus donnent un sens aux notations "$\exists (x, y) \in \mathbb{E} \times \mathbb{F}, P(x, y)$" et "$\forall (x, y) \in \mathbb{E} \times \mathbb{F}, P(x, y)$".

◇ Dépendances

Le problème des dépendances dans les phrases quantifiées est très important en mathématiques. Par exemple, considérons les deux assertions suivantes, portant sur une fonction $f : \mathbb{R} \to \mathbb{R}$:

(1) $\forall x \in \mathbb{R}, \quad \exists y \in \mathbb{R}_+, \quad y = x^2$;

(2) $\exists y \in \mathbb{R}_+, \quad \forall x \in \mathbb{R}, \quad y = x^2$.

Ces deux assertions ne sont **absolument pas** équivalentes ! Pourtant, la seule différence entre ces deux assertions est la place occupée par le "$\forall x \in \mathbb{R}$"...

Le noeud du problème réside dans les **dépendances**. Dans l'assertion (1), le réel y dépend de x : en effet, ce que signifie cette phrase quantifiée, c'est que si on fixe x dans $\mathbb{R}$, **alors** on va pouvoir trouver un y tel que la propriété soit vérifiée. Tandis que (2) nous indique que l'on va pouvoir trouver y tel que la propriété soit vraie pour tous x.

Conséquence :
Lorsque l'on manipule des phrases quantifiées, il faut apporter une attention toute particulière aux dépendances des paramètres entre eux afin d'éviter de monumentales erreurs d'interprétation. Une règle efficace en pratique est la suivante : les "$\exists$" dépendent des "$\forall$" qui les précédent. Par exemple, dans $\exists z,\ \forall t,\ \exists q, P(z,t,q)$ le paramètre q dépend de t alors que z et t ne dépendent d'aucun des autres paramètres (et ne sont pas dépendant entre eux).

◇ Difficultés

Cette définition naïve n'est pas sans risques. L'une des complications rencontrées, appelée **paradoxe de Russel**, peut s'énoncer de la façon suivante : soit $\mathscr{E} = \{E \text{ ensemble} \,|\, E \notin E\}$; a–t–on $\mathscr{E} \in \mathscr{E}$? Peu importe que l'on suppose que ce soit vrai ou faux, on arrive à une contradiction.

Pour éviter ce type de difficulté, on prendra toujours gare à définir nos ensembles à partir d'un cas de base précis, clair et sans ambiguïté.

b) Concepts élémentaires de théorie des ensembles

◇ Égalité

Axiome A. Deux ensembles sont égaux si et seulement si ils ont les mêmes éléments.

➠ **Exemple I.3.**
— $\{0,1,2\} = \{2,0,1\}$;
— $\{1,2\} \neq \{2,12\}$.

Par conséquent, la **seule** méthode valable pour démontrer que deux ensembles A et B sont égaux est la suivante :
— se donner $x \in A$ et démontrer que $x \in B$;
— réciproquement, se donner $x \in B$ et montrer que $x \in A$.

◇ Inclusion

Définition I.3. On dit qu'un ensemble A est **inclus** dans un ensemble B si $\forall x \in A,\ x \in B$.

Notation. $A \subset B$

✖ **Attention :** ne pas confondre inclusion et appartenance : $1 \in \mathbb{R}$, $\{1\} \subset \mathbb{R}$.

Proposition I.1. Soient A, B, C des ensembles. Alors :
(i) $A \subset A$ **[reflexivité]** ;
(ii) $(A \subset B) \wedge (B \subset A) \Leftrightarrow (A = B)$ **[antisymétrie]** ;
(iii) $(A \subset B) \wedge (B \subset C) \Rightarrow (A \subset C)$ **[transitivité]**.

Démonstration. Immédiat. □

✌ **Remarque I.1.** Le point (ii) nous indique que pour démontrer une égalité d'ensembles, il faut démontrer deux inclusions. **À retenir.**

⋄ Zoologie des ensembles classiques

Axiome B. Il existe un ensemble ne contenant aucun élément, appelé **ensemble vide** et noté $\emptyset$.

✌ **Remarque I.2.** Si P est un prédicat faux sur un ensemble E, alors $\{x \in E \mid P(x)\} = \emptyset$. Par exemple, $\emptyset = \{x \in \mathbb{R} \mid x^2 < 0\}$.

Profitons de ce paragraphe pour rappeler quelques définitions logiquement vues dans une vie antérieure.

— $\mathbb{N}$ est l'ensemble des entiers naturels.

— $\mathbb{Z}$ est l'ensemble des entiers relatifs, *i.e*

$$\mathbb{Z} = \{a - b \mid a, b \in \mathbb{N}\} .$$

— $\mathbb{D}$ est l'ensemble des nombres décimaux, soit :

$$\mathbb{D} = \left\{ \frac{m}{10^n} \,\middle|\, m \in \mathbb{Z},\, n \in \mathbb{N} \right\} .$$

— $\mathbb{Q}$ est l'ensemble des nombres rationnels, soit :

$$\mathbb{Q} = \left\{ \frac{p}{q} \,\middle|\, p \in \mathbb{Z},\, q \in \mathbb{N}^* \right\} .$$

— $\mathbb{R}$ est l'ensemble des nombres réels.

— $\mathbb{C}$ est l'ensemble des nombres complexes, soit :

$$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$$

où i est tel que $i^2 = -1$.

Rappelons au passage que l'on a la chaine d'inclusions suivante :

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

⋄ Parties d'un ensemble

Axiome C. Soit E un ensemble. Alors il existe un unique ensemble, noté $\mathscr{P}(E)$, tel que :

$$A \in \mathscr{P}(E) \Leftrightarrow A \subset E .$$

Cet ensemble est appelé **ensembles des parties de** E.

✌ **Remarque I.3.**

— Il s'agit donc d'un ensemble d'ensembles ...

— Quel que soit l'ensemble E, on a toujours $\emptyset \in \mathscr{P}(E)$ et $E \in \mathscr{P}(E)$.

➠ **Exemple I.4.**

— $\mathscr{P}(\emptyset) = \{\emptyset, \{\emptyset\}\}$.

— $\mathscr{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

✌ **Remarque I.4.** La construction "moderne" de l'ensemble $\mathbb{N}$ des entiers naturels s'obtient via les "ensembles parties itérés" de l'ensemble vide, *i.e* les $\mathscr{P}(\mathscr{P}(\dots\dots\mathscr{P}(\emptyset)))$.

2.– Opérations sur les ensembles

a) Réunion

Définition I.4. Soient A, B deux sous–ensembles d'un ensemble E ; on appelle **réunion** de A et B l'ensemble

$$\{x \in E \,|\, (x \in A) \vee (x \in B)\} .$$

Notation. $A \cup B$

Exemple I.5. $\{1,2\} \cup \{2,7\} = \{1,2,7\}$.

Remarque I.5. De façon plus générale, si $(A_i)_{i\in I}$ est une famille d'ensembles indexée par un ensemble I, ce qui signifie qu'à chaque élément i de I on associe un unique sous–ensemble A_i d'un ensemble E, on pose :

$$\bigcup_{i\in I} A_i = \{x \in E \,|\, \exists i \in I,\, x \in A_i\} .$$

Il s'agit du plus petit sous–ensemble de E contenant tous les A_i. Notons que I peut tout à fait être infini ; on peut par exemple montrer assez aisément (démontrer deux inclusions) que

$$\bigcup_{n\in\mathbb{N}^*} \left[0, 1 - \frac{1}{n}\right[= [0,1[.$$

Notation. Si $I = \{1, \dots, n\}$, on notera $\bigcup\limits_{i=1}^{n} A_i$ la réunion $\bigcup\limits_{i\in I} A_i$.

Proposition I.2. Soient A, B, C, D quatre ensembles. Alors :

(i) $A \cup B = B \cup A$ **[commutativité]** ;

(ii) $(A \cup B) \cup C = A \cup (B \cup C)$ **[associativité]** ;

(iii) $A \cup \emptyset = A$ **[$\emptyset$ est neutre]** ;

(iv) $A \cup A = A$ **[idempotence]** ;

(v) $(A \cup B = A) \Leftrightarrow (B \subset A)$;

(vi) $(A \subset B) \wedge (C \subset D) \Rightarrow (A \cup C \subset B \cup D)$.

Démonstration. Immédiat en utilisant les propriétés du connecteur $\vee$. Un dessin peut être utile pour (v) et (vi). □

b) Intersection

Définition I.5. Soient A, B deux sous–ensembles d'un ensemble E ; on appelle **instersection** de A et B l'ensemble

$$\{x \in E \,|\, (x \in A) \wedge (x \in B)\} .$$

Notation. $A \cap B$

Exemple I.6.

— $\{1, 2\} \cap \{2, 7\} = \{2\}$;
— $\{1, 3\} \cap \{2, 7\} = \emptyset$.

Vocabulaire. Deux ensembles A, B tels que $A \cap B = \emptyset$ sont dits **disjoints**.

Remarque I.6. De façon plus générale, si $(A_i)_{i\in I}$ est une famille de sous–ensembles d'un ensemble E indexée par un ensemble I, on pose :

$$\bigcap_{i\in I} A_i = \{x \in E \,|\, \forall i \in I,\ x \in A_i\} \ .$$

Il s'agit du plus grand sous–ensemble de E contenu dans tous les A_i. Notons que I peut tout à fait être infini ; on peut par exemple montrer assez aisément (démontrer deux inclusions) que

$$\bigcap_{n\in\mathbb{N}^*} \left[0, 1 + \frac{1}{n}\right] = [0, 1] \ .$$

Proposition I.3. Soient A, B, C, D quatre ensembles. Alors :

(i) $A \cap B = B \cap A$ **[commutativité]** ;
(ii) $(A \cap B) \cap C = A \cap (B \cap C)$ **[associativité]** ;
(iii) $A \cap \emptyset = \emptyset$ **[$\emptyset$ est absorbant]** ;
(iv) $A \cap A = A$ **[idempotence]** ;
(v) $(A \cap B = A) \Leftrightarrow (A \subset B)$;
(vi) $(A \subset B) \wedge (C \subset D) \Rightarrow (A \cap C \subset B \cap D)$.

Démonstration. Immédiat en utilisant les propriétés du connecteur $\wedge$. Un dessin peut une fois encore être utile pour (v) et (vi). □

Proposition I.4. Soient A, B, C trois ensembles. Alors :

(i) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
(ii) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Démonstration. Faisons le premier :

$$\begin{aligned} x \in A \cap (B \cup C) &\Leftrightarrow (x \in A) \wedge (x \in B \cup C) \\ &\Leftrightarrow (x \in A) \wedge ((x \in B) \vee (x \in C)) \\ &\Leftrightarrow ((x \in A) \wedge (x \in B)) \vee ((x \in A) \wedge (x \in C)) \qquad \text{par distributivité} \\ &\Leftrightarrow (x \in A \cap B) \vee (x \in A \cap C) \\ &\Leftrightarrow (x \in A \cap B) \cup (A \cap C) \ . \end{aligned}$$

□

c) Différence, complémentaire

Définition I.6. Soient A, B deux parties d'un ensemble E. On appelle :
- **différence de** A **et** B l'ensemble $A \setminus B = \{x \in A \mid x \notin B\}$;
- **complémentaire de** A l'ensemble $\overline{A} = \{x \in E \mid x \notin A\}$.

Notation. Le complémentaire de A pourra aussi être noté A^c.

Remarque I.7. Si A est une partie de E on a :
- $\overline{A} = E \setminus A.$;
- $A \setminus A = \emptyset$;
- $A \setminus \emptyset = A$.

Exemple I.7. $\{1, 2, 3\} \setminus \{1, 4, 5\} = \{2, 3\}$.

Nous disposons d'une version ensembliste des lois de de Morgan via la proposition suivante.

Proposition I.5. Soient A, B, C trois parties d'un ensemble E. Alors :

(i) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;

(ii) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

Démonstration. Utiliser les lois de de Morgan logique en traduisant l'appartenance aux ensembles étudiants en termes de connecteurs. □

◇ Négation de phrases quantifiées

Pour exprimer proprement le complémentaire d'un ensemble, il est excessivement utile de savoir nier une phrase quantifiée. Nous donnons ici les règles à suivre.

Proposition I.6. Soit P un prédicat dépendant d'un paramètre x. Alors :
1. $\overline{(\forall x, P(x))} \Leftrightarrow (\exists x, \overline{P(x)})$
2. $\overline{(\exists x, P(x))} \Leftrightarrow (\forall x, \overline{P(x)})$

Exemple I.8.

$$\overline{\forall \varepsilon > 0, \quad \forall x \in \mathbb{R}, \quad \exists \delta > 0, \quad \forall y \in \mathbb{R}, \quad (|x - y| \leq \delta) \Rightarrow (|f(x) - f(y)| \leq \varepsilon)}$$
$$\Leftrightarrow \exists \varepsilon > 0, \quad \overline{\forall x \in \mathbb{R}, \quad \exists \delta > 0, \quad \forall y \in \mathbb{R}, \quad (|x - y| \leq \delta) \Rightarrow (|f(x) - f(y)| \leq \varepsilon)}$$
$$\Leftrightarrow \exists \varepsilon > 0, \quad \exists x \in \mathbb{R}, \quad \overline{\exists \delta > 0, \quad \forall y \in \mathbb{R}, \quad (|x - y| \leq \delta) \Rightarrow (|f(x) - f(y)| \leq \varepsilon)}$$
$$\vdots$$
$$\Leftrightarrow \exists \varepsilon > 0, \quad \exists x \in \mathbb{R}, \quad \forall \delta > 0, \quad \exists y \in \mathbb{R} \quad (|x - y| \leq \delta) \wedge (|f(x) - f(y)| > \varepsilon)$$

d) Produit cartésien

Définition I.7. On appelle **couple** toute paire ordonnée d'objets. On dira que deux couples (a, b) et (c, d) sont égaux si et seulement si $(a = c) \wedge (b = d)$.

➠ **Exemple I.9.** $(\spadesuit, \hbar) \neq (\hbar, \spadesuit)$.

Définition I.8. Soient A, B deux ensembles. On appelle **produit cartésien de** A **et** B l'ensemble
$$\{(a,b) \mid a \in A,\, b \in B\}\ .$$

Notation. $A \times B$

➠ **Exemple I.10.** Vous connaissez sans doute déjà $\mathbb{R}^2$. Notons que l'on peut généraliser : $\mathbb{R}^3$ est par exemple le produit cartésien (associatif !) de $\mathbb{R}^2$ par $\mathbb{R}$.

3.⁻ Ensemble des entiers naturels, récurrence(s)

L'ensemble $\mathbb{N}$ des entiers naturels est un ensemble **infini**, muni d'une **addition** et d'une **multiplication**. Il s'agit de lois de composition internes : la somme et le produit de deux entiers naturels restent des entiers naturels. On peut également le munir de deux relations d'ordre (*cf.* chapitre V), à savoir :
- l'**ordre naturel** : on notera $a \leq b$ (pour $a, b \in \mathbb{N}$) si $\exists c \in \mathbb{N},\ b = a + c$; c est alors **noté** $b - a$ (la soustraction n'est pas une opération admissible sur $\mathbb{N}$). Il s'agit d'un ordre total : si $a, b \in \mathbb{N}$ alors $(a \leq b) \vee (b \leq a)$;
- la **divisibilité** : on notera $a|b$ ("a divise b") si $\exists c \in \mathbb{N},\ b = ac$; c est alors **noté**, lorsque $a \neq 0$, $\frac{b}{a}$. Il ne s'agit pas d'un ordre total : $2 \not| 3$ et $3 \not| 2$.

Notation. Dans toute la suite, pour $n \leq m$, on posera $[\![n, m]\!] = \{n, n+1, \ldots, m\}$.

a) Principe de récurrence

Axiome D. Toute partie non vide de $\mathbb{N}$ possède un plus petit élément (minimum).

Vocabulaire. Pour une partie A de $\mathbb{N}$ on appellera plus petit élément (resp. plus grand élément) ou minimum (resp. maximum) tout élément n vérifiant :
$$\forall a \in A, \quad a \geq n \ \text{ (resp. } a \leq n \text{)}.$$

Cet axiome, bien qu'utile en lui-même comme nous le verons par la suite, nous amène la conséquence suivante, moins "évidente".

Proposition I.7. Toute partie de $\mathbb{N}$ non vide et majorée admet un plus grand élément (maximum).

✌ **Remarque I.8.**
- Une partie A de $\mathbb{N}$ est dite **majorée** (resp. **minorée**) si $\exists M \in \mathbb{N}$ tel que $\forall x \in \mathbb{N},\ x \leq M$ (resp. $x \geq M$). Nous reviendrons sur cette notion dans le chapitre V.
- Remarquons que toute partie non vide de $\mathbb{N}$ est minorée.

Démonstration. Soit $A \subset \mathbb{N}$ non vide et majorée. Posons :

$$B = \{x \in \mathbb{N} \,|\, \forall a \in A,\, a \leq x\}$$

l'ensemble des majorants de A. Alors :
- $B \neq \emptyset$ car A est majorée ;
- $B \subset \mathbb{N}$.

Ainsi, d'après l'axiome D, il existe $b \in B$ tel que $\forall x \in B$, $b \leq x$ ($b = \min B$). Remarquons de plus que b majore A par construction.

Cas 1 : $b = 0$. Alors $A = \{0\}$ car A est majorée par 0. La démonstration est terminée.

Cas 2 : $b \neq 0$. Alors $b - 1 \in \mathbb{N}$ et, comme $b = \min B$, ne majore pas A. Ainsi, il existe $a \in A$ tel que $a > b - 1$; ce qui signifie que $b - 1 < a \leq b$. La seule possibilité est alors que $a = b$; b est alors un majorant de A appartenant à l'ensemble : $b = \max A$.

□

Nous pouvons désormais énoncer le **principe de succession**, propriété fondamentale de l'ensemble des entiers naturels.

Proposition I.8. Soit $A \subset \mathbb{N}$ telle que :
- $0 \in A$;
- $\forall n \in \mathbb{N}$, $(n \in A) \Rightarrow (n + 1 \in A)$.

Alors $A = \mathbb{N}$.

Démonstration. Supposons $A \neq \mathbb{N}$, *i.e* il existe $n \in \mathbb{N} \setminus A$. Posons $B = \mathbb{N} \setminus A$; alors :
- $B \neq \emptyset$;
- $B \subset \mathbb{N}$.

De fait, par axiome D, il existe $n_0 = \min B$. Par définition, $n_0 - 1 \in A$ et donc $n_0 = (n_0 - 1) + 1 \in A$, ce qui est absurde. □

Corollaire I.8.a (Principe de récurrence)**.**
Soit $\mathscr{P}$ un prédicat dépendant d'une variable $n \in \mathbb{N}$ tel que :
- $\mathscr{P}(0)$ est vraie **[initialisation]** ;
- $\forall n \in \mathbb{N}$, $\mathscr{P}(n) \Rightarrow \mathscr{P}(n+1)$ **[hérédité]**.

Alors $\forall n \in \mathbb{N}$, $\mathscr{P}(n)$ est vraie.

Démonstration. Appliquer la proposition précédente à l'ensemble $A = \{n \in \mathbb{N} \,|\, \mathscr{P}(n)\}$.
□

Remarque I.9.
- Si $n_0 > 0$ est entier naturel que $\mathscr{P}(n_0)$ est vérifiée, alors l'hérédité entraîne que $\forall n \geq n_0$, $\mathscr{P}(n)$ est vraie. Ceci permet de faire des démonstrations par récurrence initialisées à $n = 1, 2, 3$ ou 42.
- Toute rédaction de récurrence doit faire apparaître clairement initialisation et hérédité.

— Il est absolument **proscrit** de faire débuter une hérédité par "Supposons la propriété vraie pour tout n" ...

✍ **Exercice I.1.** Soit $n \geq 2$; démontrer que 10 divise $2^{2^n} - 6$.

➥ **Correction :** *Par récurrence ...*

— *Pour* $n = 2$, $2^{2^n} - 6 = 10$.

— *Si la propriété est vraie au rang* n, *on remarque que* $2^{2^{n+1}} - 6 = \left(2^{2^n}\right)^2 - 6$. *Or, par hypothèse de récurrence, il existe* $c \in \mathbb{N}$ *tel que* $2^{2^n} = 10c + 6$. *En réinjectant, on tombe sur*

$$\begin{aligned} 2^{2^{n+1}} - 6 &= (10c+6)^2 - 6 \\ &= 100c^2 + 120c + 36 - 6 \\ &= 10(10c^2 + 12c + 3) \end{aligned}$$

d'où le résultat.

b) Récurrence double

Proposition I.9. Soit $\mathscr{P}$ un prédicat dépendant d'une variable $n \in \mathbb{N}$ tel que :

— $\mathscr{P}(0)$ et $\mathscr{P}(1)$ sont vraies **[initialisation double]** ;

— $\forall n \in \mathbb{N}$, $(\mathscr{P}(n) \wedge \mathscr{P}(n+1)) \Rightarrow \mathscr{P}(n+2)$ **[hérédité à deux rangs]**.

Alors $\forall n \in \mathbb{N}$, $\mathscr{P}(n)$ est vraie.

✍ **Exercice I.2.** On définit la **suite de Fibonacci** (Leonardo, 1175—1250) $(F_n)_n$ de la façon suivante :

$$F_0 = 0, \quad F_1 = 1 \quad \text{et} \quad \forall n \geq 0,\ F_{n+2} = F_n + F_{n+1}\ .$$

On note ϕ et $\overline{\phi}$ les racines du polynôme $X^2 - X - 1$. Démontrer que :

$$\forall n \geq 0, \quad F_n = \frac{\phi^n - \overline{\phi}^n}{\phi - \overline{\phi}}\ .$$

➥ **Correction :** *L'initialisation double est immédiate. Si on suppose la propriété vraies aux rangs* n *et* $n+1$ *pour un certain* $n \geq 0$ *alors*

$$\begin{aligned} F_{n+2} &= F_n + F_{n+1} \\ &= \frac{\phi^n - \overline{\phi}^n}{\phi - \overline{\phi}} + \frac{\phi^{n+1} - \overline{\phi}^{n+1}}{\phi - \overline{\phi}} \quad \textit{par hypothèse de récurrence} \\ &= \frac{1}{\phi - \overline{\phi}} \left(\left(\phi^n + \phi^{n+1}\right) - \left(\overline{\phi}^n + \overline{\phi}^{n+1}\right) \right)\ . \end{aligned}$$

Il nous suffit pour conclure de remarquer que

$$\phi^n + \phi^{n+1} = \phi^n(1+\phi) = \phi^n\phi^2 = \phi^{n+2}$$

et que l'on a un résultat analogue pour $\overline{\phi}$.

c) Récurrence forte

Proposition I.10. Soit $\mathscr{P}$ un prédicat dépendant d'une variable $n \in \mathbb{N}$ tel que :
- $\mathscr{P}(0)$ est vraie **[initialisation]** ;
- $\forall n \in \mathbb{N}$, $(\forall k \in [\![0, n]\!],\ \mathscr{P}(k)) \Rightarrow \mathscr{P}(n+1)$ **[hérédité forte]**.

Alors $\forall n \in \mathbb{N}$, $\mathscr{P}(n)$ est vraie.

Démonstration. Appliquer le principe de récurrence au prédicat $\mathscr{Q}(n) : \forall k \leq n,\ \mathscr{P}(n)$.
□

➠ **Exemple I.11.** Démontrons par récurrence forte sur $n \in \mathbb{N}$ que :

$$\forall n \in \mathbb{N} \setminus \{0, 1\},\ \mathscr{P}(n)\ :\ n \text{ admet un diviseur premier.}$$

- $n = 2$ est divisible par 2, qui est premier.
- Soit $n \in \mathbb{N}$; supposons que $\mathscr{P}(k)$ soit vérifiée pour tout $k \in [\![2, n]\!]$. Si $n+1$ est premier, c'est terminé ; dans le cas contraire, il existe $a, b \in [\![2, n]\!]$ tels que $n + 1 = ab$. Or, par hypothèse de récurrence, a (par exemple) admet un diviseur premier, d'où le résultat.

✍ **Exercice I.3.** Démontrer que :

$$\forall n \in \mathbb{N}^*, \quad \exists\, (p, q) \in \mathbb{N}^2,\ n = 2^p(2q + 1)\,.$$

Chapitre II

Rappels et compléments calculatoires

1.⁻ Fonctions d'une variable réelle

a) C'est quoi ?

Soit X un ensemble (pour le moment, un intervalle ou une réunion d'intervalles style $[0,1]$, $[0,12[$ ou $\mathbb{R}^*$). On appelle **fonction** de X à valeurs dans $\mathbb{R}$ tout "mécanisme" $f : X \to \mathbb{R}$ affectant à tout point $x \in X$ une valeur numérique $f(x) \in \mathbb{R}$.

➡ **Exemple II.1.** Vous en avez vu des centaines en terminale (j'espère) : $x \mapsto x^2$, sin, exp et j'en passe ...

Notation. Nous utiliserons la convention suivante pour définir une fonction :

$$\begin{aligned} f : X &\to \mathbb{R} \\ x &\mapsto f(x) \end{aligned}$$

ou, lorsque X est clair, $f : x \mapsto f(x)$. Dans tous les cas, nous n'écrirons **PAS** d'horreurs du style "la fonction $f(x) = \ldots$" J'aime à croire que nous sommes des gens civilisés.

Définition II.1. L'ensemble X maximal des valeurs de x pour lesquelles l'expression $f(x)$ a un sens est appelé **ensemble de définition** de la fonction f.

➡ **Exemple II.2.** L'ensemble de définition de $x \mapsto \sqrt{x-1}$ est $[1, +\infty[$.

Définition II.2. Étant donné deux fonctions $f, g : X \mapsto \mathbb{R}$ nous pouvons définir :
- leur **somme** $f + g : x \mapsto f(x) + g(x)$ sur X ;
- leur **produit** $f \times g : x \mapsto f(x)g(x)$ sur X ;
- leur **quotient** $\frac{f}{g} : x \mapsto \frac{f(x)}{g(x)}$ sur l'ensemble des $x \in X$ tels que $g(x) \neq 0$.

De plus, si les valeurs d'une fonction g sont comprises dans l'ensemble de définition d'une fonction f, on peut définir la **composée** de f par g via :

$$f \circ g : x \mapsto f(g(x)) \ .$$

Nous aurons l'occasion de revenir en détails sur cette notion ultérieurement.

Exemple II.3. La fonction composée de $f : x \mapsto \sqrt{x}$ et $g : x \mapsto x^2$ est $f \circ g : x \mapsto \sqrt{x^2} = |x|$, définie sur $\mathbb{R}$ (pourquoi ?).

Remarque II.1. Si $a \in \mathbb{R}$, il est relativement aisé, connaissant la courbe d'une fonction f, d'en déduire l'allure de $x \mapsto f(x+a)$ ou $x \mapsto f(ax)$ lorsque ces composées ont un sens.

Définition II.3. Soient f, g deux fonctions définies sur un ensemble X. On dira que f est **inférieure ou égale** à g si, pour **tout** $x \in X$, $f(x) \leq g(x)$.

Notation. $f \leq g$

Remarque II.2.
- On définit de la même façon les relations $\geq, <, >$ et $=$ sur les fonctions.
- **Attention : il s'agit d'ordres partiels.** Comparer par exemple $x \mapsto x$ et $x \mapsto -x$.
- Graphiquement, $f \leq g$ si la courbe représentative de f est **toujours** au dessus de celle de g.

◇ Fonctions bornées

Définition II.4. Soit $f : X \to \mathbb{R}$ une fonction. On dit que f est :
- **majorée** si il existe un réel M tel que pour tout $x \in X$; $f(x) \leq M$;
- **minorée** si il existe un réel m tel que pour tout $x \in X$; $f(x) \geq m$;
- **bornée** si elle est majorée **et** minorée.

Remarque II.3. Une fonction f est bornée si et seulement si la fonction $|f| : x \mapsto |f(x)|$ est majorée.

Exemple II.4. La fonction $x \mapsto x^2$ est bornée sur $[0, 1]$ mais pas sur $\mathbb{R}$. La fonction $x \mapsto \frac{1}{x}$ est bornée sur $[1, \infty[$.

◇ Monotonie

Définition II.5. Soit $f : X \to \mathbb{R}$ une fonction. On dit que f est :
- **croissante** (resp. strictement croissante) si pour tous $x, y \in X$ tels que $x \leq y$ alors $f(x) \leq f(y)$ (resp. $f(x) < f(y)$) ;
- **décroissante** (resp. strictement décroissante) si pour tous $x, y \in X$ tels que $x \leq y$ alors $f(x) \geq f(y)$ (resp. $f(x) > f(y)$) ;
- **monotone** si elle est croissante **ou** décroissante.

Exemple II.5. La fonction $x \mapsto x^3 - 17$ est croissante sur $\mathbb{R}$. Elle y est donc monotone.

Remarque II.4.

— La somme de deux fonctions croissantes est croissante. Par contre, on ne peut rien dire de la différence d'une fonction croissante et d'une fonction décroissante ...
— Soyez gentils, **ne confondez pas monotone** (croissant ou décroissant) **et constante** (toujours égale à la même valeur, donc *de facto* croissante et décroissante).

Proposition II.1. La composée de deux fonctions monotones suit la "règle des signes".

➠ **Exemple II.6.** Monotonie des fonctions $x \mapsto e^{x^2}$ (croissante) et $x \mapsto e^{-x^2}$ (décroissante).

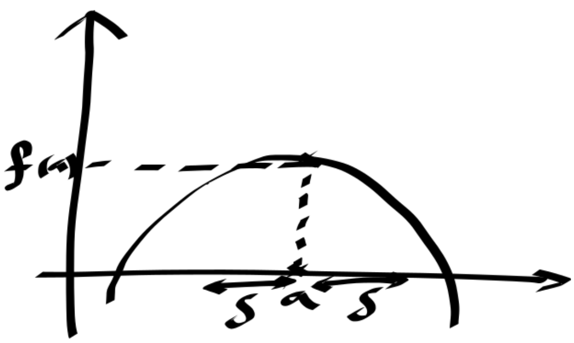
◇ **Parité**

Définition II.6. Soit I un intervalle de $\mathbb{R}$ **symétrique** par rapport à 0. On dit qu'une fonction $f : I \to \mathbb{R}$ est :
— **paire** si, pour tout $x \in I$, $f(-x) = f(x)$;
— **impaire** si, pour tout $x \in I$, $f(-x) = -f(x)$.

➠ **Exemple II.7.** Puissances paires et impaires, cosinus, sinus.

✌ **Remarque II.5.** La parité apporte des informations intéressantes relatives aux courbes représentatives : celle d'une fonction paire est symétrique par rapport à l'axe des ordonnées, celle d'une fonction impaire par rapport à l'origine. Ceci permet de réduire le domaine pertinent lors de l'étude d'une fonction.

◇ **Extrema**



Définition II.7. Soit I un intervalle de $\mathbb{R}$ et soit $f : I \to \mathbb{R}$ une fonction. Si $a \in I$, on dit que :
— f admet un maximum local en a si :

$$\exists \delta > 0, \, \forall x \in I, \quad (|x-a| \leq \delta) \Rightarrow (f(x) \leq f(a)) \, ;$$

— f admet un minimum local en a si :

$$\exists \delta > 0, \, \forall x \in I, \quad (|x-a| \leq \delta) \Rightarrow (f(x) \geq f(a)) \, .$$

Remarque II.6.

- **Attention :** caractère **local** de ces notions ; le voir sur des exemples type cos.
- Si la dernière inégalité de la définition est vraie sur I, on parle d'extremum global. Jeter un oeil à $x \mapsto \sin(x)e^{-x}$.

b) Dérivation

Ce paragraphe a vocation à n'être qu'un assemblage de recettes de cuisine pour débuter l'année. Tout ce qui suit sera démontré et mis en place proprement ultérieurement. Demain, on rase gratis.

Si $f : I \to \mathbb{R}$ est une fonction dérivable sur un intervalle I de $\mathbb{R}$, on note f' sa fonction dérivée. Si elle est dérivable plusieurs fois de suite, on notera $f'', f^{(3)}, \ldots, f^{(k)}$ ses dérivées successives. On utilisera aussi quelques fois les notations de la physique, à savoir $\frac{\mathrm{d}f}{\mathrm{d}x}$, $\frac{\mathrm{d}^k f}{\mathrm{d}x^k}$. On n'écrire **PAS** d'abominations du type $(x^2+1)'$ ...Une dérivée est une fonction, traitons la comme telle.

Proposition II.2. Si $f : I \to \mathbb{R}$ est dérivable en $a \in I$, sa tangente a pour équation

$$y = f(a) + (x-a)f'(a) .$$

◇ Opérations sur les dérivées

Logiquement, presque tout ceci est connu, mais il vaut mieux prévenir que guérir.

Proposition II.3. Soient f, g deux fonctions dérivables sur un intervalle I de $\mathbb{R}$ et $\lambda \in \mathbb{R}$. Alors :

(i) $f + \lambda g$ est dérivable sur I et $(f+\lambda g)' = f' + \lambda g'$;

(ii) $f \times g$ est dérivable sur I et $(f \times g)' = f' \times g + f \times g'$;

(iii) si g ne s'annule pas sur I, $\frac{f}{g}$ est dérivable sur I et

$$\left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2} ;$$

(iv) si g est à valeurs dans I, la composée $f \circ g$ est dérivable sur l'ensemble de dérivabilité de g et

$$(f \circ g)' = g' \times f' \circ g .$$

Exemple II.8. La formule (iv) permet de retrouver les formules de terminales sur $\ln(u)'$ (notation abominable et à proscrire désormais) et consorts.

◇ Monotonie et dérivées

Vous connaissez la musique en théorie : le signe de la dérivée est liée à la monotonie selon le schéma vu en terminale. Notons au passage que la monotonie est stricte lorsque f' ne s'annule qu'en des points isolés.

◇ **Réciproques**

Définition II.8. Soient I, J deux intervalles de $\mathbb{R}$ et soient $f : I \to J$ et $g : J \to I$ deux fonctions. On dit que f et g sont **réciproques** si, pour tout $x \in J$ $f \circ g(x) = x$ et si, pour tout $x \in I$, $g \circ f(x) = x$.

Notation. g pourra alors être noté f^{-1} (et réciproquement, *pun intended*).

➠ **Exemple II.9.**
— exp et ln sont réciproques sur leurs ensembles de définition respectifs ;
— idem pour $x \mapsto x^2$ et $\sqrt{\cdot}$.

✌ **Remarque II.7.** Graphiquement, la courbe représentative de la réciproque d'une fonction s'obtient par symétrie relativement à la première bissectrice, *i.e* la droite d'équation $y = x$.

Le théorème qui suit est important, et sera démontré ultérieurement. Si vous avez l'impression que nous prenons de mauvaises habitudes, vous avez raison.

Théorème II.4 (Dérivée d'une réciproque).
Soient I, J deux intervalles de $\mathbb{R}$ et soit $f : I \to J$ une fonction dérivable telle que f' **ne s'annule pas** sur I. Alors :
(i) f admet une réciproque f^{-1} dérivable sur J ;
(ii)
$$(f^{-1})' = \frac{1}{f' \circ f^{-1}} .$$

➠ **Exemple II.10.** On peut retrouver la dérivée de l'exponentielle. Ne me remerciez pas, c'est mon métier.

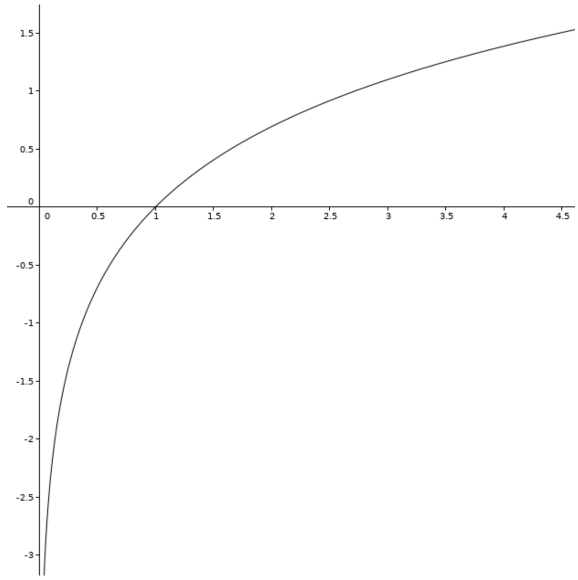
c) Logarithmes, exponentielles

◇ **Le cas néperien**

Point culture : le nom commun néperien vient de John Napier (francisé en Jean Neper), qui fut théologien, physicien, astronome, mathématicien et écossais et vécu de 1550 à 1617.

Définition II.9. On appelle **logarithme néperien** l'unique fonction, notée ln, définie sur $\mathbb{R}_+^*$ telle que :
(i) $\forall x > 0$, $\ln'(x) = \frac{1}{x}$;
(ii) $\ln(1) = 0$.

L'allure de la courbe représentative de cette fonction devrait vous être bien connu, mais réiterons la au cas où :



Proposition II.5.

(i) ln est strictement croissante;

(ii) $\ln(x) \xrightarrow[x\to\infty]{} \infty$ et $\ln(x) \xrightarrow[x\to 0]{} -\infty$;

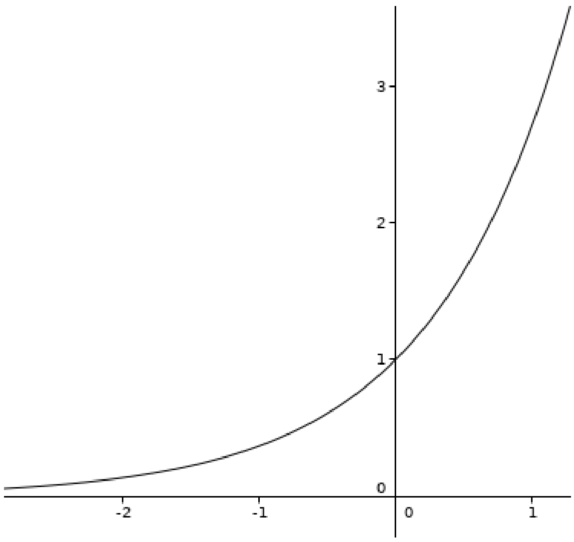
(iii) soient $x, y \in \mathbb{R}_+^*$. On a alors :
- $\ln(xy) = \ln(x) + \ln(y)$;
- $\ln\left(\frac{x}{y}\right) = \ln(x) - \ln(y)$;
- $\ln(x^y) = y\ln(x)$.

✌ **Remarque II.8.** Les puissances non–entières seront étudiées en détail au chapitre IV. En attendant, on se contentera de rappeler que si $x > 0$ on a $\sqrt{x} = x^{1/2}$.

Ceux parmi vous qui suivent auront remarqué que la dérivée du logarithme néperien ne s'annule pas sur $\mathbb{R}_+^*$; le théorème II.4 entraîne donc que cette fonction admet une réciproque, dont la dérivée sera elle–même.

Définition II.10. La réciproque de la fonction ln, est appelée **exponentielle**.

Notation. $\exp : \mathbb{R} \to \mathbb{R}_+^*$



Proposition II.6.
(i) exp est strictement croissante, à valeurs strictement positives ;
(ii) $\exp(x) \xrightarrow[x\to\infty]{} \infty$ et $\exp(x) \xrightarrow[x\to-\infty]{} 0$;
(iii) si on pose $e = \exp(1)$, alors $\ln(e) = 1$;
(iv) soient $x, y \in \mathbb{R}$. On a alors :
— $\exp(x + y) = \exp(x)\exp(y)$;
— $\exp(x - y) = \frac{\exp(x)}{\exp(y)}$;
— $\exp(xy) = \exp(x)^y$.
(v) exp est dérivable et $\exp' = \exp$.

✌ **Remarque II.9.** La troisième formule du point (iv) justifie l'écriture "$\exp(x) = e^x$" vue en terminale et que nous utiliserons désormais lorsque cela nous semblera pertinent.

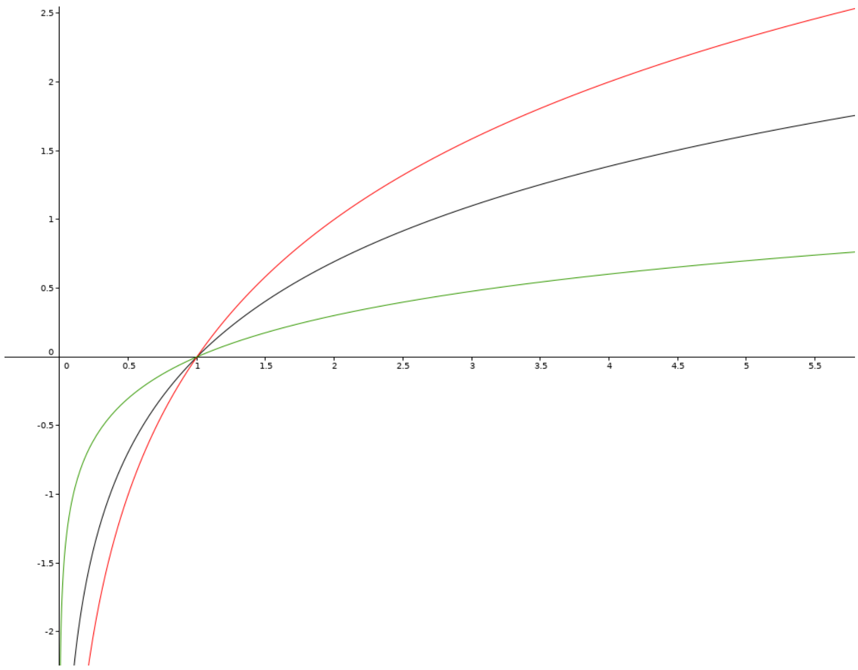
◇ **En base quelconque**

Définition II.11. Soit $a \in \mathbb{R}_+^*$ différent de 1. On appelle **logarithme en base** a la fonction

$$\log_a : \mathbb{R}_+^* \to \mathbb{R}$$
$$x \mapsto \frac{\ln(x)}{\ln(a)} \quad .$$

➠ **Exemple II.11.**
— Pour $a = 10$, on retrouve le logarithme décimal cher aux physiciens, souvent noté log.
— Pour $a = e$, pas de surprise, on obtient le logarithme néperien.
— Pour $a = 2$, on tombe sur le logarithme binaire, prisé des informaticiens, et parfois noté lg.

Les courbes de ces fonctions partagent une allure commune, modulo quelques différences d'inflexion. Plus la valeur de a est élevée, plus la courbe sera dominée à l'infini.



✌ **Remarque II.10.** Les logarithmes sont tous multiples du logarithme néperien : la proposition II.5 reste donc valide.

➠ **Exemple II.12.** Que dire du cas $0 < a < 1$?

✌ **Remarque II.11.** La réciproque d'un logarithme en base quelconque sera étudiée ultérieurement. Question sans rapport : que vaut $\log(10^{40})$?

d) Croissances comparées

✖ Ce qui suit est **absolument fondamental**, et sera démontré ultérieurement.

Proposition II.7. Soient $a, b > 0$; on a alors les limites suivantes :

(i)
$$\frac{(\ln(x))^b}{x^a} \xrightarrow[x\to\infty]{} 0\ ;$$

(ii)
$$x^a |\ln(x)|^b \xrightarrow[x\to 0]{} 0\ ;$$

(iii)
$$\frac{e^{ax}}{x^b} \xrightarrow[x\to\infty]{} \infty\ ;$$

(iv)
$$x^b e^{-ax} \xrightarrow[x\to+\infty]{} 0\ .$$

✌ **Remarque II.12.** La valeur absolue dans le (ii) n'est pas optionnelle : si $\ln(x) < 0$, on ne peut définir $\ln(x)^b$.

✍ **Exercice II.1.** Soit $x \in]-1, +\infty[$; démontrer que $\exp(x) \geq 1 + x$. En déduire que $\ln(1 + x) \leq x$.

2.⁻ Sommes, produits

L'objet de ce paragraphe est de présenter au lecteur quelques rudiments de calculs algébriques qui seront utilisés tout au long de l'année. Plusieurs notions apparaissant ici feront l'objet d'approfondissement ultérieurs.

a) Convention, notations

Fixons nous une famille de nombres réels (ou complexes) $a_0, \dots a_n$. On notera :

$$\sum_{k=0}^{n} a_k = a_0 + \ldots + a_n \, .$$

✌ **Remarque II.13.** On rencontre parfois aussi la notation $\sum\limits_{0 \leq k \leq n} a_k$.

Toutes les propriétés attendues pour une somme restent valables sous cette notation ; en particulier la "relation de Chasles"

$$\sum_{k=0}^{n} a_k = \sum_{k=0}^{m} a_k + \sum_{k=m+1}^{n} a_k$$

est vérifiée pour tout $m \in [\![0, n-1]\!]$ et exprime le fait que

$$a_0 + \ldots + a_m + a_{m+1} + \ldots + a_n = (a_0 + \ldots + a_m) + (a_{m+1} + \ldots + a_n) \, .$$

De la même façon, si λ est un nombre réel (ou complexe), on a naturellement :

$$\lambda \sum_{k=0}^{n} a_k = \sum_{k=0}^{n} \lambda a_k \, .$$

Légèrement plus technique, nous pouvons faire des changements d'indice, comme :

$$\sum_{k=0}^{n} a_k = \sum_{k=1}^{n+1} a_{k-1} \, .$$

➠ **Exemple II.13.**

$$\sum_{k=1}^{n} \frac{1}{k} = \sum_{k=0}^{n-1} \frac{1}{k+1} \, .$$

✌ **Remarque II.14.**

— Lorsque I est un ensemble quelconque et que $(a_i)_{i \in I}$ est une famille de nombres réels (ou complexes) vérifiant que seul un nombre fini des a_i sont non nuls (on parle de **famille presque nulle**), on généralise la notation *supra* en notant $\sum\limits_{i \in I} a_i$ la somme (**finie**) des termes non nuls de la famille.

— Par convention, on a $\sum_{x\in\emptyset} x = 0$.

De la même manière, nous définissons la notation "produit" :

$$\prod_{k=0}^{n} a_k = a_0 \times \ldots \times a_n \ .$$

Notons que si $\lambda \in \mathbb{C}$, on a

$$\prod_{k=0}^{n} \lambda a_k = \lambda^{n+1} \prod_{k=0}^{n} a_k \ .$$

Notons que le produit d'une famille infinie presque nulle sera... nul et que, par convention, on pose $\prod_{x\in\emptyset} x = 1$. Il est possible d'effectuer des changements d'indice sur les produits de façon similaire à ce qui a été vu pour les sommes.

b) Exemples fondamentaux

Proposition II.8. Soit $n \in \mathbb{N}$. Alors :

(i)

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

(ii)

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

Démonstration. Faisons le (i), *i.e* démontrons par récurrence sur $n \in \mathbb{N}$ que :

$$\forall n \in \mathbb{N}, \quad \mathscr{P}(n) \ : \ \sum_{k=0}^{n} k = \frac{n(n+1)}{2} \ \text{ est vraie.}$$

— $\mathscr{P}(0)$ est trivialement vérifiée.

— Supposons $\mathscr{P}(n)$ vérifiée pour un certain $n \in \mathbb{N}$. Alors :

$$\begin{aligned}\sum_{k=0}^{n+1} k &= n+1+\sum_{k=0}^{n} k \\ &= n+1+\frac{n(n+1)}{2} \quad \text{par hypothèse de récurrence} \\ &= \frac{2(n+1)+n(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}\end{aligned}$$

d'où $\mathscr{P}(n+1)$.

La propriété était initialisée et héréditaire, elle est vérifée sur $\mathbb{N}$. Le point (ii) se traite de façon similaire. □

✍ **Exercice II.2.** Démontrer que si $n \geq 0$ on a :

$$\sum_{k=0}^{n} k^3 = \frac{n^2(n+1)^2}{4}.$$

Proposition II.9. Soit $x \in \mathbb{C}$ et soit $n \in \mathbb{N}$. Alors :

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

Démonstration. Le cas $x = 1$ est trivial. Dans le cas contraire, démontrons par récurrence sur $n \in \mathbb{N}$ que :

$$\forall n \in \mathbb{N}, \quad \mathscr{P}(n) \ : \ \sum_{k=0}^{n} x^k = \frac{1-x^{n+1}}{1-x} \ \text{ est vraie.}$$

— $\mathscr{P}(0)$ est trivialement vérifiée.
— Supposons $\mathscr{P}(n)$ vérifiée pour un certain $n \in \mathbb{N}$. Alors :

$$\begin{aligned} \sum_{k=0}^{n+1} x^k &= x^{n+1} + \sum_{k=0}^{n} x^k \\ &= x^{n+1} + \frac{1-x^{n+1}}{1-x} \quad \text{par hypothèse de récurrence} \\ &= \frac{(1-x)x^{n+1} + 1 - x^{n+1}}{1-x} \\ &= \frac{1-x^{n+2}}{1-x} \end{aligned}$$

d'où $\mathscr{P}(n+1)$.

La propriété était initialisée et héréditaire, elle est vérifée sur $\mathbb{N}$. □

Proposition II.10. Soient $a, b \in \mathbb{C}$ et $n \in \mathbb{N}$. Alors :

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

Démonstration. Il suffit de vérifier que :

$$\begin{aligned}(a-b)\sum_{k=0}^{n} a^k b^{n-k} &= a\sum_{k=0}^{n} a^k b^{n-k} - b\sum_{k=0}^{n} a^k b^{n-k}\\ &= \sum_{k=0}^{n} a^{k+1} b^{n-k} - \sum_{k=0}^{n} a^k b^{n+1-k}\\ &= \sum_{k=1}^{n+1} a^k b^{n+1-k} - \sum_{k=0}^{n} a^k b^{n+1-k} \text{ par changement d'indice}\\ &= a^{n+1} - b^{n+1}\,.\end{aligned}$$

□

✌ **Remarque II.15.** La démonstration *supra* peut être vue comme un exemple de **somme télescopique**, *i.e* de somme dont les termes se compensent "deux à deux". Ces dernières sont, une fois leur structure repérée, aisées à calculer.

✍ **Exercice II.3.** Déterminer la valeur de la somme $\sum_{k=1}^{n} \dfrac{1}{k(k+1)}$ pour $n \in \mathbb{N}^*$.

c) Binôme de Newton

Définition II.12. Soit $n \in \mathbb{N}$; on appelle **factorielle** de n l'entier $n!$ défini par récurrence de la façon suivante :
- $0! = 1$;
- si $n \geq 1$, $n! = n \times (n-1)!$.

✌ **Remarque II.16.** Il découle de la définition que

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

➠ **Exemple II.14.** $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, $5! = 120$, $14! = 87178291200$, $42! = 1.4050061177528798985431426062445115699363 84.10^{51}$: la croissance est rapide !

Définition II.13. Soient $n, k \in \mathbb{N}$. On appelle **coefficient du binôme "k parmi n"** la quantité :

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

✌ **Remarque II.17.** Cette quantité prendra tout son sens lorsque nous parlerons de combinatoire dans le chapitre XVI. Pour le moment, nous pouvons admettre qu'il s'agit du nombre de façons de choisir k éléments parmi n, sans ordre.

Proposition II.11. Soient $k, n \in \mathbb{N}$ tels que $k \leq n$. Alors :

(i)
$$\binom{n}{0} = \binom{n}{n} = 1\,,\ \binom{n}{1} = n\ ;$$

(ii)
$$\binom{n}{k} = \binom{n}{n-k}$$

(iii)
$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1} \quad \textbf{[identité de Pascal]}$$

Démonstration. Immédiat en passant par la définition. □

✌ **Remarque II.18.** Le point (iii)fait écho à une contruction probablement vue en terminale : le triangle de Pascal (Blaise de son prénom, 1623—1662).

$n \backslash k$	0	1	2	3	...
0	1	0	0	0	...
1	1	1	0	0	...
2	1	2	1	0	...
3	1	3	3	1	...
⋮	⋮	⋮	⋮	⋮	

Comme son nom ne l'indique pas, la formule qui suit apparaît dés le X^e siècle dans des traités de mathématiciens arabes, indiens ou perses (Al–Karaji, Halayudha). Elle fut également démontrée indépendamment par Yang Hui en Chine au XIII^e siècle Elle fut toutefois démontrée sous sa forme moderne et généralisée par Isaac Newton en 1665.

Théorème II.12 (Formule du binôme de Newton)**.**
Soient $a, b \in \mathbb{C}$ et soit $n \geq 0$. Alors :

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

✌ **Remarque II.19.** L'addition étant commutative, les rôles de a et b sont interchangeables. Mettre ceci en parallèle avec l'égalité (ii) de la proposition II.11.

Démonstration. Devinez quoi...Une récurrence ! Plus précisément, démontrons par récurrence sur $n \in \mathbb{N}$ que :

$$\forall n \in \mathbb{N}, \quad \mathscr{P}(n)\ :\ (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k\, b^{n-k} \ \text{ est vraie.}$$

— $\mathscr{P}(0)$ est trivialement vérifiée.

— Supposons $\mathscr{P}(n)$ vérifiée pour un certain $n \in \mathbb{N}$. Alors :

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1}\, b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k\, b^{n-k+1} \\
&= \sum_{k'=1}^{n+1} \binom{n}{k'-1} a^{k'}\, b^{n-k'+1} + \sum_{k=0}^{n} \binom{n}{k} a^k\, b^{n-k+1} \\
&\text{via le changement d'indice } k = k'-1 \text{ dans la première somme} \\
&= \sum_{=1}^{n+1} \binom{n}{k-1} a^k\, b^{n-k+1} + \sum_{k=0}^{n} \binom{n}{k} a^k\, b^{n-k+1} \\
&= \binom{n}{n} a^{n+1} + \binom{n}{0} b^{n+1} + \sum_{k=1}^{n} \underbrace{\left(\binom{n}{k-1} + \binom{n}{k}\right)}_{=\binom{n+1}{k}} a^k\, b^{n-k+1} \\
&= a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k\, b^{n-k+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k\, b^{n-k+1}
\end{aligned}$$

d'où $\mathscr{P}(n+1)$.

La propriété était initialisée et héréditaire, elle est vérifiée sur $\mathbb{N}$. □

➠ **Exemple II.15.** En appliquant cette formule, on obtient immédiatement les deux (forts utiles) formules suivantes, pour $n \in \mathbb{N}^*$:

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

et

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = (1-1)^n = 0\,.$$

d) Sommes doubles

Fixons nous dans ce paragraphe deux familles $a_0, \dots, a_n$ et $b_0, \dots, b_p$ de nombres réels (ou complexes). On a alors, en développant :

$$\begin{aligned}
\left(\sum_{k=0}^{n} a_k\right)\left(\sum_{\ell=0}^{p} b_\ell\right) &= \sum_{k=0}^{n} a_k \left(\sum_{\ell=0}^{p} b_\ell\right) \\
&= \sum_{k=0}^{n} \sum_{\ell=0}^{p} a_k b_\ell\,.
\end{aligned}$$

✖ **Attention :** On a bien ici une somme **double** rassemblant tous les produits possibles des a_k et b_ℓ. En **aucun cas** ne faut–il prétendre que le produit de ces deux sommes est la somme des $a_k b_k$. Le lecteur non suicidaire prendra de fait soin de ne pas utiliser le même indice pour les deux sommes...

✍ **Exercice II.4.** Calculer les sommes suivantes, pour $n \geq 0$:

$$\sum_{k=0}^{n}\sum_{\ell=0}^{n} k\ell^2 \quad \text{et} \quad \sum_{k=0}^{n}\sum_{\ell=0}^{n} k\,.$$

Notation. On pose :

$$\sum_{0\leq i\leq j\leq n} a_i b_j = \sum_{i=0}^{n}\sum_{j=i}^{n} a_i b_j = \sum_{j=0}^{n}\sum_{i=0}^{j} a_i b_j\,.$$

Une telle somme est dite **triangulaire**.

✖ **Attention :** Dans le cas d'une somme double (ou plus, si affinités), il est possible d'intervertir l'ordre des symboles $\sum$. Cela n'est **PAS** possible pour une somme triangulaire, car les bornes de la seconde somme dépendent de l'indice de la première.

✍ **Exercice II.5.** Calculer, pour $n \geq 0$, la somme $\sum_{1\leq i\leq j\leq n} \frac{i}{j}$.

➥ **Correction :** *On a :*

$$\begin{aligned}\sum_{1\leq i\leq j\leq n} \frac{i}{j} = \sum_{j=1}^{n}\sum_{i=1}^{j} \frac{i}{j} &= \sum_{j=1}^{n} \frac{1}{j}\left(\sum_{i=1}^{j} i\right)\\ &= \sum_{j=1}^{n} \frac{1}{j}\frac{j(j+1)}{2}\\ &= \sum_{j=1}^{n} \frac{j+1}{2}\\ &= \frac{n(n+3)}{4}\,.\end{aligned}$$

✌ **Remarque II.20.** Dans le cas où les a_i et b_j coïncident, on peut décomposer une somme triangulaire de cette façon :

$$\sum_{1\leq i\leq j\leq n} a_i a_j = \underbrace{\sum_{i=1}^{n} a_i^2}_{=D} + \underbrace{\sum_{1\leq i<j\leq n} a_i a_j}_{=S}$$

pour simplifier les calculs. En effet, avec ces notations, on a :

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_i a_j = \left(\sum_{i=1}^{n} a_i\right)^2 = D + 2S\,.$$

✍ **Exercice II.6.** Calculer $\sum_{1\leq i\leq j\leq n} ij$.

Chapitre III

Nombres réels

1.⁻ Le corps $\mathbb{R}$ des nombres réels

a) C'est quoi ?

L'ensemble $\mathbb{R}$ des nombres réels est muni d'une addition, d'une multiplication et d'une division (par des nombres non nuls). Un tel ensemble (en gros, *cf.* chapitre VIII) est appelé un **corps**.

b) Sous–ensembles remarquables

Théorème III.1.
Il existe deux parties de $\mathbb{R}$, notées $\mathbb{R}_+$ et $\mathbb{R}_-$, telles que :

(A) $\mathbb{R} = \mathbb{R}_+ \cup \mathbb{R}_-$;

(B) $\mathbb{R}_+ \cap \mathbb{R}_- = \{0\}$;

(C) $\mathbb{R}_+$ est stable par addition et multiplication ;

(D) pour tout $x \in \mathbb{R}$, $(x \in \mathbb{R}_+) \Leftrightarrow (-x \in \mathbb{R}_-)$.

Démonstration. Nous ne disposons pas, hélas, de l'outillage technique requis pour aborder cette démonstration. Ce résultat sera donc admis. $\square$

✌ **Remarque III.1.**

— Si on pose $\mathbb{R}_\pm^* = \mathbb{R}_\pm \setminus \{0\}$, alors $\mathbb{R}$ est égal à la réunion disjointe $\mathbb{R}_+^* \sqcup \{0\} \sqcup \mathbb{R}_-^*$.

— $\mathbb{R}_-$ est stable par addition ; en effet, si $x, y \in \mathbb{R}_-$ alors $x+y = -\underbrace{((-x)+(-y))}_{\in \mathbb{R}_+} \in \mathbb{R}_-$.

Corollaire III.1.a. Soient $x, y \in \mathbb{R}$. Alors :

(i) $(x \in \mathbb{R}_+) \wedge (y \in \mathbb{R}_-) \Rightarrow (xy \in \mathbb{R}_-)$;

(ii) $(x \in \mathbb{R}_-) \wedge (y \in \mathbb{R}_-) \Rightarrow (xy \in \mathbb{R}_+)$;

(iii) $x^2 \in \mathbb{R}_+$;

(iv) $1 \in \mathbb{R}_+$ et $-1 \in \mathbb{R}_-$;

(v) $(x \in \mathbb{R}_+^*) \Leftrightarrow \left(\dfrac{1}{x} \in \mathbb{R}_+^*\right)$.

Démonstration.

(i) Si $x \in \mathbb{R}_+$ et $y \in \mathbb{R}_-$ alors $xy = -\underbrace{x(-y)}_{\in \mathbb{R}_+} \in \mathbb{R}_-$.

(ii) Si $x, y \in \mathbb{R}_-$ alors $-x, -y \in \mathbb{R}_+$ et donc $xy = (-x)(-y) \in \mathbb{R}_+$.

(iii) Cela découle du (ii) et du (C) du théorème.

(iv) $1 = 1^2 \in \mathbb{R}_+$ donc $-1 \in \mathbb{R}_-$.

(v) Soit $x \in \mathbb{R}_+^*$; alors si $\dfrac{1}{x} \in \mathbb{R}_-$ nous aurions $1 = x \times \dfrac{1}{x} \in \mathbb{R}_-$, ce qui contedit le point (iv).

□

c) Ordre naturel sur $\mathbb{R}$

Définition III.1. Soient $x, y \in \mathbb{R}$. On note :

— $x \leq y$ si $y - x \in \mathbb{R}_+$;

— $x < y$ si $y - x \in \mathbb{R}_+^*$.

➠ **Exemple III.1.** $3 < \pi$.

Proposition III.2. Soient $x, y, z \in \mathbb{R}$. Alors :

(i) $(x \leq y) \wedge (y \leq x) \Rightarrow (x = y)$;

(ii) $(x \leq y) \wedge (y \leq z) \Rightarrow (x \leq z)$;

(iii) $(x \leq y) \vee (y \leq x)$.

Démonstration.

(i) Si $(x \leq y) \wedge (y \leq x)$, alors $x - y \in \mathbb{R}_+$ et, comme $-(x - y) = y - x \in \mathbb{R}_+$, $x - y \in \mathbb{R}_+ \cap \mathbb{R}_- = \{0\}$. Au final, $x = y$.

(ii) Si $x \leq y$ et $y \leq z$. Alors :

$$z - x = (z - y) + (y - x) \in \mathbb{R}_+$$

d'où $x \leq z$.

(iii) Remarquons que $y - x \in \mathbb{R} = \mathbb{R}_+ \cup \mathbb{R}_-$. Ainsi, $(y - x \in \mathbb{R}_+) \vee (y - x \in \mathbb{R}_-)$, *i.e* $(x \leq y) \vee (y \leq x)$.

□

Vocabulaire. Nous dirons (*cf.* chapitre V) que la relation "$\leq$" est un ordre total sur $\mathbb{R}$.

✌ **Remarque III.2.** Notons au passage que "$<$" ne risque pas d'être un ordre total ; cette relation n'est pas réflexive !

Proposition III.3. Soient $x, y, z \in \mathbb{R}$. Alors :
- (i) $(x < y) \Leftrightarrow (x + z < y + z)$;
- (ii) si $z \in \mathbb{R}_+^*$, $(x < y) \Leftrightarrow (xz < yz)$;
- (iii) si $z \in \mathbb{R}_-^*$, $(x < y) \Leftrightarrow (xz > yz)$.

Démonstration.

(i)

$$\begin{aligned} x < y &\iff y - x \in \mathbb{R}_+^* \\ &\iff (y + z) - (x + z) = y - x \in \mathbb{R}_+^* \\ &\iff x + z < y + z \ . \end{aligned}$$

(ii) Si $z > 0$ alors :

$$\begin{aligned} x < y &\iff y - x \in \mathbb{R}_+^* \\ &\iff z(y - x) = zy - zx \in \mathbb{R}_+^* \\ &\iff xz < yz \ . \end{aligned}$$

(iii) Si $z < 0$ alors :

$$\begin{aligned} x < y &\iff y - x \in \mathbb{R}_+^* \\ &\iff z(y - x) = zy - zx \in \mathbb{R}_-^* \\ &\iff xz > yz \ . \end{aligned}$$

✌ **Remarque III.3.** En exercice, il n'y a aucune honte à faire usage de tableaux de signes "a étages" et autres techniques de ce type pour résoudre des inéquations mettant en jeu des produits...

□

Proposition III.4. Soient $x, x', y, y' \in \mathbb{R}$ tels que $x \leq x'$ et $y \leq y'$. Alors :

$$x + y \leq x' + y' \ .$$

Démonstration. Il suffit de remarquer que $x' + y' - (x + y) = (x' - x) + (y' - y) \in \mathbb{R}_+$.

□

✖ **ATTENTION :** si on peut sommer des inégalités, il est **absolument exclus de les soustraire**. En effet $0 \leq 1$ et $-1 \leq 1$ mais, aux dernières nouvelles, $1 \not\leq 0$ ...

d) Valeur absolue

Définition III.2. Soit $x \in \mathbb{R}$; on appelle **valeur absolue** de x le réel $\max(x, -x)$.

Notation. $|x|$

✌ **Remarque III.4.** Notons que $x \in \mathbb{R}_+ \Leftrightarrow |x| = x$ et $x \in \mathbb{R}_- \Leftrightarrow |x| = -x$.

Proposition III.5. Soient $x, y \in \mathbb{R}$. Alors :

(i) $|x| \in \mathbb{R}_+$;

(ii) $|x| = 0 \Leftrightarrow x = 0$;

(iii) $|xy| = |x||y|$;

(iv) $|x+y| \leq |x| + |y|$ **[inégalité triangulaire 1]** ;

(v) $||x| - |y|| \leq |x - y|$ **[inégalité triangulaire 2]**.

Démonstration.

(i), (ii) Conséquences immédiates de la remarque III.4.

(iii) Laissé en exercice au lecteur ; procéder par disjonction de cas selon les signes respectifs de x et y et utiliser (pour changer) la remarque III.4.

(iv) **Point méthode : comment gérer un maximum.**
Par définition, $|x+y| = \max(x+y, -x-y)$, or :
— $x + y \leq |x| + |y|$;
— $-x - y = (-x) + (-y) \leq |x| + |y|$.
Ainsi, $|x+y| = \max(x+y, -x-y) \leq |x| + |y|$.

(v) Échanger les rôles de x et y ne change rien à l'expression souhaitée : nous pouvons donc supposer, quitte à échanger x et y, que $|x| \geq |y|$. Remarquons alors que $x = x - y + y$; certes, me direz vous...Mais, en utilisant la première inégalité triangulaire, on obtient :

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

et donc $|x| - |y| \leq |x - y|$. Comme $|x| \geq |y|$, on a bien :

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

□

✌ **Remarque III.5.** Si $a, b \in \mathbb{R}$ avec $b > 0$, l'ensemble $\{x \in \mathbb{R} \mid |x - a| \leq b\}$ est égal à l'intervalle $[a - b, a + b]$ (faire un dessin).

2.⁻ Bornes supérieure, inférieure

a) C'est quoi ?

Définition III.3. Soit$A \subset \mathbb{R}$. On appelle **borne supérieure** (ou supremum) de A le plus petit élément (si il existe) de l'ensemble des majorants de A.

Notation. $\sup(A)$

En résumé, la borne supérieure est le **plus petit majorant de l'ensemble** A, lorsque ce dernier existe, *i.e* :

$$\sup(A) = \min\{x \in \mathbb{R} \,|\, \forall a \in A,\, a \leq x\}\,.$$

On déduit de cette reformulation une caractérisation de la borne supérieure, à privilégier en pratique : pour tout $M \in \mathbb{R}$,

$$M = \sup(A) \Longleftrightarrow \begin{cases} \forall x \in A,\, x \leq M \\ \forall y < M,\, \exists\, x \in A\,,\; y < x \end{cases}. \qquad \textbf{(E} \text{ :III.1)}$$

➠ **Exemple III.2.** La borne supérieure de $[0,1[$ est 1. En effet :
- pour tout $x \in [0,1[$, $x \leq 1$ donc 1 majore bien $[0,1[$;
- si $z < 1$, alors soit $z \leq 0$ et dans ce cas $\frac{1}{42} > z$ soit $z \in [0,1[$ et alors $\frac{z+1}{2} \in [0,1[$ et $z < \frac{z+1}{2}$. 1 est donc le plus petit majorant de $[0,1[$.

On peut définir de façon analogue le concept de borne inférieure d'un ensemble, qui sera alors son **plus grand minorant.**

Définition III.4. Soit $A \subset \mathbb{R}$. On appelle **borne inférieure** (ou infimum) de A le plus grand élément (si il existe) de l'ensemble des minorants de A.

Notation. $\inf(A)$

✖ **Attention :** l'existence de telles quantités est très loin d'être automatique : en effet, quelle pourrait être la borne supérieure de $\mathbb{Z}$?

Dans toute la suite de ce chapitre, lorsque nous énoncerons un résultat relatif aux bornes supérieures, nous laissons le soin au lecteur d'en déduire un énoncé analogue s'appliquant aux bornes inférieures. Par exemple, la proposition suivante a pour pendant : lorsqu'un minimum existe, la borne inférieure existe et lui est égale.

Proposition III.6. Soit $A \subset \mathbb{R}$ **possèdant un plus grand élément**, alors :
- A admet une borne supérieure ;
- $\sup(A) = \max(A)$.

✌ **Remarque III.6.** La réciproque est **FAUSSE** : penser à $[0,1[$ qui admet une borne supérieure mais pas de maximum.

Démonstration. Posons $a = \max(A)$ et $A^+ = \{x \in \mathbb{R} \,|\, \forall y \in A,\, y \leq x\}$ l'ensemble des majorants de A. Alors :

— il est clair que $a \in A^+$;

— $a \in A$ donc $\forall x \in A^+,\, x \geq a$.

Par caractérisation de la borne supérieure (**E** :III.1), on a bien $a = \sup(A)$. □

✌ **Remarque III.7.** Si A possède une borne supérieure, alors A est automatiquement majorée.

b) Théorème fondamental

Même si la démonstration du théorème suivant dépasse le cadre du programme de MPSI, le résultat en est absolument remarquable et formera la pierre angulaire de la suite de ce chapitre.

Théorème III.7.
Toute partie de $\mathbb{R}$ non vide et majorée admet une borne supérieure.

➠ **Exemple III.3.** Si on voit la partie $A = \{x \in \mathbb{Q} \,|\, x^2 \leq 2\}$ comme un sous–ensemble de $\mathbb{R}$, il admet une borne supérieure, qui est $\sqrt{2}$.

Afin de faciliter la vie de notre estimé lecteur, nous profitons de ce paragraphe pour anticiper sur un résultat qui sera démontré dans le chapitre VII.

Proposition III.8. [Caractérisation séquentielle de la borne supérieure] Soit $A \subset \mathbb{R}$ et soit $M \in \mathbb{R}$; alors :

$$M = \sup(A) \iff \begin{cases} \forall a \in A,\, a \leq M \\ \exists (a_n)_n \in A^{\mathbb{N}},\, a_n \xrightarrow[n\to\infty]{} M \end{cases}.$$

➠ **Exemple III.4.** 0 est la borne inférieure de $\mathbb{Q}_+^*$ dans $\mathbb{R}$; en effet, il est clair qu'il minore cet ensemble et

$$\underbrace{\frac{1}{n}}_{\in \mathbb{Q}_+^*} \xrightarrow[n\to\infty]{} 0\,.$$

c) Droite réelle achevée

Débutons ce paragraphe par fixer deux symboles, $-\infty$ et $+\infty$, sans signification particulière et posons :

$$\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, \infty\}\,.$$

Cet ensemble est appelé **droite réelle achevée.**

Nous pouvons étendre l'ordre naturel de $\mathbb{R}$ à $\overline{\mathbb{R}}$ via les conventions suivantes :

— $-\infty < +\infty$;

— si $y \in \mathbb{R}$, alors $-\infty < y < +\infty$.

On en déduit en particulier que $\overline{\mathbb{R}}$ admet un maximum et un minimum, respectivement égaux à $+\infty$ et $-\infty$.

De même, les deux opérations classiques sur $\mathbb{R}$ peuvent (presque) être généralisées à $\overline{\mathbb{R}}$ via les tables partielles suivantes.

$+$	$-\infty$	$y \in \mathbb{R}$	$+\infty$
$-\infty$	$-\infty$	$-\infty$	**?**
$x \in \mathbb{R}$	$-\infty$	$x+y$	$+\infty$
$+\infty$	**?**	$+\infty$	$+\infty$

$\times$	$-\infty$	$y \in \mathbb{R}_+^*$	0	$y \in \mathbb{R}_+^*$	$+\infty$
$-\infty$	$+\infty$	$+\infty$	**?**	$-\infty$	$-\infty$
$x \in \mathbb{R}_-^*$	$+\infty$	xy	0	xy	$-\infty$
0	**?**	0	0	0	**?**
$x \in \mathbb{R}_+^*$	$-\infty$	xy	0	xy	$+\infty$
$+\infty$	$-\infty$	$-\infty$	**?**	$+\infty$	$+\infty$

Notons que ces tables sont symétriques : les opérations étendues demeurent donc commutatives. Ces conventions nous seront, comme vous pouvez sans doute l'imaginer, très utiles pour nos futures études de limites.

✌ **Remarque III.8.** Il serait possible sans grand risque[1] de convenir du fait que $\dfrac{1}{\pm\infty} = 0$. Il n'est toutefois pas possible de convenir d'une valeur cohérente pour $\dfrac{1}{0}$ (quel serait son signe ?).

Proposition III.9. Toute partie A de $\overline{\mathbb{R}}$ admet une borne supérieure et une borne inférieure, dans le sens où les quantités

$$\sup(A) = \min\{x \in \overline{\mathbb{R}} \mid \forall a \in A,\ a \leq x\} \quad \text{et} \quad \inf(A) = \max\{x \in \overline{\mathbb{R}} \mid \forall a \in A,\ a \geq x\}$$

existent dans $\overline{\mathbb{R}}$.

Démonstration. Soit $A \subset \overline{\mathbb{R}}$. Démontrons l'existence de la borne supérieure de A ; une démonstration similaire livrera alors celle de sa borne inférieure.

Cas 1 : $A = \emptyset$ ou $A = \{-\infty\}$. Alors dans ce cas l'ensemble des majorants de A est $\overline{\mathbb{R}}$ entier, ce qui entraîne que A admet pour borne supérieure $-\infty = \min(\overline{\mathbb{R}})$.

Cas 2 : $+\infty \in A$. Dans ce cas, $\sup(A) = \max(A) = +\infty$.

Cas 3 : $B = A \setminus \{-\infty\}$ est un sous ensemble non vide $\mathbb{R}$. Si l'ensemble B est majoré, d'après le théorème III.7, il admet une borne supérieure qui sera également celle de A. Dans le cas contraire, $\sup(A) = +\infty$.

□

✌ **Remarque III.9.** Une conséquence intéressante de tout ceci est que, si $A \subset \overline{\mathbb{R}}$ est **non vide**, alors :

$$\inf(A) \leq \sup(A)\ .$$

✖ **Attention :** l'inégalité est inversée dans le cas de l'ensemble vide, dont la borne supérieure est $-\infty$ et la borne inférieure $+\infty$.

1. Hors du quotient de l'infini par lui–même, mais à ce stade, qui compte...

3.– Quelques résultats de topologie

a) Partie entière

Proposition/définition III.5. Soit $x \in \mathbb{R}$; alors il existe un unique entier $n \in \mathbb{Z}$ vérifiant :

$$n \leq x < n+1 .$$

Cet entier n est alors appelé **partie entière** (par défaut) de x.

Notation. $\lfloor x \rfloor$, $E(x)$.

➠ **Exemple III.5.** $\lfloor 1,25 \rfloor = 1$, $\lfloor -2,7 \rfloor = -3$.

Démonstration. Commençons par démontrer l'existence. L'ensemble

$$\mathscr{E} = \{k \in \mathbb{N} \,|\, k > x\} \subset \mathbb{N}$$

est non vide, par axiome D, admet un plus petit élément n_0. Il est alors clair que $n = n_0 - 1$ vérifie l'inégalité voulue.

Pour démontrer l'unicité, supposons que nous disposions de deux entier n, p vérifiant l'égalité voulue, *i.e*

$$n \leq x < n+1 \quad \text{et} \quad p \leq x < p+1$$

qui implique

$$n \leq x < p+1$$

et donc $n < p+1$, d'où $n \leq p$. De façon symétrique, on obtient $p \leq n$, *ergo* $n = p$. □

✌ **Remarque III.10.**

— $\lfloor x \rfloor$ est caractérisée par :

$$\begin{cases} \lfloor x \rfloor \in \mathbb{Z} \\ \lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \end{cases} .$$

— $\lfloor x \rfloor$ est parfois appelée *plancher* de x ; il existe également un plafond, noté $\lceil x \rceil$ et caractérisé par :

$$\begin{cases} \lceil x \rceil \in \mathbb{Z} \\ \lceil x \rceil - 1 < x \leq \lceil x \rceil \end{cases} .$$

Une application classique de la notion de partie entière est l'**approximation d'un réel à** 10^{-n} près, pour $n \geq 0$. Posons, pour $n \in \mathbb{N}$ et $x \in \mathbb{R}$:

$$x_n = \frac{\lfloor 10^n x \rfloor}{10^n} .$$

Alors, comme

$$\lfloor 10^n x \rfloor \leq 10^n x < \lfloor 10^n x \rfloor + 1$$

on a bien :

$$x_n \leq x < x_n + 10^{-n} \quad i.e \quad |x - x_n| < 10^{-n} .$$

➠ **Exemple III.6.** $\pi = 3.14$ à 10^{-2} près.

b) Résultats de densité

Proposition III.10. Soient $x, y \in \mathbb{R}$ tels que $x < y$. Alors il existe un rationnel $\zeta \in \mathbb{Q}$ et un irrationnel $\tau \in \mathbb{R} \setminus \mathbb{Q}$ tels que :
- $x \leq \zeta \leq y$;
- $x \leq \tau \leq y$.

✌ **Remarque III.11.** En itérant ce procédé, on en déduit qu'entre deux réels distincts il existe une infinité de rationnels et une infinité d'irrationnels. On dit que $\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$ sont **denses dans** $\mathbb{R}$.

Démonstration. Posons $\varepsilon = y - x$; alors, comme $\varepsilon > 0$, en posant $q = \left\lfloor \frac{1}{\varepsilon} \right\rfloor + 1 \in \mathbb{N}^*$, on a $q > \frac{1}{\varepsilon}$, *i.e*

$$0 < \frac{1}{q} < \varepsilon = y - x\,.$$

On pose ensuite $p = \lfloor qx \rfloor + 1 \in \mathbb{Z}$, de sorte que $p - 1 \leq qx < p$ et donc :

$$\frac{p-1}{q} \leq x < \frac{p}{q}\,.$$

On a alors :

$$\begin{aligned} x < \frac{p}{q} &= \frac{p-1+1}{q} \\ &\leq x + \frac{1}{q} \\ &\leq x + \varepsilon \\ &= y\,. \end{aligned}$$

On en déduit que le rationnel $\zeta = \frac{p}{q}$ est contenu dans le segment $[x, y]$. Un raisonnement identique remplaçant q par $q\sqrt{2}$ lors de l'application du corollaire **??** nous permet de démontrer que l'irrationnel $\tau = \frac{p}{q\sqrt{2}}$ appartient à ce même segment. □

c) Intervalles

Rappellons que les intervalles de $\mathbb{R}$ sont les neuf familles d'ensembles suivants, pour $a, b \in \mathbb{R}$:
- $[a, b] = \{x \in \mathbb{R} \,|\, a \leq x \leq b\}$ **[segment]** ;
- $[a, b[= \{x \in \mathbb{R} \,|\, a \leq x < b\}$;
- $]a, b] = \{x \in \mathbb{R} \,|\, a > x \leq b\}$;
- $]a, b[= \{x \in \mathbb{R} \,|\, a < x < b\}$;
- $[a, +\infty[= \{x \in \mathbb{R} \,|\, a \leq x\}$;
- $]a, +\infty[= \{x \in \mathbb{R} \,|\, a < x\}$;
- $]-\infty, b] = \{x \in \mathbb{R} \,|\, x \leq b\}$;
- $]-\infty, b[= \{x \in \mathbb{R} \,|\, x < b\}$;

— $]-\infty,+\infty[=\mathbb{R}$.

Remarque III.12.

- Les quatre premier types d'intervalles ci–dessus sont bornés, les autres non.
- Si $a > b$, l'intervalle $[a,b]$ est vide. Ceci signifie en particulier que $\emptyset$ est un intervalle.
- **Certains** (pas tous !) intervalles sont dits **ouverts** ou **fermés**, comme résumé dans le tableau *infra*.

Ouvert	**Fermé**
$]a,b[$	$[a,b]$
$]a,+\infty[$	$[a,+\infty[$
$]-\infty,b[$	$]-\infty,b]$
$\emptyset$	$\emptyset$
$\mathbb{R}$	$\mathbb{R}$

Définition III.6. Une partie A de $\mathbb{R}$ est dite **convexe** si :

$$\forall x,y \in A, \quad [x,y] \subset A\,.$$

Exemple III.7. Les intervalles sont clairement convexes. L'ensemble $\mathbb{R}^*$ ne l'est pas car (par exemple) $[-1,1] \not\subset \mathbb{R}^*$.

Proposition III.11. Les convexes de $\mathbb{R}$ sont exactement les intervalles.

Démonstration. Ceci est une ébauche de démonstration. Nous venons de voir que les intervalles étaient convexes ; reste à montrer la réciproque. Soit donc $A \subset \mathbb{R}$ un ensemble convexe.

Cas 1 : $A = \emptyset$**.** Youpi.

Cas 2 : $A \neq \emptyset$**.**

Cas 2.1 : A **n'est ni majoré ni minoré.** A est alors égal à $\mathbb{R}$.

Cas 2.2 : A **est majoré et minoré.** A admet alors une borne supérieure b et une borne inférieure a et $A=]a,b[$, $[a,b[,]a,b]$ ou $[a,b]$.

Cas 2.3 : A **est (par exemple) minorée et non majorée.** Posons $a = \inf(A)$ et montrons que $A=]a,\infty[$ ou $[a,\infty[$. L'inclusion de gauche à droite est évidente ; prenons ensuite $z > a$ et montrons que $z \in A$. Comme z ne peut minorer A, il existe alors $x \in A$ tel que $x < z$ et comme A n'est pas majorée, il existe $y \in A$ tel que $z < y$. Le réel z est donc compris dans le segment $[x,y]$ qui est inclus dans A par convexité, donc $z \in A$.

□

Proposition III.12 (Paramétrage d'un segment)**.** Soient $a,b \in \mathbb{R}$ tels que $a \leq b$. Alors :

$$[a,b] = \{(1-\lambda)a + \lambda b \,|\, \lambda \in [0,1]\}\,.$$

Démonstration. Si $a = b$, ceci est trivial. Sinon, pour tout $x \in \mathbb{R}$, on a :

$$\begin{aligned} x \in [a, b] &\Longleftrightarrow a \leq x \leq b \\ &\Longleftrightarrow 0 \leq x - a \leq b - a \\ &\Longleftrightarrow 0 \leq \frac{x-a}{b-a} \leq 1 \end{aligned}$$

d'où le résultat en remarquant que :

$$x = \left(1 - \frac{x-a}{b-a}\right) a + \frac{x-a}{b-a} b \,.$$

□

✌ **Remarque III.13.** Si $a < b$, l'application $\lambda \mapsto (1-\lambda)a + \lambda b$ réalise de plus une bijection de $[0, 1]$ dans $[a, b]$.

Corollaire III.12.a. Une partie $I \subset \mathbb{R}$ en est un intervalle si et seulement si :

$$\forall x, y \in I,\ \forall \lambda \in [0, 1], \quad (1-\lambda)x + \lambda y \in I$$

Chapitre IV

Fonctions usuelles

1.⁻ Trigonométrie circulaire

a) Cosinus, sinus, tangente

Définition IV.1. Soit $T \in \mathbb{R}$. Une fonction $f : \mathbb{R} \to \mathbb{R}$ est dite T–**périodique** si :

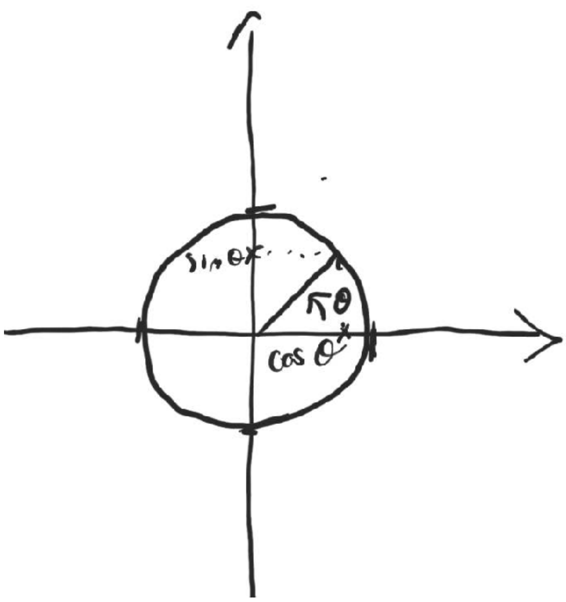
$$\forall x \in \mathbb{R}, \quad f(x+T) = f(x) .$$

✌ **Remarque IV.1.**

— Il n'y pas unicité de T (appelé période) ; certains ouvrages préfèrent introduire une "période minimale", à savoir le plus petit T positif tel que f soit T–périodique.

— Le fait qu'une fonction soit T–périodique permet de réduire son étude initiale à un intervalle de longueur T.

Les fonctions cosinus et sinus ont normalement été définies en terminale à travers une construction géometrico–graphique que nous reproduisons ci–ensuite (le truc vaguement rond est le cercle unité de $\mathbb{R}^2$). Nous ne serons hélas guère en mesure de faire mieux.



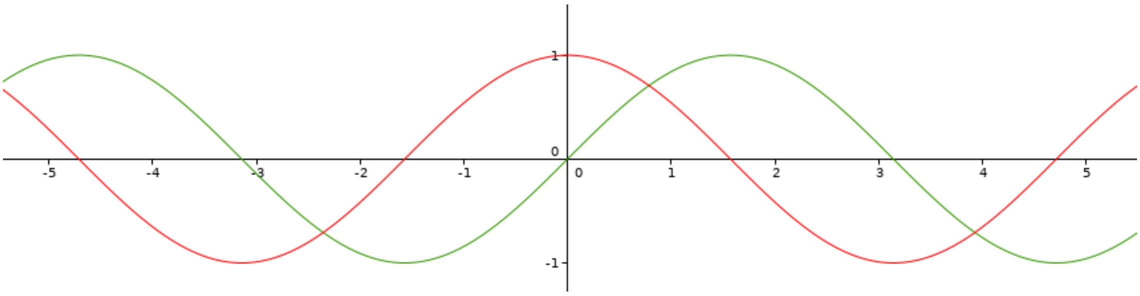
Proposition IV.1.

(i) Les fonctions cosinus et sinus sont 2π–périodiques et dérivables sur $\mathbb{R}$.

(ii) La fonction cosinus est paire, la fonction sinus impaire.

(iii) $\sin' = \cos$, $\cos' = -\sin$.

À toutes fins utiles, nous reproduisons ici l'allure courbes des fonctions cosinus (en rouge) et sinus (et vert) ci–ensuite.



Ces fonctions admettent de nombreuses valeurs remarquables, dont nous listons une selection dans le tableau *infra*.

θ	0	$\pi/2$	$\pi/3$	$\pi/4$	$\pi/6$	π	$3\pi/2$
$\cos(\theta)$	1	0	$1/2$	$\sqrt{2}/2$	$\sqrt{3}/2$	-1	0
$\sin(\theta)$	0	1	$\sqrt{3}/2$	$\sqrt{2}/2$	$1/2$	0	-1

Ces fonctions sont également remarquables de par leurs symétries : par exemple, si $\theta \in \mathbb{R}$, on a :
- $\cos(\theta + \pi) = -\cos(\theta)$;
- $\sin(\theta + \pi) = -\sin(\theta)$;
- $\cos(\pi - \theta) = -\cos(\theta)$;
- $\sin(\pi - \theta) = \sin(\theta)$.

Il est possible de "retrouver" ces formules via le cercle trigonométrique (faites un dessin !).

✍ **Exercice IV.1.** Déterminer l'ensemble $E = \left\{ \theta \in \mathbb{R} \;\middle|\; \cos(\theta) \in \left[-\frac{1}{2}, \frac{\sqrt{3}}{2} \right] \right\}$.

Arrive maintenant le moment que vous attendiez probablement avec impatience : le **formulaire de trigonométrie** ! Il est à connaître **impérativement et parfaitement**, mais ne paniquez pas (trop) : toutes les formules qui suivent peuvent être retrouvées à l'aide des cinq premières, à condition d'avoir une vague idée de ce que l'on cherche à obtenir.

Proposition IV.2 (Formulaire de trigonométrie, kit de survie)**.** Soient $a, b \in \mathbb{R}$; alors :
- $\cos^2(a) + \sin^2(a) = 1$;
- $\sin(a+b) = \sin(a)\cos(b) + \sin(b)\cos(a)$;
- $\sin(a-b) = \sin(a)\cos(b) - \sin(b)\cos(a)$;
- $\cos(a+b) = \cos(a)\cos(b) - \sin(a)\sin(b)$;
- $\cos(a-b) = \cos(a)\cos(b) + \sin(a)\sin(b)$;

Proposition IV.3 (Formulaire de trigonométrie, suite et fin)**.** Soient $a, b \in \mathbb{R}$; alors :
- $\cos(2a) = \cos^2(a) - \sin^2(a) = 2\cos^2(a) - 1 = 1 - 2\sin^2(a)$;
- $\sin(2a) = 2\sin(a)\cos(a)$;
- $\sin(a)\cos(b) = \frac{1}{2}(\sin(a+b) + \sin(a-b))$;
- $\cos(a)\cos(b) = \frac{1}{2}(\cos(a+b) + \cos(a-b))$;
- $\sin(a)\sin(b) = -\frac{1}{2}(\cos(a+b) - \cos(a-b))$.

✍ **Exercice IV.2.** Soient $p, q \in \mathbb{R}$; démontrer que :

1. $\cos(p) + \cos(q) = 2\cos\left(\dfrac{p+q}{2}\right)\cos\left(\dfrac{p-q}{2}\right)$;
2. $\cos(p) - \cos(q) = -2\sin\left(\dfrac{p+q}{2}\right)\sin\left(\dfrac{p-q}{2}\right)$;
3. $\sin(p) + \sin(q) = 2\sin\left(\dfrac{p+q}{2}\right)\cos\left(\dfrac{p-q}{2}\right)$;
4. $\sin(p) - \sin(q) = 2\sin\left(\dfrac{p-q}{2}\right)\cos\left(\dfrac{p+q}{2}\right)$.

Définition IV.2. On appelle **fonction tangente** l'application suivante :

$$\begin{aligned} \tan : \mathbb{R} \setminus \left\{ \frac{\pi}{2} + k\pi \,\middle|\, k \in \mathbb{Z} \right\} &\to \mathbb{R} \\ x &\mapsto \frac{\sin(x)}{\cos(x)} \end{aligned} .$$

Cette nouvelle fonction trigonométrique est définie partie sauf en les points d'annulation du cosinus. Elle admet des valeurs remarquables que l'on peut déduire de celles de cosinus et sinus, résumées (très partiellement) dans le tableau qui suit.

x	0	$\pi/4$	π
$\tan(x)$	0	1	0

Proposition IV.4. La fonction tangente est :
- impaire ;
- π–périodique ;
- dérivable sur son ensemble de définition, et :

$$\tan' = 1 + \tan^2 = \frac{1}{\cos^2} .$$

Démonstration. L'imparité est immédiate. Pour la périodicité, remarquons que, si

$x \in \mathbb{R}$, on a :

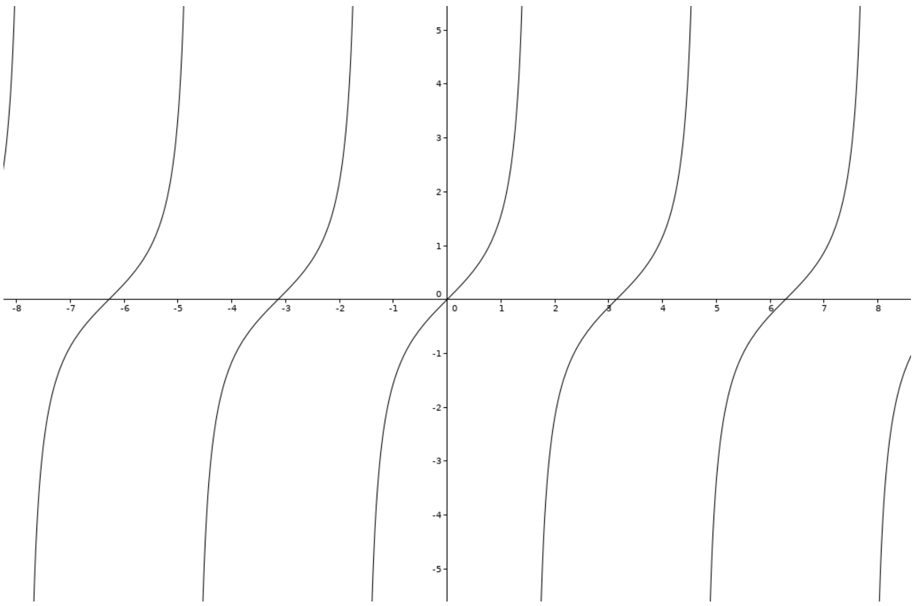
$$\begin{aligned}\tan(x+\pi) &= \frac{\sin(x+\pi)}{\cos(x+\pi)}\\ &= \frac{-\sin(x)}{-\cos(x)}\\ &= \tan(x)\,.\end{aligned}$$

La fonction tan est dérivable comme produit de fonctions dérivables partout ou le cosinus ne s'annule pas, et par dérivée d'un quotient on a :

$$\begin{aligned}\tan' &= \frac{\sin'\cos - \sin\cos'}{\cos^2}\\ &= \frac{\cos^2+\sin^2}{\cos^2}\\ &= \begin{cases} 1+\tan^2 \\ \dfrac{1}{\cos^2} \end{cases}.\end{aligned}$$

□

Ce résultat nous permet de finir l'étude de la fonction tangente, en notant que sa dérivée est positive en tout point donc qu'elle est strictement croissante avec limites infinies en chaque $\frac{\pi}{2} + k\pi$, $\pi \in \mathbb{Z}$. Sa courbe a donc l'allure suivante.



Ajoutons à ceci une formule, dont la démonstration est un calcul immonde : pour tous $a, b \in \mathbb{R}$,

$$\tan(a \pm b) = \frac{\tan(a) \pm \tan(b)}{1 \mp \tan(a)\tan(b)}\,. \qquad (\mathbf{E}\ :\mathrm{IV}.1)$$

✍ **Exercice IV.3.** Soit $x \in]-\pi, \pi[$ et soit $t = \tan(x/2)$. Établir les formules suivantes :

(i)

$$\cos(x) = \frac{1-t^2}{1+t^2}\ ;$$

(ii)
$$\sin(x) = \frac{2t}{1+t^2} \ ;$$

(iii)
$$\tan(x) = \frac{2t}{1-t^2} \ ,$$

cette dernière égalité n'étant valable que si $x \notin \left\{ \frac{\pi}{2} + k\pi \ \middle| \ k \in \mathbb{Z} \right\}$.

➥ **Correction :**

(iii) Cette formule découle du fait que :

$$\begin{aligned} \tan(x) &= \tan\left(\frac{x}{2} + \frac{x}{2}\right) \\ &= \frac{2t}{1-t^2} \ \textit{par} \ (\textbf{E} \ \textit{:IV.1}) \ . \end{aligned}$$

(ii)

$$\begin{aligned} \sin(x) &= \sin\left(2\frac{x}{2}\right) \\ &= 2\sin\left(\frac{x}{2}\right)\cos\left(\frac{x}{2}\right) \\ &= 2t\cos^2\left(\frac{x}{2}\right) \\ &= 2t \times \frac{1}{1+\tan^2(x/2)} \\ &= \frac{2t}{1+t^2} \ . \end{aligned}$$

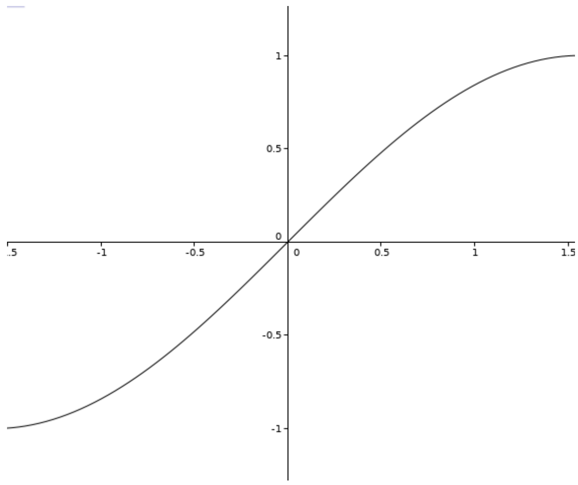
Le point (i) s'obtient comme corollaire des deux précédents.

b) Fonctions circulaires réciproques

La question qui nous vient naturellement (ou pas) à l'esprit est la suivante : les fonctions cosinus, sinus et tangente admettent–elles des réciproques ? La réponse est évidemment **NON**, pour de bêtes raisons liées à la périodicité. Par contre, la fonction suivante vérifie les hypothèses du théorème de la bijection :

$$\widehat{\sin} : \begin{array}{rcl} \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] & \to & [-1, 1] \\ x & \mapsto & \sin(x) \end{array} \ .$$

Pour s'en convaincre, il suffit de vérifier que sa dérivée est strictement positive hors des bornes (c'est le cas). La courbe représentative de $\widehat{\sin}$ est sans appel : cette fonction est strictement croissante ; elle admet donc une réciproque strictement croissante.



Définition IV.3. On appelle **fonction arc sinus** la réciproque de $\widehat{\sin}$.

Notation. $\arcsin : [-1, 1] \to \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$

✖ **ATTENTION :** arcsin n'est **PAS** la réciproque de la fonction sinus. En particulier, prenons garde à la quantification des égalités suivantes :
- si $x \in [-1, 1]$, $\sin(\arcsin(x)) = x$;
- si $x \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$, $\arcsin(\sin(x)) = x$.

La première égalité ne posera (normalement) jamais problème ; la seconde par contre peut amener quelques pièges vicieux. Par exemple, $\sin(\pi/2 + 2\pi) = 1$ et pourtant $\arcsin(\sin(\pi/2 + 2\pi)) = \arcsin(1) = \pi/2$.

Proposition IV.5. La fonction arcsin est une fonction continue strictement croissante de $[-1, 1]$ sur $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$. Il s'agit de plus d'une fonction impaire.

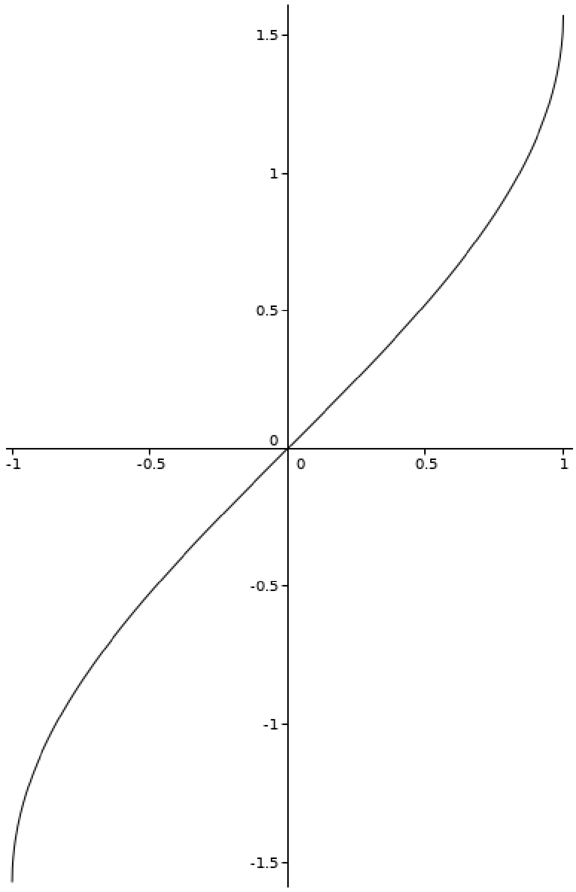
Démonstration. La seule chose qu'il nous reste à démontrer est l'imparité, qui est en fait un cas particulier d'un résultat général : si $f : E \to F$ est une impaire admettant une réciproque, alors pour tout $x \in F$ on a :

$$\begin{aligned} f^{-1}(-x) &= f^{-1}(-f(f^{-1}(x)) \\ &= f^{-1} \circ f(-f^{-1}(x)) \text{ car } f \text{ est impaire} \\ &= -f^{-1}(x) \end{aligned}$$

et donc f^{-1} est également impaire.

□

De tout ceci on peut déduire l'allure de la courbe représentative de arcsin ; il s'agit du symétrique de celle de $\widehat{\sin}$ par rapport à la première bissectrice.



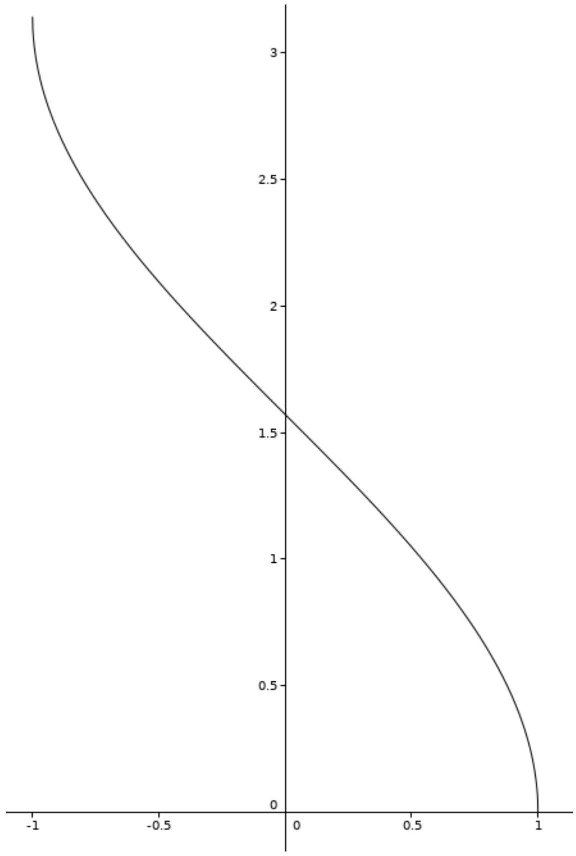
Définition IV.4. De façon analogue, on appelle **fonction arc cosinus** la réciproque de la fonction strictement décroissante

$$\begin{aligned} \widehat{\cos} : [0, \pi] &\to [-1, 1] \\ x &\mapsto \cos(x) \ . \end{aligned}$$

Il s'agit d'une fonction continue strictement décroissante qui n'est ni paire ni impaire.

Notation. arcos : $[-1, 1] \to [0, \pi]$

Les mêmes précautions d'usage sont à observer pour pour arcos que pour arcsin. Le graphique ci–dessous présente la courbe de arcos.



✌ **Remarque IV.2.** Soient $a, b, \theta \in \mathbb{R}$. Alors, si $u = \dfrac{a}{\sqrt{a^2+b^2}}$ et $v = \dfrac{b}{\sqrt{a^2+b^2}}$ on a $u, v \in [-1, 1]$ et $u^2+v^2 = 1$. De fait, on a, en posant $\varphi = \arccos(u)$ et $A = \sqrt{a^2+b^2}$:

$$\begin{aligned} a\cos(\theta) + b\sin(\theta) &= A(u\cos(\theta) + v\sin(\theta)) \\ &= A(\cos(\varphi)\cos(\theta) + \sin(\varphi)\sin(\theta)) \\ &= A\cos(\theta - \varphi) \,. \end{aligned}$$

Cette formule est particulièrement appréciée des physiciens pour des raisons qui leur sont propres.

✍ **Exercice IV.4.** Soit $x \in [-1, 1]$; déterminer une expression élémentaire de $\cos(\arcsin(x))$.

➥ **Correction :** *Remarquons tout d'abord que :*

$$\cos(\arcsin(x))^2 = 1 - \sin(\arcsin(x)^2 = 1 - x^2 \,.$$

Ainsi, on a :

$$|\cos(\arcsin(x)| = \sqrt{1-x^2} \,.$$

Or, $\arcsin(x) \in \left[-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right]$, *donc* $\cos(\arcsin(x) \geq 0$, *ce qui permet de conclure in fine que :*

$$\cos(\arcsin(x) = \sqrt{1-x^2} \,.$$

Proposition IV.6. Les fonctions arcsin et arcos sont dérivables sur $]-1,1[$ et leurs dérivées sont données par, pour $x \in]-1,1[$:

$$\arcsin'(x) = \frac{1}{\sqrt{1-x^2}}$$

et

$$\text{arcos}'(x) = -\frac{1}{\sqrt{1-x^2}} .$$

Démonstration. La démonstration est laissée en exercice au lecteur : il s'agit d'une application du théorème II.4 (dérivée d'une réciproque) et de l'exercice précédent. □

✌ **Remarque IV.3.** Le lecteur averti aura noté que ces fonctions ne sont pas dérivables en ± 1, qui sont les images des points d'annulation des dérivées de $\widehat{\sin}$ et $\widehat{\cos}$. Toute ceci sera approfondi au chapitre XI.

✍ **Exercice IV.5.** Démontrer que la fonction $\text{arcos} + \arcsin$ est constante égale à $\frac{\pi}{2}$.

Proposition IV.7. La fonction suivante est une fonction strictement croissante et continue admettant une réciproque :

$$\begin{aligned} \widehat{\tan} : \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[&\to \mathbb{R} \\ x &\mapsto \tan(x) . \end{aligned}$$

Démonstration. Il s'agit d'une conséquence immédiate du théorème II.4 et de l'étude précedemment menée de la fonction tangente. □

Définition IV.5. On appelle **fonction arc tangente** la réciproque de la fonction $\widehat{tan}$.

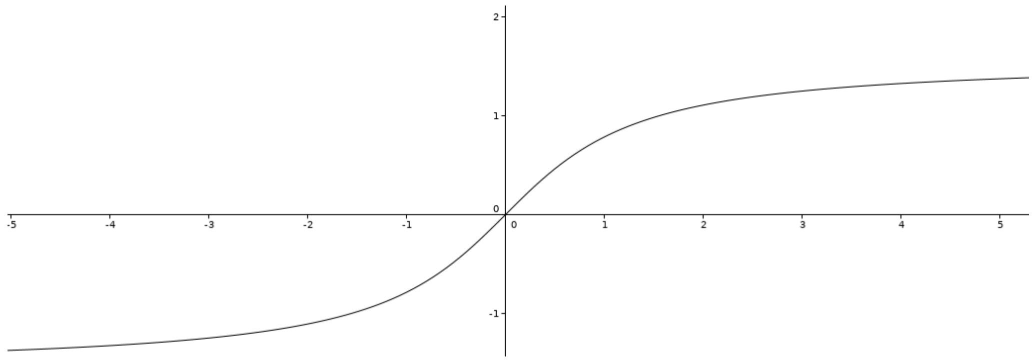
Notation. $\arctan : \mathbb{R} \to \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$

Proposition IV.8. La fonction arctan est une fonction continue impaire strictement croissante. De plus :

- $\arctan(x) \xrightarrow[x \to \pm\infty]{} \pm\pi/2$;
- arctan est dérivable sur $\mathbb{R}$ et, pour tout $x \in \mathbb{R}$:

$$\arctan'(x) = \frac{1}{1+x^2} .$$

Pour conclure, nous reproduisons ci–ensuite l'allure de la courbe représentative de la fonction arctan.



✍ **Exercice IV.6.** Étudier la fonction définie sur $\mathbb{R}^*$ par $x \mapsto \arctan\left(\frac{1}{x}\right)$.

2.⁻ Trigonométrie hyperbolique

a) Cosinus et sinus hyperboliques

Définition IV.6. Soit $x \in \mathbb{R}$; on appelle :
— **cosinus hyperbolique de** x le réel

$$\mathrm{ch}(x) = \frac{e^x + e^{-x}}{2} ;$$

— **sinus hyperbolique de** x le réel

$$\mathrm{sh}(x) = \frac{e^x - e^{-x}}{2} .$$

✌ **Remarque IV.4.** Ces formules nous permettent de définir deux fonctions $\mathrm{ch} : \mathbb{R} \to \mathbb{R}$ et $\mathrm{sh} : \mathbb{R} \to \mathbb{R}$.

Proposition IV.9. On a les résultats suivants :
(i) la fonction ch est paire ;
(ii) la fonction sh est impaire ;
(iii) les fonctions *ch* et sh sont dérivables ; de plus $\mathrm{ch}' = \mathrm{sh}$ et $\mathrm{sh}' = \mathrm{ch}$;
(iv) pour tout $x \in \mathbb{R}$, on a :

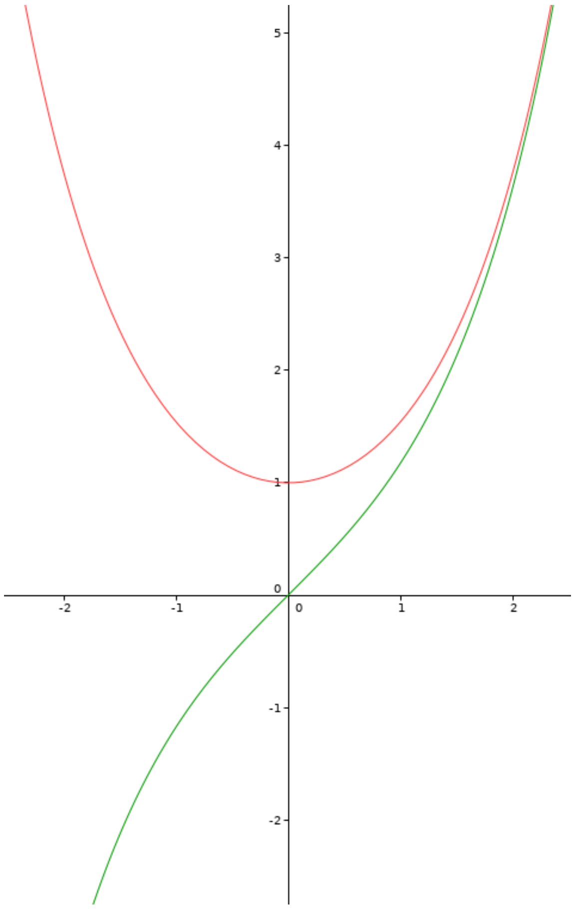
$$\mathrm{ch}^2(x) - \mathrm{sh}^2(x) = 1 .$$

Démonstration. Il s'agit d'une succession de calculs immédiats. □

Pour terminer, une brève étude de fonction révèle de plus les propriétés suivantes :
— ch est strictement positive, de valeur minimale $1 = \mathrm{ch}(0)$;
— $\mathrm{ch}(x) \xrightarrow[x\to\pm\infty]{} \infty$;

— $\operatorname{sh}(x) \xrightarrow[x\to\pm\infty]{} \pm\infty$.

Ceci nous permet de déduire l'allure des courbes représentatives de ces deux fonctions, reproduite ci–ensuite (ch en rouge, sh en vert).



b) Tangente hyperbolique

Définition IV.7. Soit $x \in \mathbb{R}$; on appelle **tangente hyperbolique de** x la quantité

$$\frac{\operatorname{sh}(x)}{\operatorname{ch}(x)} = \frac{e^{2x}-1}{e^{2x}+1}\,.$$

Notation. $\operatorname{th} : \mathbb{R} \to \mathbb{R}$

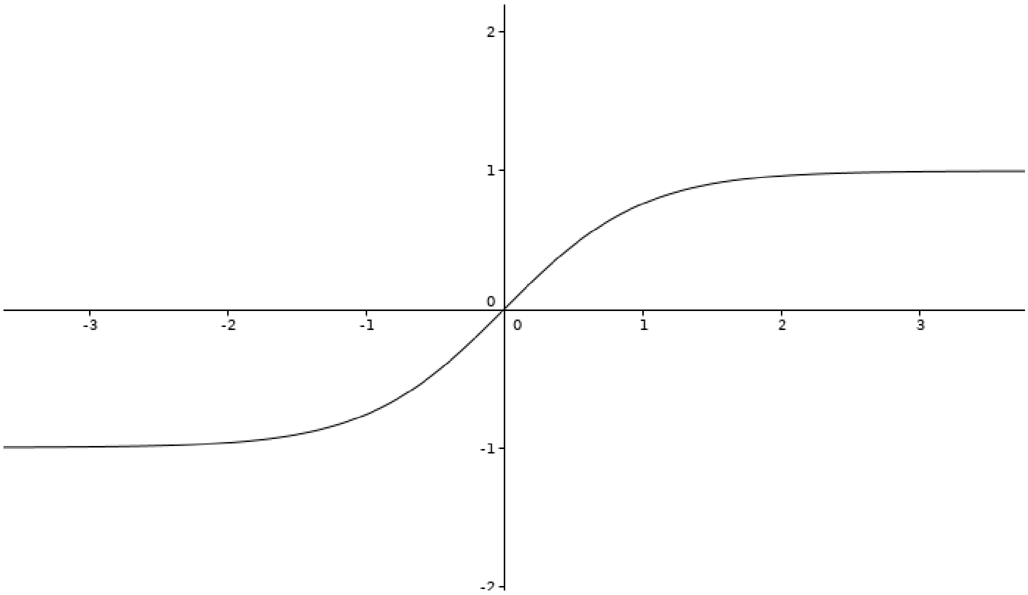
Proposition IV.10. La fonction th est impaire, strictement croissante et dérivable. Sa dérivée vérifie :

$$\operatorname{th}' = \frac{1}{\operatorname{ch}^2} = 1 - \operatorname{th}^2\,.$$

Un rapide calcul utilisant l'expression $\operatorname{th}(x) = \dfrac{e^{2x}-1}{e^{2x}+1}$ nous permet de déduire que (mettre en facteur le terme dominant au numérateur et dénominateur) :

$$\operatorname{th}(x) \xrightarrow[x\to\pm\infty]{} \pm 1\,.$$

Nous sommes donc en mesure de tracer l'allure de la courbe représentative de la fonction th.



3.⁻ Puissances

a) C'est quoi ?

Définition IV.8. Soit $a \in \mathbb{R}$. On appelle **fonction puissance** a la fonction

$$\begin{aligned} \phi_a : \mathbb{R}_+^* &\to \mathbb{R} \\ x &\mapsto e^{a\ln(x)} \end{aligned} .$$

Notation. Pour $x > 0$, on notera $x^a = \phi_a(x)$.

Remarque IV.5.

— Si a est un entier positif, $\phi_a(x) = \underbrace{x \times \ldots \times x}_{a \text{ fois}}$. On retrouve la définition usuelle de la puissance, ce qui est bienvenu. La fonction ϕ_a est alors bien définie sur $\mathbb{R}$.

— Si a est un entier strictement négatif,

$$\phi_a(x) = \underbrace{\frac{1}{x} \times \ldots \times \frac{1}{x}}_{a \text{ fois}} .$$

La fonction ϕ_a est alors bien définie sur $\mathbb{R}^*$.

— Dans tous les autres cas, la fonction ϕ_a n'est *a priori* bien définie que pour x **strictement positif**.

Exemple IV.1. Vous connaissez sans doute ϕ_2, ϕ_3 et leurs amies ; mais connaissez–vous ϕ_π ? Ou $\phi_{\frac{1}{2}}$?

Proposition IV.11. Soient $x, y \in \mathbb{R}_+^*$ et soient $a, b \in \mathbb{R}$. Alors :

(i) $x^a y^a = (xy)^a$;

(ii) $x^a x^b = x^{a+b}$;

(iii) $(x^a)^b = x^{ab}$;

(iv) $1^a = 1 = x^0$;

(v) $x^a = \dfrac{1}{x^{-a}}$

(vi) $\ln(x^a) = a\ln(x)$.

Démonstration. Utiliser la forme exponentielle. □

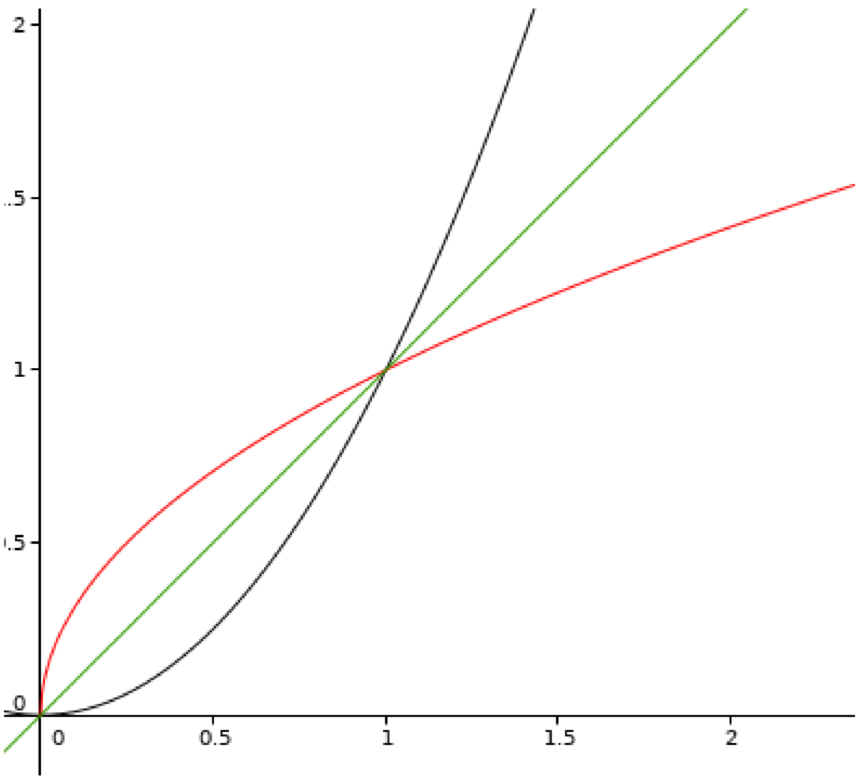
b) Variations

En utilisant la formule de dérivée d'une composée, on trouve, pour $x > 0$ et $a \in \mathbb{R}$:

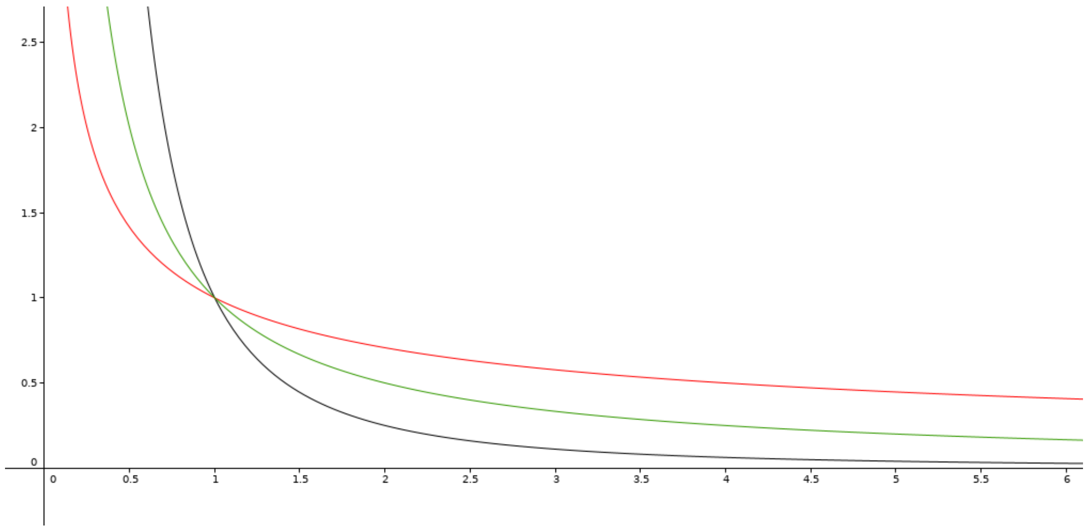
$$\boxed{\phi_a'(x) = ax^{a-1}} .$$

On retrouve de cette façon les dérivées usuelles suivantes vues en terminale : puissances entières, mais aussi puissances inverses, racine carrée. Cette formule est un véritable couteau suisse de la dérivation.

Concernant les limites, on remarque aisément que, si $a > 0$, $\phi_a(x) \xrightarrow[x \to 0]{} 0$. Ceci nous permet de poser la convention suivante : $0^a = 0$ pour tout $a > 0$. Ceci est à **ne pas confondre** avec x^0, qui vaut 1 quel que soit x et ce sans aucune ambiguïté. Pour l'allure des courbes, on différencie aisément les exposants $a > 1$ (forme parabolique convexe) des exposants $0 < a < 1$ (forme concave, penser racine carrée). Nous justifierons ces variations dans le paragraphe suivant.



La formule de la dérivée ci–dessus nous permet de justifier les variations vues précédemment dans le cas $a > 0$; le cas $a < 0$ apporte quant à lui son lot de courbes décroissantes, comme illustré ci–ensuite. Cette fois ci, les courbes dominantes à l'infini sont celles pour $|a| < 1$.



c) Racines

Définition IV.9. Soit $n \in \mathbb{N}^*$; la fonction $\phi_{\frac{1}{n}}$ est appelée **racine n–ième**.

Notation. $x \mapsto \sqrt[n]{x}$

Soit $x > 0$ et soit $n \geq 1$; effectuons un petit calcul :

$$\begin{aligned}\sqrt[n]{x^n} &= \phi_{\frac{1}{n}}(x^n) \\ &= \exp\left(\frac{1}{n}\ln(x^n)\right) \\ &= \exp(\ln(x)) \\ &= x\ .\end{aligned}$$

De la même façon, on vérifie que $(\sqrt[n]{x})^n = x$: **la fonction $\phi_{\frac{1}{n}}$ est donc la réciproque de ϕ_n.**

✌ **Remarque IV.6.**

— Si n est impair, il est possible d'étendre la fonction $\phi_{\frac{1}{n}}$ à $\mathbb{R}$ tout entier.
— Les fonctions racine ne sont jamais dérivables en 0.

Chapitre V

Applications, relations

1.⁻ Applications

a) C'est quoi ?

Définition V.1. Si E et F sont deux ensembles, on appellera **application** de E dans F la donnée de tout "mécanisme" f associant à chaque élément de E un unique élément de F, noté $f(x)$ et appelé **image** de x par f. L'ensemble E est alors appelé **ensemble de départ** de f, F son **ensemble d'arrivée** et $\mathscr{G} = \{(x, f(x)) \mid x \in E\} \subset E \times F$ son **graphe**.

Notation. $f : E \to F$ ou, plus complètement :

$$\begin{aligned} f : E &\to F \\ x &\mapsto f(x) . \end{aligned}$$

➠ **Exemple V.1.** Un exemple bien connu et qui nous exploiterons au delà de toute raison est celui de la fonction "carré" !

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R}_+ \\ x &\mapsto x^2 . \end{aligned}$$

✌ **Remarque V.1.** Deux applications seront donc considérées comme égales si elles ont même ensemble de départ, même ensemble d'arrivée et même graphe. Cela n'est pas sans soulever quelques problèmes concernant l'ensemble d'arrivée : celui de la fonction ci–dessus est $\mathbb{R}_+$, mais pourrait être (entre autres) $\mathbb{R}$ …Il nous faudra donc faire preuve de vigilance, mais parfois aussi de souplesse.

Notation. L'ensemble des fonctions partant d'un ensemble E et arrivant dans un ensemble F sera noté $\mathscr{F}(E, F)$ ou F^E.

✌ **Remarque V.2.** Mettons en exergue quelques cas particuliers :
- l'ensemble $E^{\mathbb{N}}$ est l'ensemble des fonctions de $\mathbb{N}$ dans E, que vous connaissiez déjà sous le nom de **suites** (si, si). On utilisera la notation u_n (pour $n \in \mathbb{N}$) pour $u(n)$ et $(u_n)_{n\in\mathbb{N}}$ (ou simplement $(u_n)_n$) pour u ;
- plus généralement, une **famille** d'éléments de E indexées par un ensemble I est en réalité une application de I dans E.

b) Restrictions, prolongements

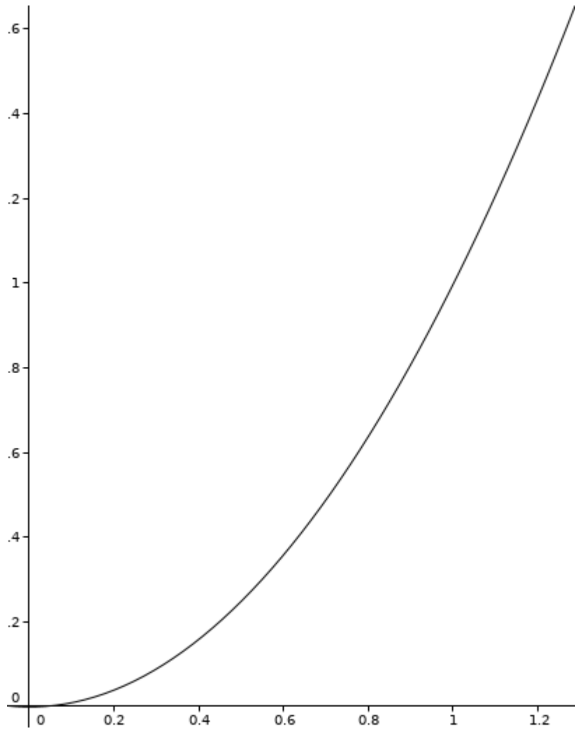
L'objectif de ce paragraphe est d'étudier deux méthodes nous permettant de modifier l'ensemble de départ d'une application en agissant de façon "naturelle" sur son graphe.

Définition V.2. Soit $f : E \to F$ une application et soit $E' \subset E$. On appelle **restriction de f à E'** l'application

$$\begin{aligned} f_{|E'} : E' &\to F \\ x &\mapsto f(x) \,. \end{aligned}$$

✌ **Remarque V.3.** La restriction de f à E' est unique.

➠ **Exemple V.2.** La restriction de $x \mapsto x^2$ à $\mathbb{R}_+$ correspond au graphe ci–ensuite.



Définition V.3. Soit $f : E \to F$ une application et soit E' un ensemble contenant E. On appelle **prolongement de f à E'** toute application $g : E' \to F$ telle que $g_{|E} = f$.

✌ **Remarque V.4.** Il n'y a **PAS** unicité du prolongement de f à E'. Par exemple, la fonction

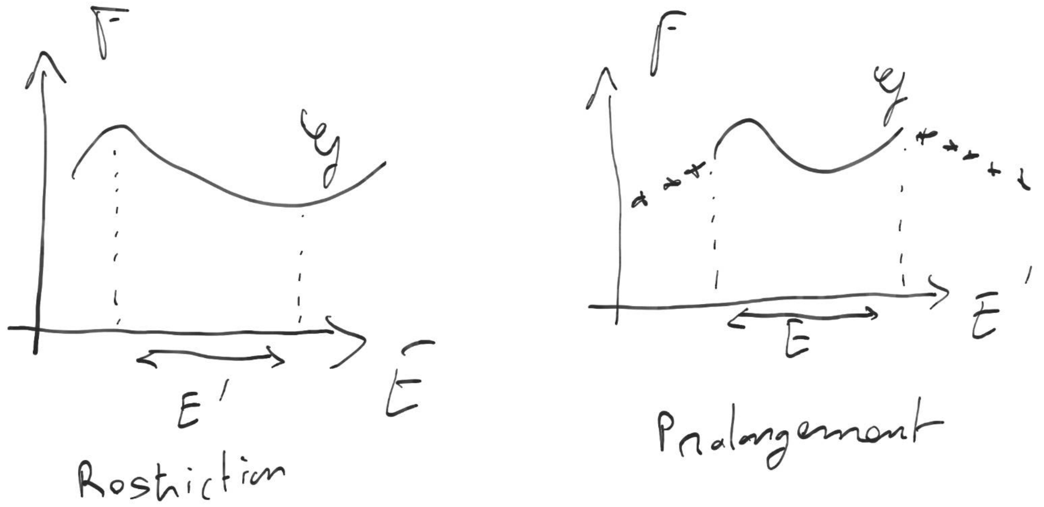
$$\begin{aligned} f : \mathbb{R}_+ &\to \mathbb{R}_+ \\ x &\mapsto x^2 \end{aligned}$$

admet pour prolongements à $\mathbb{R}$ toutes les applications du type

$$f_\alpha : \mathbb{R} \longrightarrow \mathbb{R}_+$$
$$x \mapsto \begin{cases} x^2 & \text{si } x \geq 0 \\ \alpha + 42 & \text{sinon} \end{cases}$$

pour $\alpha \in \mathbb{R}_+$

Moralement, une restriction revient donc à "couper" le graphe pour n'en garder qu'une partie, alors qu'un prolongement est un extension du graphe par des points choisis aribitrairement.



c) Injections, surjections, bijections

Disons le d'entrée de jeu : ce paragraphe est **absolument fondamental**. Voyez le un peu un rhinocéros enragé courant dans votre direction : à ignorer à vos risques et périls.

Définition V.4. Soit $f : E \to F$ une application et soit $y \in F$. Un élément x de E est appelé **antécédent de** y **par** f si $f(x) = y$.

➠ **Exemple V.3.** Un point de l'ensemble de départ peut avoir n'importe quel nombre d'antécédent(s) par l'application : penser -1 pour $x \mapsto x^2$ (0 antécédent), 0 et 1 pour cette même fonction (1 et 2 antécédents respectivement), 14 pour la fonction constante égale à 14 (une infinité d'antécédents).

Définition V.5. Une application $f : E \to F$ est dite :
- **injective** si pour tout point F admettant un antécédent par f, ce dernier est unique ;
- **surjective** si tout point F admet au moins un antécédent par f ;
- **bijective** si tout point F admet exactement un antécédent par f.

Remarque V.5.
- Une application est donc bijective si et seulement si elle est injective **et** bijective.
- Géométriquement, le caractère inj/surj/bijectif d'une application peut être observé *via* le nombre de points d'intersection entre sa courbe représentative et une droite horizontale.

Notation. L'ensemble des bijections de E dans F sera noté $\mathfrak{S}(E,F)$ ou $S(E,F)$. Lorsque $E=F$, on notera $\mathfrak{S}_E$ ou S_E.

Exemple V.4. "Par lecture graphique" (et rigoureusement, aussi), on peut remarquer que les fonctions périodiques type (co)sinus ne sont pas injectives, que $x\mapsto x$ est bijective et que $\exp:\mathbb{R}\to\mathbb{R}$ est injective non surjective.

Remarque V.6. Ces notions demandent de définir avec **précision et rigueur** les applications sur lesquelles nous travaillons. Par exemple, la fonction $x\mapsto x^2$ est :
- surjective non injective de $\mathbb{R}$ dans $\mathbb{R}_+$;
- injective non surjective de $\mathbb{R}_+$ dans $\mathbb{R}$;
- bijective de $\mathbb{R}_+$ dans $\mathbb{R}_+$;
- rien du tout de $\mathbb{R}$ dans $\mathbb{R}$.

Proposition V.1. Soit $f:E\to F$ une application. Alors :

$$f \text{ est injective}$$
$$\Longleftrightarrow$$
$$\forall x,x'\in E,\quad (f(x)=f(x'))\Rightarrow(x=x')\ .$$

Démonstration.

($\Uparrow$) Immédiat par définition d'antécédent.

($\Downarrow$) Soit $y\in F$ et soient x,x' deux antécédents de f. Alors $f(x)=f(x')=y$ donc $x=x'$. L'application f est donc injective.

□

Remarque V.7. Cela signifie que pour montrer que f est injective, il faut et il suffit de montrer que si x,x' sont tels que $f(x)=f(x')$ alors $x=x'$. **Cette méthode est à privilégier en pratique.**

Exemple V.5. Cette méthode permet aisément de démontrer que $x\mapsto x^3$ est injective sur $\mathbb{R}$ (passer à la racine cubique).

d) Composition

Définition V.6. Soient $f:E\to F$ et $g:F\to G$ deux applications. On appelle **composée** de g par f l'application

$$\begin{aligned} g\circ f: E &\longrightarrow G\\ x&\mapsto g(f(x))\ . \end{aligned}$$

Remarque V.8.
- **Attention au sens de composition :** la composée $g \circ f$ applique d'abord f, puis g.

$$\begin{tikzcd} E \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & F \arrow[r, "g"] & G \end{tikzcd}$$

- La composition des applications est associative ; la démonstration de ce résultat est un exercice aisé.
- La composition n'est **PAS** commutative ; regarder par exemple $f : x \mapsto x+1$ et $x \mapsto x^2$ (définies sur $\mathbb{R}$).

Définition V.7. Soit E un ensemble. On appelle **identité** de E l'application

$$\begin{aligned} \mathrm{id}_E : E &\to E \\ x &\mapsto x\ . \end{aligned}$$

Remarque V.9. Pour toute application $f \in E^E$, on a $f \circ \mathrm{id}_E = \mathrm{id}_E \circ f = f$. On dit que id_E est un **élément neutre** pour la composition des applications.

Proposition V.2. La composée de deux injections (resp. surjections, bijections) est une injection (resp. surjection, bijection).

Démonstration. Immédiat via la définition. □

Exemple V.6. Si f est une injection à valeurs réelles, la fonction $x \mapsto e^{f(x)}$ est injective.

Exercice V.1. Soient E, F deux ensembles **non vides** et soit $f : E \to F$ une application. Démontrer que :

1. f est injective $\Leftrightarrow \exists\, g : F \to E$ telle que $g \circ f = \mathrm{id}_E$ **[inversibilité à gauche]** ;
2. f est surjective $\Leftrightarrow \exists\, g : F \to E$ telle que $f \circ g = \mathrm{id}_F$ **[inversibilité à droite]**.

L'inverse à droite (resp. à gauche) d'une surjection (resp. d'une injection) est donc une injection (resp. une surjection).

Correction :

1. ($\Rightarrow$) *Supposons f injective et fixons un élément arbitraire $\mho \in E$. Nous pouvons alors définir g par le procédé suivant : pour tout $y \in F$, soit y admet un (unique) antécédent $x \in E$ et dans ce cas nous posons $g(y) = x$, soit ce n'est pas le cas et alors nous fixons $g(y) = \mho$.*

($\Leftarrow$) *Supposons f inversible à gauche d'inverse $g : F \to E$ et soient $x, x' \in E$ tels que $f(x) = f(x')$. Alors, en composant cette égalité à gauche par g nous obtenons $g \circ f(x) = g \circ f(x')$, i.e $x = x'$. On en déduit que f est bien injective.*

2. ($\Rightarrow$) *Supposons f surjective. Alors, pour tout $y \in F$, il existe $x \in E$ tel que $y = f(x)$; il nous suffit de poser $g(y) = x$ pour avoir $f \circ g(y) = f(x) = y$.*

   ($\Leftarrow$) *Supposons f inversible à droite d'inverse $g : F \to E$. Alors, pour tout $y \in F$, on a $f(g(y)) = y$; $g(y)$ est donc un antécédent de y, ce qui prouve la surjectivité de f.*

Proposition V.3. Soient E, F deux ensembles **non vides** et soit $f : E \to F$ une application. Alors :

(i) f est bijective $\Leftrightarrow$ f $\exists g : F \to E$ telle que $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$;

(ii) dans ce cas, la fonction g est unique. On l'appelle réciproque de f.

Notation. SI f est bijective, on note sa réciproque f^{-1}.

✌ **Remarque V.10.** Au risque de me répéter, on n'utilise la notation f^{-1} **que** lorsque f est **bijective**.

Démonstration. Le point (i) est une conséquente de l'exercice V.1. Pour montrer que les inverses à gauche et à droite sont uniques et identiques, notons g et g' deux inverses à gauche de f et h un inverse à droite de cette même application ; alors, comme $f \circ h = \mathrm{id}_F$, on a :

$$g \circ f \circ h = g' \circ f \circ h = h$$

ce qui donne, en simplifiant $g = g' = h$. □

➠ **Exemple V.7.** L'application

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N}^* \\ n &\mapsto n+1 \end{aligned}$$

est bijective, de réciproque

$$\begin{aligned} g : \mathbb{N}^* &\to \mathbb{N} \\ n &\mapsto n-1\,. \end{aligned}$$

Cet exemple est à rapprocher d'un problème attribué à David Hilbert (1862–1943) : "étant donné un hotel complet possèdant une infinité de chambres, comment accomoder un invité de plus ?".

Proposition V.4. Soient $f : E \to F$ et $g : F \to G$ deux bijections. Alors :

(i) f^{-1} est une bijection de F dans E, de réciproque $(f^{-1})^{-1} = f$;

(ii) $g \circ f$ est une bijection de E dans G, de réciproque

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}\,.$$

Démonstration. Comme les réciproques sont uniques, il nous suffit de vérifier que les applications proposées ci–dessus remplissent bien le contrat, ce qui est immédiat. □

e) Images directe et réciproque

Définition V.8. Soit $f : E \to F$ une application. Alors :

(i) si $A \subset E$, on appelle **image (directe) de** A **par** f l'ensemble

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

(ii) si $B \subset F$, on appelle **image réciproque de** B **par** f l'ensemble

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

✌ **Remarque V.11.**

— Les esprits acérés auront remarqué que nous utilisons la notation $f^{-1}(B)$ alors que l'application n'est pas bijective ...C'est triste, et cela signifie qu'il faudra être bien vigilant à ne pas confondre image directe par l'application réciproque (chose existant uniquement dans le cas bijectif) et image réciproque (machin existant quoi qu'il arrive). La seule bonne nouvelle dans tout cela est que si f est bijective, alors ces deux concepts coïncident. Il faut savoir se satisfaire de peu.
— Si $y \in F$, alors $f^{-1}(\{y\})$ est l'ensemble des antécédents de y.
— On remarque que f est surjective si et seulement si $f(E) = F$.

➠ **Exemple V.8.**

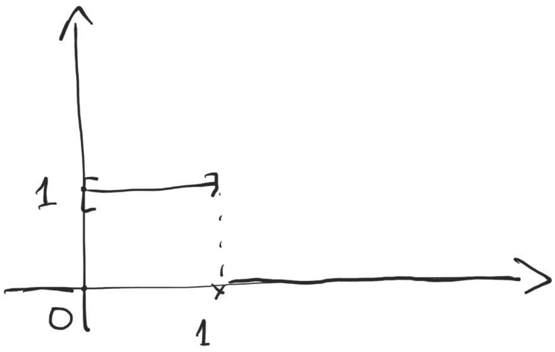
— Pour $f : x \mapsto x^2$, $f^{-1}([0, 4]) = [-2, 2]$;
— $\sin^{-1}(\{0\}) = \pi\mathbb{Z} = \{\pi k \,|\, k \in \mathbb{Z}\}$;
— $\exp(\mathbb{R}_+) = [1, \infty[$.

f) Indicatrices

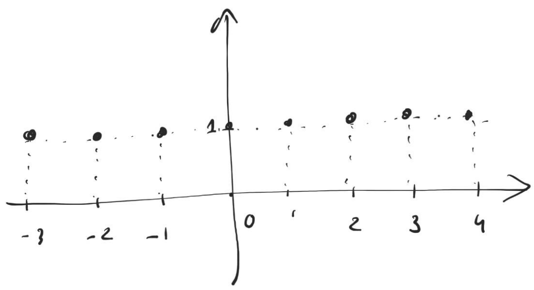
Définition V.9. Soit E un ensemble et soit $A \subset E$. On appelle **fonction indicatrice** (ou caractéristique) de A l'application

$$\begin{aligned} \mathbb{1}_A : E &\longrightarrow \{0, 1\} \\ x &\mapsto \begin{cases} 0 & \text{si } x \notin A \\ 1 & \text{si } x \in A \,. \end{cases} \end{aligned}$$

➠ **Exemple V.9.** Pour $E = \mathbb{R}$, $\mathbb{1}_{\mathbb{R}}$ est la fonction constante égale à 1, $\mathbb{1}_{[0,1]}$ ressemble à ça :



et celle de $\mathbb{Z}$ à ceci.



Nous laissons l'entière responsabilité au lecteur et à son futur psychiatre d'imaginer l'indicatrice de $\mathbb{Q}$.

✍ **Exercice V.2.** Soit E un ensemble et soient $A, B \in \mathscr{P}(E)$. Démontrer que :

1. $\mathbb{1}_{A\cap B} = \mathbb{1}_A \times \mathbb{1}_B$;
2. $\mathbb{1}_{A\cup B} = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_A \times \mathbb{1}_B$;
3. $\mathbb{1}_{B\setminus A} = \mathbb{1}_B(\mathbb{1}_B - \mathbb{1}_A)$;
4. $\mathbb{1}_{\bar{A}} = 1 - \mathbb{1}_A$.

➥ **Correction :**

1. Soit $x \in E$; alors

$$\begin{aligned}\mathbb{1}_{A\cap B}(x) = 1 &\Leftrightarrow x \in A \cap B\\ &\Leftrightarrow (x \in A) \wedge (x \in B)\\ &\Leftrightarrow (\mathbb{1}_A(x) = 1) \wedge (\mathbb{1}_B(x) = 1)\,.\end{aligned}$$

De fait, on a bien $\mathbb{1}_{A\cap B} = \mathbb{1}_A \times \mathbb{1}_B$.

2. De la même façon, on vérifie que, si $x \in E$:

$$\begin{aligned}\mathbb{1}_{A\cup B}(x) = 1 &\Leftrightarrow x \in A \cup B\\ &\Leftrightarrow (x \in A) \vee (x \in B)\\ &\Leftrightarrow (\mathbb{1}_A(x) = 1) \vee (\mathbb{1}_B(x) = 1)\,.\end{aligned}$$

Ici, il faut prendre garde au cas où $x \in A\cap B$, qui impose la formule suivante :

$$\mathbb{1}_{A\cup B} = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_{A\cap B} = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_A \times \mathbb{1}_B\,.$$

3. Soit $x \in E$; alors

$$\begin{aligned}\mathbb{1}_{B\setminus A}(x) = 1 &\Leftrightarrow x \in B \setminus A \\ &\Leftrightarrow (x \in B) \wedge (x \notin A) \\ &\Leftrightarrow (\mathbb{1}_B(x) = 1) \wedge (\mathbb{1}_A(x) = 0) .\end{aligned}$$

De fait, on a bien $\mathbb{1}_{B\setminus A} = \mathbb{1}_B(\mathbb{1}_B - \mathbb{1}_A)$.

4. En appliquant la question précédente à $B = E$, on trouve $\mathbb{1}_{\bar{A}} = 1 - \mathbb{1}_A$.

2.⁻ Relations d'ordre

a) Relations binaires

Définition V.10. Soit E un ensemble. On appelle **relation** (binaire) sur E la donnée d'un couple $\mathscr{R} = (E, \mathscr{G})$, avec $\mathscr{G} \subset E \times E$.

Notation. Si $(x, y) \in \mathscr{G}$, on notera $x\mathscr{R}y$ et on dira que x **et** y **sont en relation via** $\mathscr{R}$.

➠ **Exemple V.10.**
— $\mathscr{R}_0 = (\mathbb{R}, \{(x, -x) \,|\, x \in \mathbb{R}\})$ correspond à la relation "être égal au signe près" ;
— $\mathscr{R}_1 = (\mathbb{N}, \{(n, 2n) \,|\, n \in \mathbb{N}\})$ correspond à la relation "être le double de".

b) Ensembles ordonnés

Définition V.11. Soit E un ensemble et $\mathscr{R}$ une relation sur E. On dit que $\mathscr{R}$ est une **relation d'ordre** si :
— $\forall x \in E$, $x\mathscr{R}x$ **[reflexivité]** ;
— $\forall x, y \in E$, $(x\mathscr{R}y) \wedge (y\mathscr{R}x) \Rightarrow (x = y)$ **[antisymétrie]** ;
— $\forall x, y, z \in E$, $(x\mathscr{R}y) \wedge (y\mathscr{R}z) \Rightarrow (x\mathscr{R}z)$ **[transitivité]**.
La donnée du couple $(E, \mathscr{R})$ est appelée **ensemble ordonné**.

➠ **Exemple V.11.**
— $(\mathbb{R}, \leq)$ est un ensemble ordonné, avec $\leq$ la relation $(\mathbb{R}, \{(x, y) \,|\, y - x \in \mathbb{R}_+\})$;
— $(\mathscr{P}(E), \subset)$ est un ensemble ordonné ;
— $(\mathbb{N}, |\,)$ est un ensemble ordonné ;
— si E et F sont ordonnés, F^E est ordonné (*cf.* chapitre II).

Définition V.12. Soit $(E, \mathscr{R})$ un ensemble ordonné. On dit que $\mathscr{R}$ est un **ordre total** si

$$\forall x, y \in E, \quad (x\mathscr{R}y) \vee (y\mathscr{R}x) .$$

Dans le cas contraire, on parle d'**ordre partiel**.

Exemple V.12. L'ordre classique sur $\mathbb{N}$ est total ; l'inclusion sur $\mathscr{P}(E)$ est partiel dès que E possède au moins deux éléments car $\mathscr{P}(E)$ contient alors deux singletons disjoints.

c) Majorants, minorants

Définition V.13. Soit $(E, \leq)$ un ensemble ordonné et soit $A \subset E$. On dit que $x \in E$ est un…
- …**majorant de** A si $\forall a \in A$, $a \leq x$;
- …**minorant de** A si $\forall a \in A$, $a \geq x$.

Un majorant (resp. minorant) de A appartenant à A est appelé **plus grand élément** (resp. **plus petit élément**) ou maximum (resp. minimum) de A.

Notation. $\max(A)$, $\min(A)$.

Remarque V.12. On démontre aisément que plus petit et plus grand élément sont uniques lorsqu'ils existent.

Exemple V.13.
- $(\mathbb{R}, \leq)$ n'est pas minoré ni majoré ;
- $([0, 1[, \leq)$ est majoré par 1 qui n'est pas son maximum ;
- $(\mathbb{N}, |)$ admet pour minimum 1 et maximum 0 (en effet, tout entier n divise 0 car $0 = n \times 0$) ;
- $(\mathscr{P}(E), \subset)$ est minoré par $\emptyset$ et majoré par E. Ces deux derniers sont respectivement le plus petit et plus grand élément de $\mathscr{P}(E)$.

Remarque V.13. Merci de **ne pas confondre** minorant (resp. majorant) et minimum (resp. maximum). Penser à $]0, 1[$ muni de l'ordre classique en cas de crise de foi.

Vocabulaire. Un ensemble majoré et minoré est dit **borné**.

3.⁻ Relations d'équivalence

a) C'est quoi ?

Définition V.14. Soit E un ensemble et $\mathscr{R}$ une relation sur E. On dit que $\mathscr{R}$ est une **relation d'équivalence** si :
- $\forall x \in E$, $x \mathscr{R} x$ **[reflexivité]** ;
- $\forall x, y \in E$, $(x \mathscr{R} y) \Rightarrow (y \mathscr{R} x)$ **[symétrie]** ;
- $\forall x, y, z \in E$, $(x \mathscr{R} y) \wedge (y \mathscr{R} z) \Rightarrow (x \mathscr{R} z)$ **[transitivité]**.

Exemple V.14.
- L'égalité est une relation d'équivalence sur tout ensemble.
- La relation triviale (E, E^2) est une relation d'équivalence sur tout ensemble E.

✍ **Exercice V.3.** Soit $f : E \to F$ une application. Démontrer que la relation $\mathscr{R}$ définie sur E par
$$x\mathscr{R}y \iff f(x) = f(y)$$
est une relation d'équivalence.

➥ **Correction :** *Un sage a dit : "Yaka écrire", et il avait raison.*

b) Congruences

◇ **Sur $\mathbb{Z}$**

Définition V.15. Soient $a, b, n \in \mathbb{Z}$. On dit que a **est congru à** b **modulo** n si il existe $k \in \mathbb{Z}$ tel que $b = a + kn$.

Notation. $a \equiv b\,[n]$.

➠ **Exemple V.15.** $3 \equiv 1\,[2]$, $9 \equiv -1\,[10]$.

✌ **Remarque V.14.**
- — La congruence modulo 0 est l'égalité.
- — La congruence modulo 1 est la relation triviale.
- — Remplacer n par $-n$ ne change absolument rien. On peut donc supposer $n \in \mathbb{N}$ sans perdre de généralité.

Proposition V.5. Soit $n \in \mathbb{N}$; alors la congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

Démonstration.
- — La reflexivité est immédiate.
- — Soient $a, b \in \mathbb{Z}$ tels que $a \equiv b\,[n]$. Alors il existe $k \in \mathbb{Z}$ tel que $b = a + kn$, ce qui entraîne $a = b + (-k)n$ et donc $b \equiv a\,[n]$, d'où la symétrie.
- — Soient $a, b, c \in \mathbb{Z}$ tels que $a \equiv b\,[n]$ et $b \equiv c\,[n]$. Ceci signifie qu'il existe $k, \ell \in \mathbb{Z}$ tels que $b = a + kn$ et $c = b + \ell n$; ainsi
$$c = b + \ell n = a + kn + \ell n = a + (k + \ell)n$$
et donc $a \equiv c\,[n]$, d'où la transitivité.

□

◇ **Sur $\mathbb{R}$**

Définition V.16. Soient $a, b, \alpha \in \mathbb{R}$. On dit que a **est congru à** b **modulo** α si il existe $k \in \mathbb{Z}$ tel que $b = a + kn$.

Notation. $a \equiv b\,[\alpha]$.

Remarque V.15.
- Remarquons que le "k" de la définition est **entier**.
- Les relations de congruence modulo π et 2π sont chères aux physiciens et utiles en trigonométrie. Nous y reviendrons.

Proposition V.6. Soit $\alpha \in \mathbb{R}$; alors la congruence modulo α est une relation d'équivalence sur $\mathbb{R}$.

Démonstration. Identique au cas entier. □

c) Partitions, classes d'équivalences

Définition V.17. Soit E un ensemble. On appelle **partition** de E toute famille $(X_i)_{i\in I}$ de parties de E telle que :
- $\forall i \in I,\ X_i \neq \emptyset$;
- $\forall i, j \in I,\ (i \neq j) \Rightarrow X_i \cap X_j = \emptyset$;
- $$E = \bigcup_{i\in I} X_i\,.$$

Notation. Les X_i étant deux à deux disjoints, on pourra écrire

$$E = \overset{n}{\bigsqcup_{i\in I}} X_i$$

pour souligner ce fait.

Remarque V.16. Lorsque $E \subset \bigcup_{i\in I} X_i$, on parlera de **recouvrement disjoint** plutôt que de partition.

Exemple V.16.
- $(\mathbb{R}_+, \mathbb{R}_-^*)$ constitue une partition de $\mathbb{R}$;
- $\mathbb{N}$ est partitionné par les ensembles des entiers pairs et impairs ;
- on peut partitionner l'ensemble des réels comme suit (entre autres !) :

$$\mathbb{R} = \bigsqcup_{n\in\mathbb{Z}} [n, n+1[\,.$$

Exercice V.4. Démontrer qu'une application $f : E \to F$ est surjective si et seulement si E est partitionné par la famille $(f^{-1}\{y\})_{y\in F}$.

Définition V.18. Soit E un ensemble muni d'une relation d'équivalence $\mathscr{R}$ et soit $x \in E$. On appelle **classe de x modulo $\mathscr{R}$** l'ensemble

$$\overline{x} = \{y \in E \mid x\mathscr{R}y\}\,.$$

✌ **Remarque V.17.** Soient $x, y \in E$; alors :
— $y \in \bar{x} \iff x\mathscr{R}y \iff \bar{x} = \bar{y}$;
— $\bar{x} \cap \bar{y} \neq \emptyset \iff \bar{x} = \bar{y}$.

✍ **Exercice V.5.** On munit $\mathbb{N}^2$ de la relation suivante $\sim$ définie par :

$$(a, b) \sim (c, d) \iff a + d = b + c\,.$$

1. Démontrer que ceci définit une relation d'équivalence.
2. Établir une bijection entre l'ensemble des classes modulo $\sim$ et $\mathbb{Z}$.

Proposition V.7. Soit E un ensemble muni d'une relation d'équivalence $\mathscr{R}$. Alors les classes d'équivalence modulo $\mathscr{R}$ forment une partition de l'ensemble E.

Démonstration. En exercice ; découle de la définition de relation d'équivalence. □

Cette notion sera approfondie plus tard (principalement en MP) autour de l'exemple suivant : si $n \in \mathbb{N}^*$, il existe n classes d'équivalences disjointes pour la congruence modulo n sur $\mathbb{Z}$: $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. L'ensemble quotient est alors noté $\mathbb{Z}/n\mathbb{Z}$.

✌ **Remarque V.18.** Ce résultat est une équivalence : de toute partition ont peut construire une relation d'équivalence définie par l'appartenance à une même "composante".

Chapitre VI

Nombres complexes

1.⁻ Le corps $\mathbb{C}$ des nombres complexes

a) C'est quoi ?

L'ensemble $\mathbb{C} = \{a+ib \mid a, b \in \mathbb{R}\}$ est muni d'une structure de corps (*cf.* chapitre VIII). Il n'admet toutefois pas d'ordre "naturel" comme $\mathbb{R}$ ou $\mathbb{Q}$. Plus précisément, nous baserons ce chapitre sur le résultat (admis) suivant.

Théorème VI.1 (Corps des nombres complexes)**.**
Il existe un "unique" (à isomorphisme près) corps $(\mathbb{C}, +, \times)$ tel que :

(A) $\mathbb{R} \subset \mathbb{C}$ avec préservation de l'addition et de la multiplication ;

(B) il existe $i \in \mathbb{C}$ tel que $i^2 = -1$.

Dans ce cas, pour tout $z \in \mathbb{C}$, il existe un unique couple $(a, b) \in \mathbb{R}^2$ tel que $z = a+ib$. On appelle a (resp. b) la **partie réelle** (resp. **partie imaginaire**) de z, notée $\mathrm{Re}(z)$ (resp. $\mathrm{Im}(z)$).

Notation. On notera $i\mathbb{R}$ l'ensemble des **imaginaires purs**, à savoir $i\mathbb{R} = \{ib \mid b \in \mathbb{R}\}$. On a alors immédiatement que $\mathbb{R} \cap i\mathbb{R} = \{0\}$.

✌ **Remarque VI.1.**

— **Attention :** si $z \in \mathbb{C}$, $\mathrm{Re}(z), \mathrm{Im}(z) \in \mathbb{R}$. De plus $\mathbb{C} \neq \mathbb{R} \cup i\mathbb{R}$ (penser à $1 + i$, par exemple).

— Si $z, z' \in \mathbb{C}$ et $\lambda \in \mathbb{R}$, on a :

$$\mathrm{Re}(z + \lambda z') = \mathrm{Re}(z) + \lambda \mathrm{Re}(z') \quad \text{et} \quad \mathrm{Im}(z + \lambda z') = \mathrm{Im}(z) + \lambda \mathrm{Im}(z')\,.$$

— Si $z \in \mathbb{C}$, alors $z \in \mathbb{R} \Leftrightarrow \mathrm{Im}(z) = 0$ et $z \in i\mathbb{R} \Leftrightarrow \mathrm{Re}(z) = 0$.

— Si $z, z' \in \mathbb{C}$ alors on a, en posant $z = a + ib$ et $z' = c + id$, les formules suivantes :

$$z + z' = (a + c) + i(b + d) \quad \text{et} \quad zz' = ac - bd + i(ad + bc)\,.$$

— Le choix du nombre complexe i est arbitraire : on pourrait tout à fait choisir son opposé et développer exactement la même théorie.

— Les formules et techniques de calculs vues dans le chapitre II se généralisent, comme nous l'avions divulgâché, aux nombres complexes.

b) Lien au plan $\mathbb{R}^2$

On peut identifier $\mathbb{C}$ au plan $\mathbb{R}^2$ via la bijection suivante :

$$\begin{aligned}\varphi : \mathbb{C} &\to \mathbb{R}^2\\ z &\mapsto (\mathrm{Re}(z), \mathrm{Im}(z))\end{aligned}$$

de réciproque

$$\begin{aligned}\psi : \mathbb{R}^2 &\to \mathbb{C}\\ (x,y) &\mapsto x+iy\end{aligned} \quad .$$

Vocabulaire.

— Si $A \in \mathbb{R}^2$, le nombre complexe $\psi(A)$ est appelé **affixe** de A.

— Si $z \in \mathbb{C}$, le point du plan $\varphi(z)$ est appelé **image** de z.

✍ **Exercice VI.1.** Placer dans le plan les points d'affixes $1, i, 1+i, 1-i$ et $\dfrac{i}{2}$.

✌ **Remarque VI.2.** Géométriquement, on peut interpréter la somme de deux nombres complexes comme une translation (*cf.* paragraphe 4.⁻).

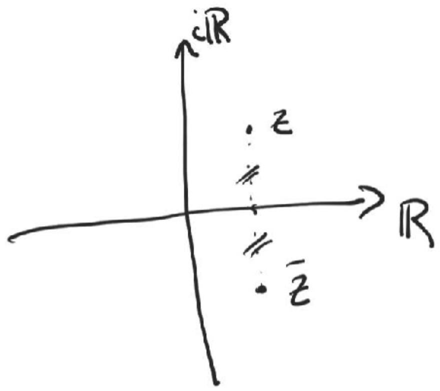
c) Conjugaison

Définition VI.1. Soit $z \in \mathbb{C}$; on appelle **conjugué** de z le nombre complexe

$$\overline{z} = \mathrm{Re}(z) - i\mathrm{Im}(z)\ .$$

➠ **Exemple VI.1.** $\overline{1+4i} = 1-4i$.

✌ **Remarque VI.3.** Géométriquement, l'image de $\overline{z}$ est le symétrique de celle de z par rapport à la droite rélle.



Proposition VI.2. Soit $z \in \mathbb{C}$; alors :

(i) $\mathrm{Re}(z) = \dfrac{z+\overline{z}}{2}$ et $\mathrm{Im}(z) = \dfrac{z-\overline{z}}{2i}$;

(ii) $\overline{\overline{z}} = z$;

(iii) $z \in \mathbb{R} \Leftrightarrow \overline{z} = z$;

(iv) $z \in i\mathbb{R} \Leftrightarrow \overline{z} = -z$

Démonstration. Il s'agit de calculs immédiats. Pour (iii) et (iv), utiliser (i). □

✌ **Remarque VI.4.** Les points (iii) et (iv) sont particulièrement utiles en pratique pour démontrer qu'un nombre complexe est en fait réel ou imaginaire pur.

Proposition VI.3. Soient $z, z' \in \mathbb{C}$. Alors :

(i) $\overline{z+z'} = \overline{z} + \overline{z'}$;

(ii) $\overline{zz'} = \overline{z}\,\overline{z'}$;

(iii) **si** $z' \neq 0$, $\overline{\left(\frac{z}{z'}\right)} = \frac{\overline{z}}{\overline{z'}}$.

Démonstration. Calculs, calculs, toujours des calculs…Le seul point légèrement technique est le (iii) ; il faut pour celui–ci remarquer que :

$$\begin{aligned}\overline{\left(\frac{z}{z'}\right)} &= \overline{\left(z \times \frac{1}{z'}\right)} \\ &= \overline{z} \times \overline{\left(\frac{1}{z'}\right)} \text{ par (ii)}\end{aligned}$$

Or, comme $z' \times \frac{1}{z'} = 1$, on déduit du point (ii) en conjugant à gauche et à droite de l'éqalité que

$$\overline{\left(\frac{1}{z'}\right)} = \frac{1}{\overline{z'}}$$

d'où le résultat. □

✍ **Exercice VI.2.** Donner une description explicite de l'ensemble

$$E = \left\{ z \in \mathbb{C} \setminus \{i\} \;\middle|\; \frac{z+i}{z-i} \in i\mathbb{R} \right\} .$$

➥ **Correction :** *Soit* $z \in \mathbb{C} \setminus \{i\}$ *; alors :*

$$\begin{aligned}\frac{z+i}{z-i} \in i\mathbb{R} &\Leftrightarrow \overline{\left(\frac{z+i}{z-i}\right)} = -\frac{z+i}{z-i} \\ &\Leftrightarrow \frac{\overline{z}-i}{\overline{z}+i} = -\frac{z+i}{z-i} \\ &\Leftrightarrow (\overline{z}-i)(z-i) = -(\overline{z}+i)(z+i) \\ &\Leftrightarrow z\overline{z} - i(z+\overline{z}) - 1 = -z\overline{z} - i(z+\overline{z}) + 1 \\ &\Leftrightarrow z\overline{z} = 1 .\end{aligned}$$

Ainsi, E est l'ensemble des complexes $z = x + iy$ tels que $z\overline{z} = 1$, *i.e* tels que $x^2 + y^2 = 1$. Il s'agit donc du cercle unité privé de i.

d) Module

Proposition VI.4. Soit $z \in \mathbb{C}$; alors $z\overline{z} \in \mathbb{R}_+$.

Démonstration. $z\overline{z} = \mathrm{Re}(z)^2 + \mathrm{Im}(z)^2 \in \mathbb{R}_+$. □

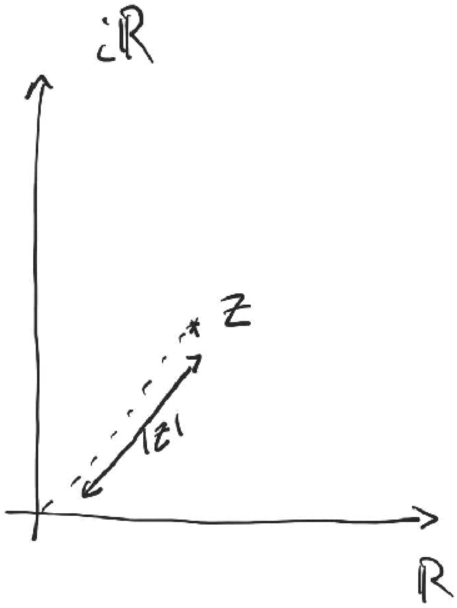
Définition VI.2. Soit $z \in \mathbb{C}$; on appelle **module** de z la quantité $\sqrt{z\overline{z}}$.

Notation. $|z|$

➠ **Exemple VI.2.** $|1+i| = \sqrt{2}$.

✌ **Remarque VI.5.**

— Géométriquement, le module de $z \in \mathbb{C}$ correspond à la distance entre le point d'affixe z et l'origine du plan $\mathbb{R}^2$.



Plus généralement, si $z, z' \in \mathbb{C}$, la quantité $|z - z'|$ est égale à la distance entre les points d'affixes respectives z et z' dans $\mathbb{R}^2$.

— Si $\omega \in \mathbb{C}$ et $R > 0$, une équation du cercle $\mathscr{C}(\omega, R)$ de centre ω et de rayon R est donc :

$$|z - \omega| = R \qquad (\mathbf{E}\ :\text{VI.1})$$

ou

$$(\mathrm{Re}(z) - \mathrm{Re}(\omega)^2 + (\mathrm{Im}(z) - \mathrm{Im}(\omega))^2 = R^2\ . \qquad (\mathbf{E}\ :\text{VI.2})$$

— De la même façon, les inéquations du type $|z - \omega| \leq R$ ont pour ensemble solutions les affixes des points d'un disque de $\mathbb{R}^2$.

Proposition VI.5. Soit $z \in \mathbb{C}$. Alors :

(i) $|z| = 0 \Leftrightarrow z = 0$;

(ii) $|z| = |\overline{z}|$;

(iii) $\mathrm{Re}(z) \leq |\mathrm{Re}(z)| \leq |z|$ et $\mathrm{Im}(z) \leq |\mathrm{Im}(z)| \leq |z|$

Démonstration. Les points (i) et (ii) découlent immédiatement de la définition. Pour le point (iii), posons $z = x + iy$; alors :

$$|z| = \sqrt{x^2 + y^2} \geq \sqrt{x^2} = |x| \geq x$$

et symétriquement avec la partie imaginaire, d'où le résultat. □

Proposition VI.6. Soient $z, z' \in \mathbb{C}$. Alors :

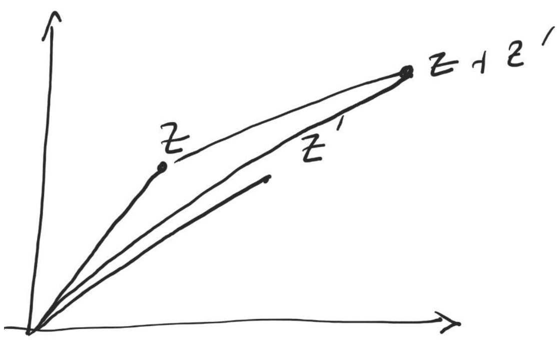
(i) $|zz'| = |z||z'|$;

(ii) si $z' \neq 0$, $\left|\frac{z}{z'}\right| = \frac{|z|}{|z'|}$;

(iii) $|z + z'| \leq |z| + |z'|$ **[inégalité triangulaire 1]** ;

(iv) $||z| - |z'|| \leq |z - z'|$ **[inégalité triangulaire 2]**.

✌ **Remarque VI.6.** Géométriquement, l'inégalité triangulaire 1 nous indique que le plus court chemin entre deux points du plan est la ligne droite : la distance du parcours $(0, z, z + z')$ est supérieure à celle du parcours $(0, z + z')$.



Démonstration.

(i) Découle de la définition et des propriétés de la conjugaison.

(ii) Idem.

(iii) Si $z' = 0$, l'inégalité est triviale. Sinon, posons $u = \frac{z}{z'}$ et montrons que $|1 + u| \leq 1 + |u|$. Pour ce faire, nous allons comparer les carrés de ces deux quantités :

$$\begin{aligned}|1+u|^2-(1+|u|)^2 &= (1+u)(1+\overline{u})-1-2|u|-|u|^2\\ &= u+\overline{u}-2|u|\\ &= 2(\mathrm{Re}(u)-|u|)\\ &\leq 0\,.\end{aligned}$$

Ne nous reste plus qu'à multiplier cette inégalité par $|z'|$ pour obtenir le résultat.

(iv) Échanger les rôles de z et z' ne change rien à l'expression souhaitée : nous pouvons donc supposer, quitte à échanger z et y, que $|z| \geq |z'|$. Remarquons alors que $z = z - z' + z'$; certes, me direz vous. . .Mais, en utilisant la première inégalité triangulaire, on obtient :

$$|x| = |z - z' + z'| \leq |z - z'| + |z'|$$

et donc $|z| - |z'| \leq |z - z'|$. Comme $|z| \geq |z'|$, on a bien :

$$||z| - |z'|| = |z| - |z'| \leq |z - z'|\,.$$

□

Remarque VI.7. Cas d'égalité dans la première inégalité triangulaire. Pour caractériser les complexes z, z' tels que $|z + z'| = |z| + |z'|$, procédons par analyse–synthèse.

Analyse. Supposons trouvés $z, z' \in \mathbb{C}$ tels que $|z + z'| = |z| + |z'|$. Si $z' \neq 0$, on pose $u = \dfrac{z}{z'}$ et on obtient

$$|1 + u| = 1 + |u|$$

ce qui est équivalent, nous venons de le voir dans la démonstration de l'inégalité triangulaire, à :

$$\mathrm{Re}(u) = |u|\,.$$

Ceci entraine, comme $|u| = \sqrt{\mathrm{Re}(u)^2 + \mathrm{Im}(u)^2}$, que $u \in \mathbb{R}_+$, *i.e* $\dfrac{z}{z'} = u \in \mathbb{R}_+$.

Synthèse. Si $z' = 0$, l'égalité est trivialement vérifiée. Si $z = uz'$, avec $u \in \mathbb{R}_+$, alors :

$$\begin{aligned}|z'+z| &= |z'+uz'|\\ &= |(1+u)z'|\\ &= |1+u||z'|\\ &= (1+u)|z'|\\ &= |z'|+|u||z'|\\ &= |z'|+|z|\,.\end{aligned}$$

En conclusion, nous venons de démontrer le résultat suivant :

$$|z + z'| = |z| + |z'| \iff (z' = 0) \vee (\exists\, u \in \mathbb{R}_+,\ z = uz')\,.$$

2.⁻ Trigonométrie, le retour

a) Nombres complexes de module 1

Ce paragraphe est, vous l'aurez deviné, dédié à l'étude de l'ensemble des nombres complexes de module 1, à savoir :

$$\mathbb{U} = \{z \in \mathbb{C} \,|\, |z| = 1\} \subset \mathbb{C}^*.$$

Proposition VI.7. L'ensemble $\mathbb{U}$ est stable par multiplication et inverse.

Démonstration. Le module du produit est le produit des modules, idem pour l'inverse. Or $1 \times 1 = \frac{1}{1} = 1 \ldots$ □

Remarque VI.8.
- Nous dirons dans le chapitre VIII que $\mathbb{U}$ possède, de par ces stabilités, une structure de groupe.
- Géométriquement, $\mathbb{U}$ correspond au cercle unité de $\mathbb{R}^2$.
- Si $z \in \mathbb{U}$, alors $|z|^2 = z\overline{z} = 1$ donc $\frac{1}{z} = \overline{z}$. En effet, si $z \in \mathbb{C}^*$, on a
$$\frac{1}{z} = \frac{\overline{z}}{|z|^2}\,.$$

Définition VI.3. Soit $\theta \in \mathbb{R}$; on **pose**

$$e^{i\theta} = \cos(\theta) + i\sin(\theta)\,.$$

✖ **Attention :** Il s'agit la d'une **notation** ; n'imaginons pas que ces quantités héritent de toutes les propriétés de l'exponentielle. Pensez à la positivité ...

Exemple VI.3.
- $e^{i\times 0} = \cos(0) + i\sin(0) = 1$; incidemment, notons que $1 = e^0$, ce qui est rassurant pour notre santé mentale à tous.
- $e^{2i\pi} = 1$;
- $e^{i\frac{\pi}{2}} = i$;
- $e^{i\frac{\pi}{4}} = \frac{\sqrt{2}}{2}(1+i)$.

Proposition VI.8. On a l'égalité ensembliste suivante :

$$\mathbb{U} = \{e^{i\theta} \,|\, \theta \in \mathbb{R}\}\,.$$

Remarque VI.9. Ce résultat est parfois appelé **paramétrage** du cercle unité ; en effet, nous décrivons ce dernier comme l'image de la fonction

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{C} \\ \theta &\mapsto e^{i\theta} \end{aligned}\,.$$

Démonstration. Montrons deux inclusions.

($\supset$) Soit $\theta \in \mathbb{R}$; alors
$$|e^{i\theta}| = \sqrt{\cos(\theta)^2 + \sin(\theta)^2} = 1$$
donc $e^{i\theta} \in \mathbb{U}$.

($\subset$) Soit $z = x + iy \in \mathbb{U}$; alors $x^2 + y^2 = 1$, ce qui entraîne que le point (x, y) se situe sur le cercle trigonométrique (ou unité) de $\mathbb{R}^2$. De fait, il existe $\theta \in \mathbb{R}$ tel que $x = \cos(\theta)$ et $y = \sin(\theta)$. *In fine*, $z = e^{i\theta}$.

□

Proposition VI.9. Soient $\theta, \theta' \in \mathbb{R}$. Alors :

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

(ii) $e^{-i\theta} = \dfrac{1}{e^{i\theta}} = \overline{e^{i\theta}}$;

(iii) $e^{i(\theta-\theta')} = \dfrac{e^{i\theta}}{e^{i\theta'}}$;

(iv) pour tout $n \in \mathbb{Z}$, $e^{in\theta} = (e^{i\theta})^n$;

(v) $e^{i\theta} = 1 \Leftrightarrow \theta \equiv 0\,[2\pi]$;

(vi) $e^{i\theta} = e^{i\theta'} \Leftrightarrow \theta \equiv \theta'\,[2\pi]$.

Démonstration.

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

(ii) L'égalité avec le conjugué est triviale ; le lien avec l'inverse découle du fait que si $z \in \mathbb{U}$, alors $|z|^2 = z\overline{z} = 1$ donc $\frac{1}{z} = \overline{z}$.

(iii) Découle des points (i) et (ii).

(iv) Par récurrence à partir des points (i) et (iii).

(v)
$$\begin{aligned} e^{i\theta} = 1 &\Leftrightarrow \cos(\theta) + i\sin(\theta) = 1 \\ &\Leftrightarrow (\cos(\theta) = 1) \wedge (\sin(\theta) = 0) \\ &\Leftrightarrow \theta \equiv 0\,[2\pi]\,. \end{aligned}$$

(vi) Découle des points (iii) et (iv).

□

✌ **Remarque VI.10.** En conséquence, l'application
$$\begin{aligned} \widehat{f} : [0, 2\pi[&\to \mathbb{U} \\ \theta &\mapsto e^{i\theta} \end{aligned}\,.$$
est une bijection. Topologiquement, $\mathbb{U}$ est obtenu en "raccordant" entre elles les extrémités de $[0, 2\pi[$.

Le résultat qui suit est attribué à Leonhard Euler (mathématicien suisse, 1707—1783) et possède de nombreuses applications sur lesquelles nous reviendront ultérieurement.

Proposition VI.10 (Formules d'Euler)**.** Soit $\theta \in \mathbb{R}$; alors :

$$\cos(\theta) = \frac{e^{i\theta} + e^{-i\theta}}{2}$$

et

$$\sin(\theta) = \frac{e^{i\theta} - e^{-i\theta}}{2i} .$$

Démonstration. Découle immédiatement des formules liant parties réelle et imaginaire au conjugué. □

✌ **Remarque VI.11.** Toute ressemblance avec le (co)sinus hyperbolique est brutalement non fortuite.

La formule qui suit doit son nom au mathématicien français Abraham de Moivre (1667—1754), qui passa la majeure partie de sa vie exilé en Angleterre en raison de sa foi protestante.

Proposition VI.11 (Formule de Moivre)**.** Soit $\theta \in \mathbb{R}$ et soit $n \in \mathbb{Z}$. Alors :

$$(\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta) .$$

Démonstration. Triviale une fois que l'on a passé le terme de gauche sous forme exponentielle. □

La question que chacun d'entre vous doit (peut–être) se poser est la suivante : ces formules sont bien jolies (et encore. . .), mais quelle est donc leur utilité ? *Oh, sweet summer child. . .*

⋄ Linéarisation

Le premier usage reconnu des ces formules est la linéarisation d'expressions trigonométriques. Par exemple, si $\theta \in \mathbb{R}$:

$$\begin{aligned}
\cos(\theta)^3 &= \left(\frac{e^{i\theta} + e^{-i\theta}}{2}\right)^3 \\
&= \frac{e^{3i\theta} + 3e^{i\theta} + 3e^{-i\theta} + e^{-3i\theta}}{8} \\
&= \frac{2\cos(3\theta) + 6\cos(\theta)}{8} \\
&= \frac{1}{4}\cos(3\theta) + \frac{3}{4}\cos(\theta) .
\end{aligned}$$

De façon plus générale, si $\theta \in \mathbb{R}$ et $n \in \mathbb{N}$, on a :

$$\begin{aligned}\cos(\theta)^n &= \left(\frac{e^{i\theta}+e^{-i\theta}}{2}\right)^n \\ &= \frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k}e^{ik\theta}e^{-i(n-k)\theta} \\ &= \frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k}e^{i(2k-n)\theta}\ .\end{aligned}$$

Or, $\cos(\theta)^n \in \mathbb{R}$; il est donc égal à sa partie réelle, *i.e*

$$\begin{aligned}\cos(\theta)^n &= \mathrm{Re}(\cos(\theta)^n) \\ &= \mathrm{Re}\left(\frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k}e^{i(2k-n)\theta}\right) \\ &= \frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k}\mathrm{Re}(e^{i(2k-n)\theta}) \\ &= \frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k}\cos((2k-n)\theta)\ .\end{aligned}$$

Cette formule (et son analogue pour le sinus) n'est évidemment pas à apprendre par coeur, mais à savoir retrouver.

⋄ "Délinéarisation"

À l'inverse, la formule de Moivre nous donne, si $\theta \in \mathbb{R}$ et $n \in \mathbb{N}$, que :

$$\begin{aligned}\cos(n\theta)+i\sin(n\theta) &= (\cos(\theta)+i\sin(\theta))^n \\ &= \sum_{k=0}^{n}\binom{n}{k}\cos(\theta)^{n-k}i^k\sin(\theta)^k\ .\end{aligned}$$

En passant à la partie réelle, qui ne conservera ici que les termes pairs de la somme, nous obtenons que :

$$\cos(n\theta) = \sum_{0\leq 2p\leq n}\binom{n}{2p}\cos(\theta)^{n-2p}(-1)^p\sin(\theta)^{2p}$$

car $i^{2p} = (i^2)^p = (-1)^p$. Une formule analogue peut évidemment être obtenue pour le sinus en passant à la partie imaginaire.

⋄ Calculs de sommes

Pour finir ce musée des horreurs calculatoires, intéressons nous au calcul, pour $\theta \in \mathbb{R}$ et $n \in \mathbb{N}$, des sommes suivantes :

$$S_n = \sum_{k=0}^{n}\cos(k\theta) \quad \text{et} \quad T_n = \sum_{k=0}^{n}\sin(k\theta)\ .$$

L'idée naturelle ici est de calculer

$$\begin{aligned}S_n + iT_n &= \sum_{k=0}^{n} \cos(k\theta) + i\sin(k\theta)\\ &= \sum_{k=0}^{n} e^{ik\theta}\,.\end{aligned}$$

En effet, on reconnait la somme des termes d'une suite géométrique. À supposer que $\theta \not\equiv 0\,[2\pi]$ (auquel cas le calcul me semble abordable sans technique particulière), on a donc :

$$S_n + iT_n = \frac{1-e^{i(n+1)\theta}}{1-e^{i\theta}}\,.$$

Pour simplifier cette fraction, on **factorise par l'angle moitié**, *i.e* :

$$\begin{aligned}\frac{1-e^{i(n+1)\theta}}{1-e^{i\theta}} &= \frac{e^{i\frac{(n+1)\theta}{2}}}{e^{i\frac{\theta}{2}}}\frac{e^{-i\frac{(n+1)\theta}{2}}-e^{i\frac{(n+1)\theta}{2}}}{e^{-i\frac{\theta}{2}}-e^{i\frac{\theta}{2}}}\\ &= e^{i\frac{n}{2}\theta}\,\frac{\sin\left(\frac{(n+1)\theta}{2}\right)}{\sin\left(\frac{\theta}{2}\right)}\,.\end{aligned}$$

De fait :

$$S_n = \mathrm{Re}(S_n + iT_n) = \cos\left(\frac{n}{2}\theta\right)\frac{\sin\left(\frac{(n+1)\theta}{2}\right)}{\sin\left(\frac{\theta}{2}\right)}$$

et

$$T_n = \mathrm{Im}(S_n + iT_n) = \sin\left(\frac{n}{2}\theta\right)\frac{\sin\left(\frac{(n+1)\theta}{2}\right)}{\sin\left(\frac{\theta}{2}\right)}\,.$$

Youpi.

✌ **Remarque VI.12.** La technique de factorisation par l'angle moitié se révèle souvent fort utile en pratique pour factoriser et/ou déterminer module et argument d'expressions du type $e^{ip} \pm e^{iq}$ avec $p, q \in \mathbb{R}$. En effet, on a alors :

$$\begin{aligned}e^{ip} \pm e^{iq} &= e^{ip}\left(1 \pm e^{i(q-p)}\right)\\ &= e^{i(p+(q-p)/2)}\left(e^{-(q-p)/2} \pm e^{(q-p)/2}\right)\,,\end{aligned}$$

le membre de droite s'exprimant alors à l'aide d'un cosinus ou sinus.

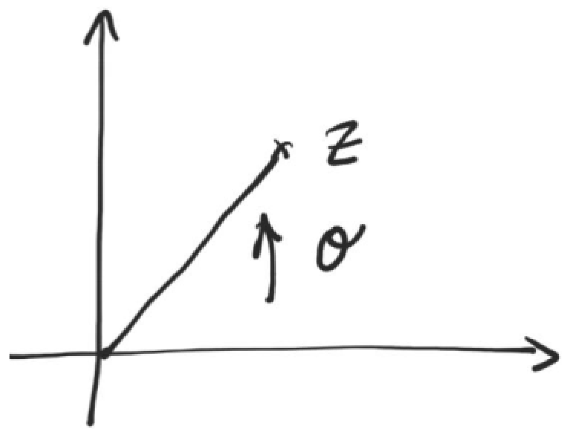
✍ **Exercice VI.3.** Retrouver, pour $p, q \in \mathbb{R}$, les formules pour $\cos(p) \pm \cos(q)$ et $\sin(p) \pm \sin(q)$.

b) Argument

Définition VI.4. Soit $z \in \mathbb{C}$; on appelle **argument** de z tout $\theta \in \mathbb{R}$ tel que

$$z = |z|e^{i\theta}\,.$$

Remarque VI.13.
- **Attention :** il n'y a **pas** unicité de l'argument ; par exemple $1 = e^{i\times 0} = e^{2i\pi}$.
- Géométriquement, un argument de $z \in \mathbb{C}$ d'image $A \in \mathbb{R}^2$ est une mesure de l'angle orienté entre l'axe des abscisses et la droite (OA).



- 0 admet tout nombre réel comme argument.

Proposition VI.12. Soit $z \in \mathbb{C}^*$ et soit θ_0 un argument de z. Alors l'ensemble des arguments de z est :
$$\mathscr{A}_z = \{\theta_0 + 2k\pi \mid k \in \mathbb{Z}\}\,.$$

Démonstration. Démontrons deux inclusions.

($\supset$) Immédiat par périodicité.

($\subset$) Soit $\eta \in \mathscr{A}_z$; alors $z = |z|e^{i\eta} = |z|e^{i\theta_0}$ donc, comme $|z| \neq 0$, $e^{i\eta} = e^{i\theta_0}$ et donc $\eta \equiv \theta_0\,[2\pi]$, d'où le résultat.

□

Remarque VI.14.
- Un piège classique à éviter : si $z = ae^{i\theta}$, θ n'est pas nécessairement un argument de z, étant qu'il pourrait être négatif...Mais pas (trop) de panique : $-1 = e^{i\pi}$.
- Sur un intervalle de longueur inférieure à 2π, l'argument est unique.

Notation. Soit $z \in \mathbb{C}$; on note $\arg(z)$ l'unique élément de $\mathscr{A}_z \cap [0, 2\pi[$. Cette notation est arbitraire ; certains préfèrent donc écrire des choses du style "$\arg(z) \equiv \theta\,[2\pi]$".

Remarque VI.15. Si $z \in \mathbb{C}^*$, on a :
$$z \in \mathbb{R} \iff \arg(z) \in \{0, \pi\}\,.$$

Exemple VI.4. Pour déterminer l'argument de $\sqrt{3} + i$, on le divise par son module et on essaie de reconnaître une exponentielle connue :
$$\frac{\sqrt{3} + i}{2} = e^{i\frac{\pi}{6}}\,.$$

Ainsi, $\arg(\sqrt{3} + i) = \dfrac{\pi}{6}$.

c) Forme trigonométrique

Définition VI.5. On appelle **forme trigonométrique** d'un nombre complexe z toute écriture de la forme $z = re^{i\theta}$, avec $r \in \mathbb{R}_+$ et $\theta \in \mathbb{R}$.

➠ **Exemple VI.5.** $-1 = e^{i\pi} = e^{3i\pi}$; notons au passage que cette écriture n'est **pas unique**.

✌ **Remarque VI.16.**

— Travailler avec des complexes sous forme trigonométrique est en général une bonne idée lorsque l'on veut les multiplier et/ou diviser, mais pas pour les additionner.

— Dans l'écriture sous forme trigonométrique "$z = re^{i\theta}$", on a nécessairement $r = |z|$ et $\theta \in \mathscr{A}_z$.

Proposition VI.13. Soient $z, z' \in \mathbb{C}^*$ et $n \in \mathbb{Z}$. Alors :

(i) $\arg(zz') \equiv \arg(z) + \arg(z')\ [2\pi]$;

(ii) $\arg\left(\frac{z}{z'}\right) \equiv \arg(z) - \arg(z')\ [2\pi]$;

(iii) $\arg(z^n) \equiv n\arg(z)\ [2\pi]$.

Démonstration. Mettre z et z' sous forme trigonométrique. □

✍ **Exercice VI.4.** Soit $t \in \mathbb{R}$; mettre sous forme trigonométrique le complexe $1 + e^{it}$.

➥ **Correction :** *On factorise par l'angle moitié :*

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

Il faut ensuite digresser selon le signe de $\cos\left(\frac{t}{2}\right)$.

✍ **Exercice VI.5.** Soient $a, b, t \in \mathbb{R}$; démontrer qu'il existe $A, \varphi \in \mathbb{R}$ tels que :

$$a\cos(t) + b\sin(t) = A\cos(t - \varphi) .$$

➥ **Correction :** *On a :*

$$\begin{aligned} a\cos(t) + b\sin(t) &= \mathrm{Re}(ae^{it} - ibe^{it}) \\ &= \mathrm{Re}((a - ib)e^{it}) \end{aligned}$$

et donc, en posant $A = |a - ib|$ *et* $\varphi = -\arg(a - ib)$ *on a :*

$$a\cos(t) + b\sin(t) = A\mathrm{Re}(e^{i(t-\varphi)}) = A\cos(t - \varphi) .$$

d) Exponentielle complexe

Définition VI.6. Soit $z \in \mathbb{C}$. On appelle **exponentielle** de z le nombre complexe
$$e^z = e^{\mathrm{Re}(z)} e^{i\mathrm{Im}(z)} .$$

✌ **Remarque VI.17.** Remarquons que les deux "exponentielles" intervenant dans cette notation sont différentes : la première est un exponentielle réelle, la seconde est de type "$e^{i\theta}$".

Proposition VI.14. Soient $z, z' \in \mathbb{C}$. Alors :

(i) $e^{\overline{z}} = \overline{e^z}$;

(ii) $|e^z| = e^{\mathrm{Re}(z)}$ et $\arg(e^z) \equiv \mathrm{Im}(z)[2\pi]$;

(iii) $e^{z+z'} = e^z e^{z'}$;

(iv) $e^z \neq 0$ et $\dfrac{1}{e^z} = e^{-z}$.

Démonstration. Immédiat en passant par la définition. □

Proposition VI.15. Soit $z \in \mathbb{C}$; alors $e^z = 1 \Leftrightarrow z \in 2i\pi\mathbb{Z}$.

✌ **Remarque VI.18.**

— En particulier, l'exponentielle complexe n'est **PAS** bijective.

— On en déduit que, si $z, z' \in \mathbb{C}$, alors $e^z = e^{z'} \Leftrightarrow z \equiv z'\ [2i\pi]$.

Démonstration.

($\Leftarrow$) Immédiat.

($\Rightarrow$) Si $z = x + iy \in \mathbb{C}$ est tel que $e^z = 1$, alors $e^x e^{iy} = 1$ et donc $e^x = |e^z| = 1$, *ergo* $x = 0$ et $e^{iy} = 1$, d'où le résultat.

□

Proposition VI.16. La fonction
$$\begin{aligned} \exp : \mathbb{C} &\to \mathbb{C}^* \\ z &\mapsto e^z \end{aligned}$$
est surjective. De plus, pour tout $a \in \mathbb{C}^*$ et $\gamma \in \mathbb{C}$ est tel que $e^\gamma = a$, on a :
$$\exp^{-1}(\{a\}) = \{\gamma + 2ik\pi \mid k \in \mathbb{Z}\} .$$

Démonstration. L'exponentielle complexe est à valeurs dans $\mathbb{C}^*$ d'après le point (iv) de la proposition VI.14. Soit ensuite $a \in \mathbb{C}^*$, que l'on peut écrire sous forme trigonométrique $a = |a|e^{i\theta}$, avec $\theta \in \mathscr{A}_a$. Alors, si on pose $\gamma = \ln(|a|) + i\theta$, on a :

$$\exp(\gamma) = e^{\ln(|a|)}e^{i\theta} = |a|e^{i\theta} = a$$

donc exp est bien surjective. Enfin, pour tout $\tau \in \mathbb{C}$:

$$a = e^{\tau} \Leftrightarrow e^{\gamma} = e^{\tau} \Leftrightarrow \gamma \equiv \tau \, [2i\pi]$$

□

✌ **Remarque VI.19.** L'exponentielle complexe réalise donc une bijection entre toute "bande" de la forme $\Lambda = \{x + iy \,|\, (x, y) \in \mathbb{R} \times [2k\pi, 2(k+1)\pi[\}$ et $\mathbb{C}^*$.

3.– Équations algébriques

a) Trinômes du second degré

Vous avez logiquement une idée assez précise de la méthode de résolutions d'équations de la forme $ax^2 + bx + c = 0$ avec $a, b, c \in \mathbb{R}$. Le but de ce paragraphe est de mettre en place un analogue complexe de ce procédé.

Définition VI.7. Soit $z \in \mathbb{C}$. On appelle **racine carrée** tout nombre complexe a tel que $a^2 = z$.

➠ **Exemple VI.6.** 2 est une racine carrée de 4, i une racine carrée de -1.

Proposition VI.17. Tout nombre complexe non nul possède exactement deux racines carrées distinctes.

Démonstration. Soit $z \in \mathbb{C}^*$ de forme trigonométrique $z = re^{i\theta}$ $(r > 0)$. Procédons par analyse–synthèse.

Analyse. Soit $a = \rho e^{i\varphi} \in \mathbb{C}$, avec $\rho > 0$ tel que $a^2 = z$, i.e $re^{i\theta} = \rho^2 e^{2i\varphi}$. Alors, en passant au module dans cette égalité, on obtient

$$\rho^2 = r \;\; i.e \;\; \rho = \sqrt{r} \,.$$

En passant ensuite à l'argument dans l'égalité initiale, on a :

$$2\varphi \equiv \theta \, [2\pi]$$

ce qui signifie qu'il existe $k \in \mathbb{Z}$ tel que $2\varphi = \theta + 2k\pi$ et donc, en divisant par 2 :

$$\varphi \equiv \frac{\theta}{2} \, [\pi] \,.$$

Ceci entraîne donc que φ est congru à $\frac{\theta}{2}$ ou $\frac{\theta}{2} + \pi$ modulo 2π. Or, comme $e^{i(\frac{\theta}{2}+\pi)} = -e^{i\frac{\theta}{2}}$ on a *in fine* que :

$$a \in \left\{\sqrt{r}e^{i\frac{\theta}{2}}, -\sqrt{r}e^{i\frac{\theta}{2}}\right\} \,.$$

Synthèse. Il est immédiat que les deux valeurs proposées ci–dessus sont des racines carrées de z.

□

Exemple VI.7. Les deux racines carrées de $i = e^{i\frac{\pi}{2}}$ sont donc $\pm e^{i\frac{\pi}{4}}$, *i.e* $\pm\frac{1}{\sqrt{2}}(1+i)$.

Remarque VI.20. Il est donc aisé de trouver la racine carrée d'un nombre complexe dont on connaît la forme trigonométrique. Si on ne connait que sa forme algébrique $z = x + iy$, on peut faire usage de la méthode suivante : si $a = X + iY$ est tel que $a^2 = z$ alors :

$$X^2 - Y^2 + 2iXY = x + iy$$

et, commme $|a|^2 = |z|$:

$$(X^2 + Y^2)^2 = x^2 + y^2 .$$

On obtient donc un système de trois équations qu'il nous sera généralement possible de résoudre :

$$\left\{\begin{array}{ccc} X^2 - Y^2 & = & x \\ 2XY & = & y \\ (X^2+Y^2)^2 & = & x^2+y^2 \end{array}\right. .$$

Exemple VI.8. Pour déterminer les racines de $1+i$, on tombe sur les équations :

$$\left\{\begin{array}{ccc} X^2 - Y^2 & = & 1 \\ 2XY & = & 1 \\ (X^2+Y^2)^2 & = & 2 \end{array}\right.$$

i.e

$$\left\{\begin{array}{ccc} X^2 - Y^2 & = & 1 \\ 2XY & = & 1 \\ X^2+Y^2 & = & \sqrt{2} \end{array}\right. .$$

En utilisant les deux équations quadratiques, on trouve :

$$X = \pm\sqrt{\frac{\sqrt{2}+1}{2}}, \quad Y = \pm\sqrt{\frac{\sqrt{2}-1}{2}} .$$

La seconde équation nous dit de plus que X et Y ont même signe, ainsi les racines de $1 + i$ sont :

$$\pm\left(\sqrt{\frac{\sqrt{2}+1}{2}} + i\sqrt{\frac{\sqrt{2}-1}{2}}\right) .$$

Proposition VI.18. Soient $a, b, c \in \mathbb{C}$ tels que $a \neq 0$. On considère l'équation :

$$az^2 + bz + c = 0 \qquad (\mathbf{E}:\text{VI.3})$$

d'inconnue $z \in \mathbb{C}$ et on pose $\Delta = b^2 - 4ac$. Alors :

— si $\Delta = 0$, l'équation (**E** :VI.3) admet un unique solution, à savoir :

$$z_0 = \frac{-b}{2a} \,;$$

— si $\Delta \neq 0$, l'équation (**E** :VI.3) admet exactement deux solutions distinctes, à savoir :

$$z_1 = \frac{-b+\delta}{2a}, \qquad z_2 = \frac{-b-\delta}{2a}$$

où δ est une racine carrée de Δ.

✌ **Remarque VI.21.** Notons que l'extension à $\mathbb{C}$ de la notion de racine carrée simplifie le cas réel en nous évitant de distinguer deux cas selon le signe du discriminant Δ.

Démonstration. Soit $z \in \mathbb{C}$; commençons par remarquer que :

$$\left(z + \frac{b}{2a}\right)^2 = z^2 + \frac{b}{a}z + \frac{b^2}{4a^2}$$

ce qui entraîne que :

$$\begin{aligned} az^2 + bz + c &= a\left(z^2 + \frac{b}{a}z + \frac{c}{a}\right) \\ &= a\left(z + \frac{b}{2a}\right)^2 - a\frac{b^2}{4a^2} + c \\ &= a\left(z + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a}\,. \end{aligned}$$

Soit $\delta \in \mathbb{C}$ une racine carrée de Δ (qui sera donc nulle si Δ l'est). Alors :

$$\begin{aligned} z \text{ est solution de } (\mathbf{E}:\text{VI.3}) &\Leftrightarrow a\left(z + \frac{b}{2a}\right)^2 = \frac{\Delta}{4a} \\ &\Leftrightarrow \left(z + \frac{b}{2a}\right)^2 = \frac{\delta^2}{4a^2} \\ &\Leftrightarrow \left(z + \frac{b}{2a}\right)^2 = \left(\frac{\delta}{2a}\right)^2 \\ &\Leftrightarrow z + \frac{b}{2a} = \pm\frac{\delta}{2a} \end{aligned}$$

d'où le résultat. □

✌ **Remarque VI.22.** On déduit de ce résultat que si r, r' sont les deux racines du trinôme (comptées avec multiplicité), on a la factorisation :

$$\forall\, z \in \mathbb{C}, \quad az^2 + bz + c = a(z-r)(z-r')\,.$$

De façon générale, si P est une fonction polynomiale complexe admettant une racine a, l'expression $P(z)$ peut se factoriser, pour tout $z \in \mathbb{C}$, par $z - a$ (*cf.* chapitre XIV).

Exemple VI.9. L'équation $z^2 - (1+2i)z + i - 1 = 0$ a pour discriminant $\Delta = 1$ et solutions $1 + i$ et i.

Remarque VI.23. Le produit (resp. la somme) des solutions de (**E** :VI.3) est égal à $\frac{c}{a}$ $\left(\text{resp. égale à } -\frac{b}{a}\right)$. Nous verrons dans le chapitre XIV qu'il ne s'agit pas d'une coïncidence.

Proposition VI.19. Soient $z, z', s, p \in \mathbb{C}$. Alors :

$$\begin{cases} z + z' & = & s \\ zz' & = & p \end{cases} \iff z \text{ et } z' \text{ sont solutions de } X^2 - sX + p = 0\,.$$

Démonstration. Le sens indirect provient de la proposition VI.18. Pour le sens direct, il suffit de développer $(X - z)(X - z')$, qui a clairement pour racines z et z' et est égal à $X^2 - sX + p$ □

Exercice VI.6. Déterminer les nombres complexes x, y tels que :

$$\begin{cases} x + y & = & i \\ xy & = & 2 \end{cases}.$$

b) Racines n–ièmes

Dans tout ce paragraphe, nous considérons comme fixé un entier $n \in \mathbb{N}^*$ et nous intéressons à la notion de racine n–ième (complexe) définie ci–ensuite.

Définition VI.8. Soit $z \in \mathbb{C}$; on appelle **racine n–ième** de z tout nombre complexe a tel que $a^n = z$.

Vocabulaire. Une racine n–ième de 1 est appelée **racine n–ième de l'unité**.

Notation. On note $\mathbb{U}_n$ l'ensemble des racines n–ièmes de l'unité ; *i.e*

$$\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}\,.$$

Remarque VI.24. Il est aisé de démontrer que :
— $\mathbb{U}_n \subset \mathbb{U} \subset \mathbb{C}^*$ (passer au module) ;
— $\mathbb{U}_n$ est stable par produit et passage à l'inverse.

Proposition VI.20. Posons, pour $k \in \mathbb{N}$, $\xi_k = e^{\frac{2ik\pi}{n}}$. Alors :

$$\mathbb{U}_n = \{\xi_0, \ldots, \xi_{n-1}\}\,.$$

En particulier, $\mathbb{U}_n$ est un ensemble contenant exactement n éléments.

✌ **Remarque VI.25.** Notons que $\xi_0 = \xi_n = 1$.

Démonstration.

($\supset$) Immédiat en remarquant que, pour tout $k \in \mathbb{N}$:

$$\xi_k^n = e^{2ik\pi} = 1 \; .$$

($\subset$) Soit $z \in \mathbb{U}_n$, i.e $z^n = 1$. Ceci entraîne en particulier que $z \in \mathbb{U}$, *i.e* $|z| = 1$, donc il existe $\theta \in \mathbb{R}$ tel que $z = e^{i\theta}$. Le fait que $z^n = 1$ a pour conséquence que $n\theta \equiv 0\,[2\pi]$, *ergo* il existe $k \in [\![0, n-1]\!]$ tel que $e^{i\theta} = e^{\frac{2ik\pi}{n}}$. Il ne nous reste plus pour conclure qu'à remarquer que $\xi_0, \dots, \xi_{n-1}$ sont deux à deux distincts.

□

✌ **Remarque VI.26.**

— Si on pose $\xi = e^{\frac{2i\pi}{n}}$, alors pour tout $k \in \mathbb{N}$, $\xi_k = \xi^k$.

— Ceci a pour conséquence que :

$$\sum_{k=0}^{n-1} \xi_k = \frac{\xi^n - 1}{\xi - 1} = 0$$

car $\xi^n = \xi_n = 1$.

➠ **Exemple VI.10.**

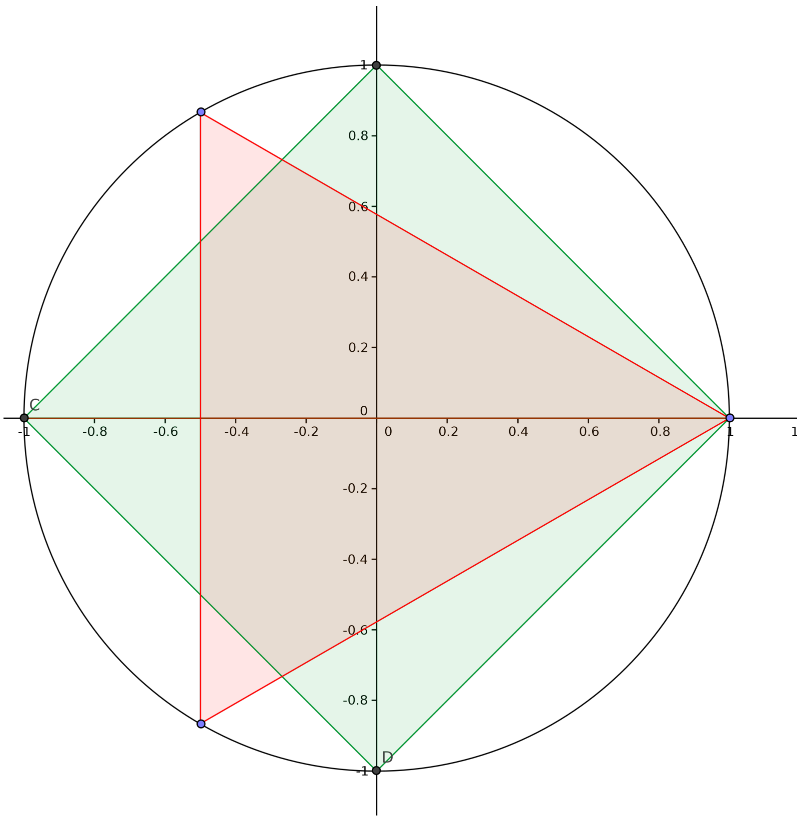
— $\mathbb{U}_1 = \{1\}$;

— $\mathbb{U}_2 = \{-1, 1\}$;

— en posant $j = e^{\frac{2i\pi}{3}}$, on a $\mathbb{U}_3 = \{1, j, j^2\}$. Remarquons que l'on a de fait $1 + j + j^2 = 0$ et $\overline{j} = j^2$;

— $\mathbb{U}_4 = \{-1, 1, -i, i\}$.

Géométriquement, les points de $\mathbb{U}_n$ forment un polygone régulier à n côtés, comme illustré sur la figure ci–ensuite pour $n = 3, 4$.



Proposition VI.21. Soit $z \in \mathbb{C}^*$ de forme trigonométrique $z = re^{i\theta}$. Alors les racines n–ièmes de z sont exactement les

$$\sqrt[n]{r}e^{\frac{i\theta}{n}}\xi_k$$

pour $k \in [\![0, n-1]\!]$.

Démonstration. Cela provient du fait que si u et u' sont deux racines n–ièmes de z, alors $\frac{u}{u'} \in \mathbb{U}_n$. □

➠ **Exemple VI.11.** Les racines cubiques de 2 sont $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$.

4.– Transformations du plan

Le but de ce paragraphe est de construire un "dictionnaire" reliant transformations géométriques du plan et applications de $\mathbb{C}$ dans $\mathbb{C}$. Rappelons que la correspondance entre ces deux ensembles est donnée par l'application

$$\begin{aligned}\varphi : \mathbb{C} &\to \mathbb{R}^2\\ z &\mapsto (\mathrm{Re}(z), \mathrm{Im}(z))\end{aligned}$$

de réciproque

$$\begin{aligned}\psi : \mathbb{R}^2 &\to \mathbb{C}\\ (x, y) &\mapsto x + iy \quad .\end{aligned}$$

✌ **Remarque VI.27.** Afin de mieux comprendre ce qui va suivre, il peut être utile de noter les deux choses suivantes : si $A, B, C \in \mathbb{R}^2$ sont des points du plans d'affixes respectives $a, b, c \in \mathbb{C}$, alors :

— le module $\left|\frac{c-a}{b-a}\right|$ est égal au quotient des longueurs (non algébriques) AC et AB ;

— l'argument $\arg\left(\frac{c-a}{b-a}\right)$ est une mesure (modulo 2π) de l'angle orienté $(\overrightarrow{AB}, \overrightarrow{AC})$.

L'argument *supra* permet de déterminer rapidement si les points A, B, C sont alignés ou orthogonaux.

a) Translations, homothéties

Soit $u = \varphi(z_o) \in \mathbb{R}^2$; on appelle **translation de vecteur** u l'application

$$\begin{aligned}\tau_u : \mathbb{R}^2 &\to \mathbb{R}^2\\ \varphi(z) &\mapsto \varphi(z + z_0) \, .\end{aligned}$$

Si $\Omega = \varphi(\omega) \in \mathbb{R}^2$ et $\lambda \in \mathbb{R}$, on appelle **homothétie de centre** Ω **et de rapport** λ l'application

$$\begin{aligned}\mu_{\Omega,\lambda} : \mathbb{R}^2 &\to \mathbb{R}^2\\ \varphi(z) &\mapsto \varphi(\omega + \lambda(z - \omega)) \, .\end{aligned}$$

b) Rotations

Soit $\theta \in \mathbb{R}$ et soit $\Omega = \varphi(\omega) \in \mathbb{R}^2$; on appelle **rotation de centre Ω et d'angle θ** l'application

$$\begin{aligned} \rho_{\Omega,\theta} : \mathbb{R}^2 &\to \mathbb{R}^2 \\ \varphi(z) &\mapsto \varphi\left(\omega + (z-\omega)e^{i\theta}\right) \ . \end{aligned}$$

c) Similitudes directes

Définition VI.9. Soient $\theta \in \mathbb{R}$, $\lambda \in \mathbb{R}^*$ et $\Omega = \varphi(\omega) \in \mathbb{R}^2$. On appelle **similitude directe de centre Ω, de rapport λ et d'angle θ** l'application :

$$\begin{aligned} \mathscr{S}_{\Omega,\lambda,\theta} : \mathbb{R}^2 &\mapsto \mathbb{R}^2 \\ \varphi(z) &\mapsto \varphi\left(\omega + \lambda(z-\omega)e^{i\theta}\right) \ . \end{aligned}$$

✌ **Remarque VI.28.** Une similitude directe est donc la composée d'une rotation et d'une homothétie. Il s'agit en fait des applications de la forme

$$\varphi(z) \mapsto \varphi(az+b)$$

avec $a, b \in \mathbb{C}$ tels que $a \neq 0$.

Proposition VI.22. Les similitudes directes conservent les angles orientés.

Démonstration. Les rotations et les homothéties conservent les angles orientés, d'où le résultat. □

Chapitre VII

Suites numériques

1.⁻ Généralités

a) Notion de suite numérique

Rappelons la définition suivante, à laquelle nous avions fait allusion dans le chapitre V.

Définition VII.1. On appelle **suite (numérique)** toute application $u : [\![n_0, \infty[\![\to \mathbb{K}$, où :

— $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$;

— $n_0 \in \mathbb{N}$ est appelé **rang initial** de la suite.

Notation. La suite u peut être notée $(u_n)_{n \geq n_0}$ (ou simplement $(u_n)_n$ si $n_0 = 0$) ; ses **termes** $u(n)$, pour $n \geq n_0$, peuvent être notés u_n. Il est **hors de question** d'écrire "la suite u_n", ou autres abominations du genre.

➠ **Exemple VII.1.** $(n^2+1)_{n\geq 0}$, $\left(\dfrac{1}{n}\right)_{n\geq 1}$.

✌ **Remarque VII.1.** Dans les faits, nous disposerons de trois façons de définir une suite numérique :

— de façon **explicite**, comme dans l'exemple *supra* ;

— de façon **implicite**, *e.g* l'unique suite u telle que $\forall n \in \mathbb{N}$, $u_n^2 + 1 = n$;

— **par récurrence**, en fixant le premier terme et donnant une relation reliant le terme de rang n à ceux le précédant (nous verrons plusieurs exemples de ce type de suite au paragraphe 5.⁻).

Dans la suite du chapitre, nous énoncerons et démontrerons les résultats en partant du principe que $n_0 = 0$. Il s'agit d'une simplification arbitraire et aisée à généraliser à toute valeur du rang initial ; nous laissons le soin de le faire à notre bienveillant lecteur. Nous nous intéresserons également dans un premier temps **uniquement aux suites à valeurs réelles** ; la généralisation au cas complexe des résultats ne sera par contre en aucun cas automatique, et nous lui dédions la partie 4.⁻ de ce chapitre.

b) Suites bornées

Définition VII.2. Une suite réelle $u \in \mathbb{R}^{\mathbb{N}}$ est dite :
— **majorée** si $\exists\, M \in \mathbb{R}$, $\forall n \in \mathbb{N}$, $u_n \leq M$;
— **minorée** si $\exists\, m \in \mathbb{R}$, $\forall n \in \mathbb{N}$, $u_n \geq m$;
— **bornée** si elle est majorée **et** minorée.

✌ **Remarque VII.2.** Une suite $(u_n)_n \in \mathbb{R}^{\mathbb{N}}$ est donc bornée si et seulement si la suite $(|u_n|)_n$ est majorée.

➠ **Exemple VII.2.** La suite $(n^2+1)_{n\geq 0}$ n'est pas majorée, mais minorée par 1, 0 ou même $-\dfrac{42\pi}{13}$.

c) Variations

Définition VII.3. Une suite réelle $u \in \mathbb{R}^{\mathbb{N}}$ est dite **croissante** (resp. **décroissante**) si :

$$\forall n, n' \in \mathbb{N} \text{ tels que } n \leq n',\ u_n \leq u_{n'} \text{ (resp. } u_n \geq u_{n'}\text{)}.$$

Si l'inégalité ci–dessus est stricte, on parle de monotonie stricte.

✌ **Remarque VII.3.** On peut (doit !) démontrer (par télescopage) que ceci est équivalent à l'étude du signe de $u_{n+1} - u_n$ pour tout $n \in \mathbb{N}$.

➠ **Exemple VII.3.** Étudions la monotonie de la suite $\left(\dfrac{n^2+1}{2n+1}\right)_n$. Soit $n \in \mathbb{N}$; alors :

$$\begin{aligned}
u_{n+1} - u_n &= \frac{(n+1)^2+1}{2(n+1)+1} - \frac{n^2+1}{2n+1} \\
&= \frac{(2n+1)((n+1)^2+1) - (2n+3)(n^2+1)}{(2n+3)(2n+1)} \\
&= \frac{(2n+1)(n^2+1) + (2n+1)^2 - (2n+1)(n^2+1) - 2(n^2+1)}{(2n+3)(2n+1)} \\
&= \frac{(2n+1)^2 - 2(n^2+1)}{(2n+3)(2n+1)} \\
&= \frac{4n^2+4n+1-2n^2-2}{(2n+3)(2n+1)} \\
&= \frac{2n^2+4n-1}{(2n+3)(2n+1)}\ .
\end{aligned}$$

Le numérateur est un trinôme du second degré en n dont l'unique racine positive est $-1+\sqrt{\dfrac{3}{2}} \cong 0.225$. De fait, $(u_n)_n$ est croissante à partir de $n=1$.

Définition VII.4. Une suite $u \in \mathbb{R}^{\mathbb{N}}$ est dite **stationnaire** si

$$\exists\, c \in \mathbb{R},\ \exists\, N \in \mathbb{N},\ \forall n \geq N,\ u_n = c\,.$$

✌ **Remarque VII.4.** Une suite stationnaire est donc une suite constante à partir d'un certain rang.

➠ **Exemple VII.4.** La suite $\left(\left\lfloor \dfrac{1}{n} \right\rfloor\right)_{n\geq 1}$ est stationnaire ; elle en effet nulle à partir de $n = 2$.

✍ **Exercice VII.1.** Démontrer que toute suite décroissante d'entiers naturels est stationnaire.

➥ **Correction :** *Soit $u \in \mathbb{N}^{\mathbb{N}}$ une suite décroissante. On pose :*

$$\mathscr{E} = \{u_n \,|\, n \geq 0\}$$

l'ensemble des termes de la suite. Il s'agit d'une partie de $\mathbb{N}$ non vide donc, par axiome D, $\mathscr{E}$ admet un minimum, soit $m_0 = u_{n_0}$. Par décroissance, pour tout $n \geq n_0$, $u_n \leq m_0$, ce qui entraîne par minimalité que $u_n = m_0$. La suite est donc bien constante à partir du rang n_0 (au moins).

2.⁻ Limite d'une suite

a) Limite réelle

Définition VII.5. Soit $u \in \mathbb{R}^{\mathbb{N}}$ et $\ell \in \mathbb{R}$; on dit que **la suite $(u_n)_n$ converge vers** ℓ si :

$$\forall \varepsilon > 0,\ \exists\, N \in \mathbb{N},\ \forall n \geq N,\ |u_n - \ell| \leq \varepsilon\,.$$

Le réel ℓ est alors appelé **limite** de la suite u.

Notation. On utilisera indifféremment $u_n \xrightarrow[n\to\infty]{} \ell$, $u_n \to \ell$, $\lim\limits_{n\to\infty} u_n = \ell$ ou $\lim u_n = \ell$.

Avant d'aller plus loin, analysons la définition de limite. Elle se découpe en trois parties :

— "$\forall \varepsilon > 0$" nous indique que ce qui va suivre sera vrai quel que soit le ε choisi. Ce dernier quantifiera la précision de notre approximation ;

— "$\exists\, N \in \mathbb{N},\ \forall n \geq N,$ " signifie que la propriété est vraie à partir d'un certain rang N ;

— "$|u_n - \ell| \leq \varepsilon$" nous dit que l'écart entre u_n et ℓ sera inférieur à la précision choisie.

In fine, la définition peut se reformuler de la façon suivante : **quelle que soit la précision choisie, u_n sera plus proche de ℓ que cette dernière pour n assez grand**.

➠ **Exemple VII.5.** Soit $\varepsilon > 0$; alors pour tout $n \geq \left\lfloor \frac{1}{\varepsilon} \right\rfloor + 1$, $\frac{1}{n} \leq \varepsilon$. Ainsi :

$$\frac{1}{n} \xrightarrow[n\to\infty]{} 0 \, .$$

Définition VII.6. Une suite convergeant vers une limite **RÉELLE** est dite **convergente.** Dans le cas contraire, elle est dite **divergente**.

➠ **Exemple VII.6.** La suite $\left(\frac{1}{n}\right) n \geq 1$ est convergente (vers 0). Nous verrons que la suite $((-1)^n)_n$ est divergente (sans limite), de même que $(n^2+1)_n$ (limite infinie).

Proposition VII.1. Une suite convergente admet exactement une limite.

Démonstration. Soit $u \in \mathbb{R}^n$ une suite convergente dont on suppose qu'elle admet deux limites ℓ et ℓ'. Soit $\varepsilon > 0$; alors, par définition de limite :
— $\exists\, N \in \mathbb{N},\ \forall n \geq N,\ ,|u_n - \ell| \leq \varepsilon$;
— $\exists N' \in \mathbb{N},\ \forall n \geq N',\ |u_n - \ell'| \leq \varepsilon$.
Ainsi, si on fixe $n \geq \max(N, N')$, on a :

$$\begin{aligned} |\ell - \ell'| &= |\ell - \ell' + u_n - u_n| \\ &\leq |u_n - \ell| + |u_n - \ell'| \\ &\leq 2\varepsilon \, . \end{aligned}$$

En posant $\varepsilon = \frac{1}{3}|\ell - \ell'|$ on obtient alors :

$$|\ell - \ell'| \leq \frac{2}{3}|\ell - \ell'|$$

ce qui n'est possible que si $|\ell - \ell'| = 0$, d'où le résultat.

□

Proposition VII.2. Une suite convergente est bornée.

Démonstration. Soit $u \in \mathbb{R}^{\mathbb{N}}$ convergeant vers $\ell \in \mathbb{R}$. Alors, en appliquant la définition de limite à $\varepsilon = 1$, on obtient :

$$\exists\, N \in \mathbb{N},\ \forall n \geq N,\ |u_n - \ell| \leq 1 \, .$$

La seconde inégalité triangulaire nous livre alors que :

$$\exists\, N \in \mathbb{N},\ \forall n \geq N,\ ||u_n| - |\ell|| \leq |u_n - \ell| \leq 1$$

et donc $|u_n| \in [1 - |\ell|, 1 + |\ell|]$. *In fine*, la suite $(u_n)_n$ est bornée par

$$\max(|u_0|, \ldots, |u_{N-1}|, 1 + |\ell|) \, .$$

□

✖ **Attention :** la réciproque est **fausse**, comme nous le verrons un peu plus tard. La suite $((-1)^n)_n$ est en effet bornée et divergente.

Proposition VII.3. Soit $u \in \mathbb{R}^{\mathbb{N}}$; alors :

(i) le produit d'une suite bornée par une suite convergeant vers 0 converge vers 0 ;

(ii) **si** $u_n \to \ell \in \mathbb{R}$, **alors** $|u_n| \to |\ell|$;

(iii) $u_n \to 0 \Leftrightarrow |u_n| \to 0$.

Démonstration.

(i) Supposons que $u_n \to 0$ et soit $v \in \mathbb{R}^{\mathbb{N}}$ une suite bornée par $M \in \mathbb{R}_+^*$. Alors, par définition de limite, pour tout $\varepsilon > 0$:

$$\exists\, N \in \mathbb{N},\ \forall n \geq N,\ |u_n - 0| \leq \frac{\varepsilon}{M}$$

et donc

$$\exists\, N \in \mathbb{N},\ \forall n \geq N,\ |u_n v_n| = |u_n||v_n| \leq M \times \frac{\varepsilon}{M} = \varepsilon$$

d'où $u_n v_n \to 0$.

(ii) Il suffit de remarquer que, pour tout $n \geq 0$, $||u_n| - |\ell|| \leq |u_n - \ell|$ et de réinjecter cela dans la définition de limite pour la suite $(u_n)_n$.

(iii) Immédiat via la définition de limite.

□

➠ **Exemple VII.7.** La suite $\left(\dfrac{(-1)^n}{n}\right)_{n\geq 1}$ converge vers 0.

Proposition VII.4. Soient $u, v \in \mathbb{R}^{\mathbb{N}}$ telles que :

— $v_n \to 0$;

— $\exists\, N \in \mathbb{N},\ \forall n \geq N,\ |u_n| \leq v_n$.

Alors $u_n \to 0$.

Démonstration. Soit $\varepsilon > 0$; alors par définition de limite, il existe $N' \in \mathbb{N}$ tel que pour tout $n \geq N$, $|v_n| = v_n \geq \varepsilon$. Ainsi, pour tout $n \geq \max(N, N')$, on a :

$$|u_n| \leq v_n \leq |v_n| \leq \varepsilon$$

d'où le résultat. □

b) "Limite" infinie

Définition VII.7. Soit $u \in \mathbb{R}^{\mathbb{N}}$; on dit que u **tend (ou diverge) vers** $+\infty$ **(resp.** $-\infty$**)** si :

$$\forall M \in \mathbb{R},\ \exists\, N \in \mathbb{N},\ \forall n \geq N,\ u_n \geq M \text{ (resp. } u_n \leq M).$$

Notation. $u_n \to \pm\infty$ ou $\lim u_n = \pm\infty$.

✖ **ATTENTION :** Une suite tendant vers $\pm\infty$ n'est **pas** convergente.

➠ **Exemple VII.8.** Soit $q \in]1, \infty[$ et posons $h = q - 1$. Alors, par binôme de Newton, pour tout $n \in \mathbb{N}$:

$$q^n = (1+h)^n \geq 1 + nh\,.$$

Ainsi, si $M \in \mathbb{R}$, alors $q^n \geq M$ dés que $n \geq \dfrac{M-1}{h}$; de fait $q^n \to \infty$.

✌ **Remarque VII.5.** Une suite divergeant vers $+\infty$ (resp. $-\infty$) n'est jamais majorée (resp. minorée). La réciproque est par contre **fausse** : considérer la suite $((-1)^n n)_n$.

Proposition VII.5. Une suite admet au plus une limite, finie ou infinie.

Démonstration. Soit $u \in \mathbb{R}^{\mathbb{N}}$. Si u est convergente, elle est bornée et donc ne peut admettre une limite infinie et possède une unique limite finie par la proposition VII.1. Dans le cas où $u_n \to \infty$, alors elle ne peut être convergente par définition et $\exists\, N \in \mathbb{N}$, $\forall n \geq N$, $u_n \geq 1$ donc u_n ne peut tendre vers $-\infty$. On traite de la même façon le cas $u_n \to -\infty$. $\square$

c) Opérations sur les limites

Commençons ce paragraphe par rappeler les opérations "étendues" que nous avons mis en place sur $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$ dans le chapitre III ; elles nous seront fort utiles pour l'énoncé des résultats de ce paragraphe.

$+$	$-\infty$	$y \in \mathbb{R}$	$+\infty$
$-\infty$	$-\infty$	$-\infty$	?
$x \in \mathbb{R}$	$-\infty$	$x+y$	$+\infty$
$+\infty$	?	$+\infty$	$+\infty$

$\times$	$-\infty$	$y \in \mathbb{R}_+^*$	0	$y \in \mathbb{R}_+^*$	$+\infty$
$-\infty$	$+\infty$	$+\infty$	?	$-\infty$	$-\infty$
$x \in \mathbb{R}_-^*$	$+\infty$	xy	0	xy	$-\infty$
0	?	0	0	0	?
$x \in \mathbb{R}_+^*$	$-\infty$	xy	0	xy	$+\infty$
$+\infty$	$-\infty$	$-\infty$	?	$+\infty$	$+\infty$

Proposition VII.6. Soient $u, v \in \mathbb{R}^{\mathbb{N}}$ et $\ell, \ell' \in \overline{\mathbb{R}}$ tels que $u_n \to \ell$ et $v_n \to \ell'$. Alors, à condition de ne pas tomber dans un cas d'indétermination, on a :

(i) $u_n + v_n \to \ell + \ell'$;

(ii) pour tout $\lambda \in \mathbb{R}$, $\lambda u_n \to \lambda \ell$;

(iii) $u_n v_n \to \ell\ell'$.

Démonstration. Traitons par exemple le cas (i) lorsque $\ell, \ell' \in \mathbb{R}$. Soit $\varepsilon > 0$; alors, quitte a prendre le maximum des deux rangs apparaissant dans la définition de limite pour u et v comme nous l'avons déjà fait auparavant, on a :

$$\exists\, N \in \mathbb{N},\ \forall n \geq N,\ \left(|u_n - \ell| \leq \frac{\varepsilon}{2}\right) \wedge \left(|v_n - \ell'| \leq \frac{\varepsilon}{2}\right)$$

et donc, pour tout $n \geq N$:

$$\begin{aligned} |u_n + v_n - (\ell + \ell')| &\leq |u_n - \ell| + |v_n - \ell'| \\ &\leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \\ &= \varepsilon \end{aligned}$$

d'où le résultat. Les autres cas se traitent selon un procédé similaire. □

Proposition VII.7. Soit $u \in \mathbb{R}^{\mathbb{N}}$ et soit $\ell \in]0, \infty]$ tel que $u_n \to \ell$. Alors :

(i) $\exists\, N \in \mathbb{N},\ \forall n \geq N,\ u_n > 0$;

(ii) $\dfrac{1}{u_n} \to \dfrac{1}{\ell}$, avec la convention que $\dfrac{1}{\infty} = 0$.

Démonstration.

Cas 1 : $\ell = \infty$. Soit $\varepsilon > 0$; alors par définition de limite :

$$\exists\, N \in \mathbb{N},\ \forall n \geq N,\ u_n \geq \frac{1}{\varepsilon}.$$

Ainsi, pour $n \geq N$, $u_n > 0$ et :

$$0 < \frac{1}{u_n} \leq \varepsilon$$

ergo $\dfrac{1}{u_n} \to 0$.

Cas 2 : $\ell \in \mathbb{R}_+^*$. Alors, par définition de limite :

$$\exists\, N \in \mathbb{N},\ \forall n \geq N,\ |u_n - \ell| \leq \frac{\ell}{2}\,.$$

Si $n \geq N$, u_n est alors strictement positif car compris entre $\dfrac{\ell}{2}$ et $\dfrac{3\ell}{2}$. En effet :

$$|u_n - \ell| \leq \frac{\ell}{2} \Longleftrightarrow u_n - \ell \in \left[-\frac{\ell}{2}, \frac{\ell}{2}\right]\,.$$

De plus, toujours pour $n \geq N$:

$$\begin{aligned} \left|\frac{1}{u_n} - \frac{1}{\ell}\right| &= \left|\frac{u_n - \ell}{u_n \ell}\right| \\ &= \frac{|u_n - \ell|}{|u_n|\ell} \\ &\leq \frac{2|u_n - \ell|}{\ell^2} \end{aligned}$$

d'où le résultat comme $u_n \to \ell$.

□

Exemple VII.9. Ceci implique (entre autres) que si $q \in]0,1[$, $q^n \to 0$; en effet $\frac{1}{q} > 1$ et donc $\left(\frac{1}{q}\right)^n \to \infty$.

Proposition VII.8. Soit $u \in \mathbb{R}^{\mathbb{N}}$ une suite telle que :
- $u_n \to 0$;
- $\exists N \in \mathbb{N}$, $\forall n \geq N$, $u_n > 0$.

Alors :
$$\frac{1}{u_n} \to \infty \,.$$

Démonstration. Analogue à celle de la proposition précédente. □

Remarque VII.6. Il existe un résultat analogue pour les suites strictement négatives à partir d'un certain rang convergeant vers 0.

Attention : l'hypothèse de stricte positivité est **essentielle**. En effet, la suite $\left(\frac{(-1)^n}{n}\right)_{n\geq 1}$ converge vers 0 en tant que produit d'une suite bornée par une suite de limite nulle (proposition VII.3), mais son inverse, la suite $((-1)^n n)_{n\geq 1}$ n'a pas de limite, comme nous le verrons un peu plus tard.

Le théorème suivant sera énoncé plus proprement et démontré au chapitre IX, mais nous en donnons une version simplifiée en avant–première afin de simplifier votre travail en exercices. Ne me remerciez pas…

Théorème VII.9 (Composition des limites)**.**
Soit $u \in \mathbb{R}^{\mathbb{N}}$ admettant pour limite $\ell \in \overline{\mathbb{R}}$ et soit f une fonction définie "autour de ℓ" telle que $f(x) \xrightarrow[x\to\ell]{} \ell' \in \overline{\mathbb{R}}$. Alors :
$$f(u_n) \to \ell' \,.$$

Exemple VII.10.
- $e^{-n^2} \to 0$, $e^{\frac{1}{n}} \to 1$.
- Posons $u_0 = 0$ et, pour $n \in \mathbb{N}$, $u_{n+1} = \sqrt{1+u_n}$. Alors, à supposer que cette suite admette une limite $\ell \in \mathbb{R}$ (nous le démontrerons plus tard dans l'année), l'unicité de la limite (proposition VII.1) entraîne que $\ell = \sqrt{1+\ell}$ et donc $\ell = \frac{1+\sqrt{5}}{2}$ (ℓ doit être positive car les termes de la suite u le sont et $\ell^2 = 1+\ell$).

d) Limites et ordre

Proposition VII.10. Soient $u, v \in \mathbb{R}^{\mathbb{N}}$ convergeant respectivement vers $\ell, \ell' \in \mathbb{R}$ telles que :

$$\exists\, N \in \mathbb{N},\ \forall n \geq N,\ u_n \leq v_n\ .$$

Alors :

$$\ell \leq \ell'\ .$$

Démonstration. Soit $\varepsilon > 0$; pour n assez grand (marre d'écrire les max de choses et autres, vous me pardonnerez probablement ; dans le cas contraire, même tarif) $|u_n - \ell| \leq \varepsilon$ et $|v_n - \ell'| \leq \varepsilon$. Ainsi :

$$\ell - \varepsilon \leq u_n \leq v_n \leq \ell' + \varepsilon$$

toujours pour n suffisamment grand. On en déduit que $\ell \leq \ell' + 2\varepsilon$ pour tout $\varepsilon > 0$, ce qui implique que $\ell - \ell'$ minore $\mathbb{R}_+^*$ et donc $\ell - \ell' \leq \inf \mathbb{R}_+^* = 0$, d'où le résultat. □

✖ **Attention :** il n'existe **pas** de résultat analogue pour les inégalités strictes ; en effet, pour tout $n \geq 0$, $n < n+1$ et pourtant les limites de ces deux quantités sont égales.

Théorème VII.11 (Existence par encadrement)**.**
Soient $u, v, w \in \mathbb{R}^{\mathbb{N}}$ et soit $\ell \in \mathbb{R}$ tels que :
- u et w convergent vers ℓ ;
- $\exists\, N \in \mathbb{N},\ \forall n \geq N,\ u_n \leq v_n \leq w_n$.

Alors :

$$v_n \to \ell\ .$$

Démonstration. Soit $\varepsilon > 0$, alors quitte à prendre le maximum des rangs associés à u et w :

$$\exists\, N' \in \mathbb{N},\ \forall n \geq N',\ (|u_n - \ell| \leq \varepsilon) \wedge (|w_n - \ell| \leq \varepsilon)\ .$$

Ainsi, pour $n \geq \max(N, N')$, on a l'inégalité :

$$\ell - \varepsilon \leq u_n \leq v_n \leq w_n \leq \ell + \varepsilon$$

qui nous permet de conclure que $|u_n - \ell| \leq \varepsilon$ et d'obtenir la convergence désirée. □

➠ **Exemple VII.11.** La suite $\left(\dfrac{(-1)^n + 2}{n}\right)_{n \geq 1}$ converge vers 0 ; en effet, pour tout $n \geq 1$ on a :

$$\frac{1}{n} \leq \frac{(-1)^n + 2}{n} \leq \frac{3}{n}\ .$$

Nous disposons également d'une "version infinie" de ce théorème, que nous énonçons dans le cas "par majoration" (limite $+\infty$) en laissant au lecteur le soin d'énoncer et démontrer son analogue "par minoration".

Proposition VII.12. Soient $u, v \in \mathbb{R}^{\mathbb{N}}$ telles que :
— $u_n \to \infty$;
— $\exists\, N \in \mathbb{N},\ \forall n \geq N,\ u_n \leq v_n$.
Alors :

$$v_n \to \infty\ .$$

✍ **Exercice VII.2.** En utilisant une intégrale, démontrer que $\displaystyle\sum_{k=1}^{n} \frac{1}{k} \xrightarrow[n\to\infty]{} +\infty$.

e) Suites extraites

Définition VII.8. Soit E un ensemble et soit $u \in E^{\mathbb{N}}$; on appelle **suite extraite** de u toute suite de la forme $(u_{\varphi(n)})_n$, où $\varphi : \mathbb{N} \to \mathbb{N}$ est une fonction strictement croissante.

✌ **Remarque VII.7.** Extraire une suite revient donc à ne "garder" que les termes indexés par l'image $\varphi(\mathbb{N})$.

➠ **Exemple VII.12.**
— $(u_{2n})_n$ et $(u_{2n+1})_n$ sont des suites extraites de u, ne contenant respectivement que ses termes d'indices pairs et impairs. De même, $(u_{n^2})_n$ est une suite extraite de u.
— Si $u = ((-1)^n)_n$, $(u_{2n})_n$ est la suite constante égale à 1.

Proposition VII.13. Soient $u \in \mathbb{R}^{\mathbb{N}}$ une suite admettant une limite $\ell \in \overline{\mathbb{R}}$; alors ses suites extraites tendent également vers ℓ.

Démonstration. Traitons par exemple le cas $\ell \in \mathbb{R}$. Soit $\varphi : \mathbb{N} \to \mathbb{N}$ est une fonction strictement croissante ; il est alors aisé de démontrer par récurrence que :

$$\forall n \in \mathbb{N},\ \varphi(n) \geq n\ .$$

Soit $\varepsilon > 0$, on a alors par définition de limite que :

$$\exists\, N \in \mathbb{N},\ \forall n \geq N,\ |u_n - \ell| \leq \varepsilon$$

et donc

$$\forall n \geq N,\ |u_{\varphi(n)} - \ell| \leq \varepsilon$$

car $\phi(n) \geq n \geq N$, d'où le résultat. □

➠ **Exemple VII.13.** Depuis le temps que nous vous le promettions : la suite $((-1)^n)_n$ n'admet pas de limite. En effet, la suite de ses termes d'indices pairs est constante égale à 1 et celle de ses termes impairs à -1 ; de fait elles n'ont pas même limite et donc la suite initiale ne peut admettre de limite.

✌ **Remarque VII.8.** L'exemple ci–dessus est loin d'être anecdotique ; cette proposition nous servira principalement démontrer que des suites n'admettent **pas** de limite.

Proposition VII.14. Soit $u \in \mathbb{R}^{\mathbb{N}}$ une suite telle que $(u_{2n})_n$ et $(u_{2n+1})_n$ tendent vers une même limite ℓ. Alors :

$$u_n \to \ell \, .$$

✌ **Remarque VII.9.** Le résultat reste vrai si $(u_{3n})_n$, $(u_{3n+1})_n$ et $(u_{3n+2})_n$ tendent vers la même limite (et ainsi de suite).

Démonstration. Traitons le cas $\ell \in \mathbb{R}$ et fixons $\varepsilon > 0$. Alors, quitte à remplacer N par le maximum des rangs associés aux extractions paire et impaire, on a :

$$\exists\, N \in \mathbb{N},\ \forall n \geq N,\ (|u_{2n} - \ell| \leq \varepsilon) \wedge (|u_{2n+1} - \ell| \leq \varepsilon) \, .$$

De fait, pour tout $n \geq 2N + 1$, on a $|u_n - \ell| \leq \varepsilon$, d'où le résultat. □

3.⁻ Théorèmes d'existence de limites

a) Le cas monotone

Notation. Si $(u_n)_n$ est une suite réelle majorée, on notera $\sup\limits_{n\in\mathbb{N}}(u_n)$ la borne supérieure de l'ensemble $\{u_n \,|\, n \in \mathbb{N}\}$. On peut bien sur étendre cette notation au cas de la borne inférieure de l'ensemble des termes d'une suite minorée.

Proposition VII.15. Soit $u \in \mathbb{R}^{\mathbb{N}}$ une suite croissante. Alors :
- si u est majorée, u converge vers $\sup\limits_{n\in\mathbb{N}}(u_n)$;
- sinon, u diverge vers $+\infty$.

✌ **Remarque VII.10.** Un résultat symétrique existe pour les suites décroissantes.

Démonstration.

Cas 1 : u est majorée. Alors l'ensemble

$$\mathscr{E} = \{u_n \,|\, n \in \mathbb{N}\}$$

est une partie de $\mathbb{R}$ non vide et majorée : elle admet donc une borne supérieure ℓ. Soit $\varepsilon > 0$; par définition de supremum, $\ell - \varepsilon$ ne majore pas $\mathscr{E}$ et donc il existe $N \in \mathbb{N}$ tel que $u_N \geq \ell - \varepsilon$. Or, $u_N \leq \ell$ donc $|u_N - \ell| \leq \varepsilon$ et comme la suite u est croissante, pour tout $n \geq N$, $u_n \geq u_N \geq \ell - \varepsilon$, *ergo*

$$\forall n \geq N,\ |u_n - \ell| \leq \varepsilon \, ,$$

d'où le résultat.

Cas 2 : **u n'est pas majorée.** Soit $M \in \mathbb{R}$; comme u n'est pas majorée, il existe $N \in \mathbb{N}$ tel que $u_N \geq M$. Or, u est croissante donc :

$$\forall n \geq N,\ u_n \geq u_N \geq M\,,$$

d'où le résultat.

$\square$

b) Adjacence

Proposition VII.16. Soient $u, v \in \mathbb{R}^{\mathbb{N}}$ deux suites telles que :
- l'une est croissante, l'autre décroissante ;
- $u_n - v_n \to 0$.

Alors $(u_n)_n$ et $(v_n)_n$ convergent vers la même limite.

Démonstration. Soient $(u_n)_n$ et $(v_n)_n$ deux telles suites, la première étant croissante, la seconde décroissante. Il est clair que dans cette configuration, comme $u_n - v_n \to 0$, pour tout $n \in \mathbb{N}$, $u_0 \leq u_n \leq v_n \leq v_0$ (car sinon la suite $({}_n - v_n)_n$ serait strictement positive, croissante et convergente vers 0). La suite $(u_n)_n$ est donc croissante et majorée par v_0 ; elle converge vers $\ell \in \mathbb{R}$.

De la même v est décroissante et minorée par u_0 donc converge vers $\ell' \in \mathbb{R}$; ainsi $u_n - v_n \to \ell - \ell'$. Par unicité de la limite, $\ell = \ell'$. $\square$

Vocabulaire. Deux telles suites sont dites *adjacentes*.

➠ **Exemple VII.14.** Posons, pour $n \geq 1$:

$$u_n = \sum_{k=1}^{n} \frac{(-1)^{k+1}}{k},\ v_n = u_{2n} \text{ et } w_n = u_{2n+1}\,.$$

Soit $n \geq 1$; alors :

$$\begin{aligned} v_{n+1} - v_n &= u_{2n+2} - u_{2n} \\ &= \sum_{k=1}^{2n+2} \frac{(-1)^{k+1}}{k} - \sum_{k=1}^{2n} \frac{(-1)^{k+1}}{k} \\ &= -\frac{1}{2n+2} + \frac{1}{2n+1} & \geq 0 \end{aligned}$$

donc v est croissante ; on montre de même que w est décroissante et

$$\begin{aligned} \forall n \geq 1,\ v_n - w_n &= \frac{-1}{2n+1} \\ &\to 0 \end{aligned}$$

donc les suites u et v sont adjacentes.

➠ **Exemple VII.15.** Les suites v et w de l'exemple précédent sont donc convergentes vers une même limite et donc, par proposition VII.14, la suite u converge vers cette même limite (nous verrons plus tard qu'il s'agit de $\ln(2)$).

c) Théorème de Bolzano–Weierstrass

Le résultat donnant son nom à ce paragraphe est nommé d'après Bernard Bolzano (autrichien, 1781—1848) et Karl Weierstass (allemand, 1815—1897).

Théorème VII.17 (Bolzano–Weierstrass)**.**
De toute suite réelle bornée on peut extraire une suite convergente.

La démonstration de ce théorème, bien qu'hors programme, nous est tout à fait accessible ; elle repose sur une dichotomie.

➠ **Exemple VII.16.** Il existe une fonction $\varphi : \mathbb{N} \to \mathbb{N}$ telle que la suite $(\cos(\varphi(n)))_n$ converge. À méditer : les $\varphi(n)$ forment une **suite d'entiers strictement croissante**. . .

4.⁻ Suites à valeurs complexes

a) Considérations liminaires

Nous avons défini au début de ce chapitre la notion de suite numérique, englobant les suites réelles et complexes. En préambule au présent paragraphe, notons que si $(z_n)_n \in \mathbb{C}^{\mathbb{N}}$ est une suite à valeurs complexes, on peut lui associer les suites **réelles** $(\mathrm{Re}(z_n))_n$, $(\mathrm{Im}(z_n))_n$ et $(|z_n|)_n$.

✖ **Attention :** la suite $(\overline{z_n})_n$ est quant à elle à valeurs complexes.

Définition VII.9. Une suite complexe $z \in \mathbb{C}^{\mathbb{N}}$ est dite **bornée** si la suite $(|z_n|)_n$ est majorée.

✖ **Attention :** on ne peut pas parler de suite complexe majorée ou minorée. . .

➠ **Exemple VII.17.** Si $\theta \in \mathbb{R}$, la suite $(e^{in\theta})_n$ est bornée.

Proposition VII.18. Soit $z \in \mathbb{C}^{\mathbb{N}}$; alors :

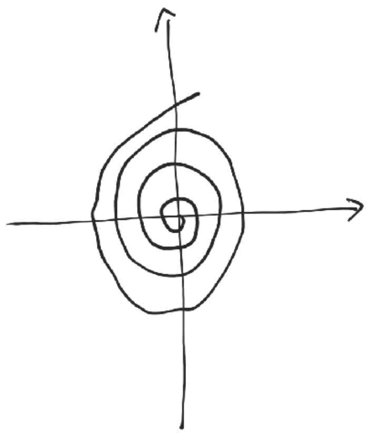
$$(z_n)_n \text{ est bornée} \\ \Longleftrightarrow \\ (\mathrm{Re}(z_n))_n \text{ et } (Im(z_n))_n \text{ sont bornées.}$$

Démonstration. Il s'agit d'une conséquence des majorations des parties réelles et imaginaires par le module vues dans le chapitre VI. □

b) Limites

La définition de limite finie se généralise sans problème aux suites complexes (lire la valeur absolue comme un module) ; la convergence d'une suite complexe est alors équivalente à la convergence des suites partie réelle et partie imaginaire associées.

✖ **Attention :** on ne parle **jamais** de limite infinie pour une suite complexe ; pour comprendre pourquoi, considérez la suite $(2^n e^{in})_n$ qui diverge "en spirale" : son module tend vers l'infini alors que son argument parcourt $[0, 2\pi[$ de façon périodique.



La plupart des résultats énoncés dans les paragraphes précédents se généralisent aux suites réelles sans avoir à en adapter les démonstrations, en particulier :
- les opérations sur les limites ;
- les théorèmes liés aux suites extraites, dont le théorème de Bolzano–Weierstrass (VII.17).

Par contre, en raison de l'absence d'ordre naturel sur $\mathbb{C}$, **aucun théorème en lien avec les inégalités ou la monotonie ne se généralise au cas complexe**.

5.⁻ Zoologie des suites usuelles

a) Suites arithmétiques, suites géométriques

Définition VII.10. Soit $u \in \mathbb{C}^{\mathbb{N}}$ et soit $a \in \mathbb{C}$. On dit que $(u_n)_n$ est une suite…
- …**arithmétique de raison** a si $\forall n \geq 0,\ u_{n+1} = u_n + a$;
- …**géometrique de raison** a si $\forall n \geq 0,\ u_{n+1} = a u_n$.

Ces suites ont été étudiées en long, en large et en travers en terminale. Rappelons tout de même les résultats suivants :
- si $u \in \mathbb{C}^{\mathbb{N}}$ est une suite arithmétique de raison $a \in \mathbb{C}$, alors son terme général est donné par la formule suivante :

$$\forall n \geq 0,\ u_n = u_0 + an$$

et sa somme par :

$$\forall n \geq 0,\ \sum_{k=0}^{n} u_k = (n+1)u_0 + a\frac{n(n+1)}{2}\ .$$

— si $u \in \mathbb{C}^{\mathbb{N}}$ est une suite géométrique de raison $a \in \mathbb{C}$, alors son terme général est donné par la formule suivante :

$$\forall n \geq 0,\ u_n = u_0 a^n$$

et sa somme par :

$$\forall n \geq 0,\ \sum_{k=0}^{n} u_k = \begin{cases} u_0(n+1) & \text{si } a = 1 \\ u_0 \dfrac{1-a^{n+1}}{1-a} & \text{sinon.} \end{cases}$$

Proposition VII.19 (Nature des suites géométriques)**.** Soit $q \in \mathbb{C}$; alors :
- si $|q| < 1$, la suite $(q^n)_n$ converge vers 0 ;
- si $|q| > 1$, la suite $(q^n)_n$ diverge et $|q^n| \to \infty$;
- si $|q| = 1$ et $q \neq 1$, la suite $(q^n)_n$ diverge.

Démonstration. Les cas $|q| < 1$ et $|q| > 1$ ont déjà été traités dans le cas réel ; la démonstration s'adapte aisément au cas complexe. Supposons à présent que $|q| = 1$ et $q \neq 1$ ($i.e$ que $q \in \mathbb{U} \setminus \{1\}$) ; alors, en passant à la limite dans l'égalité $u_{n+1} = qu_n$, on obtient :

$$\ell = q\ell$$

ce qui est absurde car $q \neq 1$ et $|\ell| = \lim |q^n| = 1$ donc $\ell \neq 0$. □

Définition VII.11. Soient $a, b \in \mathbb{C}$ tels que $a \neq 1$ et $b \neq 0$; on appelle **suite arithmético–géométrique** associée à a et b toute suite $u \in \mathbb{C}^{\mathbb{N}}$ vérifiant :

$$\forall n \geq 0,\ u_{n+1} = au_n + b\,.$$

La méthode d'étude d'une suite arithmético–géométrique est relativement aisée à mettre en œuvre ; on cherche (par analyse–synthèse) à trouver les suites $(v_n)_n = (u_n - \nu)_n$ (avec $\nu \in \mathbb{C}$) géométriques de raison a. Cela signifie que, pour $n \geq 0$ on a :

$$\begin{aligned} v_{n+1} = av_n &\Leftrightarrow u_{n+1} - \nu = a(u_n - \nu) \\ &\Leftrightarrow au_n + b - \nu = au_n - a\nu \\ &\Leftrightarrow \nu = \frac{b}{1-a}\,. \end{aligned}$$

De cette façon, on obtient que, pour tout $n \geq 0$:

$$v_n = v_0 a^n$$

i.e

$$u_n = \left(u_0 - \frac{b}{1-a}\right) a^n + \frac{b}{1-a}\,.$$

b) Récurrences linéaires d'ordre 2

On se fixe dans cette partie $a, b \in \mathbb{C}$ et on cherche à déterminer les suites complexes $u \in \mathbb{C}^{\mathbb{N}}$ définies par récurrence de la façon suivante :

$$\begin{cases} u_0, u_1 \in \mathbb{C} \\ \forall n \geq 0,\ u_{n+2} = au_{n+1} + bu_n \end{cases}.$$

Commençons par supposer la suite u géométrique de raison $q \in \mathbb{C}^*$; on aurait alors l'équation, pour $n \geq 0$:

$$u_0 q^{n+2} = u_0 q^{n+1} + u_1 q^n$$

i.e

$$u_0 q^n (q^2 - aq - b) = 0\,.$$

Il apparait ainsi que la raison q de notre suite doit être racine du polynôme $X^2 - aX - b$. Ceci nous donne l'intuition du résultat suivant.

Proposition VII.20. Soient $a, b \in \mathbb{C}$ et soit $u \in \mathbb{C}^{\mathbb{N}}$ une suite définie par récurrence de la façon suivante :

$$\begin{cases} u_0, u_1 \in \mathbb{C} \\ \forall n \geq 0,\ u_{n+2} = au_{n+1} + bu_n \end{cases}.$$

Considérons l'**équation caractéristique** associée à cette relation de récurrence, à savoir :

$$X^2 = aX + b\,. \qquad (\mathbf{E}\text{ :VII.1})$$

Alors :

- si (**E** :VII.1) admet deux racines q et q', le terme général de la suite u est donné par :
$$\forall n \geq 0,\ u_n = \alpha q^n + \beta q'^n$$
avec $\alpha, \beta \in \mathbb{C}$ à déterminer à l'aide de u_0 et u_1.
- si (**E** :VII.1) admet un unique racine q, le terme général de la suite u est donné par :
$$\forall n \geq 0,\ u_n = \alpha q^n + \beta n q^n$$
avec $\alpha, \beta \in \mathbb{C}$ à déterminer à l'aide de u_0 et u_1.

Démonstration. Par récurrence double. □

✌ **Remarque VII.11.** Les constantes α et β sont à déterminer via la système :

$$\begin{cases} u_0 &= \alpha + \beta \\ u_1 &= \alpha q + \beta q' \end{cases}$$

dans le premier cas et

$$\begin{cases} u_0 &= \alpha \\ u_1 &= (\alpha + \beta) q \end{cases}$$

dans le second.

Exemple VII.18.

— L'expression trouvée pour la suite de Fibonacci dans le chapitre I peut être retrouvée par cette méthode. Rappelons qu'il s'agit de la suite définie par

$$F_0 = 0, \quad F_1 = 1 \quad \text{et} \quad \forall n \geq 0,\ F_{n+2} = F_n + F_{n+1}\ .$$

— Étudions la suite $(u_n)_n$ définie par :

$$u_0 = 1, \quad u_1 = 1 \quad \text{et} \quad \forall n \geq 0,\ u_{n+2} = -u_n\ .$$

Son équation caractéristique étant $X^2 + 1 = 0$, on sait que son terme général sera de la forme, pour $n \geq 0$

$$u_n = \alpha i^n + \beta(-i)^n\ .$$

À l'aide des valeurs de u_0 et u_1, on trouve que $\alpha = \dfrac{1-i}{2}$ et $\beta = \dfrac{1+i}{2}$.

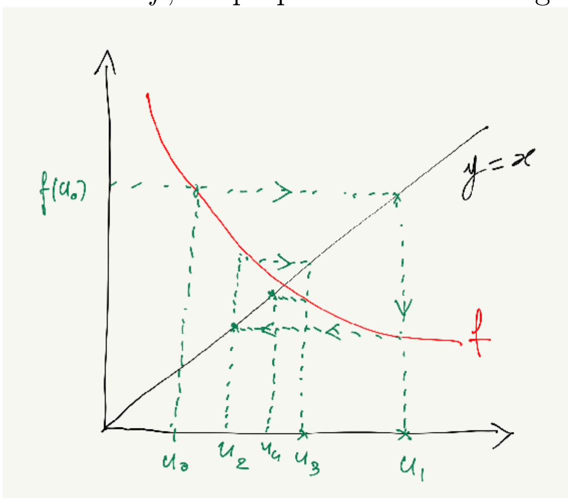
c) Suite récurrentes "générales"

Dans le cas général, une suite récurrente (du premier ordre) sera définie par la donnée de son premier terme $u_0 \in I$ (avec I un intervalle de $\mathbb{R}$) et une relation du type $\forall n \geq 0$, $u_{n+1} = f(u_n)$, avec $f : I \to \mathbb{R}$ une fonction (généralement continue).

La clé de l'étude d'une telle suite est en général de faire usage des méthodes suivantes :

— si f est continue et que $u_n \to \ell$, alors d'après le théorème VII.9, on a $f(u_n) \to f(\ell)$. On en déduit que $\ell = f(\ell)$ en utilisant la relation de récurrence, ce qui permet de déterminer ou de conjecturer la limite éventuelle de u ;

— la remarque *supra* permet d'affirmer que si convergence il y a, elle se fait vers un point fixe de la fonction f, ce qui peut être visualisé graphiquement ;



— pour déterminer la monotonie éventuelle d'une telle suite, il nous faudra étudier le signe de la fonction : $x \mapsto f(x) - x$ sur I. Pour que ceci ait un sens, il est **impératif** que l'intervalle I soit **stable** par f, *i.e* que $f(I) \subset I$. Si monotonie il y a, la limite prospective issue de la recherche de point fixe fournira naturellement le minorant/majorant requis pour conclure.

✖ **Attention** : la monotonie de f n'entraîne **en aucun cas** celle de la suite $(u_n)_n$.

✍ **Exercice VII.3.** Étudier la suite définie par $u_0 = 2$ et $\forall n \geq 0,\ u_{n+1} = u_n + \dfrac{1}{u_n}$.

➥ **Correction :** *On vérifie aisément que l'intervalle* $\mathbb{R}_+^*$ *est stable par la fonction* $f : x \mapsto x + \dfrac{1}{x}$, *ce qui entraîne que la suite* u *est à valeurs strictement positives. De fait et par continuité de* f, *si* $(u_n)_n$ *converge, sa limite* ℓ *est une solution positive de l'équation* $\ell = \ell + \dfrac{1}{\ell}$, *qui n'a pas de solution. De fait, cette suite est divergente. De plus, comme* $\forall n \geq 0,\ u_{n+1} - u_n = \dfrac{1}{u_n} > 0$, *on a que la suite* u *est strictement croissante et donc diverge vers* $+\infty$.

6.‾ Retour sur la topologie du corps des réels

Dans ce paragraphe, nous revenons sur certains résultats évoqués dans le chapitre III et les démontrons/complétons.

a) Caractérisation séquentielle des bornes

Proposition VII.21. Soit X une partie non vide de $\mathbb{R}$. Alors :
- — si X est majorée, il existe une suite $u \in X^{\mathbb{N}}$ convergeant vers $\sup(X)$;
- — sinon, il existe une suite $u \in X^{\mathbb{N}}$ divergeant vers $+\infty$.

✌ **Remarque VII.12.** Une fois n'est pas coutume, il existe un résultat symétrique relatif aux bornes inférieures et aux parties minorées.

Démonstration.

Cas 1 : X est majorée. Alors $M = \sup(X)$ existe dans $\mathbb{R}$ et, pour tout $n \geq 1$, la définition de supremum entraîne que :

$$\exists,\ x_n \in X,\ M - x_n \leq \frac{1}{n}\,.$$

Comme M majore X, alors :

$$\forall n \geq 1,\ 0 \leq |x_n - M| \leq \frac{1}{n}$$

ce qui nous permet de déduire, par théorème d'encadrement des limites (VII.11), que $x_n \to M$.

Cas 2 : X n'est pas majorée. Alors dans ce cas, pour tout $n \in \mathbb{N}$, il existe $x_n \in X$ tel que $n \leq x_n$; la suite $(x_n)_n$ diverge alors vers l'infini.

□

On déduit de ce résultat le corollaire suivant, déjà rencontré sous le nom de proposition III.8.

Proposition VII.22 (Caractérisation séquentielle de la borne supérieure)**.** Soit $A \subset \mathbb{R}$ et soit $M \in \mathbb{R}$; alors :

$$M = \sup(A) \iff \begin{cases} \forall a \in A,\ a \leq M \\ \exists (a_n)_n \in A^{\mathbb{N}},\ a_n \xrightarrow[n\to\infty]{} M \end{cases}.$$

b) Densité

Définition VII.12. Une partie X de $\mathbb{R}$ est dite **dense** si pour tout intervalle I non vide ni réduit à un point de $\mathbb{R}$, l'intersection $I \cap X$ est non vide.

Exemple VII.19. Nous avons vu dans le chapitre III que $\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$ étaient des parties denses de $\mathbb{R}$. Notons que c'est également le cas de $\mathbb{R}$...

Proposition VII.23. [Caractérisation séquentielle de la densité] Soit $X \subset \mathbb{R}$; alors :

$$X \text{ est une partie dense de } \mathbb{R}$$
$$\Leftrightarrow$$
$$\forall x \in \mathbb{R},\ \exists\, (x_n)_n \in X^{\mathbb{N}},\ x_n \to x.$$

Démonstration.

($\Downarrow$) Soit $x \in \mathbb{R}$ et soit $n \geq 1$; alors par densité

$$X \cap \left[x - \frac{1}{n}, x + \frac{1}{n}\right] \neq \emptyset$$

et donc il existe x_n dans cette intersection. Il est clair par encadrement que la suite $(x_n)_n$ converge vers x.

($\Uparrow$) Soit I un intervalle non vide de $\mathbb{R}$ et soit $x_0 \in I$ différent de ses bornes. Alors, par convexité de I, il existe $\varepsilon > 0$ tel

$$[x_0 - \varepsilon, x_0 + \varepsilon] \subset I \quad :$$

Or, par hypothèse, il existe une suite $(x_n)_n$ d'éléments de X convergeant vers x_0, ce qui entraîne que :

$$\exists\, N \in \mathbb{N},\ \forall n \geq N,\ x_n \in [x_0 - \varepsilon, x_0 + \varepsilon]$$

et donc, en particulier, $x_N \in I \cap X$.

□

Remarque VII.13. En utilisant ce résultat et l'approximation à 10^{-n} près vue dans le chapitre III, on peut démontrer que l'ensemble des nombres décimaux est dense dans $\mathbb{R}$.

Chapitre VIII

Groupes, anneaux et corps

0.⁻ Lois de composition interne

a) C'est quoi ?

Définition VIII.1. Soit E un ensemble non vide. On appelle **loi de composition interne** (LCI) sur E toute application $\star : E \times E \to E$.

➠ **Exemple VIII.1.** Nous en avons déjà rencontré un certain nombre ; par exemple

$$\begin{aligned} + : \mathbb{N} \times \mathbb{N} &\to \mathbb{N} \\ (m,n) &\mapsto m+n\ , \end{aligned}$$

$$\begin{aligned} - : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (m,n) &\mapsto m-n \end{aligned}$$

ou

$$\begin{aligned} \circ : \mathbb{R}^{\mathbb{R}} \times \mathbb{R}^{\mathbb{R}} &\to \mathbb{R}^{\mathbb{R}} \\ (f,g) &\mapsto f \circ g\ . \end{aligned}$$

Il en existe d'autres, moins évidentes : l'intersection et la réunion d'ensembles, ainsi que la différence ensembliste, sont des LCI sur $\mathscr{P}(E)$.

Notation. Si $\star$ est une LCI sur E et $x, y \in E$, nous noterons $\star(x,y)$ "$x \star y$" ; cette convention s'appelle la **notation infixée** (par opposition à la notation préfixée $\star(x,y)$ et à la notation postfixée $(x,y)\star$).

✌ **Remarque VIII.1.** Dans le cas de certaines LCI (la multiplication vient à l'esprit), nous n'écrirons parfois même pas l'opérateur : $x \times y$ deviendra xy.

Définition VIII.2. Une partie A d'un ensemble E muni d'une LCI $\star$ est dite **stable par** $\star$ si :

$$\forall x, y \in A,\ x \star y \in A\ .$$

➠ **Exemple VIII.2.** $\mathbb{N}$ est une partie de $\mathbb{Z}$ stable par addition et multiplication.

b) Propriétés remarquables

Dans ce paragraphe, nous listons certaines propriétés intéressantes pouvant être possédées par une loi de composition interne $\star$ que nous supposerons fixée sur un ensemble arbitraire E.

◇ Associativité

Définition VIII.3. La LCI $\star$ est dite **associative** si :

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

✌ **Remarque VIII.2.** Lorsque $\star$ est associative, on peut écrire des choses du style "$x \star y \star z$" sans ambiguïté.

➠ **Exemple VIII.3.**

— Nous avons vu que les opérations $+, \times, \circ$ étaient systématiquement associatives sur les ensembles *ad–hoc*.

— La soustraction n'est pas associative : $(2-3)-1 = -2 \neq 2-(3-1) = 0$. Cela signifie qu'il est logiquement insensé d'écrire des choses comme "$-2-3-1$" sans avoir préalablement décidé d'un sens prioritaire dans les opérations.

— De même, la division n'est pas associative.

— La réunion et l'intersection ensemblistes sont associatives, mais pas la différence.

◇ Élément neutre

Définition VIII.4. On dit que $e \in E$ est un **élément neutre** pour $\star$ si :

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

➠ **Exemple VIII.4.**

— Dans les sous–ensembles de $\mathbb{C}$ appropriés, 1 est le neutre pour la multiplication et 0 le neutre pour l'addition.

— Dans E^E, l'application id_E est un élément neutre pour la composition.

— Dans $\mathscr{P}(E)$, $\emptyset$ est neutre pour la réunion et E est neutre pour l'intersection.

— L'ensemble $2\mathbb{Z} = \{2k \,|\, k \in \mathbb{Z}\}$ n'admet pas d'élément neutre pour la multiplication.

Proposition VIII.1. Un élément neutre, si il existe, est unique.

Démonstration. Soient $e, e' \in E$ deux éléments neutres pour $\star$. Alors, comme e est neutre, $e \star e' = e'$, et comme e' est neutre, $e \star e' = e$, donc $e = e'$. □

✌ **Remarque VIII.3.** Un élément $\tau \in E$ tel que $\forall x \in E, \tau \star x = x \star \tau = \tau$ est appelé **élément absorbant**. Penser à 0 et à la multiplication.

◇ Inversibles

Supposons dans ce paragraphe que la loi de composition interne $\star$ soit **associative** et admette un élément neutre, que nous noterons e.

Définition VIII.5. Un élément $x \in E$ est dit **inversible** si :

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

Proposition VIII.2. Il y a unicité de l'inverse lorsqu'il existe.

Démonstration. Soit $x \in E$ d'inverse(s) y et z. Alors, comme $x\star y = e$, $z\star(x\star y) = z$ *i.e* $(z \star x) \star y = z$. Or $z \star x = e$ donc *in fine* $y = z$. □

Corollaire VIII.2.a. Soit $x \in E$ un élément inversible. Alors $(x^{-1})^{-1} = x$.

Notation. y est appelé **inverse de** x et noté x^{-1}. De plus :
- si $\star$ est l'addition, y sera noté $-x$;
- si $\star$ est la multiplication sur un sous–ensemble de $\mathbb{C}$, y sera noté $\dfrac{1}{x}$.

➠ **Exemple VIII.5.**
- Pour l'addition sur $\mathbb{R}$, $2^{-1} = -2$.
- Pour la multiplication sur ce même ensemble, $2^{-1} = \dfrac{1}{2}$

✖ **Attention :** il convient d'être extrêmement vigilant quant à la LCI considérée, et à rendre cette dernière limpide pour le correcteur au concours ou en exercices.

Qui sont les inversibles des LCI classiques ?
- pour l'addition sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$: tout le monde ;
- pour la multiplication sur $\mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$: tout le monde sauf 0 ;
- pour la composition sur E^E : les bijections ;
- pour la réunion sur $\mathscr{P}(E)$: uniquement $\emptyset$;
- pour l'intersection sur $\mathscr{P}(E)$: uniquement E.

Proposition VIII.3 (Simplification)**.** Soit $x, y, z \in E$ tels que x soit inversible. Alors :

(i) $(x \star y = x \star z) \Rightarrow (y = z)$;

(ii) $(y \star x = z \star x) \Rightarrow (y = z)$.

Démonstration. Il suffit de faire le produit (du bon côté et au sens de $\star$) par x^{-1} et d'utiliser l'associativité pour simplifier les égalités. □

✖ **Attention :** on ne peut simplifier **que** par un élément inversible. En effet, $0 \times 2 = 0 \times 1$ et pourtant $1 \neq 2$. Plus subtil : si on pose $f : x \mapsto x^2$, $g : x \mapsto \sqrt{|x|}$ et $h : x \mapsto -\sqrt{|x|}$ sur $\mathbb{R}$, on a $f \circ g = f \circ h$ et $g \neq h$.

Proposition VIII.4. Soient $x, y \in E$ deux éléments inversibles. Alors $x \star y$ est inversible et :

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

Démonstration. Vérifier que cet inverse convient et conclure par unicité. □

◇ **Distributivité**

Définition VIII.6. Soit Δ une LCE sur E ; on dit que $\star$ **est distributive par rapport à** Δ si on a, pour tous $x, y, z \in E$:

$$x \star (y \Delta Z) = (x \star y) \Delta (x \star z)$$

et

$$(y \Delta z) \star x = (y \star x) \Delta (z \star x) \, .$$

Exemple VIII.6.
- La multiplication est distributive par rapport à l'addition sur les sous–ensembles de $\mathbb{C}$.
- L'intersection et la réunion sont mutuellement distributives sur $\mathscr{P}(E)$.

◇ **Commutativité**

Définition VIII.7. La LCE $\star$ est dite **commutative** si :

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

✌ **Remarque VIII.4.** Certaines des propriétés précédentes sont plus simples à énoncer dans le cas commutatif.

Exemple VIII.7.
- La multiplication et l'addition le sont sur les sous–ensembles de $\mathbb{C}$, mais pas la soustraction ou la division.
- L'intersection et la réunion le sont sur $\mathscr{P}(E)$, mais pas la différence ensembliste.

1.⁻ Groupes

a) C'est quoi ?

Définition VIII.8. Soit G un ensemble muni d'une LCI $\star$. On dit que le couple $(G, \star)$ est un **groupe** si :

(A) la loi $\star$ est associative ;

(N) la loi $\star$ admet un élément neutre, noté e_G ;

(I) tous les éléments de G sont inversibles pour $\star$.

Si de plus la loi $\star$ est commutative, on parle de **groupe abélien** (du mathématicien norvégien Niels Henrik Abel, 1802—1829) ou commutatif.

Notation. Dans le cas général, nous utiliserons la notation multiplicative xy pour $x \star y$ afin d'alléger les énoncés des propositions lorsque cela sera pertinent. Nous réserverons la notation additive $x + y$ au cas des groupes abéliens.

✌ **Remarque VIII.5.** Un groupe est nécessairement non vide car il contient au moins son élément neutre.

➠ **Exemple VIII.8.**

— si e est neutre pour $\star$, $(\{e\}, \star)$ est un groupe, appelé **groupe trivial** ;

— $(\mathbb{Z}, +)$ est un groupe abélien, mais pas $(\mathbb{N}, +)$ (mise en défaut de la propriété (I)) ;

— $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes, abélien mais pas $(\mathbb{R}, \times)$ (même problème) ;

— $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes abéliens ;

— $(\mathbb{Q}_+^*, \times)$ et $(\mathbb{R}_+^*, \times)$ sont des groupes abéliens ;

— si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, $(\mathbb{K}^{\mathbb{N}}, +)$ est un groupe abélien ;

— $(\mathfrak{S}_E, \circ)$ est un groupe, non abélien pour tout ensemble E ayant au moins 3 éléments (*cf. infra*).

La proposition suivante, dont la démonstration est laissée en exercice à notre lecteur favori (ainsi qu'aux autres, par souci d'équité) fournit pléthore de nouveaux exemples de groupes qui nous serons fort utiles dans le chapitre XVIII.

Proposition/définition VIII.9. Soit $(G, \star)$ et (H, Δ) deux groupes. Alors le produit cartésien $G \times H$ est un groupe, appelé **groupe produit**, pour la loi

$$((x, y), (x', y')) \mapsto (x \star x', y \Delta y') .$$

Ce groupe est abélien si et seulement si G et H le sont.

➠ **Exemple VIII.9.** Les ensembles $\mathbb{R}^n$ et $\mathbb{C}^n$ (pour $n \geq 1$) sont des groupes pour l'addition terme à terme.

✍ **Exercice VIII.1.** Soient $K = \{e, a, b, c\}$ un ensemble à quatre éléments ; démontrer que la LCI suivante définit une loi de groupe abélien sur K, que l'on appelle alors **groupe de Klein** (Felix, 1849—1925, mathématicien allemand).

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\diamond$ **Un exemple fondamental : le groupe des permutations.**

Soit $n \geq 1$; on appelle **groupe des permutations de** $[\![1, n]\!]$ l'ensemble (aussi noté S_n)

$$\mathfrak{S}_n = \mathfrak{S}_{[\![1,n]\!]}$$

muni de la composition. Il s'agit d'un groupe non abélien dont les éléments sont les applications associant à chaque entier de $[\![1, n]\!]$ un autre tel nombre de façon bijective.

Exemple VIII.10.
- $\mathfrak{S}_1 = \{\mathrm{id}_{[\![1,n]\!]}\}$ est le groupe trivial ;
- $\mathfrak{S}_2 = \{\mathrm{id}_{[\![1,n]\!]}, \sigma\}$, avec σ l'application permutant 1 et 2 ;
- $\mathfrak{S}_3$ possède 6 éléments : lesquels ?

Un élément $\sigma \in \mathfrak{S}_n$ peut être construit de la façon suivante : on dispose de n choix pour l'image de 1, puis (une fois celui–ci fixé), de $n-1$ choix pour l'image de 2, $n-2$ choix pour l'image de 3, etc. On en déduit que $\mathfrak{S}_n$ possède exactement $n!$ éléments.

Exercice VIII.2. Déterminer $\mathfrak{S}_4$.

b) Puissances

Définition VIII.10. Soit G un groupe de neutre e. On définit, pour $x \in G$ et $n \in \mathbb{Z}$ l'élément **puissance n–ième de x** comme suit :
- $x^0 = e$;
- si $n \in \mathbb{N}$, $x^{n+1} = x^n x$;
- si $n < 0$, $x^n = (x^{-1})^{-n}$.

Exemple VIII.11.
- sur $(\mathbb{C}^*, \times)$, cela correspond aux puissances usuelles ;
- sur $(\mathbb{C}, +)$, pour $x \in \mathbb{C}$ et $n \geq 1$, $x^n = \underbrace{x + \ldots + x}_{n \text{ fois}} = nx$. On en déduit aisément que **les puissances additives sont les multiples**. Attention ici aux notations et à leur potentiel de confusion.
- sur $\mathfrak{S}_n$, passer une permutation à la puissance $n \in \mathbb{N}^*$ revient à la composer n fois avec elle–même.

Proposition VIII.5. Soit G un groupe et soient $x \in G$ et $n, m \in \mathbb{Z}$. Alors :

(i) $x^{n+m} = x^n x^m = x^m x^n$;

(ii) $(x^n)^m) = x^{nm}$.

Remarque VIII.6. Ce résultat, comme tous ceux de ce paragraphe, peut se reformuler en notation additive (traditionnellement utilisée dans le cas abélien uniquement) :

(i) $(n+m)x = nx + mx$;

(ii) $m(nx) = (mn)x$.

Proposition VIII.6. Soit G un groupe et soient $x, y \in G$ tels que $xy = yx$. Alors, pour tous $m, n \in \mathbb{Z}$:

$$x^n y^m = y^m x^n \ .$$

De plus :

$$(xy)^n = x^n y^n = y^n x^n \ .$$

Démonstration. Ce résultat et le précédent se démontrent par récurrence en distinguant les cas d'exposants positifs et négatifs. □

c) Sous–groupes

Définition VIII.11. Soit $(G, \star)$ un groupe. On appelle **sous–groupe** de G tout ensemble H tel que :

— $H \subset G$;

— $(H, \star)$ est un groupe.

Exemple VIII.12.

— $(\mathbb{Q}, +)$ est un sous–groupe de $(\mathbb{R}, +)$;

— $\mathfrak{S}_3$ est un sous–groupe de $\mathfrak{S}_3$.

Proposition VIII.7. Soit $(G, \star)$ un groupe et H un sous–groupe de G. Alors :

(i) $e_H = e_G$;

(ii) si $x \in H$ alors son inverse est le même dans H et dans G.

Démonstration.

(i) Remarquons que $e_H \star e_H = e_H$ dans H donc dans G. Ainsi, toujours dans G, $e_H = e_H \star e_H^{-1}$ et donc $e_H = e_G$.

(ii) Notons y l'inverse de x dans G et z son inverse dans H. Alors, en posant $e = e_H = e_G$ (*cf.* (i)) on a :

$$y \star x = e = z \star x$$

et donc

$$y \star x \star z = z \star x \star z$$

ce qui entraîne que $y = z$ car $x \star z = e$.

□

Proposition VIII.8 (Caractérisation des sous–groupes)**.** Soit G un groupe de neutre e et soit $H \subset G$. Alors :

$$H \text{ est un sous–groupe de } G \iff \begin{cases} H \neq \emptyset \\ \forall x, y \in H,\ xy \in H \\ \forall x \in H,\ x^{-1} \in H \end{cases} .$$

Remarque VIII.7. Les deux derniers points de la caractérisation peuvent être remplacés par :

$$\forall x, y \in H,\ xy^{-1} \in H .$$

Exemple VIII.13. Cette caractérisation permet de démontrer, en utilisant des résultats vus dans le chapitre précédents, que :
- $\mathbb{U}$ est un sous–groupe de $(\mathbb{C}^*, \times)$;
- pour $n \in \mathbb{N}^*$, $\mathbb{U}_n$ est un sous–groupe de $\mathbb{U}$;
- pour $n \in \mathbb{Z}$, $n\mathbb{Z} = \{nk \,|\, k \in \mathbb{Z}\}$ est un sous–groupe de $(\mathbb{Z}, +)$.
- $\mathbb{R}_+^*$ est un sous–groupe de $(\mathbb{R}^*, \times)$, qui est lui–même un sous–groupe de $\mathbb{C}^*$.

Exercice VIII.3. Soit $n \geq 1$; on pose

$$H_n = \{\sigma \in \mathfrak{S}_n \,|\, \sigma(n) = n\} .$$

Démontrer que H_n est un sous–groupe de $(\mathfrak{S}_n, \circ)$.

Correction : *H_n est non vide car il contient $\mathrm{id}_{[\![1,n]\!]}$. De même, il est clair que la composée et l'inverse de deux éléments de H_n sont dans H_n, d'où le résultat (composer par σ^{-1} dans $\sigma(n) = n$).*

Corollaire VIII.8.a. L'intersection de deux sous–groupes d'un même groupe en est un sous–groupe.

Démonstration. Soient H et K deux sous–groupes d'un groupe G de neutre e. Alors :
- $e \in H \cap K$ donc cet ensemble est non vide ;
- si $x, y \in H \cap K$, alors $xy^{-1} \in H$ et $xy^{-1} \in K$ car $x, y \in H$ et $x, y \in K$ respectivement.

D'où le résultat. □

Attention : la réunion de deux sous–groupes n'est pas un sous groupe : en effet, $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ et pourtant $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

d) Morphismes de groupes

Définition VIII.12. Soit $(G, \star)$ et (H, Δ) deux groupes. On appelle **morphisme de groupes** de G vers H toute application $f : G \to H$ telle que :

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

Exemple VIII.14. La encore nous en avons déjà croisés quelques–un :
- $\exp : (\mathbb{R},+) \to (\mathbb{R}_+^*, \times)$;
- $\ln : (\mathbb{R}_+^*, \times) \to (\mathbb{R},+)$;
- $$\begin{aligned} \varphi : (\mathbb{R},+) &\to (\mathbb{U},\times) \\ \theta &\mapsto e^{i\theta} \end{aligned} .$$

Proposition VIII.9. Soit G, H deux groupes et $f : G \to H$ un morphisme de groupes. Alors :
- (i) $f(e_G) = e_H$;
- (ii) si $x \in G$, $f(x^{-1}) = f(x)^{-1}$;
- (iii) si $x \in G$ et $n \in \mathbb{Z}$, $f(x^n) = f(x)^n$.

Démonstration.
- (i) Il suffit de remarquer que $f(e_G) = f(e_G \cdot e_G) = f(e_G)f(e_G)$ et de simplifier.
- (ii) Soit $x \in G$; alors :
$$f(x)f(x^{-1}) = f(x \cdot x^{-1}) = f(e_G) = e_H$$
d'où le résultat.
- (iii) À démontrer par récurrence en distinguant les cas d'exposants positifs et négatifs.

□

Vocabulaire. Soit G, H deux groupes. Un morphisme de groupes $f : G \to H$ est appelé...
- ...**isomorphisme** s'il est bijectif ;
- ...**endomorphisme** si $G = H$;
- ...**automorphisme** si il est bijectif et que $G = H$.

Proposition VIII.10. Soient G, H deux groupes, G' (resp. H') un sous–groupe de G (resp. H) et $f : G \to H$ un morphisme de groupes. Alors :
- (i) $f(G')$ est un sous–groupe de H ;
- (ii) $f^{-1}(H')$ est un sous–groupe de G.

Démonstration. Notons $\star$ (resp. Δ) la LCI sur G (resp. H) associée à sa structure de groupe.
- (i) Il est clair que $f(G') \subset H$; de plus $e_G \in G'$ (car G' est un sous–groupe de G) ce qui entraîne que $e_H = f(e_G) \in f(G')$. Soient ensuite $X, Y \in f(G')$; alors il existe $x, y \in G'$ tels que $X = f(x)$ et $Y = f(y)$ donc :
$$\begin{aligned} X \Delta Y &= f(x) \Delta f(y) \\ &= f(\underbrace{x \star y}_{\in G'}) \in f(G') . \end{aligned}$$

(ii) On sait que $f^{-1}(H') \subset G$; de plus $e_H \in F'$ ce qui entraîne que $e_G = f^{-1}(e_H) \in f^{-1}(H')$. Soient ensuite $x, y \in f^{-1}(H')$; alors :

$$f(x \star y) = f(x) \Delta f(y) \in H'$$

et donc $x \star y \in f^{-1}(H')$.

$\square$

➠ **Exemple VIII.15.** L'ensemble $\ln^{-1}(\mathbb{Z})$ est un sous–groupe de $\mathbb{R}^*$ (égal à $\exp(\mathbb{Z})$ par ailleurs).

Ce résultat nous permet, outre les exemples de sous–groupes qu'il fournit, de définir deux ensembles essentiels à toute étude de morphisme qui se respecte, à savoir son image et son noyau.

Proposition/définition VIII.13. Soient G, H deux groupes et soit $f : G \to H$ un morphisme de groupes. On appelle :
— **noyau** de f l'ensemble

$$\mathrm{Ker}(f) = \{x \in G \,|\, f(x) = e_H\} \,;$$

— **image** de f l'ensemble

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

Ces deux ensembles sont de plus des sous–groupes de G et H respectivement.

Démonstration. Il suffit de remarquer que $\mathrm{Ker}(f) = f^{-1}(\{e_H\})$ et $\mathrm{Im}(f) = f(G)$. $\square$

➠ **Exemple VIII.16.**
— Le noyau de l'application ln est réduit à $\{1\}$;
— le noyau de l'application

$$\begin{aligned} \phi : (\mathbb{R}, +) &\to (\mathbb{C}^*, \times) \\ \theta &\mapsto e^{i\theta} \end{aligned} \quad .$$

est égal à $2\pi\mathbb{Z} = \{2k\pi \,|\, k \in \mathbb{Z}\}$ et son image est égale à $\mathbb{U}$.

L'utilité première de ces deux sous–groupe est, à notre niveau, de fournir une CNS d'injectivité et de surjectivité fort sympathique.

Proposition VIII.11. Soient G, H deux groupes et soit $f : G \to H$ un morphisme de groupes. Alors :
(i) f est injective $\Leftrightarrow \mathrm{Ker}(f) = \{e_G\}$;
(ii) f est surjective $\Leftrightarrow \mathrm{Im}(f) = H$.

Démonstration. Notons $\star$ (resp. Δ) la LCI sur G (resp. H) associée à sa structure de groupe.

(i) ($\Rightarrow$) Immédiat car $f(e_G) = e_H$.

($\Leftarrow$) Supposons que $\mathrm{Ker}(f) = \{e_G\}$ et fixons $x, x' \in G$ tels que $f(x) = f(x')$. Alors, $f(x \star x'^{-1}) = f(x)\Delta f(x')^{-1} = e_H$ et donc $x \star x'^{-1} \in \mathrm{Ker}(f)$, ce qui entraîne que $x = x'$.

(ii) Il s'agit de la définition de surjectivité.

$\square$

2.⁻ Anneaux, corps

a) Qu'est-ce ?

Définition VIII.14. Un ensemble $\mathbb{A}$ muni de **deux** LCI distinctes $+$ et $\times$ est appelé **anneau** (unitaire) si :

(G) $(\mathbb{A}, +)$ est un groupe **abélien** ;

(A) $\times$ est associative ;

(D) $\times$ est distributive par rapport à $+$;

(N) la loi $\times$ admet un élément neutre.

Si de plus la loi $\times$ est commutative, on parle d'**anneau commutatif**.

Notation. L'élément neutre pour $+$ est noté $0_{\mathbb{A}}$ (ou simplement 0), le neutre pour $\times$ est noté $1_{\mathbb{A}}$ (ou 1).

✌ **Remarque VIII.8.** Soit $(\mathbb{A}, +, \times)$ est un anneau.

— pour tout $x \in \mathbb{A}$,
$$0 \cdot x = (1-1)x = x - x = 0$$
; 0 est donc absorbant pour la loi $\times$.

— Si $a \in \mathbb{A}$ et $n \in \mathbb{A}$, on peut définir le **multiple** na comme sa puissance additive. On ne peut toute fois pas définir la puissance a^n pour $n < 0$ lorsque a n'est pas inversible.

➠ **Exemple VIII.17.**

— les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont des anneaux pour l'addition et la multiplication standards ;

— si E est un ensemble et $\mathbb{A}$ un anneau, $\mathbb{A}^E$ est un anneau pour les opérations terme à terme (*cf.* chapitre II) ;

— le seul anneau dans lequel $0 = 1$ est l'**anneau nul** $\{0\}$. En effet, si x est un élément d'un tel anneau alors $0 \cdot x = 0 = 1 \cdot x = x$.

b) Identités remarquables

Soit $(\mathbb{A}, +, \times)$ un anneau ; alors la notation suivante a un sens, pour $a_1, \ldots, a_h \in \mathbb{A}$:

$$\sum_{k=1}^{n} a_k = a_1 + \ldots + a_n \ .$$

De plus, si $\mathbb{A}$ est commutatif, on pose :

$$\prod_{k=1}^{n} a_k = a_1 \times \ldots \times a_n .$$

On généralise ces notations au cas de familles **finies** indexées par un ensemble quelconque. De plus, toutes les propriétés et techniques élémentaires (scission, linéarité de la somme, changement d'indice) vues dans le chapitre II se généralisent au cas d'un anneau.

Proposition VIII.12. Soit $\mathbb{A}$ un anneau et $a, b \in \mathbb{A}$ tels que $ab = ba$. Alors, pour tout $n \in \mathbb{N}$:

(i)

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

(ii)

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

Démonstration. Comme a et b commutent, on peut recopier les démonstrations des propositions II.11 et II.10. □

Corollaire VIII.12.a. Soit $\mathbb{A}$ un anneau et $a \in \mathbb{A}$. Alors, pour tout $n \in \mathbb{N}^*$:

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

Démonstration. Appliquer le (ii) de la proposition VIII.12 à $b = 1$. □

✌ **Remarque VIII.9.** On peut voir dans cette formule un analogue de la somme des termes d'une suite géométrique vue dans le chapitre II.

c) Sous–anneaux, groupe des inversibles

Définition VIII.15. Soit $\mathbb{A}$ un anneau et soit $\mathbb{B} \subset \mathbb{A}$. On dit que $\mathbb{B}$ est un **sous–anneau** de $\mathbb{A}$ si :

— $\mathbb{B}$ est un anneau ;

— $1_{\mathbb{B}} = 1_{\mathbb{A}}$.

➠ **Exemple VIII.18.** $\mathbb{Z}$ est un sous–anneau de $\mathbb{R}$, qui est un sous–anneau de $\mathbb{C}$.

Comme dans le cas des sous–groupes, on dispose d'une caractérisation (analogue à a la proposition VIII.8) des sous–anneaux : si $\mathbb{A}$ est un anneau et $\mathbb{B} \subset \mathbb{A}$, alors

$$\mathbb{B} \text{ est un sous–anneau de } \mathbb{A} \iff \begin{cases} 1 \in \mathbb{B} \\ \forall x, y \in \mathbb{B},\ x - y \in \mathbb{B} \\ \forall x, y \in \mathbb{B},\ xy \in \mathbb{B} \end{cases} .$$

➠ **Exemple VIII.19.** À l'aide de cette caractérisation, il est aisé de montrer que l'ensemble des **entiers de Gauss**

$$\mathbb{Z}[i] = \{a + ib \,|\, a, b \in \mathbb{Z}\}$$

est un sous–anneau de $\mathbb{C}$.

Définition VIII.16. Soit $\mathbb{A}$ un anneau ; on dit que $x \in \mathbb{A}$ est **inversible** si il l'est pour la loi $\times$.

Notation. On note $\mathbb{A}^\times$ l'ensemble des inversibles de l'anneau $\mathbb{A}$.

✌ **Remarque VIII.10.** Remarquons que $(\mathbb{A}^\times, \times)$ est naturellement un groupe.

➠ **Exemple VIII.20.**
— $\mathbb{Z}^\times = \{-1, 1\}$;
— $\mathbb{C}^\times = \mathbb{C}^*$;
— $\{0\}^\times = \{0\}$ (et oui. . .).

d) Morphismes d'anneaux

Définition VIII.17. Soient $\mathbb{A}$ et $\mathbb{B}$ deux anneaux. On dit qu'une application $f : \mathbb{A} \to \mathbb{B}$ est un **morphisme d'anneaux** si :
— $f(1_\mathbb{A}) = 1_\mathbb{B}$;
—
$$\forall x, y \in \mathbb{A}, \quad f(x + y) = f(x) + f(y) \quad \text{et} \quad f(xy) = f(x)f(y) .$$

✌ **Remarque VIII.11.** Un morphisme d'anneau est donc un morphisme de groupes entre $(\mathbb{A}, +)$ et $(\mathbb{B}, +)$ et hérite donc de toutes les propriétés **additives** que cela implique.

Vocabulaire. Soit $\mathbb{A}, \mathbb{B}$ deux anneaux. Un morphisme d'anneaux $f : \mathbb{A} \to \mathbb{B}$ est appelé. . .
— . . .**isomorphisme** s'il est bijectif ;
— . . .**endomorphisme** si $\mathbb{A} = \mathbb{B}$;
— . . .**automorphisme** si il est bijectif et que $\mathbb{A} = \mathbb{B}$.

➠ **Exemple VIII.21.**
— $x \mapsto x$ est un morphisme d'anneaux de $\mathbb{Z}$ vers $\mathbb{Q}$;
— $z \mapsto \overline{z}$ est un endomorphisme de $(\mathbb{C}, +, \times)$;

— $k \mapsto 2k$ n'est **pas** un endomorphisme de $(\mathbb{Z}, +, \times)$ alors qu'il s'agit d'un endomorphisme du **groupe** $(\mathbb{Z}, +)$.

✌ **Remarque VIII.12.** De la même façon que pour les morphismes de groupes, on peut définir le noyau et l'image d'un morphisme d'anneaux (qui seront ceux du morphisme de groupes sous–jacent) et obtenir une CNS d'injectivité et de surjectivité.

e) Anneaux intègres, corps

Définition VIII.18. Un anneau $\mathbb{A}$ est dit **intègre** si
- il est commutatif ;
- il est différent de l'anneau nul ;
- pour tous $x, y, z \in \mathbb{A}$ tels que $z \neq 0$ on a :

$$(xz = yz) \Rightarrow (x = y)\,.$$

✌ **Remarque VIII.13.** Un anneau intègre est donc un anneau dans lequel on peut simplifier par un élément non nul dans un produit. Ceci signifie, par contraposée, qu'il existe dans tout anneau non intègre deux éléments a et b **non nuls** tels que $ab = 0$. De tels éléments sont appelés **diviseurs de zéro**.

➠ **Exemple VIII.22.**
- les anneaux $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont intègres ;
- l'anneau $\mathbb{R}^{\mathbb{R}}$ n'est pas intègre : penser au produit $\mathbb{1}_{\mathbb{R}_+^*} \times \mathbb{1}_{\mathbb{R}_-}$.

Définition VIII.19. Un anneau est appelé **corps** si :
- il est commutatif ;
- il est différent de l'anneau nul ;
- tous ses éléments non nuls sont inversibles pour la multiplication.

➠ **Exemple VIII.23.** $\mathbb{R}$ et $\mathbb{C}$ sont des corps, mais pas $\mathbb{Z}$, $\mathbb{D}$ ou $\mathbb{R}^{\mathbb{R}}$.

✌ **Remarque VIII.14.**
- un corps est automatiquement un anneau intègre ;
- si $\mathbb{K}$ est un corps, alors $\mathbb{K}^{\times} = \mathbb{K} \setminus \{0\}$.

Vocabulaire. Un sous–anneau d'un corps qui est lui–même un corps est appelé **sous–corps** du corps de base.

✌ **Remarque VIII.15.** On a naturellement la caractérisation suivante : si $\mathbb{K}$ est un corps et $\mathbb{L} \subset \mathbb{K}$, alors

$$\mathbb{L} \text{ est un sous–corps de } \mathbb{K} \Longleftrightarrow \begin{cases} 1 \in \mathbb{L} \\ \forall x, y \in \mathbb{L},\ x - y \in \mathbb{L} \\ \forall (x, y) \in \mathbb{L} \times \mathbb{L}^*,\ xy^{-1} \in \mathbb{L} \end{cases}.$$

✍ **Exercice VIII.4.** Démontrer que $\mathbb{Q}[j] = \{a + bj + cj^2 \mid a, b, c \in \mathbb{Q}\}$ est un corps.

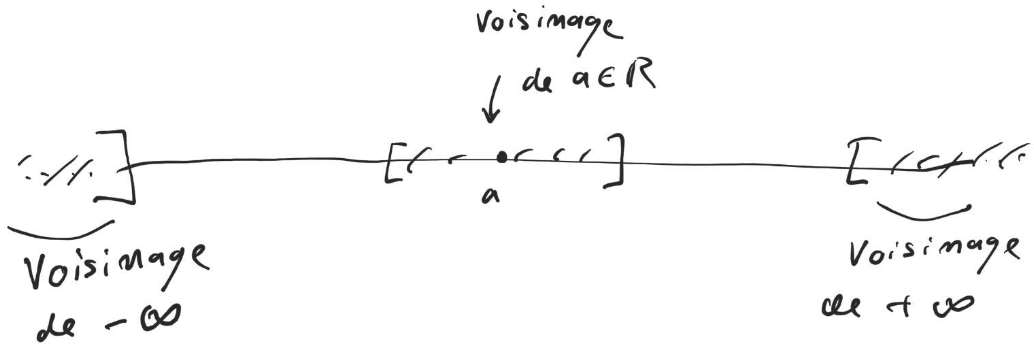
Chapitre IX

Limites, continuité

1.⁻ Étude locale d'une fonction

a) Voisinages

Définition IX.1. Soit $a \in \overline{\mathbb{R}}$. On appelle **voisinage de** a tout ensemble de la forme :
- — $[a-\delta, a+\delta]$ avec $\delta > 0$ si $a \in \mathbb{R}$;
- — $[M, +\infty[$ avec $M \in \mathbb{R}$ si $a = +\infty$;
- — $]-\infty, m]$ avec $m \in \mathbb{R}$ si $a = -\infty$.



Notation. On notera $\mathscr{V}(a)$ l'ensemble des voisinages de $a \in \overline{\mathbb{R}}$.

Exemple IX.1. $[-1,1] \in \mathscr{V}(0)$, $\mathbb{R}_+ \in \mathscr{V}(\infty)$.

Remarque IX.1. Plutôt que de travailler avec des voisinages fermés comme ici, il est possible (et courant) de considérer des voisinages ouverts (du type $]a-\delta, a+\delta[$) sans impact profond sur ce qui suit.

Proposition IX.1. Soit $a \in \overline{\mathbb{R}}$. Alors :

(i) l'intersection de deux voisinages de a est un voisinage de a ;

(ii)

$$\bigcap_{V \in \mathscr{V}(a)} V = \begin{cases} \{a\} & \text{si } a \in \mathbb{R} \\ \emptyset & \text{sinon} \end{cases} .$$

Démonstration.

(i) Immédiat si l'on prend le temps de faire une disjonction de cas selon les valeurs de a.

(ii) ($\supset$) Immédiat.

($\subset$) Si $a \in \mathbb{R}$, alors si $x \in \bigcap_{V \in \mathscr{V}(a)} V$, pour tout $\varepsilon > 0$, $x \in [a-\varepsilon, a+\varepsilon]$, *i.e* $|x-a| \leq \varepsilon$. On en déduit que $|x-a| \leq \inf \mathbb{R}_+^* = 0$ donc $x = a$.
Si $a = +\infty$, alors si on suppose qu'il existe $x \in \bigcap_{V \in \mathscr{V}(\infty)}$, il existe $M > x$ et donc $x \notin [M, +\infty[\in \mathscr{V}(\infty)$, ce qui est absurde. On règle de la même façon le cas où $a = -\infty$.

□

Proposition IX.2. [Séparation de $\overline{\mathbb{R}}$] Soient $a, b \in \overline{\mathbb{R}}$ **distincts**. Alors il existe $V \in \mathscr{V}(a)$ et $W \in \mathscr{V}(b)$ tels que :

$$V \cap W = \emptyset .$$

✌ **Remarque IX.2.** Cela signifie qu'étant donné deux points distincts de la droite réelle achevée, on peut leur trouver deux voisinages ne se rencontrant pas. Topologiquement, on dit que $\overline{\mathbb{R}}$ est **séparé**.

Démonstration. Si a et b sont réels avec $a < b$, en posant $\delta = \dfrac{b-a}{3}$ on vérifie aisément que les voisinages $[a-\delta, a+\delta] \in \mathscr{V}(a)$ et $[b-\delta, b+\delta] \in \mathscr{V}(b)$ sont disjoints. Si a ou b est égal à $\pm\infty$ se traite de façon similaire. □

Définition IX.2. Soit $\mathscr{P}$ un prédicat dépendant d'une variable réelle x et soit $a \in \overline{\mathbb{R}}$. On dira que $\mathscr{P}(x)$ **est vraie au voisinage de** a si :

$$\exists\, V \in \mathscr{V}(a),\ \forall x \in V,\ \mathscr{P}(x) .$$

➠ **Exemple IX.2.** $x^2 \leq 1$ est vraie au voisinage de 0 ; $x \mapsto x^2$ est décroissante au voisinage de -42.

b) Limite en un point

Définition IX.3. Soit I un intervalle de $\mathbb{R}$ d'extrémités $a, b \in \overline{\mathbb{R}}$. On appelle :
- **intérieur de** I l'ensemble
$$\mathring{I} = I \setminus \{a, b\} \subset \mathbb{R}\,;$$
- **adhérence de** I l'ensemble
$$\bar{I} = I \cup \{a, b\} \subset \overline{\mathbb{R}}\,.$$

➠ **Exemple IX.3.** $\overbrace{[0,2[}^{\circ} =]0,2[$ et $\overline{[0,\infty[} = \overline{\mathbb{R}}_+$.

On fixe dans toute la suite du chapitre un intervalle I de $\mathbb{R}$ d'intérieur non vide.

Définition IX.4. Soit $a \in \bar{I}$ et soit $\ell \in \overline{\mathbb{R}}$. On dit qu'une fonction $f : I \to \mathbb{R}$ **tend vers ℓ en a** lorsque :
$$\forall V \in \mathscr{V}(\ell),\ \exists W \in \mathscr{V}(a),\ f(W \cap I) \subset V\,.$$
La quantité ℓ est alors appelée **limite** de f en a.

Notation. Nous utiliserons indifféremment $f(x) \xrightarrow[x \to a]{} \ell$ et $\lim\limits_{x \to a} f(x) = \ell$.

✌ **Remarque IX.3.**
- Rappelons que l'assertion $f(W \cap I) \subset V$ signifie
$$\forall x \in W \cap I,\ f(x) \in V\,.$$
- Cette définition peut être traduite "en français" de la même façon que son analogue séquentiel vu dans le chapitre VII : pour tout voisinage de ℓ, si x est suffisamment proche de a, $f(x)$ appartiendra à ce voisinage.
- Si f est définie en a et admet une limite en a, alors
$$\lim_{x \to a} f(x) = f(a)\,.$$

✖ **ATTENTION :** ne pas confondre la limite en a et les limites directionnelles ("en a^+ ou a^-") sur lesquelles portera le paragraphe e).

Cette définition de limite possède l'avantage d'être universelle : peut importe que a ou ℓ soient réels, infinis ou un mélange des deux, elle restera valable. Pour aider dans nos considérations pratiques, nous listons malgré des considérations de type "dans le cambouis jusqu'au torse" ci–ensuite. Une fois de plus, remercier l'auteur est inutile.

◇ $a, \ell \in \mathbb{R}$ **:**
$$\forall \varepsilon > 0,\ \exists \delta > 0,\ \forall x \in I,\ (|x - a| \leq \delta) \Rightarrow (|f(x) - \ell| \leq \varepsilon)\,.$$

◇ **$a \in \mathbb{R}$, $\ell = +\infty$:**

$$\forall M \in \mathbb{R},\ \exists \delta > 0,\ \forall x \in I,\ (|x-a| \leq \delta) \Rightarrow (f(x) \geq M)\,.$$

◇ **$a \in \mathbb{R}$, $\ell = -\infty$:**

$$\forall m \in \mathbb{R},\ \exists \delta > 0,\ \forall x \in I,\ (|x-a| \leq \delta) \Rightarrow (f(x) \leq m)\,.$$

◇ **$a = +\infty$, $\ell \in \mathbb{R}$:**

$$\forall \varepsilon > 0,\ \exists M \in \mathbb{R},\ \forall x \in I,\ (x \geq M) \Rightarrow (|f(x) - \ell| \leq \varepsilon)\,.$$

◇ **$a = -\infty$, $\ell \in \mathbb{R}$:**

$$\forall \varepsilon > 0,\ \exists m \in \mathbb{R},\ \forall x \in I,\ (x \leq m) \Rightarrow (|f(x) - \ell| \leq \varepsilon)\,.$$

◇ **$a = +\infty, \ell = -\infty$:**

$$\forall m \in \mathbb{R},\ \exists M \in \mathbb{R},\ \forall x \in I,\ (x \geq M) \Rightarrow (f(x) \leq m)\,.$$

◇ **$a = -\infty, \ell = +\infty$:**

$$\forall M \in \mathbb{R},\ \exists m \in \mathbb{R},\ \forall x \in I,\ (x \leq m) \Rightarrow (f(x) \geq M)\,.$$

◇ **$a = \ell = +\infty$:**

$$\forall M \in \mathbb{R},\ \exists R \in \mathbb{R},\ \forall x \in I,\ (x \geq R) \Rightarrow (f(x) \geq M)\,.$$

◇ **$a = \ell = -\infty$:**

$$\forall m \in \mathbb{R},\ \exists r \in \mathbb{R},\ \forall x \in I,\ (x \leq r) \Rightarrow (f(x) \leq m)\,.$$

Youpi tralala, comme dirait l'autre.

➠ **Exemple IX.4.**

— La fonction $x \mapsto e^x$ tend vers $+\infty$ quand $x \to +\infty$ car, pour tout $M > 0$, $(x \geq \ln(M)) \Rightarrow (e^x \geq M)$. De même, on peut montrer que $x^3 \xrightarrow[x \to -1]{} -1$.

— La fonction $x \mapsto \dfrac{1}{x}$ n'a pas de limite en 0 ($\mathbb{R}^*$ n'est pas un intervalle).

Proposition IX.3. La limite d'une fonction en un point, lorsqu'elle existe, est unique.

Démonstration. Soit $f : I \to \mathbb{R}$ ayant deux limites ℓ et ℓ' en $a \in \bar{I}$. Soit $V \in \mathscr{V}(\ell)$ et $V' \in \mathscr{V}(\ell')$; alors par définition de limite il existe $W, W' \in \mathscr{V}(a)$ tels que

$$f(W \cap I) \subset V \text{ et } f(W' \cap I) \subset V'\,.$$

$W \cap W'$ est un voisinage de a intersectant I et, si $x \in W \cap W' \cap I$ alors $f(x) \in V \cap V'$. On en déduit que $V \cap V' \neq \emptyset$, ce qui entraîne par contraposée de la proposition IX.2 que $\ell = \ell'$. □

Proposition IX.4. Soit $f : I \to \mathbb{R}$ et soit $a \in \overline{\mathbb{R}}$. Si f admet une limite réelle en a, alors elle est bornée au voisinage de ce point.

Démonstration. Comme ℓ est réel, ses voisinages sont bornés, d'où le résultat par définition de limite. □

Proposition IX.5. Soit $f : I \to \mathbb{R}$ et soit $a \in \bar{I}$. Alors :

(i) $f(x) \xrightarrow[x\to a]{} 0 \iff |f(x)| \xrightarrow[x\to a]{} 0$;

(ii) si g est une fonction bornée au voisinage de a et si $f(x) \xrightarrow[x\to a]{} 0$ alors

$$f(x)g(x) \xrightarrow[x\to a]{} 0 \, .$$

Démonstration. Adapter la démonstration de propriétés similaires vues dans le chapitre VII. □

✌ **Remarque IX.4.** Quitte à "épointer" les voisinages (leur retirer le point a), nous pouvons définir une notion de limite en a pour $f : I \setminus \{a\} \to \mathbb{R}$ vérifiant toutes les propriétés vues ici. Notons toutefois que cela ne permet pas de doter $x \mapsto \dfrac{1}{x}$ (par exemple) d'une limite en 0.

c) Opérations sur les limites

Nous adaptons dans ce paragraphe les résultats démontrés sur les suites dans le chapitre VII. Nous laissons au lecteur le soin de transcrire les démonstrations *ad–hoc*.

Proposition IX.6. Soient $f, g : I \to \mathbb{R}$,$a \in \bar{I}$, $\lambda \in \mathbb{R}$, $\ell, \ell' \in \overline{\mathbb{R}}$ tels que $f(x) \xrightarrow[x\to a]{} \ell$ et $g(x) \xrightarrow[x\to a]{} \ell'$. Alors on a, sauf dans les cas d'indétermination :

(i) $f(x) + \lambda g(x) \xrightarrow[x\to a]{} \ell + \lambda\ell'$;

(ii) $f(x)g(x) \xrightarrow[x\to a]{} \ell\ell'$;

(iii) **si** $\ell \neq 0$, alors $f(x) \neq 0$ au voisinage de a et :

$$\frac{1}{f(x)} \xrightarrow[x\to a]{} \frac{1}{\ell} \quad \text{avec la convention que } \frac{1}{\pm\infty} = 0 \, .$$

Proposition IX.7 (Composition des limites)**.** Soient I, J deux intervalles d'intérieur non vide de $\mathbb{R}$, $a \in \bar{I}$, $b \in \bar{J}$, $\ell \in \overline{\mathbb{R}}$ et soient $f : I \to \mathbb{R}$ et $g : J \to \mathbb{R}$ deux fonctions telles que :
— $f(I) \subset J$;
— $f(x) \xrightarrow[x\to a]{} b$;
— $g(x) \xrightarrow[x\to b]{} \ell$.
Alors :

$$g \circ f(x) \xrightarrow[x\to a]{} \ell\,.$$

✖ **Attention :** il est impératif de bien vérifier toutes les hypothèses avant d'appliquer ce résultat.

Démonstration. Soit $V \in \mathscr{V}(\ell)$; alors il existe $W \in \mathscr{V}(b)$ tel que $g(W \cap J) \subset V$. Mais il existe $W' \in \mathscr{V}(a)$ tel que $f(W' \cap I) \subset W \cap J$ et donc :

$$g \circ f(W' \cap I) \subset g(W \cap J) \subset V$$

d'où le résultat. □

Exemple IX.5. La fonction définie sur $\mathbb{R}_+^*$ par $x \mapsto \sin\left(\frac{1}{x}\right)$ peut être vue comme la composée $g \circ f$ avec :

$$\begin{aligned} f : \mathbb{R}_+^* &\to \mathbb{R} \\ x &\mapsto \frac{1}{x} \end{aligned}$$

et

$$\begin{aligned} g : \mathbb{R} &\mapsto \mathbb{R} \\ x &\mapsto \sin(x) \end{aligned} \quad .$$

Or :
— $f(\mathbb{R}_+^*) \subset \mathbb{R}$;
— $f(x) \xrightarrow[x\to\infty]{} 0$;
— $g(x) \xrightarrow[x\to 0]{} 0$,
donc, par composition des limites :

$$\sin\left(\frac{1}{x}\right) \xrightarrow[x\to\infty]{} 0\,.$$

Proposition IX.8. Soient $f, g : I \to \mathbb{R}$ et soit $a \in \overline{I}$. On suppose que $f(x) \xrightarrow[x\to a]{} \ell$ et $g(x) \xrightarrow[x\to a]{} \ell'$, avec $\ell, \ell' \in \overline{\mathbb{R}}$. Alors :
(i) si $f \leq g$ au voisinage de a, $\ell \leq \ell'$;
(ii) si $\ell = \ell'$ et que h est une fonction définie au voisinage de a telle que $f \leq h \leq g$, alors $h(x) \xrightarrow[x\to a]{} \ell$.

Exemple IX.6. Au voisinage de $+\infty$, on a :

$$\frac{-1}{x} \leq \frac{\sin(x)}{x} \leq \frac{1}{x}$$

et donc

$$\frac{\sin(x)}{x} \xrightarrow[x\to\infty]{} 0 \ : .$$

d) Caractérisation séquentielle de la limite

La proposition suivante est une complétion et reformulation du théorème VII.9.

Proposition IX.9. Soit $f : I \to \mathbb{R}$, $a \in \bar{I}$ et $\ell \in \overline{\mathbb{R}}$. Alors :

$$f(x) \xrightarrow[x\to a]{} \ell$$
$$\Longleftrightarrow$$
pour toute suite $(x_n)_n \in I^{\mathbb{N}}$ de limite a, $f(x_n) \to \ell$.

Remarque IX.5. Cette caractérisation nous servira surtout à démontrer une absence de limite. Par exemple, sin n'admet pas de limite en $+\infty$ car si une telle limite existait elle serait égale à $\lim \sin(2n\pi) = 0$ et $\lim \sin\left(2n\pi + \frac{\pi}{2}\right) = 1$.

Démonstration. Faisons le pour a et ℓ réels.

($\Downarrow$) Soit $(x_n)_n \in I^{\mathbb{N}}$ convergeant vers a et soit $\delta > 0$; alors :

$$\exists\, N \in \mathbb{N},\ \forall n \geq N,\ |x_n - a| \leq \delta$$

i.e

$$\forall W \in \mathscr{V}(a), \exists\, N \in \mathbb{N},\ \forall n \geq N,\ x_n \in W\ .$$

Soit $\varepsilon > 0$; alors $V = [\ell - \varepsilon, \ell + \varepsilon]$ est un voisinage de ℓ et donc il existe $W \in \mathscr{V}(a)$ tel que $f(W \cap I) \subset V$. On déduit de tout ceci que :

$$\forall \varepsilon > 0, \exists\, N \in \mathbb{N},\ \forall n \geq N,\ |x_n - \ell| \leq \varepsilon$$

d'où la convergence de $(f(x_n))_n$ vers ℓ.

($\Uparrow$) Démontrons le par contraposée. Si f ne tend pas vers ℓ en a, alors il existe $V = [\ell - \varepsilon, \ell + \varepsilon] \in \mathscr{V}(\ell)$ tel que

$$\forall W \in \mathscr{V}(a),\ f(W \cap I) \not\subset V\ .$$

En particulier, cela est vrai pour les voisinages $W_n = \left[a - \frac{1}{n}, a + \frac{1}{n}\right]$ (pour $n \geq 1$), et donc il existe une suite $(x_n)_n \in I^{\mathbb{N}}$ telle que :

— $\forall n \geq 1,\ |x_n - a| \leq \frac{1}{n}$;

— $\forall n \geq 1,\ |f(x_n) - \ell| > \varepsilon$.

Donc, par encadrement $x_n \to a$ et $(f(x_n))_n$ ne converge pas vers ℓ, d'où le résultat.

□

e) Limites directionnelles, fonctions monotones

Définition IX.5. Soit $f : I \to \mathbb{R}$ et soit $a \in \bar{I}$.
- Si $a \neq \inf I$, on appelle **limite à gauche de f en a** la quantité (si elle existe)

$$\lim_{x\to a^-} f(x) = \lim_{x\to a} f_{|I\cap]-\infty,a[}(x) .$$

- Si $a \neq \sup I$, on appelle **limite à droite de f en a** la quantité (si elle existe)

$$\lim_{x\to a^+} f(x) = \lim_{x\to a} f_{|I\cap]a,+\infty[}(x) .$$

➠ **Exemple IX.7.**
- $\frac{1}{x} \xrightarrow[x\to 0^+]{} +\infty$.
- Si $n \in \mathbb{Z}$, $\lfloor x\rfloor \xrightarrow[n\to n^-]{} n-1$ et $\lfloor x\rfloor \xrightarrow[n\to n^+]{} n$.

Proposition IX.10. Soit $f : I \to \mathbb{R}$ et soit $a \in \mathring{I}$. Alors :

$$f \text{ admet une limite en } a$$
$$\Longleftrightarrow$$
$$f \text{ admet une limite à gauche et à droite en } a \text{ qui sont égales à } f(a).$$

✖ **Attention :** La condition d'égalité à $f(a)$ n'est pas superfétatoire : l'indicatrice $\mathbb{1}_{\{0\}}$ n'admet pas de limite en 0 (utiliser la caractérisation séquentielle en se rappelant que la suite nulle converge vers 0) et pourtant y admet une limite à gauche et à droite.

➠ **Exemple IX.8.** Revenir à et méditer sur

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\mapsto \begin{cases} 1 & \text{si } x \geq 0 \\ -1 & \text{sinon} \end{cases} . \end{aligned}$$

✍ **Exercice IX.1.** En quels points de $\mathbb{R}_+$ la fonction $x \mapsto \lfloor\sqrt{x}\rfloor$ admet–elle une limite ?

Théorème IX.11 (Limite monotone)**.**
Soit $f : I \to \mathbb{R}$ une fonction croissante et soit $a \in \bar{I}$. Alors :

(i) si $a \in \mathring{I}$ alors les limites directionnelles de f en a existent, avec les égalités

$$\lim_{x \to a^+} f(x) = \inf\{f(x) \mid x > a\} \in \mathbb{R}$$

et

$$\lim_{x \to a^-} f(x) = \sup\{f(x) \mid x < a\} \in \mathbb{R}\,,$$

avec de plus

$$\lim_{x \to a^-} f(x) \leq f(a) \leq \lim_{x \to a^+} f(x)\,;$$

(ii) si $a = \sup(I)$, et $a \in I$, alors f admet une limite à gauche en a donnée par

$$\lim_{x \to a^-} f(x) = \sup\{f(x) \mid x < a\} \in \mathbb{R}\,,$$

avec de plus

$$\lim_{x \to a^-} f(x) \leq f(a)\,;$$

(iii) si $a = \sup(I)$, et $a \notin I$, alors f admet une limite à gauche en a donnée par

$$\lim_{x \to a^-} f(x) = \sup\{f(x) \mid x < a\}\,,$$

cette borne supérieure étant prise dans $\overline{\mathbb{R}}$.

✌ **Remarque IX.6.** Ce résultat peut évidemment être adapté dans le cas décroissant.

Démonstration. Démontrons le point (i) ; pour ce faire, remarquons que l'ensemble

$$\mathscr{E} = \sup\{f(x) \mid x < a\}$$

est une partie de $\mathbb{R}$ non vide et majorée par $f(a)$; elle admet donc une borne supérieure $M \leq f(a)$. De plus, pour tout $\varepsilon > 0$, $M - \varepsilon$ ne majore pas $\mathscr{E}$ et donc il existe $x_0 < a$ tel que $f(x_0) > M - \varepsilon$, $i.e$ $|M - f(x_0)| \leq \varepsilon$.

Si $x_1 \in]x_0, a[$, alors $f(x_1) \geq f(x_0) \geq M - \varepsilon$; ce qui signifie que :

$$f(]x_0, a[) \subset [f(a) - \varepsilon, f(a) + \varepsilon]\,.$$

On termine en remarquant que $]x_0, a[$ est l'intersection d'un voisinage de a avec $]-\infty, a[$, ce qui permet de conclure quant à la limite, et en raisonnant de façon similaire pour obtenir la seconde inégalité. □

2.⁻ Fonctions continues

a) C'est quoi ?

Définition IX.6. Une fonction $f : I \to \mathbb{R}$ est dite **continue** en un point $a \in I$ si elle admet une limite finie en a. Si cela est vrai en tout point de I, on dira que f est continue sur I.

Notation. L'ensemble des fonctions continues sur I sera noté $\mathscr{C}^0(I,\mathbb{R})$ ou simplement $\mathscr{C}^0(I)$.

➠ **Exemple IX.9.** La fonction $f : x \mapsto \sqrt{x}$ est continue sur $\mathbb{R}_+$.

Vocabulaire. Si la limite à gauche (resp. à droite) de f en a existe, on dira que f est **continue à gauche** (resp. **à droite**) en a.

➠ **Exemple IX.10.** La fonction partie entière est continue à droite sur $\mathbb{R}_+$.

Proposition IX.12. Soit $f : I \to \mathbb{R}$ et soit $a \in I$. Alors :

$$f \text{ est continue en } a$$
$$\Longleftrightarrow$$
$$f(x) \xrightarrow[x\to a]{} f(a)\ .$$

Démonstration. ($\Uparrow$) Trivial.

($\Downarrow$) Supposons que f soit continue en a, *i.e* qu'il existe $\ell \in \mathbb{R}$ tel que $f(x) \xrightarrow[x\to a]{} \ell$.

Cela signifie que :

$$\forall V \in \mathscr{V}(\ell),\ \exists W \in \mathscr{V}(a),\ f(W \cap I) \subset V\ .$$

Or, pour tout $W \in \mathscr{V}(a)$, $a \in W \cap I$ ce qui entraîne que :

$$f(a) \in \bigcap_{V \in \mathscr{V}(\ell)} V = \{\ell\}$$

d'où le résultat.

□

➠ **Exemple IX.11.**

— Toutes les fonctions usuelles (*cf.* chapitre II) sont continues sur leurs ensembles de définition respectifs.

— La fonction suivante n'est pas continue en 0 :

$$f : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \mapsto \begin{cases} 1 & \text{si } x \geq 0 \\ -1 & \text{sinon} \end{cases}\ .$$

En effet, si elle admettait une limite finie en 0, celle–ci devrait être égale à 1 et -1 à la fois, ce qui est, vous en conviendrez, compliqué.

— La fonction valeur absolue est continue sur $\mathbb{R}$, mais pas la fonction partie entière.

Les propriétés relatives aux opérations sur les limites se traduisent par les résultats suivants, relatifs aux opérations présentées dans le chapitre II.

Proposition IX.13. $(\mathscr{C}^0(I), +, \times)$ est un anneau commutatif, de neutres $x \mapsto 0$ et $x \mapsto 1$. De plus, pour tous $\lambda \in \mathbb{R}$ et $f \in \mathscr{C}^0(I)$, $\lambda f \in \mathscr{C}^0(I)$ et l'inverse de toute fonction continue **ne s'annulant pas** est une fonction continue.

✖ **ATTENTION :** l'anneau $\mathscr{C}^0(I)$ n'est pas intègre.

Proposition IX.14. La composée de deux fonctions continues compatibles est continue.

Démonstration. Cela découle de la composition des limites. □

b) Prolongement par continuité

La question que nous nous posons dans ce paragraphe est la suivante : étant donné une fonction continue sur une intervalle "à trou", est–il possible de la prolonger de façon continue sur l'intervalle entier ?

Définition IX.7. Soit $a \in I$ et soit $f : I \setminus \{a\} \to \mathbb{R}$ une fonction continue. On dit que f est **prolongeable par continuité** en a si il existe $g \in \mathscr{C}(I)$ telle que

$$g_{|I\setminus\{a\}} = f\ .$$

➠ **Exemple IX.12.** La fonction ln n'est pas prolongeable par continuité en 0.

Proposition IX.15. Soit $a \in I$ et soit $f : I \setminus \{a\} \to \mathbb{R}$ une fonction continue. Alors :

$$f \text{ est prolongeable par continuité en } a \iff f \text{ admet une limite réelle en } a.$$

✌ **Remarque IX.7.** Ceci est donc équivalent à l'existence et égalité des limites à droite et à gauche en a **LORSQUE** $a \in \mathring{I}$.

Démonstration.

($\Uparrow$) Immédiat via :

$$g : x \mapsto \begin{cases} f(x) & \text{si } x \in I \\ \lim\limits_{x\to a} f(x) & \text{si } x = a \end{cases}.$$

($\Downarrow$) Si il existe un prolongement par continuité g de f en a, alors $g(x) \xrightarrow[x\to a]{} g(a)$ et donc, comme $g_{|I\setminus\{a\}} = f$ alors $f(x) \xrightarrow[x\to a]{} g(a)$.

□

➠ **Exemple IX.13.** La fonction définie sur $\mathbb{R}_+^*$ par $x \mapsto e^{-\frac{1}{x}}$ se prolonge par continuité en 0 par 0. Attention, elle n'est pas prolongeable par continuité sur $\mathbb{R}$ car

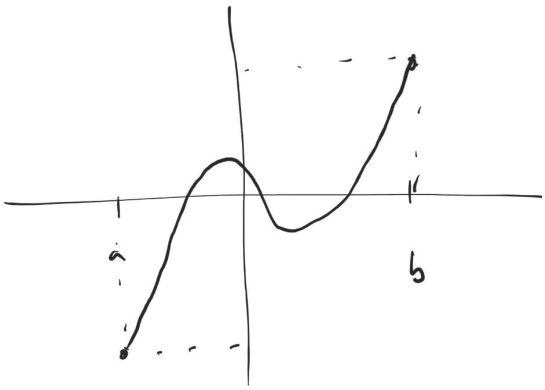
$$\lim_{x\to 0^-} e^{-\frac{1}{x}} = +\infty\ .$$

c) Images d'intervalles

Théorème IX.16 (Théorème des valeurs intermédiaires)**.**
Soit $f \in \mathscr{C}^0([a,b])$ telle que $f(a)f(b) < 0$. Alors :

$$\exists\, c \in]a,b[,\ f(c) = 0 .$$

Remarque IX.8.
- La condition $f(a)f(b) < 0$ impose que $f(a)$ et $f(b)$ soient de signes opposés.
- Il n'y a pas nécessairement unicité du point d'annulation c.



- Notons cependant que si l'on rajoute la condition que f soit strictement monotone, le point c est unique.

Démonstration. On peut définir par récurrence trois suites $(a_n)_n$, $(b_n)_n$ et $(c_n)_n$ selon le procédé suivant : posons $a_0 = a$, $b_0 = b$ et $c_0 = \frac{a+b}{c}$, puis, pour tout $n \geq 0$
- si $f(a_n)f(c_n) < 0$, on pose $a_{n+1} = a_n$ et $b_{n+1} = c_n$;
- dans le cas contraire, on pose $a_{n+1}c_n$ et $b_{n+1} = b_n$.

Enfin, dans tous les cas, on pose :

$$c_{n+1} = \frac{a_{n+1} + b_{n+1}}{2} .$$

On remarque alors que les suites $(a_n)_n$ et $(b_n)_n$ sont respectivement croissantes et décroissantes. De plus, si $n \geq 1$ on a :

$$\begin{aligned} 0 \leq b_n - a_n &= \frac{1}{2}(b_{n-1} - a_{n-1}) \\ &\vdots \\ &= \frac{1}{2^n}(b-a) \end{aligned}$$

et donc, par théorème VII.11, $b_n - a_n \to 0$. Les deux suites $(b_n)_n$ et $(a_n)_n$ étant adjacentes, elles convergent vers une même limite $c \in]a,b[$. De plus, comme pour tout $n \geq 0$, $f(a_n)f(b_n) < 0$ on obtient par passage à la limite que $f(c)^2 \leq 0$ ce qui implique $f(c) = 0$, d'où le résultat.

□

Remarque IX.9. Dans la démonstration *supra*, on resserre donc petit à petit une "fenêtre" autour du point d'annulation de f, ce que l'on peut implémenter en `python` via le code suivant (on parle de **recherche de zéro par dichotomie**) étant donné que la suite $(c_n)_n$ converge par encadrement vers c.

```
def dicho(f,a,b,p):
    if f(a)*f(b) > 0:
        raise ValueError("f ne s'annule pas")
    while b-a>10**(-p):
        c=(a+b)/2
        if f(c) == 0:
            return c
        if f(a)*f(c)<0:
            b=c
        else:
            a=c
    return c
```

Exercice IX.2. Démontrer que toute fonction continue de $[0,1]$ dans lui même admet un point fixe, *i.e* un $x \in [0,1]$ tel que $f(x) = x$.

➥ **Correction :** *Si* $f(0) = 0$ *ou* $f(1) = 1$, *c'est terminé. Sinon, posons* $g : x \mapsto x - f(x)$ *; alors* $g(0) = -f(0) < 0$ *et* $g(1) = 1 - f(1) > 0$ *; par TVI, il existe* $x \in]0,1[$ *tel que* $g(x) = 0$, *i.e* $f(x) = x$.

Corollaire IX.16.a. Soit $f \in \mathscr{C}^0([a,b])$; posons $\alpha = f(a)$ et $\beta = f(b)$. Alors :

$$\forall \gamma \in [\alpha, \beta] \text{ (ou } [\beta, \alpha]), \exists\, c \in [a,b],\ f(c) = \gamma\,.$$

Démonstration. Appliquer le théorème IX.16 à $x \mapsto f(x) - \gamma$. □

Corollaire IX.16.b. Soit $f \in \mathscr{C}^0([a,b])$ **strictement monotone** ; posons $\alpha = f(a)$ et $\beta = f(b)$. Alors :

$$\forall \gamma \in [\alpha, \beta] \text{ (ou } [\beta, \alpha]), \exists!\, c \in [a,b],\ f(c) = \gamma\,.$$

Démonstration. La stricte monotonie entraîne l'injectivité de f et donc l'unicité de γ. □

Corollaire IX.16.c. L'image d'un intervalle par une fonction continue est un intervalle.

Démonstration. Se rappeler que les intervalles de $\mathbb{R}$ sont exactement les convexes et utiliser le corollaire précédent. □

Corollaire IX.16.d (Théorème des bornes atteintes)**.** Soit $f \in \mathscr{C}^0([a,b])$. Alors :

(i) f admet un maximum M et un minimum m atteints sur $[a,b]$;

(ii) $f([a,b]) = [m, M]$.

En particulier, **l'image d'un segment par une fonction continue est un segment.**

Démonstration. Commençons par poser $M = \sup f([a,b])$ (pourquoi existe–t–il ?). Alors, par caractérisation séquentielle, il existe une suite $(x_n)_n$ de points de $[a,b]$ telle que $f(x_n) \to M$. De plus, la suite $(x_n)_n$ est bornée, donc il existe par théorème de Bolzano–Weierstrass (théorème VII.17) une suite extraite $(x_{\varphi}(n))_n$ de cette dernière convergeant vers $c \in [a,b]$. Par continuité de f et unicité de la limite, on obtient que $M = f(c)$. Un raisonnement similaire nous donne l'existence de $m = \min f([a,b])$ et nous pouvons alors conclure par le théorème IX.16. □

➠ **Exemple IX.14.** Le TVI nous permet de démontrer que le cosinus est surjectif sur $[-1, 1]$.

d) Continuité et (stricte) monotonie

Proposition IX.17. Toute fonction continue sur un intervalle, à valeurs réelles et injective est strictement monotone.

Démonstration. En exercice : raisonner par contraposée via le TVI (théorème IX.16). □

Théorème IX.18 (Théorème de la bijection)**.**
Soit I un intervalle de $\mathbb{R}$ et soit $f : I \to \mathbb{R}$ une application continue strictement monotone. Alors :

(i) f réalise une bijection de I vers $J = f(I)$;

(ii) J est un intervalle du même type que I (*i.e* ouvert et fermé le même nombre de fois) ;

(iii) $f^{-1} : J \to I$ est de même monotonie que f.

Démonstration. Ce résultat est admis. □

✌ **Remarque IX.10.** Nous avons vu de nombreuses applications de ces résultats dans le chapitre II.

3.– Brêve extension aux fonctions à valeurs complexes

Une fois n'est pas coutume, tous les résultats de ce chapitre ne faisant pas intervenir d'inégalité se généralisent aux fonctions $f : I \to \mathbb{C}$ lorsque I est un intervalle de $\mathbb{R}$ (on ne parlera pas ici de fonction de variables complexes). En particulier, notons que le TVI ne se généralise pas. On peut par contre passer à la limite dans les parties réelle et imaginaire et caractériser la continuité d'une fonction à valeurs complexes par celle de celles-ci.

➠ **Exemple IX.15.** $e^{i\theta} \underset{\theta \to 0}{\longrightarrow} 1$.

Chapitre X

Entiers relatifs, arithmétique

1.– Divisibilité

On rappelle que $(\mathbb{Z}, +, \times)$ est un anneau commutatif intègre sur lequel l'ordre naturel "$\leq$" est total.

a) Diviseurs, multiples

Définition X.1. Soient $a, b \in \mathbb{Z}$. On dit que a **divise** b si il existe $c \in \mathbb{Z}$ tel que $b = ac$. On dit alors que b est un **multiple** de a.

Notation. On notera $a|b$ si a divise b et on pose $a\mathbb{Z} = \{ak \,|\, k \in \mathbb{Z}\}$ l'ensemble des multiples de a.

✌ **Remarque X.1.**
- Si a divise b et que a et b ne sont pas tous les deux nuls, l'entier relatif c tel que $b = ac$ est unique par intégrité ; on l'appelle **quotient** de b par a et on le note, **si** $a \neq 0$, $\frac{b}{a}$. Cette notation est à utiliser avec parcimonie et à réserver au cas où $a|b$.
- On vérifie aisément que $a|b \iff b\mathbb{Z} \subset a\mathbb{Z}$.
- Pour tout $a \in \mathbb{Z}$, $0 = a \times 0$ et donc $a|0$: **tout le monde divise zéro**. À l'inverse, 0 ne divise que lui–même.

Proposition X.1. La relation "divise" est réflexive et transitive. De plus, si $a, b \in \mathbb{Z}$ alors :

$$(a|b) \wedge (b|a) \Leftrightarrow a = \pm b\ .$$

✌ **Remarque X.2.** Ceci implique que $a\mathbb{Z} = b\mathbb{Z} \Leftrightarrow a = \pm b$.

Démonstration. La réflexivité et la transitivité sont immédiates (*cf.* chapitre V). Il ensuite clair que si $a = \pm b$, alors $a = (\pm 1) \times b$ et donc $a|b$ et $b|a$. Réciproquement, si a et b se divisent mutuellement, il existe c et d dans $\mathbb{Z}$ tels que $b = ac$ et $a = bd$. On a alors $b = bdc$, ce qui entraîne par intégrité que $dc = 1$ et donc $d = c = \pm 1$. □

b) Division euclidienne

Théorème X.2.
Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$. Alors :

$$\exists!\,(q,r) \in \mathbb{Z}^2,\ \begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}.$$

Vocabulaire. a est appelé **dividende**, b **diviseur**, q **quotient** et r **reste** de la division euclidienne.

Démonstration. Il suffit pour l'existence de remarquer que par corollaire de la propriété d'Archimède (proposition **??**) il existe $u \in \mathbb{Z}$ tel que :

$$|b|u \leq a < |b|(u+1)$$

puis de poser $q = |u|$ et $r = a - |b|u$.

Pour l'unicité, si on suppose qu'il existe deux tels couples (q, r) et (q', r') alors $b(q - q') = r' - r$ et donc $b | r' - r$. Or $r, r' \in [\![0, |b|[\![$, *ergo* $r' - r \in]\!] - |b|, |b|[\![$, ce qui entraîne que $r' - r = 0$. Par conséquent, $q - q' = 0$, d'où le résultat. □

➠ **Exemple X.1.** $15 = 7 \times 2 + 1$ est une division euclidienne, mais pas $15 = 7 \times 3 - 6$.

Proposition X.3. [Sous–groupes de $\mathbb{Z}$] Soit G un sous–groupe de $(\mathbb{Z}, +)$. Alors il existe un unique $n \in \mathbb{N}$ tel que $G = n\mathbb{Z}$.

Démonstration.

Existence : Considérons l'ensemble $\mathscr{E} = G \cap \mathbb{N}^*$. S'il est vide, alors $G = \{0\} = 0\mathbb{Z}$; dans le cas contraire, il admet par axiome D un plus petit élement n_0. Un sous–groupe étant stable par puissances (ici multiples), on a alors $n_0\mathbb{Z} \subset G$.

Pour montrer l'inclusion réciproque, prenons $a \in G$ et effectuons sa division euclidienne par n_0 (qui est non nul) : par le théorème X.2, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que :

$$\begin{cases} a = n_0 q + r \\ 0 \leq r < |n_0| = n_0 \end{cases}.$$

Le reste vérifie $r = a - n_0 q$ et donc appartient à G comme différence de deux éléments du sous–groupe. Il ne peut donc pas être dans $\mathscr{E}$ et strictement inférieur à n_0, *ergo* $r = 0$ d'où $a \in n_0\mathbb{Z}$.

Unicité : S'il existe deux tels entiers naturels n, n' alors $G = n\mathbb{Z} = n'\mathbb{Z}$ et donc $n = n'$ car $n, n' \geq 0$.

□

2.⁻ PGCD, algorithme d'Euclide

a) Plus Grand Commun Diviseur

Proposition/définition X.2. Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$. On appelle **plus grand commun diviseur** (PGCD) de a et b la quantité :

$$\max\{\delta \in \mathbb{N}^* \mid (\delta|a) \wedge (\delta|b)\} .$$

Notation. $\operatorname{pgcd}(a, b)$, $a \wedge b$.

Démonstration. L'ensemble $\mathscr{E} = \{\delta \in \mathbb{N}^* \mid (\delta|a) \wedge (\delta|b)\}$ est une partie de $\mathbb{N}$ non vide (elle contient 1) et majorée (brutalement) par $\max(|a|, |b|)$ donc le PGCD est bien défini. □

✌ **Remarque X.3.** On a alors naturellement, pour $a, b \in \mathbb{Z}$, l'égalité $a \wedge b = |a| \wedge |b|$.

➠ **Exemple X.2.**
- $2 \wedge 3 = 1$;
- $2 \wedge (-3) = 1$;
- $(-2) \wedge (-4) = 2$.

✖ **Attention :** le PGCD sera toujours, selon notre définition, un **entier naturel non nul**. D'autres conventions existent dans la littérature ; nous invitons le lecteur à faire preuve de vigilance.

✌ **Remarque X.4.** Si $a, b \in \mathbb{Z}$ et $k \in \mathbb{N}^*$, on vérifie aisément que $(ka) \wedge (kb) = k(a \wedge b)$.

b) Détermination pratique du PGCD

Pour des raisons d'efficacité heuristique, nous utiliserons dans ce paragraphe la notation, pour $a \in \mathbb{Z}$:

$$\mathscr{D}(a) = \{k \in \mathbb{Z} \mid k|a\}$$

pour l'ensemble des diviseurs de a. Cet ensemble vérifie clairement que $\mathscr{D}(a) = \mathscr{D}(|a|)$ et, par définition :

$$a \wedge b = \max(\mathscr{D}(a) \cap \mathscr{D}(b)) .$$

Remarquons que si $a, b \in \mathbb{Z}$ sont tels que $b \neq 0$ ont pour division euclidienne

$$a = bq + r$$

avec q, r vérifiant les conditions du théorème X.2, alors on peut vérifier rapidement (il s'agit d'un bon exercice pour le lecteur avisé) que :

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(b) \cap \mathscr{D}(r)$$

i.e pour tout $k \in \mathbb{Z}$:

$$(k|a) \wedge (k|b) \Leftrightarrow (k|b) \wedge (k|r) .$$

En particulier, cela implique que $a \wedge b = b \wedge r$.

Proposition X.4. Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$ et soit $\delta \in \mathbb{N}^*$. Alors :

$$\delta = a \wedge b$$

$$\iff$$

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(\delta) .$$

✌ **Remarque X.5.** Remarquons que cet énoncé est équivalent au suivant, qui est une caractérisation, très utile en pratique, du PGCD :

$$\delta = a \wedge b$$

$$\iff$$

$$\begin{cases} (\delta|a) \wedge (\delta|b) \\ \forall d \in \mathbb{Z},\ (d|a) \wedge (d|b) \Rightarrow (d|\delta) \end{cases} .$$

Cela signifie que le PGCD est en fait le "maximum", au sens de la relation "|" (qui n'est pas un ordre) des diviseurs communs à a et b.

Démonstration.

($\Leftarrow$) Si d est un diviseur strictement positif de a et b alors $d|\delta$ et donc $d|\delta$. Comme δ divise a et b, on a bien $\delta = \max(\mathscr{D}(a) \cap \mathscr{D}(b)) \cap \mathbb{N}^* = a \wedge b$.

($\Rightarrow$) Démontrons par récurrence forte sur $|b| \in \mathbb{N}^*$ que $\mathscr{D}(a \wedge b) = \mathscr{D}(a) \cap \mathscr{D}(b)$.

— Si $|b| = 1$, alors

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a) \cap \mathscr{D}(1) = \mathscr{D}(a) = \mathscr{D}(a \wedge 1) .$$

— Si la propriété est vraie pour tout $k \leq |b| - 1$, alors, en posant $a = bq + r$ la division euclidienne de a par b, on a :

$$\begin{aligned} \mathscr{D}(a) \cap \mathscr{D}(b) &= \mathscr{D}(b) \cap \mathscr{D}(r) \\ &= \mathscr{D}(b \wedge r) \text{ par hypohtèse de récurrence} \\ &= \mathscr{D}(a \wedge b) \end{aligned}$$

d'où le résultat.

□

◇ Algorithme d'Euclide

Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$; pour déterminer le PGCD de a et b on définit une suite récurrente $(r_n)_n$ selon le procédé suivant :

— $r_0 = |a|$;

— $r_1 = |b|$;

— pour $n \geq 0$, r_{n+2} sera le reste de la division euclidienne de r_n par r_{n+1} si ce dernier est non nul ; dans le cas contraire on pose $r_{n+2} = 0$.

Proposition X.5. La suite $(r_n)_n$ est décroissante et stationnaire à 0.

Démonstration. La décroissance est claire. Pour le côté stationnaire, commençons par remarquer que si il existe $N \geq 0$ tel que $r_N = 0$ alors $\forall n \geq N$, $r_n = 0$ par construction ; il nous suffit donc de démontrer l'existence d'un tel rang N.

Procédons par l'absurde en supposant que la suite $(r_n)_n$ ne s'annule jamais ; alors on a pour tout $n \geq 0$, $r_n < r_{n+1}$ par division euclidienne ; nous sommes donc en présence d'une suite décroissante d'entiers naturels ; d'après la proposition **??** cette dernière est stationnaire égale à $c \in \mathbb{N}$. Or, si $r_n = r_{n+1} = c \neq 0$ pour $n \geq 0$, $r_{n+2} = 0$, ce qui contredit notre hypothèse. □

Proposition X.6 (Euclide)**.** Posons :

$$N_0 = \min\{N \in \mathbb{N}^* \,|\, r_N = 0\} \ .$$

Alors :

$$a \wedge b = r_{N_0-1} \ .$$

Démonstration. Le minimum de l'énoncé existe par axiome D. D'après nos travaux préliminaires :

$$\begin{aligned}
\mathscr{D}(a) \cap \mathscr{D}(b) &= \mathscr{D}(r_0) \cap \mathscr{D}(r_1) \\
&= \mathscr{D}(r_1) \cap \mathscr{D}(r_2) \\
&\ \vdots \\
&= \mathscr{D}(r_{N_0-1}) \cap \underbrace{\mathscr{D}(0)}_{=\mathbb{Z}} \\
&= \mathscr{D}(r_{N_0-1})
\end{aligned}$$

et donc $r_{N_0-1} = a \wedge b$. □

Cet algorithme peut se retranscrire sans trop de difficulté en langage `python`.

```
def euclide(a,b):
    s=a
    t=b
    while t!=0:
        s,t=t,s%t
    return s
```

➠ **Exemple X.3.** Pour 137 et 12, on passe par les étapes suivantes :
— $137 = 12 \times 11 + 5$;
— $12 = 5 \times 2 + 2$;
— $5 = 2 \times 2 + 1$;
— $2 = 1 \times 2 + 0$.
Ainsi $137 \wedge 12 = 1$.

c) Relation de Bézout

Proposition X.7. Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$. Alors :

$$\exists\, u, v \in \mathbb{Z},\ au + bv = a \wedge b\,.$$

✖ **Attention :** : cette proposition n'est pas une équivalence : 4 n'est pas le PGCD de 2 et 3 et pourtant $2 \times 2 + 3 \times 0 = 4$.

Démonstration. Comme $a \wedge b = |a| \wedge |b|$, on peut supposer $a, b \in \mathbb{N}$ sans perte de généralité. La démonstration de ce résultat repose sur l'**algorithme d'Euclide étendu**. Conservons la suite $(r_n)_n$ définie au paragraphe précédent et posons :

— $u_0 = 1$, $u_1 = 0$;

— $v_0 = 0$, $v_1 = 1$.

Démontrons par récurrence double sur $n \in \mathbb{N}$ que :

$$\forall n \in \mathbb{N},\ \exists\, u_n, v_n \in \mathbb{Z},\ au_n + bv_n = r_n\ .$$

— Pour $n = 0, 1$ c'est immédiat.

— Supposons la propriété vérifiée aux rangs n et $n+1$ pour un certain $n \geq 0$. Alors, par définition de la suite $(r_n)_n$ il existe $q \in \mathbb{Z}$ tel que (notons que r_{n+1} peut être nul) :

$$r_n = r_{n+1}q + r_{n+2}$$

et donc :

$$\begin{aligned} r_{n+2} &= r_n - r_{n+1}q \\ &= au_n + b_n - q(au_{n+1} + bv_{n+1}) \text{ par hypothèse de récurrence} \\ &= a(u_n - qu_{n+1}) + b(v_n - qv_{n+1})\ . \end{aligned}$$

Ne reste qu'à poser $u_{n+2} = u_n - qu_{n+1}$ et $v_{n+2} = v_n - qv_{n+1}$.

On conclut la démonstration en appliquant ce résultat à

$$n = \min\{N \in \mathbb{N} \,|\, r_N = 0\} - 1\ .$$

□

➠ **Exemple X.4.** Pour 33 et 21, l'algorithme d'Euclide livre les étapes suivantes :

— $33 = 21 \times 1 + 12$;

— $21 = 12 \times 1 + 9$;

— $12 = 9 \times 1 + 3$;

— $9 = 3 \times 3 + 0$.

En "remontant" ces opérations, on obtient :

$$\begin{aligned} 33 \wedge 21 = 3 &= 12 - 9 \times 1 \\ &= (33 - 21) - (21 - 12) \\ &= (33 - 21) - (21 - (33 - 21)) \\ &= 33 \times 2 + (-3) \times 21\ . \end{aligned}$$

d) Plus Petit Commun Multiple

Proposition/définition X.3. Soient $a, b \in \mathbb{Z} \setminus \{0\}$; on appelle **plus petit commun multiple** (PPCM) de a et b la quantité :

$$\min((a\mathbb{Z} \cap b\mathbb{Z}) \cap \mathbb{N}^*) .$$

Démonstration. Le minimum existe par axiome D. □

Notation. $\text{ppcm}(a, b), a \vee b$.

✌ **Remarque X.6.** Tout comme pour le PGCD, on dispose d'une caractérisation du PPCM ; si $\mu \in \mathbb{N}$ alors :

$$\mu = a \vee b$$
$$\Longleftrightarrow$$
$$\begin{cases} \mu \in a\mathbb{Z} \cap b\mathbb{Z} \\ \forall m \in \mathbb{Z},\ (m \in a\mathbb{Z} \cap b\mathbb{Z}) \Rightarrow (m \in \mu\mathbb{Z}) \end{cases}$$
$$\Longleftrightarrow$$
$$\begin{cases} \mu \geq 0 \\ \mu\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z} \end{cases} .$$

Proposition X.8. Soient $a, b \in \mathbb{Z}$. Alors :

$$|ab| = (a \vee b)(a \wedge b) .$$

Nous démontrerons ce résultat ultérieurement ; nous le mentionnons cependant à ce stade du cours pour la raison qu'il s'agit de la meilleure façon de déterminer un PPCM en pratique.

✍ **Exercice X.1.** Soient $a, b \in \mathbb{Z}$ tel que $b \neq 0$. Démontrer que :

$$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z} .$$

3.⁻ Entiers premiers entre eux

a) C'est quoi ?

Définition X.4. On dit que deux entiers entiers a et b sont **premiers entre eux** si $a \wedge b = 1$.

➠ **Exemple X.5.** 3 et 7 sont premiers entre eux.

Proposition X.9. Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$; alors $\dfrac{a}{a \wedge b}$ et $\dfrac{b}{a \wedge b}$ sont premiers entre eux.

Démonstration. Immédiat via la caractérisation du PGCD. □

b) Théorème de Bézout

Le théorème qui suit est du à Claude–Gaspard Bachet de Méziriac (français, 1581—1638). Étienne Bézout (français, 1730—1783) a généralisé cet énoncé à des structures plus générales, notamment les anneaux de polynômes (*cf.* chapitre XIV).

Théorème X.10 (Bézout)**.**
Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$. Alors :

$$a \text{ et } b \text{ sont premiers entre eux}$$

$$\Longleftrightarrow$$

$$\exists\, u, v \in \mathbb{Z},\ au + bv = 1\ .$$

Démonstration. ($\Downarrow$) Il s'agit d'un cas particulier de la proposition X.7.

($\Uparrow$) Soit $d \in \mathscr{D}(a) \cap \mathscr{D}(b)$. Alors, comme il existe $u, v \in \mathbb{Z}$ tel que $au + bv = 1$ on a $d|1$. On en déduit que $a \wedge b = 1$.

□

Corollaire X.10.a. Soient $a, b, c \in \mathbb{Z}$ tels que $a \wedge c = b \wedge c = 1$. Alors $ab \wedge c = 1$.

Démonstration. Par théorème de Bézout (X.10), il existe $u, v, s, t \in \mathbb{Z}$ tels que

$$1 = au + cv = bs + ct\,.$$

Ainsi :

$$\begin{aligned} 1 &= au \times 1 + cv \\ &= au(bs + ct) + cv \\ &= abus + c(aut + v) \end{aligned}$$

d'où le résultat, toujours par théorème de Bézout. □

c) Lemme de Gauss

Le résultat qui suit est une généralisation, nommée en l'honneur de Johann Carl Friedrich Gauss (allemand, 1777—1855) d'un lemme apparaissant dans le livre VII des *Éléments* d'Euclide. Par ailleurs, cet énoncé apparaît sous sa forme moderne dans un traité de Jean Prestet (mathématicien et prêtre français, 1648—1690).

Théorème X.11 (Lemme de Gauss)**.**
Soient $a, b, c \in \mathbb{Z}$ tels que :
— a et b sont premiers entre eux ;
— $a|bc$.
Alors $a|c$.

Démonstration. D'après le théorème de Bézout (X.10), il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. De plus, comme $a|bc$, il existe $w \in \mathbb{Z}$ tel que $bc = aw$. Alors :

$$\begin{aligned} c &= c \times 1 \\ &= uac + bvc \\ &= uav + awv \end{aligned}$$

d'où le résultat. □

Corollaire X.11.a. Si a et b sont deux entiers premiers entre eux, alors $a \vee b = |ab|$.

Démonstration. Soit $m \in a\mathbb{Z} \cap b\mathbb{Z}$; alors il existe $g, h \in \mathbb{Z}$ tel que $m = ah = bg$ et donc $b|ah$ ce qui entraîne par lemme de Gauss que $b|h$ et donc $ab|m$. □

Ce corollaire nous permet de démontrer la proposition X.8 ; en effet, on a alors (avec les hypothèse de l'énoncé de cette proposition) :

$$\frac{a}{a \wedge b} \vee \frac{b}{a \wedge b} = \frac{a \vee b}{a \wedge b} = |ab|$$

car $\dfrac{a}{a \wedge b}$ et $\dfrac{b}{a \wedge b}$ sont premiers entre eux.*In fine*, on a bien :

$$(a \wedge b)(a \vee b) = |ab| \, .$$

Corollaire X.11.b. Soient $a, b, n \in \mathbb{Z}$ tels que $a \wedge b = 1$. Alors :

$$(a|n) \wedge (b|n) \Rightarrow (ab|n) \, .$$

Démonstration. Comme $a \wedge b = 1$, $a \vee b = |ab|$, d'où le résultat. □

⋄ Application : équations diophantiennes

Considérons dans ce paragraphe une équation de la forme suivante, pour $a, b, c \in \mathbb{Z}$ fixés tels que $ab \neq 0$ et d'inconnues $x, y \in \mathbb{Z}$:

$$ax + by = c \, . \qquad \text{(}\mathbf{E}\text{ :X.1)}$$

Commençons par poser $\delta = a \wedge b$ et par remarquer que si $\delta \not| c$, alors l'équation ne possède aucune solution. Dans le cas contraire, celle–ci est équivalente à la forme réduite suivante :

$$a'x + b'x = c' \qquad \text{(}\mathbf{E}\text{ :X.2)}$$

avec $a' = \dfrac{a}{\delta}$, $b' = \dfrac{b}{\delta}$ et $c' = \dfrac{c}{\delta}$.

Les entiers a' et b' étant premiers entre eux, l'algorithme d'Euclide étendu nous permet de trouver $u, v \in \mathbb{Z}$ tels que $a'u + b'v = 1$; une solution particulière de (**E** :X.2) est alors le couple

$$(x_0, y_0) = (uc, vc)$$

et

Supposons que nous disposions d'une autre solution $(x, y) \in \mathbb{Z}^2$ de (**E** :X.2) ; on obtient alors par soustraction des égalités $a'x + b'y = c'$ et $a'x_0 + b'y_0 = c'$ que :

$$a'(x - x_0) = b'(y_0 - y)$$

ce qui implique que $a'|b'(y_0 - y)$. Or, $a' \wedge b' = 1$ donc, par lemme de Gauss :

$$a'|y_0 - y$$

et donc il existe $k \in \mathbb{Z}$ tel que :

$$y = y_0 - ka' \ .$$

Revenant à l'égalité précédente on a désormais :

$$a'(x - x_0) = ka'b'$$

et donc, par intégrité :

$$x = x_0 + kb' \ .$$

En conclusion les solutions de (**E** :X.2) sont les éléments de l'ensemble :

$$\mathscr{S}_{\text{red}} = \{(x_0 + kb', y_0 - ka') \mid k \in \mathbb{Z}\}$$

et donc les solutions de (**E** :X.1) parcourent cet ensemble, les deux équations étant équivalentes.

➠ **Exemple X.6.** L'équation $12x + 4y = 8$ est équivalente à $3x + y = 2$. On trouve comme solution particulière le couple $(1, -1)$ et donc les solutions sont les $(1 + k, -1 - 3k)$, pour $k \in \mathbb{Z}$.

◇ Application : forme irréductible d'une fraction rationnelle

Soit $x \in \mathbb{Q}$; alors il existe, par définition, $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que $x = \dfrac{p}{q}$. Posons $\delta = p \wedge q$, $p' = \dfrac{p}{\delta}$ et $q' = \dfrac{q}{\delta}$; il est alors trivial que :

$$\frac{p'}{q'} = \frac{p}{q} = x.$$

Nous venons de trouver une écriture de x comme quotient de deux entiers premiers entre eux, le dénominateur étant strictement positif. Une telle écriture s'appelle **forme irréductible de** x et est unique. En effet si $x = \dfrac{a}{b}$ avec $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ tels que $a \wedge b = 1$ alors :

$$p'b = aq'$$

et donc $q'|p'b$, ce qui entraîne par lemme de Gauss que $q'|b$. On montre symétriquement que $b|q'$ et donc, par positivité, $q' = b$ *ergo* $p' = a$.

d) Généralisations diverses

Il est possible de définir le PGCD et le PPCM d'une famille d'entiers $a_1, \dots a_n$ via les formules récursives :

$$\mathrm{pgcd}(a_1, \dots, a_n) = \mathrm{pgcd}(\mathrm{pgcd}(a_1, \dots, a_{n-1}), a_n)$$

et

$$\mathrm{ppcm}(a_1, \dots, a_n) = \mathrm{ppcm}(\mathrm{ppcm}(a_1, \dots, a_{n-1}), a_n) \ .$$

On a alors un analogue de la relation de Bézout, à savoir l'existence d'une famille $(u_1, \dots, u_n) \in \mathbb{Z}^n$ telle que :

$$\sum_{i=1}^{n} u_i a_i = \mathrm{pgcd}(a_1, \dots, a_n) \ .$$

✖ **Attention :** Il convient de différencier les familles d'entiers premiers entre eux deux à deux de celles dont le PGCD "global" est égal à 1 (on parle dans ce cas d'entiers **premiers entre eux dans leur ensemble**).

➠ **Exemple X.7.** Les entiers $2, 3, 4$ sont premiers entre eux dans leur ensemble mais $2 \wedge 4 \neq 1$.

4.⁻ Nombres premiers

a) C'est quoi ?

Définition X.5. Un entier $p \in \mathbb{N}$ est dit **premier** si $p \neq 1$ et

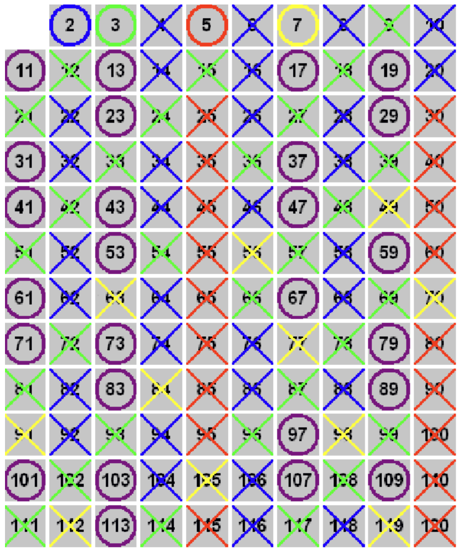
$$\mathscr{D}(p) = \{-1, -p, p, 1\} \ .$$

✖ **Attention :** : avec cette convention, les nombres premiers seront des entiers **naturels**.

➠ **Exemple X.8.** 1 n'est pas premier, 24 non plus ; 3 et 11 sont premiers.

Vocabulaire. Un entier naturel non premier différent de 1 sera dit **composé**.

✌ **Remarque X.7.** Pour dresser une table des premiers nombres premiers (ah ah), on peut utiliser un procédé appellé **crible d'Ératosthène** (grec, 276 av. J.-C. — 194 av. J.-C.) : il s'agit de supprimer d'une table des entiers tous les multiples d'un entier. En supprimant tous les multiples, à la fin il ne restera que les entiers qui ne sont multiples d'aucun entier, et qui sont donc les nombres premiers.



Proposition X.12.
(i) Deux nombres premiers distincts sont premiers entre eux ;
(ii) toute entier naturel supérieur ou égal à 2 admet un diviseur premier.

Démonstration. Le point (i) est immédiat par intersection des ensembles de diviseurs. Le point (ii) a été traité par récurrence forte au chapitre I. □

Proposition X.13. Il existe une infinité de nombres premiers.

Démonstration. Supposons qu'il existe un nombre fini et notons les $p_1, \dots p_n$; posons :

$$p = \prod_{i=1}^{n} p_i + 1 \ .$$

L'entier p est supérieur ou égal à 2 donc admet un diviseur premier. Or, tous les p_i sont premiers avec p par Bézout, d'où absurdité. □

b) Décomposition en produits de facteurs premiers

Proposition X.14. Soit $a \geq 2$ un entier naturel. Alors, il existe une unique (à l'ordre près) famille de nombres premiers $p_1, \dots, p_n$ et d'exposants associés $\alpha_1, \dots, \alpha_n \in \mathbb{N}^*$ telle que :

$$a = \prod_{k=1}^{n} p_k^{\alpha_k} \ .$$

Démonstration. L'existence se démontre par récurrence forte sur le modèle de l'existence d'un diviseur premier. Pour l'unicité, supposons qu'il existe deux telles familles, *i.e* que a admette pour écritures

$$a = \prod_{k=1}^{n} p_k^{\alpha_k} \quad \text{et} \quad a = \prod_{k=1}^{m} q_k^{\beta_k} \ .$$

Commençons par remarquer que les p_k et q_k sont en fait nécessairement les diviseurs premiers de a et donc $m = n$ et, quitte à les réorganiser, $\forall k \in [\![1, n]\!]\ p_k = q_k$. De plus, à k fixé on a :

$$p_k^{\alpha_k} | \prod_{j=1}^{n} p_k^{\beta_j}$$

ce qui entraîne par théorème de Gauss (p_k est premiers avec les p_j pour $j \neq k$) que $p_k^{\alpha_k} | p_k^{\beta_k}$ et donc α_k. Il ne nous reste qu'à démontrer symétriquement l'inégalité inverse pour conclure. □

Exemple X.9. $12 = 2^2 \times 3$, $15 = 3 \times 5$, $32 = 2^5$.

c) Valuation p–adique

Proposition/définition X.6. Soit $n \in \mathbb{N}^*$ et soit p un nombre premier. On appelle **valuation p–adique de n** l'entier :

$$\nu_p(n) = \max\{k \in \mathbb{N} \,|\, p^k | n\} \ .$$

Démonstration. Le maximum existe par axiome D (la partie est majorée d'après la proposition X.14). □

Exemple X.10. $\nu_5(250) = 3$.

Remarque X.8.

— Pour $n \in \mathbb{N}$, p premier et $k \geq 0$ on a l'équivalence suivante :

$$\nu_p(n) = k \quad \Longleftrightarrow \quad \begin{cases} p^k | n \, ; \\ p^{k+1} \nmid n \, . \end{cases}$$

— La proposition X.14 entraîne l'égalité :

$$n = \prod_{p \text{ premier}} p^{\nu_p(n)} \ .$$

Notons que ce produit est fini car seul un nombre fini de valuations sont non nulles.

Proposition X.15. Soient $a, b \in \mathbb{N}^*$ et soit p un nombre premier. Alors :

(i) $\nu_p(ab) = \nu_p(a) + \nu_p(b)$;

(ii) $\nu_p(a + b) \geq \min(\nu_p(a), \nu_p(b))$.

Démonstration. Il s'agit d'une conséquence de l'unicité dans la proposition X.14. □

Proposition X.16. Soient $a, b \in \mathbb{N}^*$ et soit p un nombre premier. Alors :

(i) $a|b \Leftrightarrow$ pour tout p premier, $\nu_p(a) \leq nu_p(b)$;

(ii)
$$a \wedge b = \prod_{p \text{ premier}} p^{\min(\nu_p(a),\nu_p(b))}$$

(iii)
$$a \vee b = \prod_{p \text{ premier}} p^{\max(\nu_p(a),\nu_p(b))} .$$

Démonstration. (i) Immédiat.

(ii) Découle de la caractérisation : si d divise a et b alors pour tout p premier, $\nu_p(d) \leq \nu_p(a)$ et $\nu_p(d) \leq \nu_p(b)$ *ergo* $\nu_p(d) \leq \min(\nu_p(a), \nu_p(b))$ ce qui entraîne que :
$$d| \prod_{p \text{ premier}} p^{\min(\nu_p(a),\nu_p(b))} .$$

(iii) Adapter la démonstration du point précédent.

□

5.⁻ Congruences

On fixe dans tout ce paragraphe $n \in \mathbb{N}$.

◇ **Rappels (chapitre V)**

Soient $a, b \in \mathbb{Z}$. On dit que a **est congru à** b **modulo** n (noté $a \equiv b\,[n]$) si il existe $k \in \mathbb{Z}$ tel que $b = a + kn$. Ceci définit une relation d'équivalence admettant exactement n classes $\bar{0}, \bar{1}, \ldots, \overline{n-1}$.

a) Opérations sur les congruences

Proposition X.17. La relation de congruence modulo n est compatible avec l'addition et la multiplication.

Démonstration. Soient $a, b, a', b' \in \mathbb{Z}$ tels que $a \equiv a'\,[n]$ et $b \equiv b'\,[n]$. Alors il existe $k, h \in \mathbb{Z}$ tels que $a = a' + kn$ et $b = b' + hn$. Ainsi :

$$\begin{aligned} a + b &= a' + b' + n(k + h) \\ &\equiv a' + b'\,[n] \end{aligned}$$

et

$$\begin{aligned} ab =& (a' + kn)(b' + hn) \\ &= a'b' + n(kb' + ha' + kh)n \\ &\equiv a'b' \,[n] \end{aligned}$$

d'où le résultat. □

Remarque X.9.

— Notons que l'on ne peut pas *a priori* inverser dans une congruence. Par exemple, $2 \times 2 \equiv 0\,[4]$.

— Cependant, si $a \in \mathbb{Z}$ est premier avec $n \in \mathbb{N}^*$, le théorème de Bézout (X.10) nous livre l'existence de $u, v \in \mathbb{Z}$ tels que $1 = au+nv$. De fait, on a $au \equiv 1\,[n]$, ce qui signifie que multiplier par u revient à "diviser par a modulo n". Ceci est fort utile pour résoudre des équations mettant en jeu des congruences.

b) Petit théorème de Fermat

Lemme X.1. Soit p un nombre premier et soient $a, b \in \mathbb{Z}$. Alors :

(i) $\forall k \in [\![1, p-1]\!]$, $p | \binom{p}{k}$;

(ii) $(a+b)^p \equiv a^p + b^p\,[p]$.

Démonstration. (i) Soit $k \in [\![1, p-1]\!]$; alors :

$$p! = k!(p-k)!\binom{p}{k}$$

donc $p | k!(p-k)!\binom{p}{k}$. Or, p n'apparaît pas dans le produit $k!(p-k)!$ d'entiers compris entre 1 et $p-1$ donc, comme p est premier, $p \wedge (k!(p-k)!) = 1$ d'où, par lemme de Gauss (théorème X.11) :

$$p|\binom{p}{k}.$$

(ii) Il suffit d'appliquer le binôme de Newton :

$$\begin{aligned} (a+b)^p &= \sum_{k=0}^{p} \binom{p}{k} a^k b^{n-k} \\ &= a^p + b^p + \underbrace{\sum_{k=1}^{p-1} \binom{p}{k} a^k b^{n-k}}_{\text{divisible par } p} \\ &\equiv a^p + b^p\,[p]\,. \end{aligned}$$

□

Le théorème suivant est souvent appelé "petit théorème de Fermat", du nom de Pierre de Fermat (français, ∼1610—1665), qui l'énonce dans une lettre à Bernard Frénicle de Bessy, autre mathématicien français et son contemporain.

Théorème X.18 (Fermat)**.**
Soit p un nombre premier. Alors :

$$\forall a \in \mathbb{Z},\ a^p \equiv a\,[p]\ .$$

Démonstration. Supposons dans un premier temps a positif ; nous pouvons alors démontrer ce résultat par récurrence sur a.
- $a = 0$: immédiat.
- Supposons la propriété vraie au range $a \geq 0$. Alors :

$$\begin{aligned}(a+1)^p &\equiv a^p + 1^p\,[p]\\ &\equiv a+1\,[p]\end{aligned}$$

d'où le résultat.

Dans le cas négatif, nous devons distinguer deux cas :
- si $p > 2$, alors p est impair et donc

$$\begin{aligned}a^p &= -(-a)^p\\ &\equiv -(-a)\,[p]\\ &\equiv a\,[p]\ ;\end{aligned}$$

- si $p = 2$ alors $-1 \equiv 1\,[2]$ donc $a \equiv -a\,[2]$.

Nous pouvons donc dans les deux cas conclure via le cas $a \geq 0$. □

Corollaire X.18.a. Soit p un nombre premier ; alors :

$$\forall a \in \mathbb{Z} \setminus p\mathbb{Z},\ a^{p-1} \equiv 1\,[p]\ .$$

Démonstration. Nous savons par le théorème de Fermat que $p|a^p-a$. Or $a^p-a = a(a^{p-1}-1)$ et $p \wedge a = 1$ car $a \notin p\mathbb{Z}$ donc, par lemme de Gauss (théorème X.11) :

$$p|a^{p-1}-1$$

d'où le résultat. □

Ce dernier résultat a été quelques temps utilisé comme test de primalité : si p vérifie la congruence indiquée, on le considérait comme premier. Malheureusement, la réciproque du corollaire est fausse, donc le test est faussé : les faux positifs, appelés nombres de Carmichael (Robert Daniel Carmichael, américain, 1879—1967) comprennent $561, 1105, 1729, 2465, 2821, 6601$ et 8911. Il a été démontré en 1994 par William Alford, Andrew Granville et Carl Pomerance qu'il en existe une infinité.

Chapitre XI

Dérivation

Dans tout ce chapitre, nous fixons un intervalle I de $\mathbb{R}$ d'intérieur non vide.

1.⁻ Notion de dérivée

a) Qu'est–ce ?

Définition XI.1. Soit $f : I \to \mathbb{R}$ une fonction et $a \in I$. On dit que f est **dérivable en** a si son taux d'accroissement en a admet une limite finie, *i.e* si

$$\lim_{x \to a} \frac{f(x) - f(a)}{x - a} \text{ existe dans } \mathbb{R}.$$

Cette limite est alors appelée **nombre dérivé de** f **en** a.

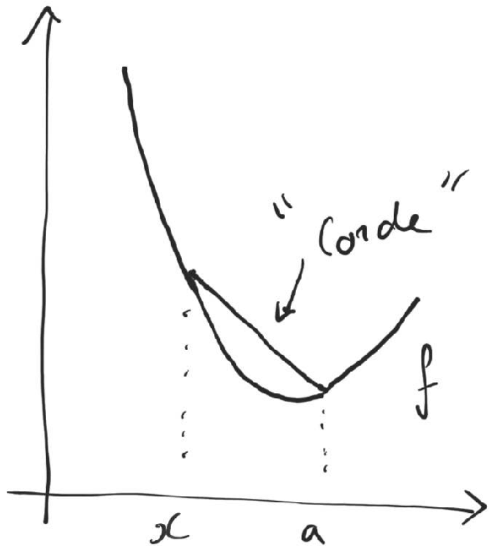
Notation. *Si* f est dérivable, on pose $f'(a) = \lim_{x \to a} \dfrac{f(x) - f(a)}{x - a}$.

✌ **Remarque XI.1.**

— Il peut être parfois utile de se ramener à l'écriture alternative suivante (lorsque les quantités existent) :

$$\lim_{x \to a} \frac{f(x) - f(a)}{x - a} = \lim_{h \to 0} \frac{f(a + h) - f(a)}{h} .$$

— Géométriquement, les taux d'accroissement correspondent aux pentes des "cordes" associées à la courbe représentative de f.



— En sciences appliquées, la dérivée en un point s'interprète cinématiquement comme une vitesse instantanée.

Exemple XI.1.

Pour la fonction $f : x \mapsto x^2$ on a, au voisinage de $a \in \mathbb{R}$ (excluant a) :

$$\begin{aligned}\frac{f(x) - f(a)}{x - a} &= \frac{x^2 - a^2}{x - a} \\ &= x + a \\ &\xrightarrow[x \to a]{} 2a\end{aligned}$$

et donc f est dérivable en a et $f'(a) = 2a$.

Proposition XI.1. Soit $f : I \to \mathbb{R}$ une fonction et soit $a \in I$. Alors :

f est dérivable en a

$\Longleftrightarrow$

il existe $\lambda \in \mathbb{R}$ et ε une fonction définie au voisinage de a et de limite nulle en a tels que $f(x) = f(a) + \lambda(x - a) + (x - a)\varepsilon(x)$ au voisinage de a.

Dans ce cas, on a de plus $f'(a) = \lambda$.

Vocabulaire. L'expression *supra* est appelée **développement limité** à l'ordre 1 de la fonction f en a (*cf.* chapitre XVII). Le terme en $(x - a)\varepsilon(x)$ sera dit **négligeable** par rapport à $x - a$ au voisinage de a.

Remarque XI.2. On retrouve le résultat vu en première : la courbe représentative de f peut être approximée par une droite au voisinage de a ; celle–ci admet pour équation

$$y = (x - a)f'(a) + f(a)$$

et est appelée **tangente à la courbe de f en a**. Notons au passage que si $f'(a) = 0$, la tangente est **horizontale** et que si le taux d'accroissement tend vers l'infini, notre courbe représentative admet une **tangente verticale** (elle n'est alors évidemment pas dérivable).

✖ **Attention :** Ne pas confondre la notion de tangente et celle d'asymptote, que nous étudierons au chapitre XVII.

Démonstration.

($\Downarrow$) Si f est dérivable en a, il suffit de poser $\varepsilon : x \mapsto \dfrac{f(x)-f(a)}{x-a} - f'(a)$. On a alors bien $\varepsilon(x) \xrightarrow[x\to a]{} 0$ et l'égalité voulue avec $\lambda = f'(a)$.

($\Uparrow$) On a, au voisinage de a (excluant a) :

$$\begin{aligned}\frac{f(x)-f(a)}{x-a} &= \lambda + \varepsilon(x) \\ &\xrightarrow[x\to a]{} \lambda\end{aligned}$$

d'où le résultat.

□

Proposition XI.2. Toute fonction dérivable en un point de I y est continue.

✖ **Attention :** la réciproque est **fausse**. La fonction valeur absolue est continue en 0 et pourtant :

$$\frac{|x|}{x} \xrightarrow[x\to 0^+]{} 1$$

et

$$\frac{|x|}{x} \xrightarrow[x\to 0^-]{} -1$$

ce qui signifie que cette fonction n'est pas dérivable en 0.

Démonstration. Soit $a \in I$ et soit f dérivable en a. Alors d'après la proposition XI.1 on a, au voisinage de a :

$$\begin{aligned}f(x) &= f(a) + (x-a)f'(a) + (x-a)\underbrace{\varepsilon(x)}_{\xrightarrow[x\to a]{}0} \\ &\xrightarrow[x\to a]{} f(a)\end{aligned}$$

et donc f est continue en a. □

Définition XI.2. Une fonction dérivable en tout point de I est dite dérivable sur I. La fonction

$$\begin{aligned}f' : I &\to \mathbb{R} \\ x &\mapsto f'(x)\end{aligned}$$

est alors appelée **dérivée de** f.

Notation. On note $\mathscr{D}(I)$ l'ensemble des fonctions dérivables sur I. La dérivée pourra être noté f', $\dfrac{\mathrm{d}f}{\mathrm{d}x}$ ou même $\mathrm{D}f$, mais **surtout pas** $\dfrac{\partial f}{\partial x}$.

◇ **Dérivées usuelles**

Les fonctions vues dans le chapitre II sont dérivables en presque tout point de leurs ensembles de définition respectifs. Nous rappelons dans le tableau ci–ensuite les valeurs de leurs nombres dérivés en les points *ad–hoc*.

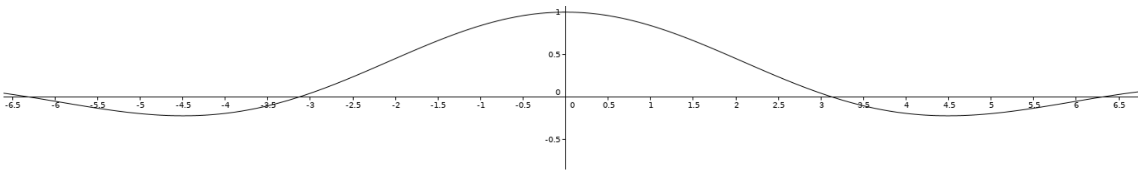
Valeur de $f(x)$	**Ensemble de dérivabilité**	**Valeur de** $f'(x)$
x^a	$\mathbb{R}_+^*$	ax^{a-1}
a^x $(a > 0)$	$\mathbb{R}$	$\ln(a)a^x$
$\log_a(x)$ $(a > 0,\ a \neq 1)$	$\mathbb{R}_+^*$	$\frac{1}{x\ln(a)}$
$\cos(x)$	$\mathbb{R}$	$-\sin(x)$
$\sin(x)$	$\mathbb{R}$	$\cos(x)$
$\tan(x)$	$\mathbb{R} \setminus \left\{\frac{\pi}{2} + k\pi \,\middle|\, k \in \mathbb{Z}\right\}$	$1 + \tan^2(x) = \frac{1}{\cos^2(x)}$
$\operatorname{arcos}(x)$	$]-1,1[$	$-\frac{1}{\sqrt{1-x^2}}$
$\arcsin(x)$	$]-1,1[$	$\frac{1}{\sqrt{1-x^2}}$
$\arctan(x)$	$\mathbb{R}$	$\frac{1}{1+x^2}$
$\operatorname{ch}(x)$	$\mathbb{R}$	$\operatorname{sh}(x)$
$\operatorname{sh}(x)$	$\mathbb{R}$	$\operatorname{ch}(x)$
$\operatorname{th}(x)$	$\mathbb{R}$	$1 - \operatorname{th}^2(x) = \frac{1}{\operatorname{ch}^2(x)}$

Un cas particulier mérite d'être souligné : les fonctions puissances $x \mapsto x^a$ sont dérivables sur $\mathbb{R}$ si $a \in \mathbb{N}$, $\mathbb{R}^*$ si $a \in \mathbb{Z} \setminus \mathbb{N}$. Les racines n–ièmes ne sont jamais dérivables en 0,mais sont dérivables sur $\mathbb{R}^*$ si n est impair.

➠ **Exemple XI.2.** Comme la fonction sinus est dérivable en 0, on a

$$\frac{\sin(x)}{x} \xrightarrow[x\to 0]{} \cos(0) = 1$$

et donc la fonction sinus cardinal sinc : $x \mapsto \dfrac{\sin(x)}{x}$, définie sur $\mathbb{R}^*$ est prolongeable par continuité à $\mathbb{R}$.



b) Dérivées directionnelles

Définition XI.3. Soit $f : I \to \mathbb{R}$ et soit $a \in \mathring{I}$.
- Si $a \neq \min I$, on appelle **dérivée à gauche de** f **en** a la quantité (si elle existe)

$$f_g'(a) = \lim_{x\to a^-} \frac{f(x) - f(a)}{x - a}\ .$$

- Si $a \neq \max I$, on appelle **dérivée à droite de** f **en** a la quantité (si elle existe)

$$f_d'(a) = \lim_{x\to a^+} \frac{f(x) - f(a)}{x - a}\ .$$

Exemple XI.3. Soit $f : x \mapsto |x|$; alors f est dérivable à droite et à gauche en 0 et $f'_d(0) = 1$, $f'_g(0) = -1$.

Proposition XI.3. Soit $f : I \to \mathbb{R}$ et soit $a \in \mathring{I}$. Alors :

$$f \text{ est dérivable en } a$$
$$\Longleftrightarrow$$
$$f \text{ admet une dérivée à gauche et à droite en } a \text{ qui sont égales.}$$

Démonstration. Cela découle du résultat analogue sur les limites directionnelles, à savoir la proposition IX.10 □

c) Classes de fonctions

Définition XI.4. Soit $k \geq 1$; une fonction $f : I \to \mathbb{R}$ est dite k–fois dérivable sur I si :
- $k = 1$ et f est dérivable sur I ; on note alors $f^{(1)} = f'$;
- $k \geq 2$ et la fonction $f^{(k-1)}$ est dérivable sur I ; on note alors $f^{(k)} = (f^{(k-1)})'$.

Notation. On note $\mathscr{D}^k(I)$ l'ensemble des fonctions k fois dérivables sur I. La fonction dérivée k–ième $f^{(k)}$ pourra également être notée $\mathrm{D}^k f$ ou $\dfrac{\mathrm{d}^k f}{\mathrm{d}x^k}$.

Exemple XI.4. La fonction $x \mapsto x^2$ est 7 fois dérivable sur $\mathbb{R}$, de dérivée septième nulle. Sa dérivée seconde est $x \mapsto 2$.

Convention. On notera, pour $f \in \mathscr{C}^0(I)$, $f^{(0)} = f$.

Remarque XI.3. Soit $k \geq 1$; alors si f est une fonction k–fois dérivable sur I, pour tout $0 \leq j < k$, la fonction $f^{(j)}$ est continue (car dérivable).

Définition XI.5. Soit $k \in \mathbb{N}^*$. On dira qu'une fonction $f : I \to \mathbb{R}$ est **de classe $\mathscr{C}^k$ sur I** si :
- $f \in \mathscr{D}^k(I)$;
- $f^{(k)} \in \mathscr{C}^0(I)$.

Si f est de classe $\mathscr{C}^k$ sur I pour tout $k \in \mathbb{N}^*$, on dira que f est **de classe $\mathscr{C}^\infty$ sur** I.

Notation. On notera, sans surprise, $\mathscr{C}^k(I)$ (resp. $\mathscr{C}^\infty$) l'ensemble des fonctions de classe $\mathscr{C}^k$ (resp. $\mathscr{C}^\infty$) sur I.

Exemple XI.5. Les fonctions usuelles sont de classe $\mathscr{C}^\infty$ dans les ensembles mentionnés dans le tableau du paragraphe a).

Remarque XI.4.

— On a la chaîne d'inclusions suivante :

$$\mathscr{C}^0(I) \supset \mathscr{D}^1(I) \supset \mathscr{C}^1(I) \supset \mathscr{D}^2(I) \supset \ldots \supset \mathscr{C}^{(k)}(I) \supset \mathscr{D}^{(k+1)}(I) \supset \ldots \supset \mathscr{C}^\infty(I)$$

et toutes ces inclusions sont **strictes**. Par exemple, $\sqrt{\cdot} \in \mathscr{C}^0(\mathbb{R}_+) \setminus \mathscr{D}^1(\mathbb{R}_+)$ et $x \mapsto x^{\frac{3}{2}} \in \mathscr{C}^1(\mathbb{R}_+) \setminus \mathscr{D}^2(\mathbb{R}_+)$.

— Si f est de classe $\mathscr{C}^k$ sur I, alors $f' \in \mathscr{C}^{(k-1}(I)$.

— On a

$$\mathscr{C}^\infty(I) = \bigcap_{k \in \mathbb{N}^*} \mathscr{D}^k(I) \; .$$

✍ **Exercice XI.1.** Démontrer que la fonction $x \mapsto x^2 \sin\left(\frac{1}{x}\right)$ se prolonge en 0 en une fonction dérivable mais pas de classe $\mathscr{C}^1$.

d) Opérations sur les dérivées

◇ Au premier ordre

Proposition XI.4. Soient $f, g \in \mathscr{D}^1(I)$ et soit $\lambda \in \mathbb{R}$. Alors :

(i) $f + \lambda g$ est dérivable sur I et $(f+\lambda g)' = f' + \lambda g'$;

(ii) $f \times g$ est dérivable sur I et $(f \times g)' = f' \times g + f \times g'$;

(iii) si g ne s'annule pas sur I, $\frac{f}{g}$ est dérivable sur I et

$$\left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2} \; ;$$

Démonstration. (i) Immédiat par opération sur les limites (passer aux taux d'accroissement).

(ii) Soient $x, a \in I$ tels que $x \neq a$. Alors :

$$\begin{aligned}\frac{f(x)g(x) - f(a)g(a)}{x-a} &= \frac{f(x)g(x) - f(x)g(a) + f(x)g(a) - f(a)g(a)}{x-a} \\ &= f(x)\frac{g(x)-g(a)}{x-a} + g(a)\frac{f(x)-f(a)}{x-a} \\ &\xrightarrow[x \to a]{} f(a)g'(a) + g(a)f'(a)\end{aligned}$$

d'où le résultat.

(iii) S'obtient de façon analogue au précédent, avec des calculs un tantinet plus crades.

□

✖ **Attention :** il convient de prêter à la rédaction une attention particulière ; en particulier, on ne saurait dériver une fonction sans avoir préalablement justifié sa dérivabilité.

Proposition XI.5. Soient I, J deux intervalles d'intérieur non vide de $\mathbb{R}$ et soient $f \in \mathscr{D}^(I)$ et $g \in \mathscr{D}^1(J)$ telles que $f(I) \subset J$. Alors :

(i) $g \circ f \in \mathscr{D}^1(I)$;

(ii)
$$(g \circ f)' = f' \times g' \circ f\ .$$

Démonstration. Soit $a \in I$ et soit $b = f(a) \in J$. Alors, par proposition XI.1, il existe $W \in \mathscr{V}(b)$ tel que :

$$\forall y \in W \quad : g(y) = g(b) + (y - b)g'(b) + (y - b)\varepsilon(y)$$

avec $\varepsilon(y) \xrightarrow[y \to b]{} 0$. Comme $f(a) = b$ et que f est continue, il existe de plus $V \in \mathscr{V}(a)$ tel que $f(V) \subset W$ et donc, si $x \in V \cap I$ on a $f(x) \in W$ *ergo* :

$$g \circ f(x) = g \circ f(a) + (f(x) - f(a))g' \circ f(a) + (f(x) - f(a))\underbrace{\varepsilon(f(x))}_{\xrightarrow[x \to a]{} 0}\ .$$

Ainsi :

$$\begin{aligned}\frac{g \circ f(x) - g \circ f(a)}{x - a} &= \frac{f(x) - f(a)}{x - a} g' \circ f(a) + \frac{f(x) - f(a)}{x - a}\varepsilon(f(x)) \\ &\xrightarrow[x \to a]{} f'(a)g' \circ f(a)\end{aligned}$$

ce qui conclut la démonstration. □

Exemple XI.6. La fonction définie sur $\mathbb{R}_+^*$ par $x \mapsto e^{\frac{1}{x}}$ est dérivable comme composée des fonctions dérivables

$$\begin{aligned} f : \mathbb{R}_+^* &\to \\ x &\mapsto \frac{1}{x}\end{aligned}$$

et $\exp : \mathbb{R} \to \mathbb{R}$. Sa dérivée vérifie, pour tout $x > 0$:

$$(\exp \circ f)'(x) = \frac{-1}{x^2} e^{\frac{1}{x}}\ .$$

Proposition XI.6. Soient I, J deux intervalles d'intérieur non vide de $\mathbb{R}$ et soit $f : I \to J$ une fonction **bijective et continue sur** I. Soit $a \in I$ tel que :

— f soit dérivable en a ;

— $f'(a) \neq 0$.

Alors

(i) f^{-1} est dérivable en $b = f(a)$;

(ii) $(f^{-1})'(b) = \dfrac{1}{f'(a)}$, *i.e* :

$$(f^{-1})'(b) = \frac{1}{f'(f^{-1}(b))}\ .$$

Remarque XI.5.
- Ce théorème a donc **quatre** hypothèses à vérifier : deux globales (portant sur la fonction) et deux locales (relatives au point a).
- On retrouve le résultat énoncé dans le théorème II.4 : une bijection dérivable admet une réciproque dérivable en tout point de non–annulation de sa dérivée.
- Par la proposition IX.17, la fonction f est strictement monotone.

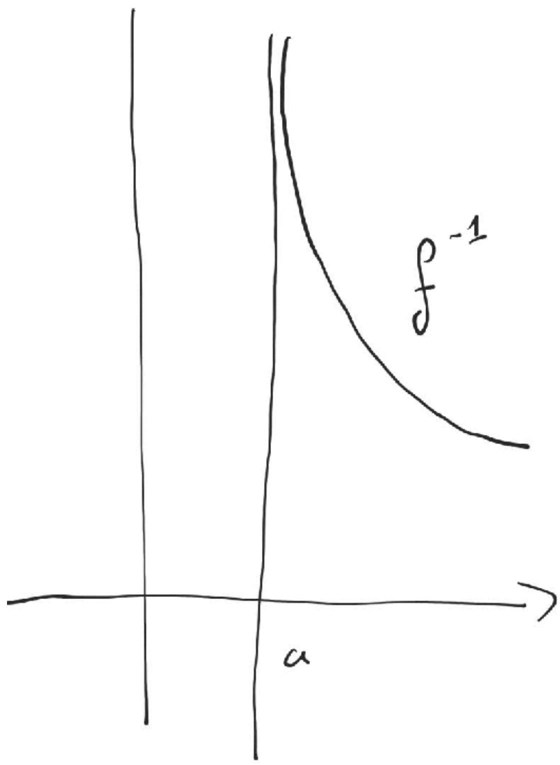
Exemple XI.7. Nous avons vu plusieurs applications de ce théorème dans le chapitre II (fonctions trigonométriques réciproques).

Démonstration. Soit $V \in \mathscr{V}(a)$, $x \in V \setminus \{a\}$ et $y = f(x)$. Alors

$$\begin{aligned} \frac{f^{-1}(y) - f^{-1}(b)}{y - b} &= \frac{x - a}{f(x) - f(a)} \\ &\xrightarrow[x \to a]{} \frac{1}{f'(a)} \end{aligned}$$

d'où le résultat. □

Remarque XI.6. Si la dérivée de f s'annule en a, la fonction réciproque y admet une tangente verticale car le taux d'accroissement ci–dessus tend vers l'infini.



Dans le cas contraire, la fonction réciproque admet au point $f(a)$ une tangente dont le coefficient directeur est l'inverse de celui de la tangente à la courbe de f en a.

On retrouve, en reformulant, la proposition vue au chapitre II.

Corollaire XI.6.a. Soit $f : I \to \mathbb{R}$ une fonction dérivable telle que f' **ne s'annule pas** sur I. Alors :

(i) f admet une réciproque f^{-1} dérivable sur $f(I)$;

(ii)

$$(f^{-1})' = \frac{1}{f' \circ f^{-1}} .$$

◇ Aux ordres supérieurs

Les choses se passent très bien concernant les dérivées d'ordre supérieur d'une combinaison linéaire ; les formules se compliquent (un peu) pour le produit, avec le résultat suivant du au mathématicien allemand Gottfried Wilhelm Leibniz (1646—1716).

Proposition XI.7 (Formule de Leibniz)**.** Soient $f, g \in \mathscr{D}^n(I)$ $(n \geq 1)$. Alors la fonction $fg \in \mathscr{D}^n(I)$ et :

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

Démonstration. Démontrons le par récurrence sur $n \in \mathbb{N}^*$.

— $n = 1$: se référer au paragraphe précédent.

— Supposons la propriété vérifiée pour un certain $n \in \mathbb{N}^*$. Soit $f : I \to \mathbb{R}$ et $g : I \to \mathbb{R}$ deux fonctions $n+1$ fois dérivables sur I.

Les fonctions f et g sont, en particulier, n fois dérivables sur I et donc par hypothèse de récurrence la fonction fg l'est aussi avec

$$\forall\, x \in I, \quad (fg)^{(n)}(x) = \sum_{k=0}^{n} \binom{n}{k} f^{(n-k)}(x) g^{(k)}(x) .$$

Pour tout $k \in [\![1, n-1]\!]$, les fonctions $f^{(n-k)}$ et $g^{(k)}$ sont dérivables sur I donc par opération sur les fonctions dérivables, la fonction $(fg)^{(n)}$ est encore dérivable sur I. Ainsi la fonction fg est $(n+1)$ fois dérivable et :

$$\forall\, x \in I, \quad (fg)^{(n+1)}(x) = \sum_{k=0}^{n} \binom{n}{k} \left(f^{(n+1-k)}(x) g^{(k)}(x) + f^{(n-k)}(x) g^{(k+1)}(x) \right) .$$

En décomposant la somme en deux et en procédant à un changement d'indice sur la deuxième somme, on obtient, pour $x \in I$:

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

La propriété était initialisée et héréditaire, elle est vérifiée sur $\mathbb{N}$. □

✍ **Exercice XI.2.** Le lecteur possédé de tendances masochistes pourra calculer les dérivées successives de $\sin \times \cos$.

La succession de résultats suivante est énoncée sans démonstration. Le lecteur pourra si il le souhaite combler ce manque à la sueur de son front.

Proposition XI.8.
(i) L'inverse d'une fonction de classe $\mathscr{C}^k$ ne s'annulant pas est de classe $\mathscr{C}^k$.
(ii) La composée de deux fonctions de classes $\mathscr{C}^k$ compatibles est de classe $\mathscr{C}^k$.
(iii) La réciproque d'une bijection de classe $\mathscr{C}^k$ dont **la dérivée première** ne s'annule pas est de classe $\mathscr{C}^k$.

Nous ne donnons pas dans les cas énoncés *supra* de formules pour le calcul explicite des dérivées successives, et nous suggérons au lecteur de nous en être reconnaissant.

2.– Accroissements finis

a) Extrema locaux

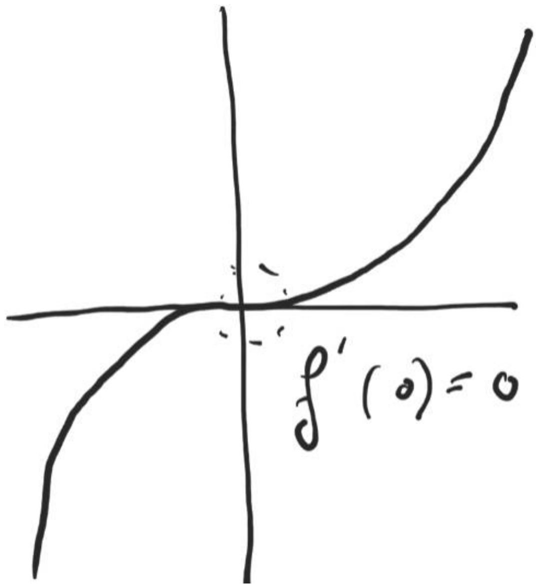
Nous pouvons reformuler les définitions vues au chapitre II en utilisant un langage un peu plus évolué. Notons le gain de place occasionné.

Définition XI.6. Soit $f : I \to \mathbb{R}$ une fonction. Si $a \in I$, on dit que :
— f admet un maximum local en a si $f(x) \leq f(a)$ au voisinage de a ;
— f admet un minimum local en a si $f(x) \geq f(a)$ au voisinage de a.

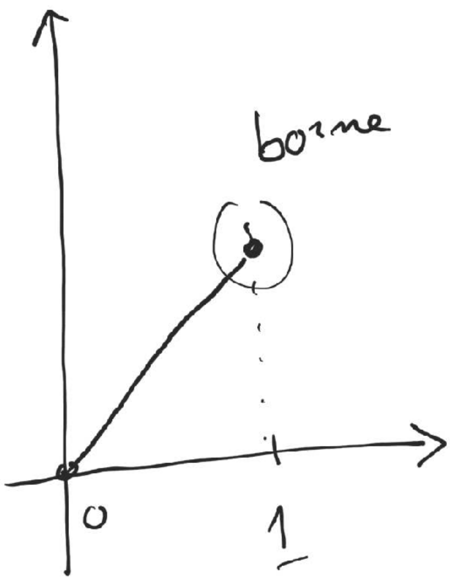
Proposition XI.9. Soit f une fonction dérivable sur $\mathring{I}$ et soit $a \in \mathring{I}$. **Si** f admet un extremum local en a, **alors** $f'(a) = 0$.

Vocabulaire. Un point d'annulation de f' est appelé **point critique** de la fonction f.

✖ **Attention :** la réciproque est **fausse**. En effet, la fonction $x \mapsto x^3$ admet pour dérivée $x \mapsto 3x^2$ qui s'annule en 0 sans que ce dernier ne soit un extremum local de la fonction initiale.



De même, il est **essentiel** que a ne soit pas une borne de I ; penser à la fonction $x \mapsto x$ sur $[0, 1]$...



Démonstration. Plaçons nous dans le cas où a est un maximum local de f. Alors, au voisinage de a :

— si $x < a$,
$$\frac{f(x) - f(a)}{x - a} \geq 0$$
et donc par passage à la limite $f'_g(a) \geq 0$;

— si $x > a$,
$$\frac{f(x) - f(a)}{x - a} \leq 0$$
et donc par passage à la limite $f'_d(a) \leq 0$.

Or f est dérivable en a, donc $f'_g(a) = f'_d(a) = f'(a)$. On en déduit que $f'(a) = 0$. □

✌ **Remarque XI.7.** Dans le cas $\mathscr{C}^1$, on peut démontrer ce résultat en appliquant le TVI (théorème IX.16) à f'.

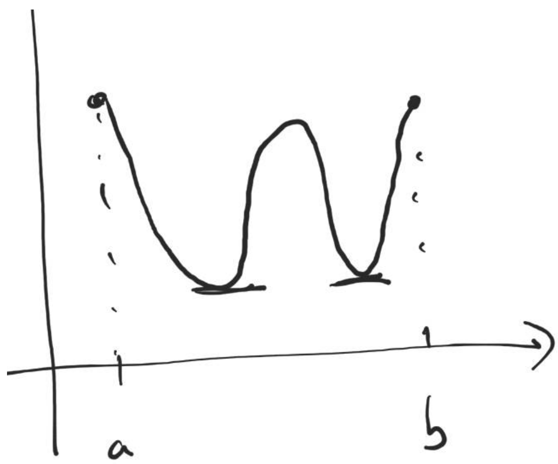
b) Théorème de Rolle

L'heuristique du résultat suivant se trouve dans les écrits de Michel Rolle (français, 1652—1719). Sa forme moderne, liée au théorème des accroissements finis, doit beaucoup aux écrits d'Augustin Louis Cauchy (français,1789—1857) et Joseph–Louis Lagrange (italien naturalisé français, 1736—1813). La démonstration proposée ici s'inspire de celle proposée par Joseph–Alfred Serret (français, 1819—1885).

Théorème XI.10 (Rolle)**.**
Soient $a, b \in \mathbb{R}$ tels que $a < b$ et soit $f : [a, b] \to \mathbb{R}$ telle que :
- — $f \in \mathscr{C}^0([a, b])$;
- — $f \in \mathscr{D}^1(]a, b[)$;
- — $f(a) = f(b)$.

Alors :
$$\exists\, c \in]a, b[,\ f'(c) = 0\ .$$

✌ **Remarque XI.8.** L'idée derrière ce théorème n'a rien d'ésotérique (rétrospectivement) : si $f(a) = f(b)$, alors la courbe représentative de la fonction f admettra au moins une tangente horizontale entre a et b.



Démonstration. Si f est constante, c'est trivial. Sinon, il existe (par exemple) $y \in]a, b[$ tel que $f(y) < f(a)$ et donc f admet un minimum local en un point (non déterminé) $c \in]a, b[$ par le corollaire IX.16.d. Ainsi, $f'(c) = 0$ par proposition XI.9. □

Exemple XI.8.
- — La dérivée d'un polynôme admet une racine entre chaque paire de racines de ce dernier.
- — En physique, un mobile unidimensionnel revenant à son point de départ devra annuler sa vitesse à un instant donné.

c) Théorème des accroissements finis

Le théorème qui suit, point central de ce chapitre, est du à Augustin Louis Cauchy (français,1789—1857) et Joseph–Louis Lagrange (italien naturalisé français, 1736—1813).

Théorème XI.11 (Accroissements finis)**.**
Soient $a, b \in \mathbb{R}$ tels que $a < b$ et soit $f : [a, b] \to \mathbb{R}$ telle que :

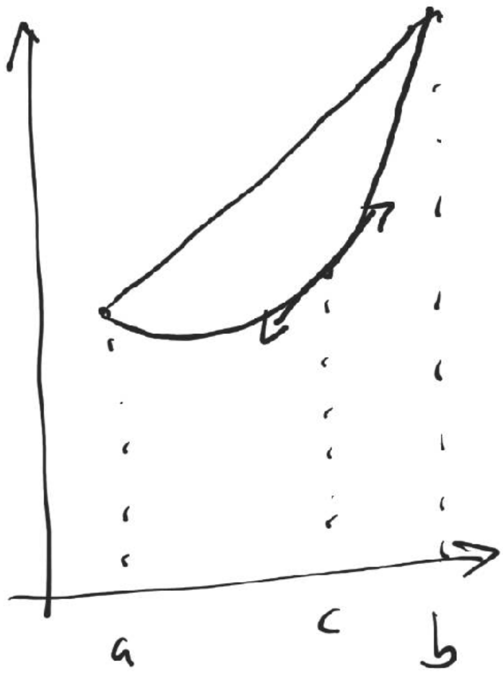
— $f \in \mathscr{C}^0([a, b])$;
— $f \in \mathscr{D}^1(]a, b[)$.

Alors :

$$\exists\, c \in]a, b[,\ f'(c) = \frac{f(b) - f(a)}{b - a}\ .$$

✌ **Remarque XI.9.**

— Géométriquement, ce résultat se traduit de la façon suivante : il existe un point c en lequel la tangente à la courbe représentative de f est parallèle à la "corde" reliant les points $(a, f(a))$ et $(b, f(b))$.



— En physique, ce résultat implique qu'il existe un instant dans tout mouvement en lequel vitesses instantanée et moyenne sont confondues.

Démonstration. Il suffit d'applique le théorème de Rolle à la fonction

$$\begin{aligned} g : [a, b] &\to \mathbb{R} \\ x &\mapsto f(x) - \frac{f(b) - f(a)}{b - a}(x - a)\ . \end{aligned}$$

□

Corollaire XI.11.a (Inégalité des accroissements finis)**.** Soient $a, b \in \mathbb{R}$ tels que $a < b$ et soit $f : [a, b] \to \mathbb{R}$ telle que :
- — $f \in \mathscr{C}^0([a, b])$;
- — $f \in \mathscr{D}^1(]a, b[)$;
- — il existe $M \in \mathbb{R}$ tels que :

$$\forall x \in]a, b[,\ |f'(x)| \leq M\ .$$

Alors :

$$\left|\frac{f(b) - f(a)}{b - a}\right| \leq M\ .$$

✌ **Remarque XI.10.** La troisième hypothèse *supra* est toujours vérifiée par les fonctions de classe $\mathscr{C}^1$ sur un segment.

➠ **Exemple XI.9.** Pour tout $x \in \mathbb{R}$, $|\sin(x)| \leq |x|$.

◇ **Une application : fonctions lipschitziennes**

La classe de fonctions définies ci–ensuite est nommée en l'honneur du mathématicien allemand Rudolph Otto Sigismund Lipschitz (1832—1903).

Définition XI.7. Soit $M \in \mathbb{R}_+^*$. Une fonction $f : I \to \mathbb{R}$ est dite M**–lipschitzienne** si :

$$\forall x, y \in I,\ |f(x) - f(y)| \leq M|x - y|\ .$$

➠ **Exemple XI.10.** La fonction $x \mapsto x^2$ est 2–lipschitzienne sur $[0, 1]$. En effet, pour tous $x, y \in [0, 1]$:

$$|x^2 - y^2| = |(x + y)(x - y| \leq 2|x - y|\ .$$

Proposition XI.12. Toute application lipschitzienne est continue.

Démonstration. Soit $f : I \to \mathbb{R}$ une fonction M–lipschitzienne et soit $a \in I$. Alors, pour tout $x \in I$:

$$|f(x) - f(a)| \leq M|x - a| \underset{x \to a}{\longrightarrow} 0$$

d'où le résultat. □

✖ **Attention :** la réciproque est fausse. La fonction exponentielle n'est pas exemple pas lipschitzienne sur $\mathbb{R}$.

Proposition XI.13. Une fonction dérivable est lipschitzienne si et seulement si sa dérivée est bornée.

Démonstration. Il s'agit d'un corollaire de l'inégalité des accroissements finis. □

Exemple XI.11. Les fonctions continues sur un segment, les fonctions sinus, cosinus sont lipschitziennes.

◇ **Une autre application : suites récurrentes et applications contractantes**

On se fixe une application $f : I \to I$ **contactante**, *i.e* lipschitzienne de rapport $K \in]0,1[$. On fixe $u_0 \in \mathring{I}$ et on pose, pour $n \geq 0$:

$$u_{n+1} = f(u_n)\,.$$

Si on suppose que f admet un point fixe c, alors pour tout $n \geq 0$:

$$\begin{aligned}|u_{n+1} - c| &= |f(u_n) - f(c)| \\ &\leq K|u_n - c| \\ &\;\;\vdots \\ &\leq K^n|u_1 - c| \\ &\to 0\end{aligned}$$

et donc $u_n \to c$.

Remarque XI.11. Il est possible de démontrer l'existence de ce point fixe dans le cas général.

Exercice XI.3. Soit $\alpha \in \mathbb{R}_+$ et soit $(u_n)_n$ la suite définie par récurrence via :

$$\begin{cases} u_0 = \alpha \\ \forall n \in \mathbb{N},\ u_{n+1} = \sqrt{1 + u_n} \end{cases}.$$

Démontrer que $(u_n)_n$ converge vers $\dfrac{1+\sqrt{5}}{2}$.

➥ **Correction :** *Nous avons déjà remarqué dans le chapitre VII que l'unicité de la limite (proposition VII.1) entraîne que $\ell = \sqrt{1+\ell}$ et donc $\ell = \dfrac{1+\sqrt{5}}{2}$ (ℓ doit être positive car les termes de la suite u le sont et $\ell^2 = 1 + \ell$). Par inégalité des accroissements finis, la fonction $f : x \mapsto \sqrt{1+x}$ est $\frac{1}{2}$–lispschitzienne sur $\mathbb{R}_+$. Elle admet de plus un point fixe (nous venons de le trouver !), d'où le résultat en appliquant l'heuristique vue supra.*

d) Monotonie

Théorème XI.14.
Soit $f \in \mathscr{C}^0(I) \cap \mathscr{D}^1(\mathring{I})$. Alors :

(i) f est croissante sur $I \iff f' \geq 0$ sur $\mathring{I}$;

(ii) f est décroissante sur $I \iff f' \leq 0$ sur $\mathring{I}$;

(iii) f est constante sur $I \iff f' = 0$ sur $\mathring{I}$.

✖ **Attention :** I est un **intervalle**. Considérer la fonction $x \mapsto |x|$ sur $\mathbb{R}^*$ qui est de dérivée seconde nulle sans que sa dérivée première ne sont constante.

Démonstration. (i)

($\Rightarrow$) Soient $a \in \mathring{I}$ et $x \in I$ tels que $x > a$. Alors :

$$\frac{f(x) - f(a)}{x - a} \geq 0$$

et donc, en passant à la limite $f'(a) = f'_d(a) \geq 0$.

($\Leftarrow$) Soient $x, y \in I$ tels que $x \geq y$. Alors, par TAF (théorème XI.11, applicable car $f \in \mathscr{C}^0([y,x]) \cap \mathscr{D}^1(]y,x[)$), il existe $c \in]y,x[$ tel que :

$$f(x) - f(y) = f'(c)(x - y) \geq 0$$

d'où le résultat.

(ii) Se traite de façon analogue.

(iii) Découle immédiatement de (i) et (ii).

□

Corollaire XI.14.a. Soit $f \in \mathscr{C}^0(I) \cap \mathscr{D}^1(\mathring{I})$ une fonction **croissante**. On pose :

$$\mathscr{E} = \{x \in \mathring{I} \mid f'(x) = 0\}.$$

Alors :

f est strictement croissante

$\iff$

$\mathscr{E}$ non contient aucun intervalle d'intérieur non vide.

Vocabulaire. Un ensemble $\mathscr{E}$ vérifiant la propriété *supra* est dit **discret**.

Démonstration. Cela découle du point (iii) de la proposition précédente. □

✌ **Remarque XI.12.**

— Cela signifie que tout va bien si $\mathscr{E}$ ne contient aucun convexe non trivial, *i.e* si il est "rempli de trous".

— Un résultat analogue existe évidemment pour les fonctions décroissantes.

e) Limite de la dérivée

La question qui nous intéresse dans ce paragraphe est la suivante : étant donné un point $a \in I$ et $f \in \mathscr{C}^0(I) \cap \mathscr{D}^1(I \setminus \{a\})$, comment vérifier que f est dérivable en a ? Cela nous sera en particulier utile pour tester la régularité de prolongements par continuité.

Proposition XI.15. Soit $a \in I$ et soit $f \in \mathscr{C}^0(I) \cap \mathscr{D}^1(I \setminus \{a\})$. Alors :

— si $f'(x) \xrightarrow[x \to a]{} \ell \in \mathbb{R}$, f est dérivable en a et $f'(a) = \ell$;

— si $f'(x) \xrightarrow[x \to a]{} \pm\infty$, f n'est pas dérivable en a et sa courbe y admet une tangente verticale ;

— sinon, on ne peut conclure.

✌ **Remarque XI.13.** Dans le premier cas, la fonction f' est *de facto* continue en a.

Démonstration. Soit $x \in I \setminus \{a\}$, par exemple $x > a$. En appliquant le TAF au segment $[a, x]$, on obtient l'existence de $c_x \in]a, x[$ tel que

$$f'(c_x) = \frac{f(x) - f(a)}{x - a}$$

et $c_x \xrightarrow[x \to a]{} a$ par encadrement. On en déduit le résultat en examinant les différentes limites possibles pour $f'(c_x)$ quand $x \to a$. □

➠ **Exemple XI.12.** Le prolongement par continuité en 0 de la fonction $x \mapsto e^{-\frac{1}{x}}$ (initialement définie sur $\mathbb{R}_+^*$, *cf.* chapitre IX) est dérivable en 0 de dérivée nulle car

$$\frac{1}{x^2} e^{-\frac{1}{x}} \xrightarrow[x \to 0^+]{} 0 \,.$$

3.– Fonctions convexes

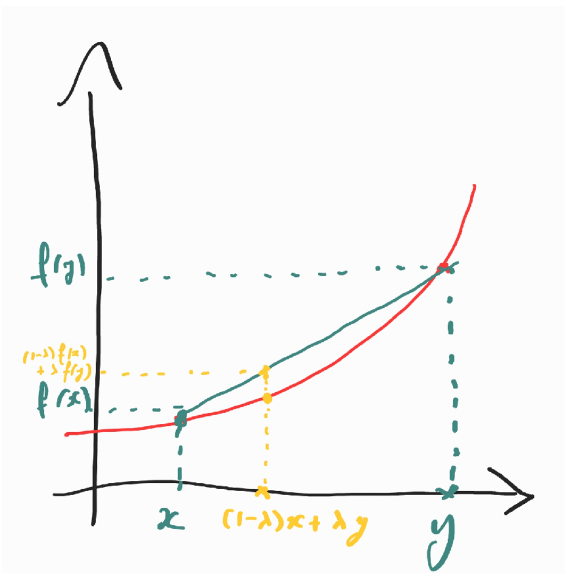
a) C'est quoi ?

Définition XI.8. Une fonction $f : I \to \mathbb{R}$ est dite **convexe** si :

$$\forall\, x, y \in I,\ \forall\, \lambda \in [0, 1], \quad f((1 - \lambda)x + \lambda y) \leq (1 - \lambda) f(x) + \lambda f(y) \,.$$

Vocabulaire. Si $-f$ est une fonction convexe, on dira que f est concave.

✌ **Remarque XI.14.** L'inégalité définissant les fonctions convexes nous indique que la droite sécante passant par deux points sur la courbe représentative d'une telle fonction est située **au dessus** de l'arc (portion de courbe) délimité par ceux–ci.



Il peut également être intéressant de faire le lien entre cette définition et la caractérisation paramétrique des convexes de $\mathbb{R}$ (corollaire III.12.a).

Exemple XI.13.

— les fonctions affines $x \mapsto \alpha x + \beta$, pour $\alpha, \beta \in \mathbb{R}$, sont clairement convexes (et concaves) ;
— la fonction $x \mapsto x^2$ est convexe ;
— la fonction exponentielle est convexe (à ce stade, on peut le "voir" géométriquement ; nous le démontrerons au paragraphe suivant) ;
— la fonction ln est concave ;
— la fonction $x \mapsto x^3$ n'est ni concave, ni convexe ;
— la réciproque d'une bijection convexe est concave (et inversement !) : penser à la symétrie existant entre leurs courbes représentatives.

Proposition XI.16 (Inégalité de Jensen)**.** Soient $x_1, \ldots, x_n \in I$, $f : I \to \mathbb{R}_+$ une fonction convexe et $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ tels que $\sum_{k=1}^{n} \lambda_k = 1$. Alors :

$$f\left(\sum_{k=1}^{n} \lambda_k x_k\right) \leq \sum_{k=1}^{n} \lambda_k f(x_k)\,.$$

Remarque XI.15. On a nécessairement $\lambda_1 \ldots, \lambda_n \in [0,1]$.

Démonstration. Procédons par récurrence sur $n \in \mathbb{N}^*$.

— $n = 1$: trivial.
— Supposons l'inégalité vraie à un certain rang $n \geq 1$ et montrons-la pour $n+1$.
On doit donc démontrer que, si $\sum_{i=1}^{n+1} \lambda_i = 1$ alors :

$$f\left(\sum_{i=1}^{n} \lambda_i a_i + \lambda_{n+1} a_{n+1}\right) \leq \sum_{i=1}^{n} \lambda_i f\left(a_i\right) + \lambda_{n+1} f\left(a_{n+1}\right)$$

Si $\lambda_{n+1} = 0$, c'est terminé. Sinon, posons

$$\lambda_i' = \frac{\lambda_i}{1 - \lambda_{n+1}}$$

pour $i \in \{1, \ldots, n\}$ de sorte que $\lambda_1' + \ldots + \lambda_n' = 1$. L'inégalité voulue devient alors

$$f\left((1-\lambda_{n+1}) \sum_{i=1}^{n} \lambda_i' a_i + \lambda_{n+1} a_{n+1}\right) \leq (1-\lambda_{n+1}) \sum_{i=1}^{n} \lambda_i' f\left(a_i\right) + \lambda_{n+1} f\left(a_{n+1}\right).$$

Par la définition de convexité, on a d'abord

$$f\left((1-\lambda_{n+1}) \sum_{i=1}^{n} \lambda_i' a_i + \lambda_{n+1} a_{n+1}\right) \leq (1-\lambda_{n+1})\, f\left(\sum_{i=1}^{n} \lambda_i' a_i\right) + \lambda_{n+1} f\left(a_{n+1}\right),$$

et l'hypothèse de récurrence nous permet ensuite de conclure puisqu'elle nous donne

$$\begin{aligned}(1-\lambda_{n+1})\, f\left(\sum_{i=1}^{n} \lambda_i' a_i\right) + \lambda_{n+1} f\left(a_{n+1}\right) &\leq (1-\lambda_{n+1}) \sum_{i=1}^{n} \lambda_i' f\left(a_i\right) + \lambda_{n+1} f\left(a_{n+1}\right) \\ &= \sum_{i=1}^{n+1} \lambda_i f\left(a_i\right).\end{aligned}$$

□

✍ **Exercice XI.4.** Soient $x_1, \dots, x_n \in \mathbb{R}_+^*$; montrer que :

$$\left(\prod_{k=1}^{n} x_k\right)^{\frac{1}{n}} \leq \frac{1}{n}\sum_{k=1}^{n} x_k\,.$$

➥ **Correction :** *Par inégalité de Jensen, en posant $f = -\ln$, on a :*

$$f\left(\sum_{k=1}^{n} \frac{1}{n} x_k\right) \leq \sum_{k=1}^{n} \frac{1}{n} f(x_k)$$

i.e

$$\ln\left(\sum_{k=1}^{n} \frac{1}{n} x_k\right) \geq \sum_{k=1}^{n} \frac{1}{n} \ln(x_k)\,.$$

On a donc :

$$\ln\left(\left(\prod_{k=1}^{n} x_k\right)^{\frac{1}{n}}\right) \leq \ln\left(\sum_{k=1}^{n} \frac{1}{n} x_k\right)$$

d'où le résultat par croissance de la fonction exp.

b) Fonctions convexes régulières

La caractérisation géométrique des fonctions convexes évoquée *supra* se traduit par la proposition suivante, qui nous dit qu'une fonction est convexe si et seulement si les pentes de ses tangentes sont croissantes.

Proposition XI.17. Soit $f : I \to \mathbb{R}$ une fonction. Alors les propositions suivantes sont équivalentes :

(i) f est convexe ;

(ii) $\forall\, x, y, z \in I$,

$$(x < y < z) \Rightarrow \left(\frac{f(y) - f(x)}{y - x} \leq \frac{f(z) - f(x)}{z - x}\right)\ ;$$

(iii) $\forall\, x, y, z \in I$,

$$(x < y < z) \Rightarrow \left(\frac{f(y) - f(x)}{y - x} \leq \frac{f(z) - f(y)}{z - y}\right)\ ;$$

(iv) $\forall\, x, y, z \in I$,

$$(x < y < z) \Rightarrow \left(\frac{f(z) - f(x)}{z - x} \leq \frac{f(z) - f(y)}{z - y}\right)\,.$$

Démonstration. Nous allons démontrer que (i) $\Leftrightarrow$ (ii) ; on procède ensuite de façon analogue pour les deux autres assertions.

(i)⇒(ii) Si on suppose f convexe et que l'on fixe $x, y, z \in I$, tels que $x < y < z$, alors $y \in]x, z[$ et donc il existe $\lambda \in]0, 1[$ tel que $y = (1-\lambda)x + \lambda z$. Par convexité de f, on a alors :

$$f(y) = f((1-\lambda)x + \lambda z) \leq (1-\lambda)f(x) + \lambda f(z)\,.$$

Ainsi :

$$f(y) - f(x) \leq \lambda(f(z) - f(x))$$

et il nous suffit pour conclure de remarquer que $\lambda = \dfrac{y-x}{z-x}$ par définition.

(ii)⇒(i) Soient $x, z \in I$ et soit $\lambda \in]0, 1[$ (l'inégalité de convexité est triviale lorsque $\lambda \in \{0, 1\}$. Alors, en posant $y = (1-\lambda)x + \lambda z$ on a $x < y < z$ et $\lambda = \dfrac{y-x}{z-x}$. Il nous suffit alors de remonter les calculs *supra* pour vérifier que f est bien convexe.

□

Corollaire XI.17.a. Une fonction $f : I \to \mathbb{R}$ est convexe si et seulement si, pour tout $a \in I$, la fonction $x \mapsto \dfrac{f(x) - f(a)}{x - a}$ est croissante sur $I \setminus \{a\}$.

✌ **Remarque XI.16.** Ce résultat nous indique que la courbe représentative d'une fonction convexe se situe **au dessus** de ses tangentes.

La convexité d'une fonction se traduit de façon simple lorsque cette dernière est une ou deux fois dérivable, comme nous l'exposons dans la proposition suivante.

Proposition XI.18. Soit $f : I \to \mathbb{R}$ une fonction.

(i) Si f est dérivable, alors f est convexe si et seulement si f' est croissante ;

(ii) si f est deux fois dérivable, alors f est convexe si et seulement si $f'' \geq 0$.

Démonstration. (i) Découle du corollaire XI.17.a.

(ii) Découle du point (i) et du théorème XI.14.

□

Vocabulaire. Un point où f'' change de signe est appelé **point d'inflexion** de la courbe de f. Ces points correspondent à un changement de convexité de la courbe de f.

➠ **Exemple XI.14.** On démontre ainsi aisément la concavité du logarithme et la convexité de l'exponentielle. Ceci nous livre une démonstration rapide des inégalités $\ln(1+x) \leq x$ et $1 + u \leq e^u$ pour $x \in]-1, \infty$ et $u \in \mathbb{R}$.

4.⁻ Brêve extension aux fonctions à valeurs complexes

Il est aisé de vérifier qu'une fonction $f : I \to \mathbb{C}$ est dérivable si et seulement si ses parties réelle et imaginaire le sont. On en déduit par exemple que la fonction $x \mapsto e^{\alpha x}$, pour $\alpha \in \mathbb{C}$ est dérivable, de dérivée $x \mapsto \alpha e^{\alpha x}$.

✖ **Attention :** le théorème de Rolle (XI.10) et le théorème des accroissements finis (XI.11) sont faux sur $\mathbb{C}$. On a cependant une version complexe de l'inégalité des accroissements finis (corollaire XI.11.a), dont nous admettrons la démonstration pour le moment (elle découle d'une simple majoration d'intégrale).

Théorème XI.19 (Inégalité des accroissements finis, cas complexe)**.**
Soit $f : [a, b] \to \mathbb{C}$ une fonction continue sur $[a, b]$ et dérivable sur $]a, b[$ telle que :

$$\exists\, K \in \mathbb{R}_+,\ \forall x \in]a, b[,\ |f'(x)| \leq K\ .$$

Alors :

$$|f(b) - f(a)| \leq K|b - a|\ .$$

La notion de fonction convexe reposant sur des inégalités, elle ne se généralise évidemment pas aux fonctions à valeurs complexes (du moins pas sous cette forme).

Chapitre XII

Matrices, systèmes linéaires

On fixe dans tout ce chapitre un corps $\mathbb{K}$ égal à $\mathbb{R}$ ou $\mathbb{C}$.

1.⁻ Généralités

a) C'est quoi ?

Définition XII.1. Soient $n, p \in \mathbb{N}$; on appelle **matrice** à n lignes et p colonnes sur $\mathbb{K}$ toute application

$$M : [\![1, n]\!] \times [\![1, p]\!] \to \mathbb{K}\,.$$

Notation. Du point de vue pratique, nous représenterons une matrice sous la forme d'un tableau à n lignes et p colonnes, le coefficient en position (i, j) correspondant à la valeur de $M(i, j)$. Ceci donnera des objets ressemblant à :

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \\ 10 & 11 & 12 \end{pmatrix} \quad \text{ou} \quad \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \\ 10 & 11 & 12 \end{bmatrix},$$

les deux notations étant usitées aux concours.
L'ensemble des matrices à n lignes et p colonnes sera quant à lui noté $\mathscr{M}_{n,p}(\mathbb{K})$. Si $M \in \mathscr{M}_{n,p}(\mathbb{K})$, on notera généralement $m_{i,j}$ son coefficient ligne i, colonne j.

Vocabulaire.

— Lorsque $n = p$, on parle de **matrices carrées** ; l'ensemble correspondant est simplement noté $\mathscr{M}_n(\mathbb{K})$.

— On appelle **matrice diagonale** toute matrice **carrée** $M = (m_{i,j})_{i,j \in [\![1,n]\!]} \in \mathscr{M}_n(\mathbb{K})$ telle que

$$\forall (i, j) \in [\![1, n]\!]^2,\ (i \neq j) \Rightarrow (m_{i,j} = 0)\,.$$

Une telle matrice est donc de la forme :

$$\operatorname{diag}(d_1, \dots, d_n) = \begin{pmatrix} d_1 & & (0) & \\ & d_2 & & \\ & & \ddots & \\ & (0) & & d_n \end{pmatrix}$$

avec $d_1, \dots, d_n \in \mathbb{K}$. L'ensemble de ces matrices sera noté $D_n(\mathbb{K})$.

— Une **matrice scalaire** est une matrice de la forme

$$\operatorname{diag}(\lambda, \dots, \lambda) = \begin{pmatrix} \lambda & & (0) \\ & \lambda & \\ & & \ddots & \\ (0) & & & \lambda \end{pmatrix} \in \mathscr{M}_n(\mathbb{K}) \ :,$$

Les plus célèbres étant la matrice nulle et la matrice identité, respectivement :

$$\begin{pmatrix} 0 & \dots & \dots & 0 \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \dots & \dots & 0 \end{pmatrix} \quad \text{et} \quad I_n = \begin{pmatrix} 1 & & (0) \\ & 1 & \\ & & \ddots & \\ (0) & & & 1 \end{pmatrix} .$$

— On appelle **matrice triangulaire supérieure** toute matrice **carrée** $M = (m_{i,j})_{i,j \in [\![1,n]\!]} \in \mathscr{M}_n(\mathbb{K})$ telle que

$$\forall (i,j) \in [\![1,n]\!]^2, \ (i > j) \Rightarrow (m_{i,j} = 0) .$$

Une telle matrice est donc de la forme :

$$\begin{pmatrix} \star & & (\star) \\ & \star & \\ & & \ddots & \\ (0) & & & \star \end{pmatrix}$$

L'ensemble des matrices triangulaires supérieures est noté $T_n^+(\mathbb{K})$. On définit de la même façon l'ensemble $T_n^-(\mathbb{K})$ des matrices triangulaires inférieures ; on a alors naturellement :

$$T_n^+(\mathbb{K}) \cap T_n^-(\mathbb{K}) = D_n(\mathbb{K}) .$$

b) Combinaisons linéaires

Il est aisé de définir deux lois de compositions sur les matrices ; en l'occurrence :

— la somme de deux matrices $A = (a_{i,j})_{i,j}$ et $B = (b_{i,j})_{i,j}$ de $\mathscr{M}_{n,p}(\mathbb{K})$ est définie comme étant la matrice $A + B = (c_{i,j})_{i,j}$ telle que :

$$\forall (i,j) \in [\![1,n]\!] \times [\![1,p]\!], \quad c_{i,j} = a_{i,j} + b_{i,j} .$$

Ceci définit une loi de composition interne commutative sur $\mathscr{M}_{n,m}(\mathbb{K})$;

— si $M = (m_{i,j})_{i,j} \in \mathscr{M}_{n,p}(\mathbb{K})$ et $\lambda \in \mathbb{K}$, on définit la matrice $\lambda M = (a_{i,j})_{i,j}$ *via*

$$\forall (i,j) \in [\![1,n]\!] \times [\![1,p]\!], \quad a_{i,j} = \lambda m_{i,j} .$$

Ceci définit une loi de composition dite **externe** sur $\mathscr{M}_{n,p}(\mathbb{K})$ (*cf.* chapitre XVIII).

Proposition XII.1. Le couple $(\mathscr{M}_{n,p}(\mathbb{K}), +)$ est un groupe abélien. Dans le cas où $n = p$, les ensembles $D_n(\mathbb{K})$, $T_n^+(\mathbb{K})$ et $T_n^-(\mathbb{K})$ en sont des sous–groupes.

◇ **Matrices élémentaires**

Posons, pour $(i,j) \in [\![1,n]\!] \times [\![1,p]\!]$:

$$E_{i,j} = (\delta_{i,k}\delta_{j,\ell})_{(k,\ell)\in[\![1,n]\!]\times[\![1,p]\!]} ,$$

où $\delta_{i,j}$ est, pour tous objects i, j, le **symbole de Kronecker** valant 0 si $i \neq j$ et 1 sinon. Ceci signifie que tous les coefficients de la matrice $E_{i,j}$ sont nuls, à l'exception de celui situé ligne i, colonne j, qui est égal à 1 ; *e.g* pour $n = p = 2$ nous avons :

$$E_{1,1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad E_{1,2} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$E_{2,1} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad E_{2,2} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} .$$

On a alors naturellement que, si $A = (a_{i,j})_{i,j} \in \mathscr{M}_{n,p}(\mathbb{K})$:

$$A = \sum_{i=1}^{n} \sum_{j=1}^{p} a_{i,j} E_{i,j} .$$

On dit que la matrice A est **combinaison linéaire** de matrices élémentaires.

c) Produit matriciel

Définition XII.2. Soient $A = (a_{i,j})_{i,j} \in \mathscr{M}_{r,q}(\mathbb{K})$ et $B = (b_{i,j})_{i,j} \in \mathscr{M}_{q,p}(\mathbb{K})$. On appelle **produit** de A par B la matrice, notée $A \times B \in \mathscr{M}_{r,p}(\mathbb{K})$ dont le coefficient en position (i,j), pour $i \in [\![1,r]\!]$ et $j \in [\![1,p]\!]$, est :

$$\sum_{k=1}^{q} a_{i,k} b_{k,j} .$$

✖ **Attention :** il ne nous est possible de former le produit de deux matrices A et B que si leurs dimensions sont **compatibles** : il est nécessaire que le nombre de colonnes de A soit égal au nombre de lignes de B.

➠ **Exemple XII.1.**

—
$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix} .$$

— Soient $(i,j) \in [\![1,r]\!] \times [\![1,q]\!]$ et $(k,\ell) \in [\![1,q]\!] \times [\![1,p]\!]$. Alors il est possible de former le produit $E_{i,j} \times E_{k,\ell} \in \mathscr{M}_{r,p}(\mathbb{K})$ et cette matrice admet pour coefficient en position $(a,b) \in [\![1,r]\!] \times [\![1,p]\!]$:

$$\sum_{c=1}^{q} \delta_{i,a}\delta_{j,c}\delta_{c,k}\delta_{\ell,b} = \delta_{i,a}\delta_{\ell,b} \sum_{c=1}^{q} \delta_{j,c}\delta_{c,k} .$$

La somme de droite *supra* est non nulle à la seule condition que $j = k$, et égale à 1 dans ce cas, entraînant que :

$$\sum_{c=1}^{q} \delta_{i,a}\delta_{j,c}\delta_{c,k}\delta_{\ell,b} = \delta_{i,a}\delta_{\ell,b}\delta_{j,k}$$

le produit des deux symboles de Kronecker de gauche étant reconnaissable (si, si) comme le coefficient en position (a, b) de la matrice $E_{i,\ell}$. On en déduit donc que :

$$E_{i,j} \times E_{k,\ell} = \delta_{j,k} E_{i,\ell}\ .$$

Remarque XII.1.

— Le lecteur fou à lier s'empressera alors de vérifier dans la doubleur que le produit matriciel est **associatif** et **bilinéaire** (*i.e* si A, B, C sont des matrices raisonnables et $\lambda \in \mathbb{K}$, alors $(A+\lambda B)C = AC+\lambda BC$. Il est cependant, lorsque les matrices sont carrées, **non commutatif** (*cf.* paragraphe 2.⁻)

— Le produit de deux matrices triangulaires (resp. diagonales, scalaires) reste triangulaire de même "orientation" (resp. diagonal, scalaire).

— Si $A \in \mathscr{M}_{n,p}(\mathbb{K})$ et $X \in \mathscr{M}_{p,1}(\mathbb{K})$, la matrice AX est combinaison linéaire des colonnes de A.

◇ Produit par blocs

Pour manipuler des matrices de tailles plus ou moins déraisonnables, nous pourrons avoir recours à l'écriture "par blocs", *i.e* nous poserons des matrices sous la forme :

$$M = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$$

avec A, B, C, D des matrices de tailles compatibles. Il nous sera possible d'utiliser les opérations classiques sur les matrices directement sur les blocs, pour peu que ceux–ci soient raisonnables (*i.e* que les dites opérations soient légales).

Exemple XII.2. Soit $M = \begin{pmatrix} 1 & 2 & 0 \\ 3 & 4 & 0 \\ 0 & 0 & 5 \end{pmatrix}$; alors on peut écrire M sous la forme

$$M = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$$

avec $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, $B = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $C = \begin{pmatrix} 0 & 0 \end{pmatrix}$ et $D = (5)$. De fait :

$$\begin{aligned} M^2 &= \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right) \\ &= \left(\begin{array}{c|c} A^2+BC & AB+BD \\ \hline CA+DC & CB+D^2 \end{array}\right) \\ &= \left(\begin{array}{c|c} A^2 & 0 \\ \hline 0 & D^2 \end{array}\right) \end{aligned}$$

ce qui permet de déduire que :

$$M^2 = \begin{pmatrix} 7 & 10 & 0 \\ 15 & 22 & 0 \\ 0 & 0 & 25 \end{pmatrix}\ .$$

d) Transposition

Définition XII.3. Soit $A = (a_{i,j})_{i,j} \in \mathscr{M}_{n,p}(\mathbb{K})$. On appelle **transposée** de A la matrice de $\mathscr{M}_{p,n}(\mathbb{K})$ dont le coefficient en position $(i,j) \in [\![1,p]\!] \times [\![1,n]\!]$ est $a_{j,i}$.

Notation. $A^\top$.

➠ **Exemple XII.3.**

—
$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}^\top = \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix} ;$$

—
$$\begin{pmatrix} 0 & 1 & 0 \\ 2 & 2 & 42 \end{pmatrix}^\top = \begin{pmatrix} 0 & 2 \\ 1 & 2 \\ 0 & 42 \end{pmatrix} .$$

Proposition XII.2. Soient $A, B \in \mathscr{M}_{n,p}(\mathbb{K})$ et soit $\lambda \in \mathbb{K}$. Alors :

(i) $(A + \lambda B)^\top = A^\top + \lambda B^\top$;

(ii) $(A^\top)^\top = A$;

(iii) si $C \in \mathscr{M}_{p,q}(\mathbb{K})$, $(AC)^\top = C^\top A^\top$.

Démonstration. Les points (i) et (ii) sont triviaux. Pour le point (iii), fixons $(i,j) \in [\![1,p]\!] \times [\![1,n]\!]$; alors le coefficient en position (i,j) de $C^\top A^\top$ est

$$\sum_{k=0}^{p} c_{k,i} a_{j,k} .$$

Il s'agit donc bien du coefficient situé ligne j, colonne i de la matrice AC, d'où le résultat. □

✍ **Exercice XII.1.** Soit $X \in \mathscr{M}_{n,1}(\mathbb{K})$. Exprimer de façon simple la quantité $X^\top X$.

➥ **Correction :** *Posons* $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. *Alors* $X^\top X \in \mathscr{M}_{1,1}(\mathbb{K})$ *aura pour seul coefficient la quantité :*

$$\sum_{k=1}^{n} x_k^2 .$$

Définition XII.4. Soit $A \in \mathscr{M}_n(\mathbb{K})$ une matrice **carrée**. On dira que A est :

— **symétrique** si $A = A^\top$;

— **antisymétrique** si $A = -A^\top$.

Notation. On notera $\mathscr{S}_n(\mathbb{K})$ l'ensemble des matrices symétriques $n \times n$ et $\mathscr{A}_n(\mathbb{K})$ celui des matrices antisymétriques.

➠ **Exemple XII.4.** Les matrices diagonales sont symétriques. La matrice $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ est antisymétrique.

✌ **Remarque XII.2.**

— Une matrice A est symétrique si et seulement si pour tout $(i,j) \in [\![1,n]\!]^2$ on a $a_{i,j} = a_{j,i}$. De même, une telle matrice sera antisymétrique à condition d'avoir $a_{i,j} = -a_{j,i}$; en particulier, $a_{i,i} = -a_{i,i}$. La diagonale d'une matrice antisymétrique est donc toujours nulle.

— Toute combinaison linéaire de matrices symétriques (resp. anitsymétriques) reste symétrique (resp. antisymétrique).

— On a, si $M \in \mathscr{M}_n(\mathbb{K})$, on a :

$$M = \underbrace{\frac{M + M^\top}{2}}_{\in \mathscr{S}_n(\mathbb{K})} + \underbrace{\frac{M - M^\top}{2}}_{\in \mathscr{A}_n(\mathbb{K})},$$

cette décomposition étant unique (pourquoi ?).

2.– L'anneau $\mathscr{M}_n(\mathbb{K})$

a) Qui est-ce ?

Proposition XII.3. Soit $n \geq 0$. Alors $(\mathscr{M}_n(\mathbb{K}), +, \times)$ est un anneau.

Démonstration. Il s'agit d'une synthèse des propriétés évoquées précédemment dans ce chapitre. Notons que le neutre pour le produit matriciel dans $\mathscr{M}_n(\mathbb{K})$ est la matrice identité I_n. □

✖ **ATTENTION :** cet anneau n'est évidemment **PAS** commutatif dés que $n \geq 2$: en effet

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

et

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

⋄ Abominations diverses

L'anneau $\mathscr{M}_n(\mathbb{K})$ n'est pas un endroit particulièrement bien famé ; on y trouve divers objets inconnus dans des contrées civilisées, dont nous donnons quelques exemples ci–ensuite, de façon à encourager notre lecteur à une saine paranoïa en matière de calcul matriciel.

Diviseurs de zéro. La nullité d'un produit matriciel n'entraîne absolument pas celle de l'un des facteurs ; par exemple :

$$\begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} .$$

L'anneau $\mathscr{M}_n(\mathbb{K})$ n'est donc PAS intègre (sauf si $n = 1$).

Nilpotents. Pire, certaines matrices non nulles ont la discourtoisie d'admettre une puissance nulle ; par exemple :

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} .$$

Compte tenu de ces exemples, il serait réellement de mauvais ton de considérer le produit matriciel comme intègre. À bon entendeur ...

◇ Binôme de Newton

Notons, en contraste avec le musée des horreurs *supra*, que si deux matrices $A, B \in \mathscr{M}_n(\mathbb{K})$ sont telles que $AB = BA$ (on dit qu'elles **commutent**), nous disposons de la formule du binôme de Newton (proposition VIII.12), pour $p \in \mathbb{N}$:

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

✍ **Exercice XII.2.** Calculer les puissances successives de la matrice $A = \begin{pmatrix} 3 & 0 & 1 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$.

➥ **Correction :** *Remarquons que $A = D + N$ avec*

$$D = 3I_3 \quad \textit{et} \quad N = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} ,$$

ces deux matrices commutant. De plus, pour tout $k \geq 2$, on a $N^k = 0$, ce qui entraîne que, pour tout $p \in \mathbb{N}^*$:

$$\begin{aligned} A^p &= (D + N)^p \\ &= \sum_{k=0}^{p} \binom{p}{k} N^k D^{p-k} \\ &= N^0 D^p + pND^{p-1} \\ &= 3^p I_3 + p3^{p-1} N \\ &= \begin{pmatrix} 3^p & 0 & p3^{p-1} \\ 0 & 3^p & 0 \\ 0 & 0 & 3^p \end{pmatrix} \end{aligned}$$

b) Groupe linéaire

Définition XII.5. Le groupes des inversibles de l'anneau $(\mathscr{M}_n(\mathbb{K}), +, \times)$ est appelé **groupe linéaire** d'ordre n sur $\mathbb{K}$.

Notation. $GL_n(\mathbb{K}) = \mathscr{M}_n(\mathbb{K})^\times$.

✖ **Attention :** seules les matrices **carrées** peuvent être inversibles. De plus, en raison du caractère non commutatif de l'anneau $\mathscr{M}_n(\mathbb{K})$, il convient de ne pas oublier que (*cf.* chapitre VIII) :

$$\forall A, B \in GL_n(\mathbb{K}), \quad (AB)^{-1} = B^{-1}A^{-1} .$$

➠ **Exemple XII.5.** Soient $a, b, c, d \in \mathbb{R}$; alors on peut vérifier que $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est inversible si et seulement si $ad - bc \neq 0$. On a alors :

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} .$$

✌ **Remarque XII.3.** Nous verrons dans le paragraphe 3.– une méthode de calcul pratique de l'inverse d'une matrice carrée inversible.

Proposition XII.4. Soit $A \in GL_n(\mathbb{K})$. Alors $A^\top \in GL_n(\mathbb{K})$ et $(A^{-1})^\top = (A^\top)^{-1}$

Démonstration. Il s'agit d'un corollaire de la proposition XII.2. □

3.– Systèmes linéaires

a) Définition

Définition XII.6. Soient $p, q \in \mathbb{N}^*$. On appelle **système linéaire** à p équations et q inconnues toute famille d'équations de la forme :

$$\forall i \in [\![1, p]\!], \quad \sum_{j=1}^{q} a_{i,j}x_j = b_i$$

avec les $a_{i,j}, b_i \in \mathbb{K}$ fixés et les x_i inconnus scalaires.

✌ **Remarque XII.4.** Un tel système est équivalent à une **équation matricielle** du type

$$AX = B$$

avec $A=(a_{i,j})_{i,j}\in\mathscr{M}_{p,q}(\mathbb{K})$, $X=\begin{pmatrix}x_1\\ \vdots\\ x_q\end{pmatrix}\in\mathscr{M}_{q,1}(\mathbb{K})$ et $B=\begin{pmatrix}b_1\\ \vdots\\ b_p\end{pmatrix}\in\mathscr{M}_{p,1}(\mathbb{K})$.

Dans ce cas, A est appelée **matrice du système**, B son **second membre** et X son **inconnue**.

Exemple XII.6. Le système linéaire

$$\begin{cases} 2x+3y+z &= 1\\ x-y &= 42\end{cases}$$

peut s'écrire sous la forme

$$\underbrace{\begin{pmatrix}2 & 3 & 1\\ 1 & -1 & 0\end{pmatrix}}_{A}\underbrace{\begin{pmatrix}x\\ y\\ z\end{pmatrix}}_{X}=\underbrace{\begin{pmatrix}1\\ 42\end{pmatrix}}_{B}.$$

Définition XII.7. On considère un système linéaire $AX=B$. Alors :
- on dira que le système est **compatible** si il admet au moins une solution $X\in\mathscr{M}_{q,1}(\mathbb{K})$;
- le système sera dit **homogène** si $B=0$.

Remarque XII.5. Tout système homogène est compatible : $X=0$ est solution.

Proposition XII.5. Soit $A\in\mathscr{M}_{p,q}(\mathbb{K})$ et soit $B\in\mathscr{M}_{p,1}(\mathbb{K})$. Alors, lorsque ce dernier est compatible, les solutions du système $AX=B$ sont de la forme X_0+X_H avec X_0 une solution particulière du système et X_H une solution du système homogène $AX=0$.

Démonstration. Il s'agit d'une analyse–synthèse immédiate. □

b) Opérations élémentaires

Pour résoudre un système linéaire, il nous est possible de faire usage des opérations suivantes, dites **élémentaires**, sur les lignes L_i du système :

(A) …échanger la position de deux lignes dans le système ($L_i\leftrightarrow L_j$) ;

(B) …multiplier une ligne par un nombre réel **non nul** λ ($L_i\leftarrow\lambda L_j$) ;

(C) …ajouter à une ligne une combinaison linéaire des **autres** $\left(L_i\leftarrow u_i+\sum_{j\neq i}\lambda_j L_j\right)$.

Il est possible de donner une vision totalement matricielle de ces opérations élémentaires, que nous donnons ici.

Nous fixons dans tout ce paragraphe une matrice $A=(a_{i,j})_{i,j}\in\mathscr{M}_{p,q}(\mathbb{K})$.

Rappelons que nous avons défini précédemment la matrice $E_{k,l} \in \mathscr{M}_q(\mathbb{K})$ dont le coefficient en position (i,j) est $\delta_{i,k}\delta_{j,\ell}$.

Alors, pour $(i,j) \in ([\![1,p]\!] \times [\![1,q]\!])$, le coefficient situé en position (i,j) de la matrice $AE_{k,\ell} \in \mathscr{M}_{p,q}(\mathbb{K})$ est :

$$\sum_{s=1}^{q} a_{i,s}\delta_{s,k}\delta_{j,\ell} = a_{i,k}\delta_{j,\ell}$$

et donc, si l'on note $C_1, \ldots, C_q$ les colonnes de la matrice A on a :

$$AE_{k,\ell} = \left(\begin{array}{c|c|c|c|c|c|c} 0 & \ldots & 0 & C_k & 0 & \ldots & 0 \end{array} \right),$$

la colonne C_k se situant en position ℓ. De la même façon, on vérifie que, si on note $L_1, \ldots, L_p$ les lignes de A :

$$E_{k,\ell}A = \left(\begin{array}{c} 0 \\ \hline \vdots \\ \hline 0 \\ \hline L_\ell \\ \hline 0 \\ \hline \vdots \\ \hline 0 \end{array} \right) \in \mathscr{M}_p(\mathbb{K})$$

la ligne L_ℓ se situant en position k.

✖ **Attention :** Les matrices élémentaires SUPRA ne sont pas de mêmes dimension : la première est $q \times q$, la seconde $p \times p$ ...Nous allons commettre ce type d'abus tout au long de ce paragraphe.

◇ Multiplication par un scalaire

Soit $\lambda \in \mathbb{K}$; posons $n \in \{p,q\}$, $\ell \in [\![1,n]\!]$ et :

$$M_\ell^\lambda = I_n + (\lambda - 1)E_{\ell,\ell}\,.$$

Les calculs du paragraphe précédent nous permettent d'affirmer que :

(i) l'opération élémentaire $C_\ell \leftarrow \lambda C_\ell$ sur A est équivalente au calcul du produit AM_ℓ^λ (pour $n = q$) ;

(ii) l'opération élémentaire $L_\ell \leftarrow \lambda L_\ell$ sur A est équivalente au calcul du produit $M_\ell^\lambda A$ (pour $n = p$).

◇ Échange

On pose, pour $n \in \{p,q\}$ et $i,j \in [\![1,n]\!]$: :

$$X_{i,j} = I_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}\,.$$

On vérifie alors que :

(i) l'opération élémentaire $C_i \leftrightarrow C_j$ est équivalente au calcul du produit $AX_{i,j}$ (pour $n = q$) ;

(ii) l'opération élémentaire $L_i \leftrightarrow L_j$ est équivalente au calcul du produit $X_{i,j}A$ (pour $n = p$).

◇ **Combinaisons linéaires**

Pour $\lambda \in \mathbb{K}$, $n \in \{p, q\}$ et $i, j \in [\![1, n]\!]$, on pose :

$$\Omega_{i,j}^{\lambda} = I_n + \lambda E_{i,j} .$$

Il est alors aisé de vérifier que :

(i) l'opération élémentaire $C_j \leftarrow C_j + \lambda C_i$ sur A est équivalente au calcul du produit $A\Omega_{i,j}^{\lambda}$ (pour $n = q$) ;

(ii) l'opération élémentaire $L_i \leftarrow L_i + \lambda L_j$ sur A est équivalente au calcul du produit $\Omega_{i,j}^{\lambda}A$ (pour $n = p$).

◇ **Conséquences**

La vision exposée *supra* des opérations élémentaires nous permet de démontrer que :

— les opérations élémentaires préservent l'inversibilité ;

— les opérations élémentaires sur les lignes ne modifient pas les solutions d'un système linéaire.

Ceci offre donc une justification théorique à l'algorithme du pivot, présenté *infra*.

c) Pivot de Gauss

L'objet de ce chapitre est de présenter une vision matricielle et générale de l'algorithme exposé dans le chapitre II. Nous ferons volontairement l'impasse sur diverses technicités et justification théoriques.

◇ **Cas d'étude**

On se place dans ce paragraphe dans le cas d'un système linéaire de la forme $AX = B$ avec $A = (a_{i,j})_{i,j} \in \mathscr{M}_{p,q}(\mathbb{K})$ et $B = \begin{pmatrix} b_1 \\ \vdots \\ b_p \end{pmatrix} \in \mathscr{M}_{p,1}(\mathbb{K})$. Son inconnue est de la forme $X = \begin{pmatrix} x_1 \\ \vdots \\ x_q \end{pmatrix} \in \mathscr{M}_{q,1}(\mathbb{K})$.

◇ **Initialisation**

Si A est la matrice nulle. Nous avons entière confiance en la capacité de notre lecteur à résoudre le système linéaire étudié.

Dans le cas contraire, la matrice A admet *a minima* un coefficient non nul. Quitte à échanger des lignes (équations) ou colonnes (**inconnues** : prendre garde à ne pas oublier que l'on a procédé à cet échange !), il nous est possible de supposer que $a_{1,1} \neq 0$.

On effectue alors les opérations élémentaires suivantes (dans l'ordre) sur les matrices A **et** B :

— $L_1 \leftarrow \dfrac{1}{a_{1,1}} L_1$;

— $L_i \leftarrow L_i - a_{i,1} L_1$ pour $i \in [\![2, p]\!]$.

Nous venons de transformer notre système en un autre, noté $A_1X = B_1$, tel que la matrice A_1 ait la forme suivante :

$$A_1 = \begin{pmatrix} 1 & & \\ 0 & (\star) & \\ \vdots & & \\ 0 & & \end{pmatrix}.$$

◇ **Hérédité**

L'objectif de cette étape est de donner un procédé permettant de transformer (*via* équivalence matricielle) un système linéaire de la forme $A_kX = B_k$ avec

$$A_k = \left(\begin{array}{c|c} I_k & (\star) \\ \hline 0 & (\star) \end{array}\right) \in \mathscr{M}_{p,q}(\mathbb{K})$$

en un système de la forme $A_{k+1}X = B_{k+1}$, avec

$$A_{k+1} = \left(\begin{array}{c|c} I_{k+1} & (\star) \\ \hline 0 & (\star) \end{array}\right).$$

Quitte à opérer sur les lignes et (prudemment) sur les colonnes, nous pouvons supposer que $a_{k+1,k+1} \neq 0$ (à moins d'avoir déjà terminé, ce qui est une excellente nouvelle !). Il nous suffit alors d'effectuer les opérations élémentaires suivantes :

— $L_{k+1} \leftarrow \dfrac{1}{a_{k+1,k+1}} L_{k+1}$;

— $L_i \leftarrow L_i - a_{i,k+1}L_{k+1}$ pour $i \neq k+1$.

Une fois ce procédé terminé, on itère jusqu'à tomber sur une matrice A_r peut être transformée, quitte à opérer sur les lignes, en :

$$A' = \left(\begin{array}{c|c} I_r & (\star) \\ \hline 0 & 0 \end{array}\right).$$

Le système peut alors être résolu par remontée si il est compatible. Dans le cas contraire, une équation contradictoire apparaîtra, mettant fin à nos efforts. Notons que dans le cas compatible certaines inconnues peuvent ne pas être déterminées de façon unique : cela signifie que l'on dispose de familles de solution à paramètres, les valeurs de ces derniers pouvant être choisies arbitrairement.

d) Inversion d'une matrice carrée

Nommés ainsi en l'honneur du mathématicien et philosophe genevois Gabriel Cramer (1704—1752), les systèmes de Cramer représentent d'une certaine façon le "cas idéal" de l'étude des systèmes linéaires.

Définition XII.8. Un système linéaire est dit **de Cramer** si :

(i) il admet autant d'équations que d'inconnues ;

(ii) sa matrice est inversible.

✌ **Remarque XII.6.** En résumé, un système de Cramer est un système linéaire de la forme $AX = B$ avec $A \in GL_p(\mathbb{K})$.

➠ **Exemple XII.7.** Le système

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

est de Cramer.

✌ **Remarque XII.7.** Soit $AX = B$ un système de Cramer. Alors il admet une unique solution, donnée par $X = A^{-1}B$.

Pour déterminer l'inverse d'une matrice $A \in GL_n(\mathbb{K})$, on peut donc lui appliquer le pivot de Gauss jusqu'à obtenir la matrice I_n. Si l'on effectue les mêmes opérations élémentaires, dans le même ordre, sur la matrice identité, on obtient la matrice inverse A^{-1}. On parle alors de **méthode de Gauss–Jordan**.

➠ **Exemple XII.8.** Déterminons l'inverse de la matrice $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{pmatrix}$. Pour ce faire, nous partons de :

$$\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 4 & 5 & 6 & 0 & 1 & 0 \\ 7 & 8 & 10 & 0 & 0 & 1 \end{array}$$

et effectuons les opérations $L_2 \leftarrow L_2 - 4L_1$ et $L_3 \leftarrow L_3 - 7L_1$, obtenant :

$$\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 0 & -6 & -11 & -7 & 0 & 1 \end{array}.$$

Nous effectuons ensuite $L_2 \leftarrow \dfrac{-1}{3} L_2$:

$$\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & \frac{4}{3} & -\frac{1}{3} & 0 \\ 0 & -6 & -11 & -7 & 0 & 1 \end{array}$$

puis $L_1 \leftarrow L_1 - 2L_2$ et $L_3 \leftarrow L_3 + 6L_2$:

$$\begin{array}{ccc|ccc} 1 & 0 & -1 & -\frac{5}{3} & \frac{2}{3} & 0 \\ 0 & 1 & 2 & \frac{4}{3} & -\frac{1}{3} & 0 \\ 0 & 0 & 1 & 1 & -2 & 1 \end{array}$$

avant de conclure par $L_1 \leftarrow L_1 + L_3$ et $L_2 \leftarrow L_2 - 2L_3$:

$$\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{2}{3} & -\frac{4}{3} & 1 \\ 0 & 1 & 0 & -\frac{2}{3} & \frac{11}{3} & -2 \\ 0 & 0 & 1 & 1 & -2 & 1 \end{array}.$$

In fine, on trouve :

$$A^{-1} = \begin{pmatrix} -\frac{2}{3} & -\frac{4}{3} & 1 \\ -\frac{2}{3} & \frac{11}{3} & -2 \\ 1 & -2 & 1 \end{pmatrix}.$$

Une conséquence de ce procédé est le résultat suivant, fort utile au demeurant et sur lequel nous reviendrons dans le chapitre XXI.

Proposition XII.6. Soit $M = (m_{i,j})_{i,j \in [\![1,n]\!]}$ une matrice triangulaire de $\mathscr{M}_n(\mathbb{K})$. Alors :

$$M \in GL_n(\mathbb{K}) \iff \forall k \in [\![1,n]\!],\ m_{k,k} \neq 0\,.$$

Dans ce cas, l'inverse de M est également triangulaire, dans le même "sens" que M.

✍ **Exercice XII.3.** Retrouver l'inverse de la matrice $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{pmatrix}$ en résolvant un système linéaire.

Chapitre XIII

Équations différentielles

On fixe dans ce paragraphe un corps $\mathbb{K}$ égal à $\mathbb{R}$ ou $\mathbb{C}$ et un intervalle I de $\mathbb{R}$ d'intérieur non vide.

1.⁻ Primitives

a) C'est quoi ?

Définition XIII.1. Soit $f : I \to \mathbb{K}$. Une **primitive** de f est une application $F : I \to \mathbb{K}$ telle que :
- $F \in \mathscr{D}^1(I)$;
- $F' = f$.

Exemple XIII.1. Soit $\alpha \in \mathbb{C} \setminus \{-1\}$. Alors la fonction

$$f : \mathbb{R}_+^* \to \mathbb{R}, \quad x \mapsto x^\alpha$$

admet pour primitive $F : x \mapsto \dfrac{x^{\alpha+1}}{\alpha+1}$.

Le résultat qui suit devra pour l'instant être admis. Nous le démontrerons au chapitre XX.

Théorème XIII.1.
Soit $f \in \mathscr{C}^0(I)$. Alors :
- f admet une infinité de primitives ;
- si F et $\hat{F}$ sont deux primitives de f, la fonction $F - \hat{F}$ est constante.

Notation.
- Soit $f \in \mathscr{C}^0(I)$ et soit F une primitive de f. SI $a, b \in I$ on appellera **intégrale de f entre a et b** la quantité :

$$\int_a^b f(t)\,\mathrm{d}t := F(b) - F(a)\ .$$

Il est aisé de vérifier que cette dernière ne dépend pas du choix de la primitive F. De plus, la dérivation étant linéaire, l'intégrale l'est naturellement.

— On pourra également noter $x \mapsto \int^x f(t)\,\mathrm{d}t$ une primitive générique d'une fonction $f \in \mathscr{C}^0(I)$ lorsqu'il ne sera pas pertinent de déterminer la constante d'intégration.

✌ **Remarque XIII.1.** Il découle de la "définition" donnée *supra* de l'intégrale que, pour tous $a, x \in I$:

$$\frac{\mathrm{d}}{\mathrm{d}x} \int_a^x f(t)\,\mathrm{d}t = f(x)\ .$$

◇ Primitives usuelles

Il suffit de lire "à l'envers" le tableau des dérivées usuelles pour obtenir ceci. Nous verrons plus tard comment obtenir les primitives "moins évidentes" des fonctions usuelles omises *infra*.

Valeur de $f(x)$	**Ensemble de continuité**	**Valeur d'une primitive**
x^α $(\alpha \neq -1)$	$\mathbb{R}_+^*$	$\frac{x^{\alpha+1}}{\alpha+1}$
$\frac{1}{x}$	$\mathbb{R}_+^*$	$\ln(x)$
e^{ax} $(a \in \mathbb{C}^*)$	$\mathbb{R}$	$\frac{1}{a}e^{ax}$
a^x $(a > 0,\, a \neq 1)$	$\mathbb{R}$	$\frac{a^x}{\ln(a)}$
$\cos(x)$	$\mathbb{R}$	$\sin(x)$
$\sin(x)$	$\mathbb{R}$	$-\cos(x)$
$-\frac{1}{\sqrt{1-x^2}}$	$]-1,1[$	$\arccos(x)$
$\frac{1}{\sqrt{1-x^2}}$	$]-1,1[$	$\arcsin(x)$
$\frac{1}{1+x^2}$	$\mathbb{R}$	$\arctan(x)$
$\mathrm{ch}(x)$	$\mathbb{R}$	$\mathrm{sh}(x)$
$\mathrm{sh}(x)$	$\mathbb{R}$	$\mathrm{ch}(x)$

✌ **Remarque XIII.2.** Le fait de savoir déterminer une primitive de $x \mapsto e^{ax}$ pour $a \in \mathbb{C}^*$ permet de faire de même pour les fonctions du type $x \mapsto e^{ux}\cos(vx)$ et $x \mapsto e^{ux}\sin(vx)$.

b) Outils calculatoires

◇ Reconnaître une forme composée usuelle

Cette méthode est transparente : si on reconnaît la dérivée d'une composée, c'est gagné. Par exemple, la primitive de $x \mapsto \dfrac{\ln(x)}{x}$ est $x \mapsto \dfrac{1}{2}(\ln(x))^2$ et celle de $x \mapsto \dfrac{1}{x\ln(x)}$ est $\ln \circ \ln$. Même chose pour déterminer une primitive de tan et th.

✍ **Exercice XIII.1.** Déterminer toutes les fonctions $y \in \mathscr{C}^1(\mathbb{R}_+, \mathbb{R}_+^*)$ telles que $\forall x \in \mathbb{R},\ y'(x) = \sqrt{y(x)}$.

➥ **Correction :** *On procède par analyse–synthèse : si y est une telle fonction, elle ne s'annule pas et donc on a :*

$$\forall x \in \mathbb{R}_+, \qquad \frac{y'(x)}{\sqrt{x}} = 1\ .$$

Ceci entraîne que :

$$\forall x \in \mathbb{R}_+, \qquad \frac{\mathrm{d}}{\mathrm{d}x}\sqrt{y(x)} = \frac{1}{2}$$

et donc il existe $c \in \mathbb{R}_+$ tel que :

$$\forall x \in \mathbb{R}_+, \quad \sqrt{y(x)} = \frac{x}{2} + c, \quad i.e \quad y(x) = \left(\frac{x}{2} + c\right)^2 .$$

On vérifie ensuite aisément que ces fonctions sont bien solutions de l'équation initiale.

◇ Intégration par parties (IPP)

Proposition XIII.2. Soient f et g deux fonctions **de classe** $\mathscr{C}^1$ sur I. Alors, pour tous $a, b \in I$:

$$\int_a^b f'(t)g(t)\,\mathrm{d}t = [f(t)g(t)]_a^b - \int_a^b f(t)g'(t)\,\mathrm{d}t\,,$$

avec

$$[f(t)g(t)]_a^b = f(b)g(b) - f(a)g(b)\,.$$

Démonstration. Il suffit de remarquer que la fonction fg est une primitive de $(fg)'$; on a donc :

$$\begin{aligned}[f(t)g(t)]_a^b &= \int_a^b (fg)'(t)\,\mathrm{d}t \\ &= \int_a^b f'(t)g(t)\,\mathrm{d}t + \int_a^b f(t)g'(t)\,\mathrm{d}t\end{aligned}$$

d'où le résultat. □

✖ **Attention :** il est absolument **essentiel** de bien préciser le caractère $\mathscr{C}^1$ de f et g lorsque l'on fait une IPP.

Cette proposition est extrêmement utile pour calculer les primitives de produits dont l'un des termes est peu sensible à la dérivation et/ou contenant un terme polynomiale (qui disparaîtra après un certain nombre de dérivées). En particulier, toutes les constructions de la forme "polynôme × exponentielle" et "polynôme × cosinus ou sinus" devront être traitées de la sorte.

✍ **Exercice XIII.2.** Soit $n \geq 1$ et $x \in \mathbb{R}$. Déterminer

$$I_n(x) := \int_0^x t^n e^{-t}\,\mathrm{d}t\,.$$

➥ **Correction :** *Les fonctions $t \mapsto t^n$ et $t \mapsto -e^{-t}$ (primitive de $t \mapsto e^{-t}$) étant de classe $\mathscr{C}^1$ sur $[0, x]$, nous pouvons procéder par IPP (proposition XIII.2) :*

$$\begin{aligned}I_n(x) &= \left[t^n(-e^{-t})\right]_0^x - \int_0^x nt^{n-1}(-e^{-t})\,\mathrm{d}t \\ &= -x^n e^{-x} + nI_{n-1}(x)\,.\end{aligned}$$

Ceci constitue une relation de récurrence ; il est ensuite aisé de démontrer que :

$$\begin{aligned}
I_n(x) - x^n e^{-x} + nI_{n-1}(x) & \\
&= -x^n e^{-x} + n(-x^{n-1}e^{-x} + (n-1)I_{n-2}(x)) \\
&\vdots \\
&= -x^n e^{-x} - \sum_{k=2}^{n} n \times \ldots \times k\, x^{k-1} e^{-x} + n! I_0(x) \\
&= - - x^n e^{-x} - \sum_{k=2}^{n} \frac{n!}{(k-1)!} x^{k-1} e^{-x} + n!(1 - e^{-x}) \\
&= -\sum_{k=2}^{n+1} \frac{n!}{(k-1)!} x^{k-1} e^{-x} + n!(1 - e^{-x})
\end{aligned}$$

◇ Changement de variable

Théorème XIII.3.
Soit $\varphi \in \mathscr{C}^1(I)$ et soit $f \in \mathscr{C}^0(\varphi(I))$. Alors, pour tous $a, b \in I$ on a :

$$\int_{\varphi(a)}^{\varphi(b)} f(x)\,\mathrm{d}x = \int_a^b f \circ \varphi(t) \varphi'(t)\,\mathrm{d}t\,.$$

Démonstration. Soit F une primitive de f sur $\varphi(I)$ (une telle fonction existe par continuité, *cf.* théorème XIII.1). Alors :

$$\begin{aligned}
\int_a^b f \circ \varphi(t)\varphi'(t)\,\mathrm{d}t &= \int_a^b F' \circ \varphi(t)\varphi'(t)\,\mathrm{d}t \\
&= \int_a^b (F \circ \varphi)'(t)\,\mathrm{d}t \\
&= [F \circ \varphi]_a^b \\
&= F(\varphi(b)) - F(\varphi(a)) \\
&= \int_{\varphi(a)}^{\varphi(b)} f(x)\,\mathrm{d}x\,.
\end{aligned}$$

□

Cette technique de calcul peut paraître un peu déroutante au début ; il est possible de la visualiser "à la physicienne" de la façon suivante : si $x = \varphi(t)$ alors :

$$\begin{aligned}
\int_{\varphi(a)}^{\varphi(b)} f(x)\,\mathrm{d}x &= \int_a^b f(\varphi(t))\,\mathrm{d}(\varphi(t)) \\
&= \int_a^b f \circ \varphi(t)\varphi'(t)\,\mathrm{d}t\,.
\end{aligned}$$

➠ **Exemple XIII.2.**

— Calculons l'intégrale
$$\int_0^1 \frac{e^x}{1+e^{2x}}\,\mathrm{d}x$$
par changement de variable. Pour ce faire, nous posons $\varphi : t \mapsto \ln(t)$; cette fonction est de classe $\mathscr{C}^1$ sur $[1, e]$ d'image $[0, 1]$ (nous cherchons donc à "poser $x = \ln(t)$"). On a donc :
$$\begin{aligned}\int_0^1 \frac{e^x}{1+e^{2x}}\,\mathrm{d}x &= \int_1^e \frac{t}{1+t^2}\frac{\mathrm{d}t}{t}\\ &= \int_1^e \frac{1}{1+t^2}\,\mathrm{d}t\\ &= \arctan(e) - \frac{\pi}{4}\,.\end{aligned}$$

— De la même façon, on peut calculer (pour $u \in [-1, 1]$)
$$\int_0^u \arccos(x)\,\mathrm{d}x$$
en posant $\varphi : t \mapsto \cos(t)$. On obtient :
$$\int_0^u \arccos(x)\,\mathrm{d}x = -\int_{\frac{\pi}{2}}^{\arccos(u)} t\sin(t)\,\mathrm{d}t$$
que nous pouvons ensuite calculer par IPP en remarquant que $t \mapsto t$ et $\cos(t)$ sont de classe $\mathscr{C}^1$ sur notre intervalle, *i.e*
$$\begin{aligned}\int_0^u \arccos(x)\,\mathrm{d}x &= -\left[-t\cos(t)\right]_{\frac{\pi}{2}}^{\arccos(u)} + \int_{\frac{\pi}{2}}^{\arccos(u)} (-\cos(t))\,\mathrm{d}t\\ &= u\mathrm{arcos}(u) + \int_{\arccos(u)}^{\frac{\pi}{2}} \cos(t)\,\mathrm{d}t\\ &= u\mathrm{arcos}(u) + 1 - \sin(\arccos(u))\\ &= u\mathrm{arcos}(u) + 1 - \sqrt{1-u^2}\,.\end{aligned}$$

◇ Primitives des inverses de trinômes du second degré

L'objectif de ce paragraphe est de déterminer les primitives des fonctions de la forme
$$f : x \mapsto \frac{1}{ax^2+bx+c}$$
avec $a, b, c \in \mathbb{C}$.

Cas 1 : $a \neq 0$. Posons alors $\Delta = b^2 - 4ac$ et distinguons deux sous–cas.

Cas 1.1 : $\Delta \neq 0$. Alors il existe $r_1, r_2 \in \mathbb{C}$ tels que pour tous $x \in \mathbb{R}$, $ax^2 + bx + c = a(x - r_1)(x - r_2)$. Cherchons à déterminer $\lambda, \mu \in \mathbb{C}$ tels que :
$$\forall x \in \mathbb{R} \setminus \{r_1, r_2\},\ f(x) = \frac{\lambda}{x-r_1} + \frac{\mu}{x-r_2}\,.$$
Pour ce faire, nous multiplions cette égalité par $x - r_1$:
$$f(x)(x-r_1) = \lambda + \mu\frac{x-r_1}{x_2}$$

puis évaluons en $x = r_1$, ce qui nous donne

$$\lambda = \frac{1}{a(r_1 - r_2)} .$$

En procédant de même pour μ, nous obtenons que :

$$\forall x \in \mathbb{R} \setminus \{r_1, r_2\},\ f(x) = \frac{1}{a(r_1 - r_2)} \left(\frac{1}{x - r_1} - \frac{1}{x - r_2} \right)$$

et donc admet pour primitive, si $r_1, r_2 \in \mathbb{R}$:

$$\begin{aligned} F : \mathbb{R} \setminus \{r_1, r_2\} &\longrightarrow \mathbb{C} \\ x &\mapsto \frac{1}{a(r_1 - r_2)} (\ln(|x - r_1|) - \ln(|x - r_2|)) . \end{aligned}$$

Si les racines sont complexes, il suffit de remarquer que, pour tout x raisonnable et $p, q \in \mathbb{R}$:

$$\begin{aligned} \frac{1}{x - (p + iq)} &= \frac{1}{(x - p) - iq} \\ &= \frac{(x - p) + iq}{(x - p)^2 + q^2} \end{aligned}$$

et donc cette quantité admet pour primitive

$$x \mapsto \frac{1}{2} \ln((x - p)^2 + q^2) + i \arctan\left(\frac{x - p}{q}\right) .$$

Cas 1.2 : $\Delta = 0$**.** Dans ce cas, il existe $r \in \mathbb{C}$ tel que f soit la fonction

$$f : x \mapsto \frac{1}{a(x - r)^2}$$

de primitive

$$\begin{aligned} F : \mathbb{R} \setminus \{r\} &\to \mathbb{C} \\ x &\mapsto -\frac{1}{a(x - r)} . \end{aligned}$$

Cas 2 : $a = 0$**.** Si $b = 0$, c'est trivial. Sinon, on a pour tout $x \neq \frac{-c}{b}$:

$$f(x) = \frac{1}{b} \frac{b}{bx + c}$$

et donc f admet pour primitive, si $b, c \in \mathbb{R}$:

$$\begin{aligned} F : \mathbb{R} \setminus \left\{ -\frac{c}{b} \right\} &\to \mathbb{C} \\ x &\mapsto \frac{1}{b} \ln(|bx + c|) . \end{aligned}$$

Notons que si $-\frac{c}{b} \notin \mathbb{R}$, $\mathbb{R} \setminus \left\{ -\frac{c}{b} \right\} = \mathbb{R}$. Dans le cas où b ou c n'est pas réel, on obtient en suivant la même méthode que dans le cas 2.1 une primitive combinaison linéaire d'un logarithme et d'une arc tangente.

2.⁻ Équations différentielles linéaires du premier ordre

a) C'est quoi ?

Définition XIII.2. Soient $a, b \in \mathscr{C}^0(I, \mathbb{K})$; on appelle **équation différentielle linéaire d'ordre** 1 l'équation

$$y' + ay = b \qquad (\mathscr{E})$$

d'inconnue $y \in \mathscr{D}^1(I, \mathbb{K})$. L'**équation homogène associée** à $(\mathscr{E})$ est alors :

$$y' + ay = 0 \qquad (\mathscr{H})\ .$$

Vocabulaire. La fonction a est appelée **coefficient** de l'équation, la fonction b est quand à elle dénommée **second membre** de celle–ci.

Remarque XIII.3.
- **Résoudre** une équation différentielle linéaire d'ordre 1 revient à déterminer l'ensemble
$$\mathrm{Sol}_{\mathscr{E}} = \{y \in \mathscr{D}^1(I) \,|\, y' + ay = b\}$$
et similairement pour l'équation homogène associée.
- Si $y \in \mathrm{Sol}_{\mathscr{E}}$, alors comme $y' = -ay + b$, y est automatiquement de classe $\mathscr{C}^1$.

Convention. Nous avons longuement évoqué le fait qu'il était déraisonnable d'écrire des choses du genre $y' + x^2 y = e^x$. C'est cependant la norme dans l'étude des équations différentielles. Ne vous posez pas trop de questions ...

Exemple XIII.3. $y' + 13y = e^{-x^2+18}$ est une équation différentielle linéaire d'ordre 1 .

b) Résolution

Proposition XIII.4. Soit $(\mathscr{E})$ une équation différentielle linéaire d'ordre 1 d'équation homogène $(\mathscr{H})$ et soit $y_0 \in \mathrm{Sol}_{\mathscr{E}}$. Alors :

$$\mathrm{Sol}_{\mathscr{E}} = \{y_0 + y \,|\, y \in \mathrm{Sol}_{\mathscr{H}}\}\ .$$

Démonstration.
($\supset$) Immédiat, il suffit de réinjecter dans $(\mathscr{E})$.
($\subset$) Soit y une solution de $(\mathscr{E})$; alors on vérifie aisément en réinjectant que $y - y_0 \in \mathrm{Sol}_{\mathscr{H}}$.
□

Cela signifie que la résolution d'une équation différentielle linéaire d'ordre 1 devra nécessairement se faire en trois temps :
1. résoudre l'équation homogène associée ;
2. déterminer une solution particulière y_0 de l'équation ;
3. combiner ces deux données via la proposition précédente.

◇ Résolution homogène

Proposition XIII.5. Soit $a \in \mathscr{C}^0(I)$; on considère l'équation différentielle linéaire d'ordre 1 homogène

$$y' + ay = 0 \qquad (\mathscr{H}) \,.$$

Alors, si A est une primitive de a :

$$\mathrm{Sol}_{\mathscr{H}} = \{x \mapsto Ce^{-A(x)} \,|\, C \in \mathbb{K}\} \,.$$

Démonstration.

($\supset$) Si y est de la forme $x \mapsto Ce^{-A(x)}$, on vérifie rapidement que $y' = -ay$.

($\subset$) Soit $y \in \mathrm{Sol}_{\mathscr{H}}$; alors, pour tout $x \in I$:

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}x}\left(y(x)e^{A(x)}\right) &= y'(x)e^{A(x)} + a(x)y(x)e^{A(x)} \\ &= \left(y'(x) + a(x)y(x)\right)e^{A(x)} \\ &= 0\end{aligned}$$

et donc la fonction $x \mapsto y(x)e^{A(x)}$ est constante car de dérivée nulle sur l'intervalle I. Ceci entraîne le résultat.

□

Remarque XIII.4. Si a est une fonction constante égale à $\kappa \in \mathbb{R}$, on a donc :

$$\mathrm{Sol}_{\mathscr{H}} = \{x \mapsto Ce^{-\kappa x} \,|\, C \in \mathbb{K}\} \,.$$

Exemple XIII.4. Résolvons l'équation

$$y' + \frac{3}{x}y = 0 \qquad (\mathscr{H})$$

sur $\mathbb{R}_+^*$. Il s'agit d'une équation différentielle linéaire d'ordre 1 homogène de coefficient $a : x \mapsto \frac{3}{x}$ continu sur $\mathbb{R}_+^*$ et de primitive $x \mapsto \ln(x^3)$. Ainsi :

$$\begin{aligned}\mathrm{Sol}_{\mathscr{H}} &= \left\{x \mapsto Ce^{-\ln(x^3)} \,\middle|\, C \in \mathbb{C}\right\} \\ &= \left\{x \mapsto \frac{C}{x^3} \,\middle|\, C \in \mathbb{C}\right\} \,.\end{aligned}$$

◇ Recherche d'une solution particulière

La seconde étape du procédé de résolution d'une équation différentielle linéaire d'ordre 1 est un tantinet moins codifiée et repose parfois sur des techniques *ad–hoc*. Nous donnons ici quelques méthodes utilisables, à compléter en TD.

Recherche d'une solution évidente. Cela arrive, parfois. Par exemple, une solution particulière de $y' + 3y = 7$ est $x \mapsto \dfrac{7}{3}$ et une solution de $y' + xy = x$ est $x \mapsto 1$. De façon générale, toujours vérifier si il existe des solutions constantes à notre équation. . .

Nous verrons en TD que l'on peut appliquer des méthodes de ce type de façon heuristique si a est constante et que b est d'une certaine forme.

Méthode de variation de la constante. L'idée de cette méthode est relativement simple : on remplace le "C" dans l'expression des solutions homogène par une fonction, faisant ainsi "varier la constante". Plus rigoureusement, on recherche une solution particulière sous la forme

$$y_0 : x \mapsto \lambda(x)e^{-A(x)}$$

où A est une primitive du coefficient a de notre équation et $\lambda \in \mathscr{C}^1(I)$. On a alors, pour tout $x \in I$:

$$\begin{aligned} y_0'(x) + a(x)y_0(x) &= \lambda'(x)e^{-A(x)} - a(x)y_0(x) + a(x)y_0(x) \\ &= \lambda'(x)e^{-A(x)} \end{aligned}$$

et donc, si b est le second membre de l'équation :

$$\lambda'(x) = b(x)e^{A(x)} .$$

Nous sommes donc en capacité de déterminer une solution particulière de l'équation à condition de savoir "primitiver" la fonction $x \mapsto b(x)e^{A(x)}$ (ce qui n'est pas automatique !).

✖ **Attention :** ne pas oublier de multiplier λ par la solution homogène à la fin du procédé !

➠ **Exemple XIII.5.** En recherchant une solution particulière de

$$y' + xy = e^{-\frac{x^2}{2}} \qquad (\mathbf{E}\ \text{:XIII.1})$$

sous la forme $y_0 : x \mapsto e^{-\frac{x^2}{2}}$, on tombe sur $\lambda' = 1$ et donc $y_0 : x \mapsto xe^{-\frac{x^2}{2}}$ convient.

✍ **Exercice XIII.3.** Résoudre l'équation :

$$(x+1)y' - xy + 1 = 0 \qquad (\mathbf{E}\ \text{:XIII.2})$$

sur $I =]-1, \infty[$.

➥ **Correction :** *Il faut commencer par mettre cette équation sous forme normale :*

$$y' - \frac{x}{x+1}y = -\frac{1}{x+1} \qquad (\mathbf{E}\ \text{:XIII.3})$$

et d'appliquer les méthodes vu précédemment ; on peut alors reconnaître une équation différentielle linéaire d'ordre 1 à coefficient et second membre continus sur I. Pour trouver une primitive du coefficient, on remarque que :

$$\forall x \in I,\ \frac{x}{x+1} = \frac{x+1-1}{x+1} = 1 - \frac{1}{x+1}$$

et donc $x \mapsto x - \ln(x+1)$ convient. Les solutions homogènes sont donc les

$$x \mapsto C\frac{e^x}{x+1}$$

pour $C \in \mathbb{C}$. La méthode de variation de la constante livre ensuite l'équation différentielle $\lambda' = -e^{-x}$ et donc les solutions de ($\mathbf{E}$:XIII.2) sont les

$$x \mapsto \frac{1}{x+1} + C\frac{e^x}{x+1}$$

pour $C \in \mathbb{C}$.

Notons que ces techniques permettent, via changement de fonction inconnue, de résoudre certaines équations différentielles non linéaires, telles les équations de Riccati (Jacopo, 1676—1754, mathématicien et juriste vénitien) *infra*.

✍ **Exercice XIII.4.** Soient $a, b \in \mathscr{C}^0(I)$. On considère l'équation suivante, d'inconnue $z \in \mathscr{C}^1(I, \mathbb{R}_+^*)$:

$$z' = a + bz + z^2\,. \qquad (\mathbf{E}\ \text{:XIII.4})$$

1. Supposons connue une solution particulière z_0 de (**E** :XIII.4).
   (a) Vérifier que (**E** :XIII.4) est équivalente à une équation du type :
   $$w' = cw + w^2\,, \quad \text{avec } c \in \mathscr{C}^0(I)\,. \qquad (\mathbf{E}\ \text{:XIII.5})$$
   (b) Démontrer que (**E** :XIII.5) est équivalente à une équation différentielle linéaire d'ordre 1 que l'on précisera.
2. Résoudre les équations de Riccati suivantes sur des intervalles pertinents :
   (a) $(x^2+1)z' = z^2 - 1$;
   (b) $x^3 z' + z^2 + zx^2 + 2x^4 = 0$;
   (c) $(z' - z^2)\cos(x) + (2\cos^2(x) + \sin(x))z = \cos^3(x)$.

➥ **Correction :**

1. (a) Soit $z \in \mathscr{C}^1(I)$; alors, en posant $w = z - z_0$, on a :

$$w' = a + bz + z^2 - a - bz_0 - z_0^2 = bw + (z^2 - z_0^2)\,.$$

Or

$$\begin{aligned} z^2 - z_0^2 &= (z - z_0)(z + z_0) \\ &= w(w + 2z_0) \\ &= w^2 + 2z_0 w \end{aligned}$$

ergo :

$$w' = (b + 2z_0)w + w^2\,.$$

*(b) Pour tout $w \in \mathscr{C}^1(I, \mathbb{R}_+^*)$, on peut poser $y = \frac{1}{w}$ et remarquer que w est solution de **E** :XIII.5 si et seulement si :*

$$\begin{aligned} y' &= \frac{-w'}{w^2} \\ &= -\frac{cw + w^2}{w^2} \\ &= -cy + 1\,. \end{aligned}$$

2. Il suffit de remarquer que 1, $x \mapsto -x^2$ et $\cos$ sont solutions particulières et d'appliquer la méthode supra.

Principe de superposition. Notons au passage que si le second membre b d'une équation différentielle linéaire d'ordre 1 est de la forme $b = \sum_{i=1}^{n} b_i$, la linéarité de l'équation entraîne qu'il suffit de déterminer une solution particulière associée à chaque b_i et des les sommer.

c) Problèmes de Cauchy

Définition XIII.3. Soient $a, b \in \mathscr{C}^0(I)$ et soit $(x_0, y_0) \in I \times \mathbb{K}$. On appelle **problème de Cauchy linéaire du premier ordre** associé à ces données le système :

$$\begin{cases} y' + ay = b \\ y(x_0) = y_0 \end{cases}$$

d'inconnue $y \in \mathscr{D}^1(I)$.

Vocabulaire. Les données x_0 et y_0 sont appelées **conditions initiales du système**.

➠ **Exemple XIII.6.**

$$\begin{cases} y' + 3y = \pi e^{-18x^9} \\ y(0) = 127\gamma + 2i \end{cases}$$

est un problème de Cauchy sur $I = \mathbb{R}$.

Théorème XIII.6 (Cauchy linéaire, ordre 1)**.**
Tout problème de Cauchy linéaire du premier ordre admet une unique solution.

Démonstration. Par variation de la constante, on sait qu'il existe une solution particulière y_p de l'équation différentielle sous–jacente. De fait, il existe une infinité de solutions de celle–ci, de la forme :

$$y : x \mapsto y_p(x) + Ce^{-A(x)}$$

avec $C \in \mathbb{K}$ et A une primitive de a. La constante C est alors déterminée par l'équation $y(x_0) = y_0$, qui entraîne que :

$$C = -y_p(x_0)e^{A(x_0)}$$

d'où le résultat. □

➠ **Exemple XIII.7.** Si on rajoute à l'équation **E** :XIII.2 la condition initiale $y(0) = 1$, l'unique solution du problème de Cauchy est :

$$y : x \mapsto \frac{1}{x+1}.$$

3.– Équations différentielles linéaires du second ordre à coefficients constants

a) C'est quoi ?

Définition XIII.4. Soient $a, b \in \mathbb{K}$ et $f \in \mathscr{C}^0(I, \mathbb{K})$. On appelle **équation différentielle linéaire d'ordre** 2 **à coefficients constants** associée à ces données l'équation

$$y'' + ay' + by = f \qquad (\mathscr{E})$$

d'inconnue $y \in \mathscr{D}^2(I, \mathbb{K})$. L'**équation homogène associée** est alors

$$y'' + ay' + by = 0 \qquad (\mathscr{H})$$

Vocabulaire. Les **constantes** a et b sont appelées **coefficients** de l'équation. La **fonction** f est appelée **second membre** de celle–ci.

✌ **Remarque XIII.5.** De la même façon que pour les équation différentielle linéaire d'ordre 1, une solution d'une telle équation sera automatiquement de classe $\mathscr{C}^2$.

➠ **Exemple XIII.8.**
— $y'' + iy' + \cos(13 + \sqrt{2}\pi)y = x^2$ est une équation différentielle linéaire d'ordre 2 à coefficients constants.
— $y'' + y = 0$ est une équation différentielle linéaire d'ordre 2 homogène à coefficients constants dont on connaît déjà deux solutions sur $\mathbb{R}$: cos et sin.

Définition XIII.5. Soit $y'' + ay' + by = 0$ une équation différentielle linéaire d'ordre 2 homogène à coefficients constants ; on appelle **équation caractéristique** associée l'équation polynomiale

$$X^2 + aX + b = 0 \qquad (\chi)\ .$$

➠ **Exemple XIII.9.** L'équation caractéristique associée à $y''+y = 0$ est $X^2+1 = 0$.

b) Résolution

Proposition XIII.7. Soit $(\mathscr{E})$ une équation différentielle linéaire d'ordre 2 à coefficients constants d'équation homogène $(\mathscr{H})$ et soit $y_0 \in \mathrm{Sol}_{\mathscr{E}}$. Alors :

$$\mathrm{Sol}_{\mathscr{E}} = \{y_0 + y \,|\, y \in \mathrm{Sol}_{\mathscr{H}}\}\ .$$

Ce résultat, analogue à celui vu pour le premier ordre, nous indique que la résolution d'une équation différentielle linéaire d'ordre 2 à coefficients constants se fera selon les mêmes "temps" que celle d'une équation différentielle linéaire d'ordre 1.

◇ Résolution homogène

Proposition XIII.8. On considère une équation différentielle linéaire d'ordre 2 homogène à coefficients constants

$$y'' + ay' + bt = 0 \qquad (\mathscr{H})$$

dont l'équation caractéristique a pour discriminant $\Delta = a^2 - 4b$. Alors :
— si $\Delta \neq 0$, l'équation caractéristique admet deux solutions distinctes $r_1, r_2 \in \mathbb{C}$ et :
$$\mathrm{Sol}_{\mathscr{H}} = \{x \mapsto \lambda e^{r_1 x} + \mu e^{r_2 x} \mid \lambda, \mu \in \mathbb{C}\} \ ;$$
— si $\Delta = 0$, l'équation caractéristique admet une unique solution $r_0 \in \mathbb{C}$ et :
$$\mathrm{Sol}_{\mathscr{H}} = \{x \mapsto (\lambda x + \mu) e^{r_0 x} \mid \lambda, \mu \in \mathbb{C}\} \ .$$

Démonstration. Dans les deux cas, l'inclusion de droite à gauche est triviale. Pour la réciproque, fixons $\phi \in \mathrm{Sol}_{\mathscr{H}}$ et α une racine de l'équation caractéristique $X^2+aX+b=0$. Alors, en posant
$$g : x \mapsto \phi(x) e^{-\alpha x}$$
on a :
$$\begin{aligned} 0 &= \phi'' + a\phi' + b\phi \\ &= g'' + (2\alpha + a) g' + \underbrace{(\alpha^2 + a\alpha + b)}_{=0} g \end{aligned}$$
car pour tout $x \in I$, $\phi(x) = g(x) e^{\alpha x}$. Au final, on obtient donc
$$g'' + (2\alpha + a) g' = 0 \qquad (\mathbf{E}\ \text{:XIII.6})$$
qui est une équation différentielle linéaire d'ordre 1 homogène en g'. En la resolvant, on obtient qu'il existe $C \in \mathbb{K}$ tel que :
$$\forall x \in I,\ g'(x) = C e^{-(2\alpha+a)x} \ .$$

Cas 1 : $\Delta \neq 0$. Soit β l'unique racine de l'équation caractéristique distincte de α ; nous savons que $\alpha + \beta = -a \neq 2\alpha$ donc $2\alpha + a \neq 0$. Nous pouvons donc intégrer sans crainte l'expression de g' *supra* et obtenir qu'il existe $A, B \in \mathbb{K}$ tels que
$$\forall x \in I,\ g(x) = A e^{-(2\alpha+a)x} + B$$
et donc
$$\begin{aligned} \forall x \in I,\ \phi(x) &= g(x) e^{\alpha x} \\ &= A e^{-(\alpha+a)x} + B e^{\alpha x} \\ &= A e^{\beta x} + B e^{\alpha x} \end{aligned}$$
d'où le résultat.

Cas 2 : $\Delta = 0$.Dans ce cas, $2\alpha = -a$ car α est l'unique racine double de l'équation caractéristique, donc g' est constante. Il suffit alors d'intégrer et de multiplier par $x \mapsto e^{\alpha x}$ comme dans le cas précédent pour obtenir le résultat voulu.

□

✌ **Remarque XIII.6.**

— Notons que l'expression des solutions présente deux "degrés de liberté".

— Si Δ est un réel strictement négatif, les racines de l'équation caractéristique sont complexes conjuguées, *i.e* $r_1 = a + ib$ et $r_2 = a - ib$ pour $a, b \in \mathbb{R}$. De fait, les solutions **réelles** de $(\mathscr{H})$ sont de la forme

$$x \mapsto e^{ax}(\alpha \cos(bx) + \beta \sin(bx))$$

pour $\alpha, \beta \in \mathbb{R}$.

➠ **Exemple XIII.10.** Les solutions complexes de $y' + y = 0$ sont les

$$x \mapsto Ae^{ix} + Be^{-ix}$$

pour $A, B \in \mathbb{C}$. En passant à la partie réelle, on obtient que ses solutions réelles sont les

$$x \mapsto C\cos(x) + D\sin(x)$$

pour $C, D \in \mathbb{R}$.

◇ Recherche d'une solution particulière

Recherche d'une solution évidente. Comme à l'ordre 1, il convient de vérifier si notre équation n'admet pas de solution "immédiate". Par exemple, $x \mapsto \frac{e^x}{3}$ est solution de $y'' + y' + y = e^x$.

Cas particuliers. La méthode de variations des constantes est hors–programme. Nous donnons cependant quelques "recettes" pour traiter les cas le plus couramment rencontrés aux concours. Plus précisément, si le second membre de l'équation étudiée est de la forme

$$x \mapsto Ae^{\alpha x}$$

avec $A, \alpha \in \mathbb{C}$, il convient de rechercher une solution particulière sous la forme

$$x \mapsto P(x)e^{\alpha x}$$

avec :

— si α n'est pas une racine de l'équation caractéristique, P constant ;

— si α est racine simple de l'équation caractéristique, P de degré 1 ;

— si α est racine double de l'équation caractéristique, P de degré 2.

Notons que cette méthode nous permet, via l'exponentielle complexe et un passage à la partie réelle ou imaginaire de résoudre les cas où le second membre est une fonction cos ou sin.

➠ **Exemple XIII.11.** Cette méthode permet de résoudre rapidement les équations

$$y'' + y = e^x \qquad (\mathbf{E}\ \text{:XIII.7})$$

et

$$y'' - y = e^x \ . \qquad (\mathbf{E} : \text{XIII.8})$$

Pour les solutions particulières, la première en admet une évidente ($x \mapsto \frac{e^x}{2}$) et la seconde admet $x \mapsto \frac{x}{2}e^x$, obtenue via la méthode *supra* (1 est racine simple de $X^2 - 1 = 0$).

✌ **Remarque XIII.7.** Le principe de superposition se généralise au second ordre.

c) Problèmes de Cauchy

Définition XIII.6. Soient $a, b \in \mathbb{K}$, $f \in \mathscr{C}^0(I)$ et soit $(x_0, y_0, y_1) \in I \times \mathbb{K} \times \mathbb{K}$. On appelle **problème de Cauchy linéaire du second ordre** associé à ces données le système :

$$\begin{cases} y'' + ay' + by = f \\ y(x_0) = y_0 \\ y'(x_0) = y_1 \end{cases}$$

d'inconnue $y \in \mathscr{D}^2(I)$.

Vocabulaire. Les données x_0, y_0 et y_1 sont appelées **conditions initiales du système**.

➠ **Exemple XIII.12.**

$$\begin{cases} y'' + y = 0 \\ y(0) = 1 \\ y'(0) = 0 \end{cases}$$

est un problème de Cauchy sur $I = \mathbb{R}$.

Théorème XIII.9 (Cauchy linéaire, ordre 2)**.**
Tout problème de Cauchy linéaire du second ordre admet une unique solution.

➠ **Exemple XIII.13.** L'unique solution du problème de Cauchy de l'exemple précédent est :

$$y : x \mapsto \cos(x) \ .$$

Chapitre XIV

Polynômes

On fixe dans tout ce chapitre un corps $\mathbb{K}$ égal à $\mathbb{R}$ ou $\mathbb{C}$.

1.⁻ L'algèbre $\mathbb{K}[X]$

a) Polynômes à une indéterminée

Définition XIV.1. On appelle **polynôme à une indéterminé** toute suite $(a_n)_n \in \mathbb{K}^{\mathbb{N}}$ telle que :

$$\exists\, d \in \mathbb{N},\ \forall n \geq d,\ a_n = 0\,.$$

Les termes de cette suite sont appelés **coefficients** du polynôme.

Vocabulaire. Une suite vérifiant la propriété *supra* est dite **presque nulle** : seul un nombre fini de ses termes sont en effet différents de 0.

Notation.

— L'ensemble des polynômes à une indéterminée sur $\mathbb{K}$ est noté $\mathbb{K}[X]$.
— Le polynôme correspondant à la suite nulle sera noté 0.
— Le polynôme correspondant à la suite $(1, 0, \ldots)$ est noté 1 ou X^0.
— De façon générale, le polynôme correspondant à la suite $(\delta_{k,n})_n$ pour $k \geq 0$ est noté X^k, où $\delta_{k,n}$ est le **symbole de Kronecker** valant 0 si $k \neq n$ et 1 sinon.

Proposition XIV.1. $(\mathbb{K}[X], +)$ est un sous–groupe de $(\mathbb{K}^{\mathbb{N}}, +)$. Il s'agit donc d'un groupe abélien de neutre $(0)_n$.

Démonstration. Trivial. □

Exemple XIV.1. $1 + X$ est le polynôme correspondant à la suite $(1, 1, 0 \ldots)$.

Remarquons ensuite que si $\lambda \in \mathbb{K}$ et $P = (a_n)_n$ est un polynôme, nous pouvons définir (de façon compatible avec l'addition des suites) le polynôme

$$\lambda P = (\lambda a_n)_n \ \in \mathbb{K}[X].$$

In fine, nous avons donc additionner les polynômes entre eux et les multiplier par des éléments de $\mathbb{K}$ (nous parlerons plus tard de **scalaires**, *cf.* chapitre XVIII). De plus, nous pouvons avec ces conventions écrire, pour $P = (a_n)_n \in \mathbb{K}[X]$ que :

$$P = a_0 X^0 + a_1 X + a_2 X^2 + \dots$$

soit

$$P = \sum_{k=0}^{\infty} a_k X^k \ .$$

✖ **Attention :** cette somme n'est **PAS** réellement infinie, étant donné que seul un nombre fini des termes a_k sont non nuls.

Définition XIV.2. Soit $P \in \mathbb{K}[X]$. On appelle **degré** de P la quantité

$$\deg(P) = \begin{cases} \max\{N \in \mathbb{N} \,|\, a_N \neq 0\} \text{ si } P \neq 0 \\ -\infty \text{ si } P = 0 \end{cases} .$$

Un polynôme de degré nul ou $-\infty$ est dit **constant**.

✌ **Remarque XIV.1.** Le degré est bien défini car toute partie de $\mathbb{N}$ non vide et majorée admet un plus grand élément (proposition I.7).

➠ **Exemple XIV.2.** $\deg(1) = 0$, $\deg(X^{17} - X) = 17$.

Notation. Pour $d \in \mathbb{N} \cup \{-\infty\}$, on note $\mathbb{K}_d[X]$ l'ensemble des polynômes de degré inférieur ou égal à d. Rappelons que par convention sur la droite réelle achevée, $-\infty$ est strictement inférieur à tout entier naturel.

Par conséquent, si $P = (a_n)_n \in \mathbb{K}[X]$ est de degré $d \geq 0$, nous pouvons écrire :

$$P = \sum_{k=0}^{d} a_k X^k \ .$$

✌ **Remarque XIV.2.** Il découle de tout ceci que si $P = (a_n)_n, Q = (b_n)_n \in KK[X]$ alors :

$$P = Q$$
$$\iff$$
$$(\deg(P) = \deg(Q)) \wedge (\forall k \leq \deg(P),\ a_k = b_k) \ .$$

Définition XIV.3. Soit $P \in \mathbb{K}[X] \setminus \{0\}$. On appelle **coefficient dominant** de P son coefficient non nul d'indice le plus élevé. Si le coefficient dominant de P est égal à 1, le polynôme est dit **unitaire**.

Notation. $\mathrm{cd}(P)$

✌ **Remarque XIV.3.** Si P est non nul de degré d, $\mathrm{cd}(P)$ est le coefficient placé devant X^d dans l'écriture de P en tant que somme.

Convention. $\mathrm{cd}(0) = 0$ (et il s'agit donc du seul polynôme de coefficient dominant nul).

➠ **Exemple XIV.3.** $\mathrm{cd}(1 + X^2 + 2X^4) = 2$.

Proposition XIV.2. Soient $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}^*$. Alors :

(i) $\deg(\lambda P) = \deg(P)$;

(ii) $\deg(P + Q) \leq \max(\deg(P), \deg(Q)$ avec égalité si $\deg(P) \neq \deg(Q)$.

Démonstration.

(i) Trivial.

(ii) Posons $P = \sum_{k=0}^{d} a_k X^k$ et $Q = \sum_{k=0}^{d'} b_k X^k$ avec $(d, d') = (\deg(P), \deg(Q))$. Alors :
- si $d \neq d'$, par exemple $d < d'$ $P + Q$ admet $b_{d'}$ et son degré est clairement d'.
- si $d = d'$ alors pour tout $k > d$ on a $a_k + b_k = 0$ ce qui entraîne le résultat.

Pour un contre exemple à l'égalité dans le cas où les degrés sont égaux, additionner 1 et -1.

□

b) Produit de polynômes

Proposition/définition XIV.4. Soient $P, Q \in \mathbb{K}[X]$, de coefficients respectifs $(a_i)_i$ et $(b_i)_i$. Alors :

(i) la suite de terme général (pour $k \geq 0$)

$$\sum_{j=0}^{k} a_j b_{k-j}$$

est un polynôme, appelé produit de P et Q et noté PQ ;

(ii) $\deg(PQ) = \deg(P) + \deg(Q)$.

✌ **Remarque XIV.4.** On vérifie par récurrence que, pour tout $k \in \mathbb{N}^*$, $\prod_{i=1}^{k} X = X^k$, ce qui est rassurant.

Démonstration. Si P ou Q est le polynôme nul, inutile de trop se fatiguer. Dans le cas contraire, posons $d = \deg(P)$ et $d' = \deg(Q)$. Alors, pour tout $k > d + d'$ on a :

$$R_k = \sum_{j=0}^{k} a_j b_{k-j} = 0$$

car si $j > d$, $a_j = 0$ et si $j \leq d$ alors $k - j > d'$ et donc $b_{k-j} = 0$. Le produit PQ est donc bien un polynôme (suite presque nulle) et

$$\deg(PQ) \leq d + d' \ .$$

Pour obtenir l'égalité des degrés, il nous suffit de constater que

$$R_{d+d'} = a_d b_{d'} \neq 0 \ .$$

□

✌ **Remarque XIV.5.** On a de fait la formule suivante :

$$\left(\sum_{k=0}^{d} a_k X^k\right)\left(\sum_{k=0}^{d'} b_k X^k\right) = \sum_{k=0}^{d+d'}\left(\sum_{j=0}^{k} a_j b_{k-j}\right) X^k \ .$$

Corollaire XIV.2.a. $(\mathbb{K}[X], +, \times)$ est un anneau intègre (et donc commutatif) de neutres 0 et $1 = X^0$.

Démonstration. Tout a déjà été fait sauf la simplification par un élément non nul, qui découle de la formule du degré d'un produit. □

Proposition XIV.3. Les inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls.

Démonstration. Si $P \in \mathbb{K}[X]^\times$, alors il existe $Q \in \mathbb{K}[X]$ tel que $PQ = 1$. En passant au degré, on obtient que $\deg(P) + \deg(Q) = 0$, d'où le résultat. □

c) Composition

Définition XIV.5. Soient $P, Q \in \mathbb{K}[X]$, avec $P = \sum_{k=0}^{d} a_k X^k$. On appelle composée de P par Q le polynôme :

$$P \circ Q = \sum_{k=0}^{d} a_k Q^k \ .$$

✌ **Remarque XIV.6.** Il s'agit bien d'un polynôme par structure d'anneau sur $\mathbb{K}[X]$.

➠ **Exemple XIV.4.** $X^2 \circ (X + 1) = (X + 1)^2$.

Proposition XIV.4. Soient $P, Q \in \mathbb{K}[X]$ avec Q non constant. Alors :

$$\deg(P \circ Q) = \deg(P)\deg(Q)\,.$$

✖ **Attention :** cela est faux si $\deg(Q) = 0$; en effet, la composée de $X - 1$ par 1 est de degré $-\infty$.

Démonstration. Posons $d = \deg(P)$ et $P = \sum_{k=0}^{d} a_k X^k$. Alors

$$P \circ Q = \sum_{k=0}^{d} a_k Q^k$$

donc, par somme et comme tous les $\deg(Q^k)$ sont distincts car Q est non constant, $\deg(P \circ Q) = \max_{k \leq d} \deg(a_k Q^k)$, ce dernier étant égal à $\deg(Q^d)$ car $a_d \neq 0$. □

Proposition XIV.5. La composition des polynômes est associative, non commutative, admet X pour neutre et est distributive **à droite** par rapport à l'addition.

Démonstration. Hastur, Hastur, Hastur. □

En résumé, il convient de retenir que :
- $X^2 \circ (X+1) = (X+1)^2 \neq (X+1) \circ X^2 = X^2 + 1$;
- si $P, Q, H \in \mathbb{K}[X]$ on a $P \circ (Q \circ H) = (P \circ Q) \circ H$ et $(P+Q) \circ H = P \circ Q + Q \circ H$ mais, comme vu *supra*, $P \circ (Q + H) \neq P \circ Q + P \circ H$.

2.⁻ Arithmétique des polynômes

a) Multiples, diviseurs

Définition XIV.6. Soient $A, B \in \mathbb{K}[X]$. On dira que A **divise** B, ou que B est un **multiple** de A, si il existe $C \in \mathbb{K}[X]$ tel que $B = AC$.

Notation.
- $A|B$.
- On notera $\mathscr{D}(A)$ l'ensemble des diviseurs de A et $A\mathbb{K}[X]$ l'ensemble de ses multiples.

✌ **Remarque XIV.7.**
- Comme sur $\mathbb{Z}$, 0 est divisible par tout polynôme et $A|B \Leftrightarrow B\mathbb{K}[X] \subset A\mathbb{K}[X]$.
- Soit $P \in \mathbb{K}[X]$ et soit $\lambda \in \mathbb{K}^*$. Alors $P = (\lambda P) \times \frac{1}{\lambda}$ et donc $\lambda | P$.
- Par degré d'un produit, si $A|B$ alors $\deg(A) \leq \deg(B)$ lorsque $B \neq 0$.

✍ **Exercice XIV.1.** Soient $a, b, c, r \in \mathbb{C}$ tels que $a \neq 0$. À quelle condition sur a, b, c et r a–t–on $(X - r) \,|\, aX^2 + bX + c$?

Proposition XIV.6. La relation "|" est réflexive et transitive. De plus, pour tous $A, B \in \mathbb{K}[X]$ on a :

$$(A|B) \wedge (B|A) \\ \Leftrightarrow \\ \exists\, \lambda \in \mathbb{K}^*,\ A = \lambda B.$$

On dit alors que les polynômes A et B sont **associés**.

Démonstration. Le premier point se traite de façon analogue à ce que nous avons vu au chapitre X. Pour le second, le sens "bas vers haut" est trivial et si A, B sont tels que $(A|B) \wedge (B|A)$ alors il existe $P, Q \in \mathbb{K}[X]$ tels que $A = PB$ et $B = AQ$ et donc $A = PQA$, *i.e* $A(1 - PQ) = 0$, ce qui entraîne que soit $A = 0$ (et dans ce cas $B = 0$) soit $PQ = 1$ ce qui n'est possible que si $P, Q \in \mathbb{K}[X]^\times = \mathbb{K}^*$. □

Théorème XIV.7 (Division euclidienne)**.**
Soient $A, B \in \mathbb{K}[X]$ tels que $B \neq 0$. Alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que :
- — $A = BQ + R$;
- — $\deg(R) < \deg(B)$.

Vocabulaire. Comme dans le cas entier, on parle de quotient, reste, diviseur et dividende.

Exemple XIV.5. $X^2 + X + 1 = X(X + 1) + 1$ est une division euclidienne.

Démonstration.

Existence. Si $\deg(A) < \deg(B)$ ou $A = 0$ alors $Q = 0$ et $R = A$ conviennent. Dans le cas contraire, démontrons l'existence du couple (Q, R) par récurrence forte sur $d = \deg(A)$. **Attention à la formulation de l'hypothèse de récurrence :** nous voulons montrer que, pour tout $d \geq 0$, pour tous polynômes A, B tels que $d = \deg(A) \geq deg(B)$ il existe un couple (Q, R) vérifiant les conclusions du théorème.

- — Si $d = 0$, alors A et B sont inversibles ($\deg(B) \leq \deg(A)$) et donc $A = B \times \frac{A}{B} + 0$.
- — Si on suppose l'hypothèse vérifiée jusqu'à un certain rang $d \geq 0$ et que l'on se donne $A = \sum_{k=0}^{d+1} a_k X^k$ et $B = \sum_{k=0}^{d'} b_k X^k$ deux polynômes tels que $d + 1 = \deg(A) \geq d' = \deg(B)$ alors :

$$A' = A - \frac{a_{d+1}}{b_{d'}} X^{d+1-d'} B$$

est un polynôme de degré au plus d. Par hypothèse de récurrence (ou, au pire, car $\deg(B) > \deg(A')$), il existe donc $(Q, R) \in \mathbb{K}[X]^2$ tels que $A' = BQ + R$ et $\deg(R) < \deg(B)$. Ceci entraîne que :

$$A = B\left(\frac{a_{d+1}}{b_{d'}} X^{d+1-d'} + Q\right) + R$$

d'où le résultat.

Unicité. Si il existe deux couples (Q, R) et (Q', R') vérifiant les conclusions du théorème alors $B(Q-Q') = R' - R$ et donc

$$\deg(B) + \deg(Q-Q') = \deg(R'-R) < \deg(B)$$

d'où $\deg(Q-Q') = -\infty$ et le résultat.

□

✌ **Remarque XIV.8.** La démonstration du théorème XIV.7 nous livre un algorithme récursif implémentable en pratique.

b) PGCD

Proposition/définition XIV.7. Soient $A, B \in \mathbb{K}[X]$ tels que $B \neq 0$. On appelle **plus grand commun diviseur** de A et B tout élément de degré maximal de $\mathscr{D}(A) \cap \mathscr{D}(B)$.

Démonstration. Un tel élément existe car $\{\deg(P) \mid P \in \mathscr{D}(A) \cap \mathscr{D}(B)\}$ est une partie de $\mathbb{N}$ (car $B \neq 0$ donc $\mathscr{D}(B)$ ne contient pas $-\infty$) non vide (il contient 0 car les constantes non nulles divisent tout polynôme) et majorée par $\max(\deg(A), \deg(B))$. □

✖ **Attention :** il n'y a pas unicité : X^2 et $X^2 + X$ admettent (entre autres) X et $-X$ comme PGCD. En fait, c'est même bien pire que cela : si D est un PGCD de A et B alors λD l'est également pour tout $\lambda \in \mathbb{K}^*$ ...

Proposition XIV.8. Soient $A, B \in \mathbb{K}[X]$ tels que $B \neq 0$ et soit $\Delta \in \mathbb{K}[X]$. Alors :

$$\Delta \text{ est } \textbf{un} \text{ PGCD de } A \text{ et } B \iff \mathscr{D}(A) \cap \mathscr{D}(B) = \mathscr{D}(\Delta)\,.$$

Démonstration. Analogue au cas entier vu dans le chapitre X. □

Corollaire XIV.8.a. Soient $A, B \in \mathbb{K}[X]$ tels que $B \neq 0$ et soient Δ, Δ' deux PGCD de A et B. Alors Δ et Δ' sont associés.

✌ **Remarque XIV.9.** Par conséquent, si Δ est **un** PGCD de A et B alors l'ensemble des PGCD de ces deux polynômes est

$$\{\lambda\Delta \mid \lambda \in \mathbb{K}^*\}\,.$$

Cet ensemble contient donc un unique polynôme unitaire.

Définition XIV.8. On appelle PGCD de deux polynômes leur unique PGCD unitaire.

Notation. $A \wedge B$

Ceci nous permet d'énoncer une caractérisation du PGCD de $A, B \in \mathbb{K}[X]$ analogue à celle vue au chapitre X :

$$\Delta = A \wedge B \Longleftrightarrow \begin{cases} \mathscr{D}(A) \cap \mathscr{D}(B) = \mathscr{D}(\Delta) \\ \mathrm{cd}(\Delta) = 1 \end{cases} .$$

Remarque XIV.10. Si $A \neq 0$ alors $A \wedge 1 = 1$ et $A \wedge A = \frac{A}{\mathrm{cd}(A)}$.

À la question "comment trouver le PGCD de deux polynômes ?", nous donnerons la réponse suivante : il faut commencer par suivre l'algorithme d'Euclide vu dans le chapitre X puis ensuite diviser le dernier reste non nul par son coefficient dominant. Il est **essentiel de ne pas omettre cette dernière étape.**

Exemple XIV.6.
— $(X^2 + 3X + 1) \wedge (X + 1) = 1$;
— $(X^2 - 3X + 2) \wedge (X^3 - 2X^2 + X - 2) = X - 2$.

Remarque XIV.11. Comme dans le cas entier, l'algorithme d'Euclide étendu permet d'obtenir un couple U, V tel que $AU + BV = A \wedge B$.

c) Bézout et Gauss

Définition XIV.9. Deux polynômes A et B sont dits **premiers entre eux** si $A \wedge B = 1$.

Le théorème qui suit est, contrairement au théorème X.10, réellement du à Étienne Bézout(français, 1730—1783).

Théorème XIV.9 (Bézout)**.**
Soient $A, B \in \mathbb{K}[X]$ tels que $B \neq 0$. Alors :

$$\begin{array}{c} A \text{ et } B \text{ sont premiers entre eux} \\ \Longleftrightarrow \\ \exists\, U, V \in \mathbb{K}[X],\ AU + BV = 1. \end{array}$$

Démonstration. Analogue au cas entier. □

De la même façon, le lemme de Gauss vu au chapitre X se généralise au cas d'anneaux de polynômes.

Théorème XIV.10 (Lemme de Gauss)**.**
Soient $A, B, C \in \mathbb{K}[X]$ tels que $B \neq 0$. On suppose que :
— $A | BC$;
— $A \wedge B = 1$.
Alors A divise C.

Démonstration. Analogue au cas entier. □

✍ **Exercice XIV.2.** Résoudre dans $\mathbb{K}[X]$ l'équation $(X^3-1)U+(X^2+1)V = 2X^2$.

➥ **Correction :** *Il s'agit d'adapter la méthode vue lors de l'étude des équations diophantiennes. Comme $X^3 - 1$ et $X^2 + 1$ sont premiers entre eux, on trouve par Euclide étendu que :*

$$(X^3 - 1)(X - 1) + (1 + X - X^2)(X^2 + 1) = 2$$

et donc on trouve une solution particulière $U_0 = X^2(X - 1)$, $V_0 = X^2(1 + X - X^2)$ et on démontre à l'aide du lemme de Gauss que les seules solutions sont alors de la forme $(U_0 + (X^2 + 1)C, V_0 - (X^3 - 1)C)$, avec $C \in \mathbb{K}[X]$.

d) PPCM et généralisations

De la même façon, on définit le PPCM de deux polynômes A et B comme l'unique polynôme **unitaire** $A \vee B$ tel que $A\mathbb{K}[X] \cap B\mathbb{K}[X] = (A \vee B)\mathbb{K}[X]$. Il s'agit de l'unique élément unitaire de degré minimal de $A\mathbb{K}[X] \cap B\mathbb{K}[X]$. On retrouve alors l'égalité :

$$(A \wedge B)(A \vee B) = \frac{AB}{\mathrm{cd}(AB)} .$$

De plus, on peut définir le PGCD (resp. le PPCM) d'une famille de polynômes de la même façon que pour les entiers. On généralise également l'existence de relations de Bézout aux familles de n polynômes premiers entre eux dans leur ensemble.

3.– Fonctions polynomiales

a) C'est quoi ?

Définition XIV.10. Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{K}[X]$. On appelle **fonction polynomiale associée à** P l'application

$$\begin{aligned} f : \mathbb{K} &\longrightarrow \mathbb{K} \\ x &\mapsto \sum_{k=0}^{d} a_k x^k . \end{aligned}$$

Notation. On note $\mathbb{K}[x]$ l'ensemble des fonctions polynomiales sur $\mathbb{K}$.

✖ **Attention :** si $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$, la quantité "$P(a)$" n'a a priori aucun sens. Si f est la fonction polynomiale associée à P, $f(a)$ est par contre bien défini. On parle malgré tout d'**évaluation** du polynôme P en a.

➠ **Exemple XIV.7.** La fonction polynomiale associée à X^2 est (normalement) bien connue du lecteur.

Remarque XIV.12.
- On montre aisément que $(\mathbb{K}[x], +, \times)$ est un sous–anneau de $\mathbb{K}^{\mathbb{K}}$.
- De plus, si $\lambda \in \mathbb{K}$ et $f \in \mathbb{K}[x]$ alors $\lambda f \in \mathbb{K}[x]$.
- Soit $P = \sum_{k=0}^{d} a_k X^k$ un polynôme de degré $d \geq 0$. On appelle **forme de Hörner** (nommée en l'honneur William George Hörner, mathématicien britannique, 1786—1837, bien que l'on en retrouve des traces dans des écrits chinois et perses des siècles plus tôt) de P l'écriture

$$P = a_0 + X(a_1 + X(a_2 + X(\dots X(a_{d-1} + a_d X))) .$$

Par exemple, la forme de Hörner de X^3+3X^2+X+7 est $7+X(1+X(3+X))$. Cette forme est intéressante car elle permet d'évaluer un polynôme de degré n à l'aide de n multiplications et n additions, ce qui est la complexité algorithmique optimale d'une telle opération.

◇ Lien à la choucroute

On considère désormais l'application suivante, que l'on sait surjective par construction :

$$\begin{aligned} \varphi : \mathbb{K}[X] &\longrightarrow \mathbb{K}[x] \\ \sum_{k=0}^{d} a_k X^k &\mapsto \left(x \mapsto \sum_{k=0}^{d} a_k x^k \right) . \end{aligned}$$

Ceci signifie, rappelons le, que toute fonction polynôme correspond à (au moins) un polynôme. Cool. Mais encore ? Eh bien on peut vérifier que, pour tous $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$ on a :

$$\varphi(P + \lambda Q) = \varphi(P) + \lambda\varphi(Q) \quad \text{et} \quad \varphi(PQ) = \varphi(P)\varphi(Q) .$$

L'application φ est donc un morphisme d'anneaux (et une application linéaire, *cf.* chapitre XVIII).

La question qui nous brûle les lèvres à ce stade est naturellement la suivante : φ est–elle injective ? À savoir, étant donné deux polynômes P, Q tels que $\varphi(P) = \varphi(Q)$, a–t–on $P = Q$? La réponse devra hélas attendre quelques temps ...

b) Racines

Définition XIV.11. Soit $P \in \mathbb{K}[X]$ et soit $f = \varphi(P)$. On appelle **racine** (ou zéro) **de** P tout scalaire $a \in \mathbb{K}$ vérifiant $f(a) = 0$.

Notation. On notera $\mathrm{Rac}(P)$ l'ensemble des racines de P. Il sera souvent utile de spécifier le corps sur lequel nous travaillons ; on notera alors $\mathrm{Rac}_{\mathbb{K}}(P)$.

Exemple XIV.8.
- $\mathrm{Rac}_{\mathbb{C}}(X^2 + 1) = \{i, -i\}$;
- $\mathrm{Rac}_{\mathbb{R}}(X^2 + 1) = \emptyset$;

— $\mathrm{Rac}_{\mathbb{C}}(X^n - 1) = \mathbb{U}_n$ pour tout $n \geq 1$.

Proposition XIV.11. Soit $P \in \mathbb{K}[X]$ et soit $a \in \mathbb{K}$. Alors :

$$a \in \mathrm{Rac}(P)$$
$$\iff$$
$$X - a \text{ divise } P.$$

Démonstration.

($\Uparrow$) Immédiat : si $P = (X-a)Q$ avec $Q \in \mathbb{K}[X]$ alors $\varphi(P) = x \mapsto (x-a)\varphi(Q)(x)$.

($\Downarrow$) Supposons que $a \in \mathrm{Rac}(p)$. Par division euclidienne, il existe un unique couple (Q, R) de polynômes tels que

$$P = (X - a)Q + R$$

et $\deg(R) < 1$. De fait, R est constant et comme $\varphi(P)(a) = 0$ on a $\varphi(R)(a) = 0$. Ainsi, $R = 0$ (car il est constant).

□

Corollaire XIV.11.a. Soit $P \in \mathbb{K}[X]$ et soient $a_1, \dots a_n \in \mathrm{Rac}(P)$ deux à deux distincts. Alors $\prod_{k=1}^{n}(X - a_k)$ divise P.

Démonstration. Par récurrence à l'aide du lemme de Gauss (théorème XIV.10). □

On déduit de tout ceci la proposition fondamentale suivante, qui sera centrale à l'étude des racines de polynômes.

Proposition XIV.12. Soit $P \in \mathbb{K}[X]$ de degré $n \geq 0$. Alors $\mathrm{Rac}(P)$ contient au plus n éléments.

Démonstration. Si $a_1, \dots, a_k$ sont des racines deux à deux distinctes de P on a que

$$\prod_{i=1}^{k}(X - a_i) \text{ divise } P$$

et donc

$$k = \deg\left(\prod_{i=1}^{k}(X - a_i)\right) \leq \deg(P) = n\,,$$

d'où le résultat. □

✌ **Remarque XIV.13.** On déduit de ceci le résultat suivant, fort utile en pratique : **tout polynôme admettant plus de racines que son degré est nul**.

Théorème XIV.13.
L'application φ est bijective.

Démonstration. Il ne reste qu'à montrer que φ est injective. Si on suppose trouvé $P \in \mathbb{K}[X]$ tel que $P \in \operatorname{Ker}(\varphi)$, alors $\varphi(P) = 0$ et donc

$$\forall a \in \mathbb{K}, \quad \varphi(P)(a) = 0\,.$$

Ceci entraîne, comme le corps $\mathbb{K}$ est infini, que P admet une infinité de racines. Il s'agit donc du polynôme nul, *ergo* $P = 0$. □

Remarque XIV.14. Il nous sera donc possible d'identifier (comme vous le faisiez probablement depuis un bon moment) fonctions polynomiales et polynômes. Ceci entraîne qu'il est désormais permis d'écrire des choses sulfureuses comme "$P(a)$" en toute impunité.

Définition XIV.12. Soit $P \in \mathbb{K}[X] \setminus \{0\}$ et soit $a \in \mathbb{K}$. On appelle **multiplicité de a relativement à P** la quantité

$$\mu_P(a) = \max\{k \in \mathbb{N} \,|\, (X-a)^k | P\}\,.$$

Vocabulaire. Si $\mu_P(a) = 1$, on parle de racine simple ; si $\mu_P(a) \geq 2$, on parle de racine multiple (double, triple,...).

Remarque XIV.15. Il apparaît clairement que $a \in \operatorname{Rac}(P) \Leftrightarrow \mu_P(a) \neq 0$.

Exemple XIV.9. On pourra faire le parallèle avec le cours de première et les racines simples, doubles, des trinômes du second degré.

Définition XIV.13. Un polynôme $P \in \mathbb{K}[X] \setminus \{0\}$ est dit **scindé sur** $\mathbb{K}$ si la relation suivante est vérifiée :

$$\sum_{a \in \operatorname{Rac}_{\mathbb{K}}(P)} \mu_P(a) = \deg(P)\,.$$

Exemple XIV.10. Tout polynôme de degré 2 est scindé sur $\mathbb{C}$.

✖ **Attention :** le caractère scindé dépend lui aussi du corps : comparer X^2+1 vu comme polynôme à coefficients complexes et son jumeau maléfique dans $\mathbb{R}[X]$...

Proposition XIV.14. Soit $P \in \mathbb{K}[X] \setminus \{0\}$. Alors :

$$P \text{ est scindé}$$

$$\Longleftrightarrow$$

$$P = \operatorname{cd}(P) \prod_{a \in \operatorname{Rac}(P)} (X-a)^{\mu_P(a)}\,.$$

Démonstration.

($\Uparrow$) Trivial.

($\Downarrow$) Par définition de la multiplicité, pour tout $a \in \mathrm{Rac}(P)$, $(X-a)^{\mu_P(a)}$ divise P ; ces polynômes étant premiers entre eux on a, par lemme de Gauss :

$$\prod_{a \in \mathrm{Rac}(P)} (X-a)^{\mu_P(a)} \mid P\,.$$

De plus, le degré de ces deux polynômes sont, comme P est scindé, égaux. On en déduit que leur quotient est de degré 0. Ce dernier est alors obligatoirement égal à $\mathrm{cd}(P)$ par identification des coefficients dominants.

□

c) Relations coefficients–racines

Autorisons nous à présent une (relativement) brève digression ; si $P = aX^2+bX+c \in \mathbb{K}[X]$ est un trinôme du second degré (avec donc $a \neq 0$), et que son discriminant est $\Delta = b^2-4ac$, il admet deux racine(s) (éventuellement égale(s)) donnée(s) par la formule

$$r_\pm = \frac{-b \pm \delta}{2a}$$

avec $\delta^2 = \Delta$. On en déduit que :

$$\begin{cases} r_+ + r_- = -\dfrac{b}{a} \\ r_+ r_- = \dfrac{b^2-\Delta}{4a^2} = \dfrac{c}{a} \end{cases}$$

ce qui entraîne que :

$$\begin{aligned} aX^2+bX+c &= a\left(X^2+\frac{b}{a}X+\frac{c}{a}\right) \\ &= a(X^2-(r_++r_-)X+r_+r_-) \\ &= a(X-r_+)(X-r_-)\,. \end{aligned}$$

Ces relations entre coefficients et racines sont appelées, dans un élan d'originalité à faire pâlir un scénariste de chez Marvel, des **relations coefficients–racines**.

En dégré 3, on voit apparaître des choses similaires ; en effet, si $P = (X-x_1)(X-x_2)(X-x_3)$ est un polynôme scindé de degré 3, on obtient, en développant :

$$\begin{aligned} P &= (X-x_1)(X-x_2)(X-x_3) \\ &= X^3+aX^2+bX+c \end{aligned}$$

avec

$$\begin{cases} a = -(x_1+x_2+x_3) \\ b = x_1x_2+x_1x_3+x_2x_3 \\ c = -x_1x_2x_3 \end{cases}.$$

De façon plus générale, si $n, k \in \mathbb{N}^*$ sont tels que $k \leq n$, on appelle **k–ième fonction symétrique élémentaire à n variables** l'application

$$\begin{aligned} \sigma_k : \mathbb{K}^n &\longrightarrow \mathbb{K}^n \\ (x_1, \ldots, x_n) &\to \sum_{1 \leq i_1 < \ldots < i_k \leq n} x_{i_1} \ldots x_{i_k}\,. \end{aligned}$$

En particulier, pour tout $(x_1,\dots,x_n)\in\mathbb{K}^n$, on a :

$$\sigma_1(x_1,\dots,x_n)=\sum_{i=1}^{n} x_i\,,$$

$$\sigma_2(x_1,\dots,x_n)=\sum_{i=1}^{n}\sum_{j=i+1}^{n} x_ix_j$$

et

$$\sigma_n(x_1,\dots,x_n)=\prod_{i=1}^{n} x_i\,.$$

Ces fonctions ont un lien fort avec les relations que nous venons de voir pour les degrés 2 et 3. Celles–ci se généralisent via le théorème suivant (sont exigibles les formules pour σ_1 et σ_n ; les autres doivent "pouvoir être retrouvées rapidement").

Théorème XIV.15 (Relations coefficients–racines)**.**
Soit $P=\sum\limits_{k=1}^{n} a_kX^k$ un polynôme scindé de degré n dont les racines (comptées avec multiplicité) sont notées $r_1,\dots,r_n$. Alors :

$$\forall k\in[\![1,n]\!],\quad \sigma_k(r_1,\dots,r_n)=(-1)^k\frac{a_{n-k}}{a_n}\,.$$

✍ **Exercice XIV.3.** Résoudre :

$$\left\{\begin{array}{ccc} x+y+z & = & 2\\ \frac{1}{x}+\frac{1}{y}+\frac{1}{z} & = & \frac{5}{6}\\ xyz & = & -6\end{array}\right. .$$

➥ **Correction :** *En multipliant la ligne 2 par la ligne 3, on arrive au système :*

$$\left\{\begin{array}{ccc} x+y+z & = & 2\\ yz+xz+xy & = & -5\\ xyz & = & -6\end{array}\right. .$$

Les solutions sont donc les racines du polynôme $X^3-2X^2-5X+6=(X-1)(X^2-X-6)$.

4.⁻ Dérivation

a) Dérivée formelle d'un polynôme

Définition XIV.14. Soit $P=\sum\limits_{k=0}^{d} a_kX^k\in\mathbb{K}[X]$. On appelle **dérivée** (formelle) de P le polynôme

$$P'=\sum_{k=1}^{d} ka_kX^{k-1}\,.$$

Exemple XIV.11. $(X^3 + X + 1)' = 3X^2 + 1$.

Remarque XIV.16.
- On définit par récurrence les dérivées formelles d'ordre supérieur d'un polynôme.
- On vérifie aisément que la fonction polynomiale (lorsque $\mathbb{K} = \mathbb{R}$) associée à la dérivée formelle d'un polynôme est la dérivée de la fonction polynomiale associée à ce même polynôme. En particulier, les fonctions polynomiales sont de classe $\mathscr{C}^\infty(\mathbb{R})$.
- Il découle du point précédent que les formules usuelles de dérivation se généralisent à la dérivée formelle, quitte dans la cas complexe à travailler sur la restriction de la fonction polynomiale à $\mathbb{R}$. On peut également vérifier ces résultats par le calcul.

Proposition XIV.16. Soit $P \in \mathbb{K}[X]$ un polynôme **non constant**. Alors $\deg(P') = \deg(P) - 1$.

Démonstration. Immédiat par définition. □

Exercice XIV.4. Soit $P \in \mathbb{R}[X]$ un polynôme de degré $n \geq 2$ admettant $2 \leq k \leq n$ racines réelles distinctes. Que dire des racines de P' ?

b) Formule de Taylor polynomiale

Proposition XIV.17. Soit $P \in \mathbb{K}[X]$ et soit $a \in \mathbb{K}$. Alors

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

Remarque XIV.17.
- La notation "$P^{(k)}(a)$" est abusive, mais nous sommes entre gens de bonne compagnie.
- Comme de coutume, la somme apparaissant dans la formule est en faite finie, car (par décroissance du degré), $\exists N \in \mathbb{N}, \forall n \geq N, P^{(n)} = 0$.
- On peut donc déduire des valeurs successives des dérivées d'un polynôme en un point l'expression générale de celui–ci.
- Un conséquence de cette formule est que si l'on note $(a_k)_k$ les coefficients de P on a :
$$\forall k \in \mathbb{N}, \quad a_k = \frac{P^{(k)}(0)}{k!} .$$

Démonstration. Vous l'aurez deviné, c'est reparti pour une récurrence sur le $n = \deg(P)$ ...
- Si P est constant, tout va bien.
- Sinon, yaka appliquer l'hypothèse de récurrence à P' et "primitiver", puis être content.

□

Exemple XIV.12. La formule de Taylor permet de déterminer l'unique polynôme P de degré inférieur ou égal à deux vérifiant $P(0) = 0$, $P'(0) = 2$ et $P'(0) = 3$.

Nous verrons dans le chapitre XVII que la formule de Taylor permet d'approximer des fonctions à l'aide de polynômes.

Corollaire XIV.17.a. Soit $a \in \mathbb{K}$, $k \in \mathbb{N}$ et $P \in \mathbb{K}[X]$. Alors :

$$\mu_p(a) = k \iff \begin{cases} P(a) = P'(a) = \ldots = P^{(k-1)}(a) = 0 \\ P^{(k)}(a) \neq 0 \end{cases}.$$

Démonstration.

($\Leftarrow$) Cela découle de la formule de Taylor : P est divisible par $(X-a)$, $(X-a)^2$, …, $(X-a)^{k-1}$ mais pas par $(X-a)^k$.

($\Rightarrow$) On le fait par récurrence sur k et c'est la fête. Pour l'hérédité, remarquer que si $\mu_P(a) = k+1$ alors $P = (X-a)^{k+1}Q$ avec $Q(a) \neq 0$ et $P' = (X-a)^k R$ avec $R(a) \neq 0$ (c'est un calcul), ce qui permet de conclure.

□

5.⁻ Irréductibilité

a) C'est quoi ?

Définition XIV.15. Un polynôme $P \in \mathbb{K}[X]$ est dit **irréductible** si :
- P est non constant ;
- si $P = QR$ avec $Q, R \in \mathbb{K}[X]$ alors Q ou R est constant.

Exemple XIV.13. Les polynômes de degré 1 sont constants sur $\mathbb{R}$ ou $\mathbb{C}$ et les polynômes de degré deux de discriminant négatif sur $\mathbb{R}$.

✖ **Attention :** l'irréductibilité dépend du corps sur lequel on travaille : $X^2+1 = (X-i)(X+i)$ sur $\mathbb{C}$.

Théorème XIV.18.
Tout polynôme non constant s'écrit de façon unique (à l'ordre près des facteurs et à constante multiplicative près) comme produit de polynômes irréductibles.

Remarque XIV.18. Ce résultat est analogue à la proposition X.14 (décomposition en produits de facteurs premiers sur $\mathbb{Z}$). Ceci n'est pas une coïncidence.

Exemple XIV.14. $X^3 - 1 = (X-1)(X-j)(X-j^2) = (X-1)(X^2+X+1)$; on remarque que la décomposition dépend (sans surprise) du corps sur lequel on travaille.

Démonstration. **Existence.** Youpi, une récurrence forte sur le degré ! Attention à la formulation de l'hypothèse. . . .

- $d = 1$. C'est plié.
- **Supposons la propriété vérifiée pour tout** $k \in [\![1, n]\!]$ **avec** $n \geq 1$ **fixé.** Si P est irréductible, c'est fini. Sinon, il existe deux polynômes $Q, R \in \mathbb{K}[X]$ non constants tels que $P = QR$. Nous pouvons appliquer l'hypothèse de récurrence à ceux–ci et voila, c'est plié.

Unicité. Nous en parlerons plus tard. Là, j'ai water–poney.

□

➠ **Exemple XIV.15.** Le polynôme $X^n - 1$ (pour $n \geq 1$) admet exactement n racines sur $\mathbb{C}$: les éléments de $\mathbb{U}_n$. Ceci entraîne la factorisation suivante (**sur** $\mathbb{C}$) :

$$X^n - 1 = \prod_{\xi \in \mathbb{U}_n} (X - \xi) .$$

b) C'est qui (édition complexe) ?

Le théorème central de ce paragraphe est le suivant, parfois appelé théorème fondamental de l'algèbre. Son histoire est complexe (ah ah) et intrinsèquement lié à celle du corps $\mathbb{C}$ dont on peut considérer qu'il est la motivation première pour l'étude. On trouve des traces de ce résultat chez François Viète (français, 1540—1603), Albert Girard (français, 1595—1632) et Renée Descartes, que l'on ne présente plus (1596—1650), entre autres.

Une première démonstration de ce résultat est esquissée par Jean le Rond d'Alembert (français, 1717—1783). Celle–ci est incomplète, malgré quelques ajouts ultérieurs par Jean–Robert Agrand (amateur suisse, 1768—1822). Une démonstration complète n'apparaîtra que suite aux efforts (indépendants) de Lagrange, Euler et Gauss, qui en produit la première démonstration complète (et fort analytique) en 1816.

Théorème XIV.19 (D'Alembert—Gauss). Tout polynôme non constant de $\mathbb{C}[X]$ admet une racine.

Démonstration. Admis. □

Corollaire XIV.19.a. Les polynômes irréductibles de $\mathbb{C}$ sont les polynômes de degré un.

Démonstration. Il est clair que les polynômes de degré un sont irréductibles. Réciproquement, si $P \in \mathbb{C}[X]$ est irréductible, il admet une racine $a \in \mathbb{C}$ d'après le théorème XIV.19 et donc est divisible par $X - a$. Par irréductibilité, P est de la forme $\lambda(X - a)$ avec $\lambda \in \mathbb{K}$. □

✌ **Remarque XIV.19.** La décomposition apparaissant dans le théorème XIV.18 est donc unique car déterminée par les racines. Plus précisément, si $P \in \mathbb{C}[X]$, on a :

$$P = \mathrm{cd}(P) \prod_{\alpha \in \mathrm{Rac}_{\mathbb{C}}(P)} (X - \alpha)^{\mu_P(\alpha)} .$$

Proposition XIV.20. Soient $P, Q \in \mathbb{C}[X]$. Alors :

$$P|Q \iff \begin{cases} \mathrm{Rac}_{\mathbb{C}}(P) \subset \mathrm{Rac}_{\mathbb{C}}(Q) \\ \forall \alpha \in \mathbb{C},\ \mu_P(\alpha) \leq \mu_Q(\alpha) \end{cases} .$$

Démonstration. Ceci découle de la décomposition énoncée **supra**. □

Exemple XIV.16. Comparer les racines de $X^2 + X + 1$ et $(X^3 - 1)^2$.

Remarque XIV.20. Ceci entraîne que si $P, Q \in \mathbb{C}[X] \setminus \{0\}$ on a :

$$P \wedge Q = \prod_{\alpha \in \mathrm{Rac}_{\mathbb{C}}(P) \cap \mathrm{Rac}_{\mathbb{C}}(Q)} (X - \alpha)^{\min(\mu_P(\alpha), \mu_Q(\alpha))}$$

et

$$P \vee Q = \prod_{\alpha \in \mathrm{Rac}_{\mathbb{C}}(P) \cup \mathrm{Rac}_{\mathbb{C}}(Q)} (X - \alpha)^{\max(\mu_P(\alpha), \mu_Q(\alpha))} .$$

Corollaire XIV.20.a. Deux polynômes de $\mathbb{C}[X]$ sont premiers entre eux si et seulement si ils n'ont pas de racine commune.

c) C'est qui (retour au(x) réel(s)) ?

Les choses se compliquent : il est temps de dégainer les lemmes ...

Lemme XIV.1. Soit $P \in \mathbb{R}[X]$. Alors, pour tout $\alpha \in \mathbb{C}$:

$$(\alpha \in \mathrm{Rac}_{\mathbb{C}}(P)) \Rightarrow (\overline{\alpha} \in \mathrm{Rac}_{\mathbb{C}}(P)) .$$

Démonstration. Si $P = \sum_{k=0}^{d} a_k X^k$, on a :

$$\begin{aligned} 0 &= \overline{P(\alpha)} \\ &= \overline{\sum_{k=0} a_k \alpha^k} \\ &= \sum_{k=0} a_k \overline{\alpha}^k \\ &= P(\overline{\alpha}) \end{aligned}$$

d'où le résultat. □

Lemme XIV.2. Soit $P \in \mathbb{R}[X]$ de degré supérieur ou égal à 3. Alors P est réductible sur $\mathbb{R}$.

Démonstration. Si P admet une racine réelle, Bob's your uncle. Sinon, d'après le théorème de d'Alembert Gauss (XIV.19), il existe $\alpha \in \mathrm{Rac}_{\mathbb{C}}(P)$ (avec $\alpha \notin \mathbb{R}$) et $\overline{\alpha}$ est également une racine de P (distincte de α). De fait, il existe $Q \in \mathbb{C}[X]$ tel que :

$$P = (X - \alpha)(X - \overline{\alpha})Q .$$

Or $(X-\alpha)(X-\overline{\alpha}) = X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2 \in \mathbb{R}[X]$ donc, par unicité dans la division euclidienne (théorème XIV.7), $Q \in \mathbb{R}[X]$. Ce polynôme est de plus non constant car $\deg(P) \geq 3$, d'où le résultat. □

Théorème XIV.21.
Les polynômes irréductibles de $\mathbb{R}$ sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant négatif.

Démonstration. Les polynômes cités sont clairement irréductibles. Réciproquement, si P est irréductible de degré 2, son discriminant est négatif (sans quoi il admet des racines réelles et donc une factorisation). Le cas du degré 3 et supérieur a été traité dans le lemme précédent. □

Remarque XIV.21. La décomposition apparaissant dans le théorème XIV.18 est unique : cela découle du fait que la décomposition complexe est unique. On a de plus la formule suivante, pour tout $P \in \mathbb{R}[X]$:

$$P = \mathrm{cd}(P) \prod_{\alpha \in \mathrm{Rac}_{\mathbb{R}}(P)} (X-\alpha)^{\mu_P(\alpha)} \prod_{\substack{\beta \in \mathrm{Rac}_{\mathbb{C}}(P) \setminus \mathrm{Rac}_{\mathbb{R}}(P) \\ \text{tel que } \mathrm{Im}(\beta) > 0}} (X^2 - 2\mathrm{Re}(\beta)X + |\beta|^2)^{\mu_P(\beta)} ,$$

la condition sur $\mathrm{Im}(\beta)$ nous permettant de nous assurer qu'aucune racine complexe ne soit comptée "en double". Notons que ceci entraîne que deux racines complexes conjuguées d'un polynôme à coefficients réels sont de même multiplicité.

Exemple XIV.17.

$$\begin{aligned} X^4 - 1 &= (X-1)(X+1)(X-i)(X+i) \\ &= (X-1)(X+1)(X^2+1) . \end{aligned}$$

6.⁻ Interpolation de Lagrange

Dans ce paragraphe, nous nous intéressons à la question suivante : étant donné $(x_0, y_0), \dots, (x_n, y_n) \in \mathbb{K}^2$, comment trouver un polynôme $P \in \mathbb{K}[X]$ tel que :

$$\forall k \in [\![0, n]\!],\ P(x_k) = y_k \ ? \qquad \textbf{(E} :\text{XIV.1)}$$

Pour $n = 0$, le polynôme constant égal à y_0 fera l'affaire. Pour $n = 1$, nous avons deux points à relier ; une droite (et donc un polynôme de degré 1) conviendra. Dans ces deux cas, la solution au problème semble unique.

Proposition XIV.22. Soit $n \geq 0$ et soient $x_0, \dots x_n \in \mathbb{K}$ deux à deux distincts. Alors, pour toute famille $y_0, \dots, y_n \in \mathbb{K}$, il existe un unique polynôme $P \in \mathbb{K}_n[X]$ tel que :

$$\forall k \in [\![0, n]\!],\ P(x_k) = y_k .$$

Démonstration. **Unicité.** Si deux tels polynômes existent, leur différence admet $n+1$ racines (les x_k) et est donc nulle par argument de degré.

Existence. Posons, pour $k \in [\![0, n]\!]$:

$$L_k = \prod_{j \neq k} \frac{(X - x_j)}{(x_k - x_j)}.$$

On a alors l'égalité $L_k(x_j) = \delta_{k,j}$ pour tous $k, j \in [\![0, n]\!]$ et donc

$$P = \sum_{k=0}^{n} y_k L_k$$

convient.

□

✌ **Remarque XIV.22.** L'unicité n'est plus garantie si la condition de degré est supprimée ; il existe même une infinité de solutions possibles à l'équation **E** :XIV.1.

➠ **Exemple XIV.18.** $X+1$ interpole les couples $(0,1)$ et $(1,2)$. Mais $(X+1)+X(X-1)$ aussi ...

✌ **Remarque XIV.23.** Tout ceci se code très bien en `python`. Une instabilité numérique est présente si n est très grand, car le polynôme "cherche" toujours à s'annuler autant de fois que son degré. La fonction suivante prend en argument les listes `X` et `Y` contenant respectivement les x_k et les y_k.

```python
def lagrange(X,Y,a):
    def L(k,X,a):
        p=1
        for i in range(len(X)):
            if i != k:
                p*=(a-X[i])/(X[k]-X[i])
        return p

    if len(X) != len(Y):
        raise ValueError("Tailles␣incompatibles")
    n = len(X)
    res=0
    for k in range(n):
        res+=Y[k]*L(k,X,a)
    return res
```

Chapitre XV

Fractions rationnelles

On fixe dans tout ce chapitre un corps $\mathbb{K}$ égal à $\mathbb{R}$ ou $\mathbb{C}$.

1.⁻ Corps des fractions rationnelles

a) Notion de fraction rationnelle

Nous ne rentrerons pas cette fois–ci dans les détails ; les techniques nous manquent pour définir proprement tout ceci.

Théorème XV.1.
Il existe un corps $\mathbb{K}(X)$, appelé **corps des fractions rationnelles sur** $\mathbb{K}$ tel que :
- $\mathbb{K}[X] \subset \mathbb{K}(X)$;
- tout corps contenant $\mathbb{K}[X]$ contient également $\mathbb{K}(X)$.

Un tel corps est de plus unique à isomorphisme près.

✌ **Remarque XV.1.** Le corps $\mathbb{K}(X)$ contient donc :
- les polynômes ;
- leurs inverses (sauf pour 0, évidemment), notés $\dfrac{1}{P}$ pour $P \in \mathbb{K}[X] \setminus \{0\}$.

Il en découle par minimalité que les éléments de $\mathbb{K}[X]$ sont tous de la forme $P \times \dfrac{1}{Q}$ avec $P, Q \in \mathbb{K}[X]$ et $Q \neq 0$. Nous utiliserons la notation fractionnelle $\dfrac{P}{Q}$ pour de tels objets.

➠ **Exemple XV.1.** $\dfrac{1}{X}, \dfrac{X^2+4X-1}{X-1} \in \mathbb{K}(X)$.

Opérations sur les fractions rationnelles
Si $P, Q, R, S \in \mathbb{K}[X]$ sont tels que $QS \neq 0$, alors on a :

(i) $\dfrac{P}{Q} = \dfrac{R}{S} \Leftrightarrow PS = QR$;

(ii) $\dfrac{P}{Q} + \dfrac{R}{S} = \dfrac{PS+QR}{QS}$;

(iii) $\dfrac{P}{Q} \times \dfrac{R}{S} = \dfrac{PR}{QS}$.

✖ **Attention :** la représentation d'une fraction rationnelle n'est pas unique :

$$\frac{X}{1} = \frac{X^2}{X} = X \, .$$

Théorème XV.2 (Forme irréductible d'une fraction rationnelle)**.**
Soit $F \in \mathbb{K}(X)$. Alors il existe un unique couple $(P, Q) \in \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$ tel que :

(i) $P \wedge Q = 1$;
(ii) Q soit unitaire ;
(iii) $F = \dfrac{P}{Q}$.

Démonstration. Similaire à la forme irréductible d'une fraction rationnelle dans $\mathbb{Q}$ vue au chapitre X. □

b) Degré

Proposition/définition XV.1. Soit $F = \dfrac{P}{Q} \in \mathbb{K}(X)$. Alors la quantité $\deg(P) - \deg(Q) \in \mathbb{Z} \cup \{-\infty\}$ ne dépend pas de la représentation choisie et est appelée **degré** de F.

Notation. $\deg(F)$

Démonstration. Si F admet une autre écriture $F = \dfrac{R}{S}$, alors $PS = QR$ et donc $\deg(P) + \deg(S) = \deg(Q) + \deg(R)$, ce qui entraîne que :

$$\deg(P) - \deg(Q) = \deg(R) - \deg(S) \, .$$

□

➠ **Exemple XV.2.** $\deg\left(\dfrac{X^2+1}{X^3}\right) = -1$.

✖ **Attention :** une fraction rationnelle de degré nulle peut ne pas être constante : considérer $\dfrac{X}{X+2}$.

✌ **Remarque XV.2.**
— *deg*$(F) = -\infty \Leftrightarrow F = 0$;
— $\deg(F) \leq 0 \Leftrightarrow \deg(P) \leq \deg(Q)$.

Proposition XV.3. Soient $F, G \in \mathbb{K}(X)$. Alors :

(i) $\deg(F+G) \leq \max(\deg(F), \deg(G))$, avec égalité lorsque $\deg(F) \neq \deg(G)$;

(ii) $\deg(FG) = \deg(F) + \deg(G)$.

Démonstration. Posons, pour fixer les idées, $F = \dfrac{P}{Q}$ et $G = \dfrac{R}{S}$.

(i) On sait que $F + G = \dfrac{PS+QR}{QS}$ et donc :

$$\begin{aligned}
\deg(F+G) &= \deg(PS+QR) - \deg(QS) \\
&\leq \max(\deg(PS), \deg(QR)) - (\deg(Q) + \deg(S)) \text{ par degrés polynomiaux} \\
&= \max(\deg(P) + \deg(S), \deg(Q) + \deg(R)) - (\deg(Q) + \deg(S)) \\
&= \max(\deg(P) - \deg(Q), \deg(R) - \deg(S)) \\
&= \max(\deg(F), \deg(G))
\end{aligned}$$

avec égalité lorsque les degrés sont différents par résultat sur les degrés de polynômes.

(ii) Procéder de façon similaire en développant les degrés.

□

c) Racines, pôles

Définition XV.2. Soit $F = \dfrac{P}{Q} \in \mathbb{K}(X)$ une fraction rationnelle **irréductible**. On appelle :

— **racines** de F les racines de P sur $\mathbb{K}$;

— **pôles** de F les racines de Q sur $\mathbb{K}$.

La multiplicité d'une racine (resp. d'un pôle) de F est définie comme étant sa multiplicité en tant que racine de P (resp. de Q).

Notation. $\mathrm{Rac}_{\mathbb{K}}(F)$, $\mathrm{Pol}_{\mathbb{K}}(F)$.

✖ **Attention :** l'irréductibilité est ici essentielle : 0 n'est pas un pôle (ni une racine) de $\dfrac{X(X+1)}{X}$.

➠ **Exemple XV.3.** Les pôles de $\dfrac{X}{X^2+1}$ sur $\mathbb{C}$ sont i et $-i$, et elle n'admet aucun pôle sur $\mathbb{R}$. Son unique racine sur les deux corps est 0.

✌ **Remarque XV.3.**

— Toute fraction rationnelle admet un nombre fini de pôles.

— Toute fraction rationnelle **non nulle** admet un nombre fini de racines.

— De façon analogue aux fonctions polynomiales, il est possible étant donné $F = \dfrac{P}{Q} \in \mathbb{K}(X)$ de définir une fonction

$$\begin{aligned} f : \mathbb{K} \setminus \mathrm{Pol}_{\mathbb{K}}(F) &\longrightarrow \mathbb{K} \\ x &\mapsto \frac{P(x)}{Q(x)}. \end{aligned}$$

2.– Éléments simples

a) C'est quoi ?

Définition XV.3. On appelle **élément simple** sur $\mathbb{K}$ toute fraction rationnelle du type $\dfrac{P}{Q^n} \in \mathbb{K}(X)$ avec :
- Q unitaire et irréductible sur $\mathbb{K}$;
- $n \in \mathbb{N}^*$;
- $\deg(P) < \deg(Q)$.

✌ **Remarque XV.4.** L'étude menée au chapitre XIV nous permet de classifier les éléments simples sur $\mathbb{R}$ et $\mathbb{C}$.
- Sur $\mathbb{C}$, ce sont les fractions de la forme :
$$\frac{\alpha}{(X-\beta)^n}$$
avec $\alpha, \beta \in \mathbb{C}$ et $n \geq 1$.
- Sur $\mathbb{R}$ ce sont les fractions de la forme :
$$\frac{\alpha}{(X-\beta)^n}$$
avec $\alpha, \beta \in \mathbb{R}$ et $n \geq 1$ ainsi que celles de la forme :
$$\frac{aX+b}{(X^2+pX+q)^n}$$
avec $a, b, p, q \in \mathbb{R}$ et $n \geq 1$.

b) Partie entière d'une fraction rationnelle

Proposition/définition XV.4. Soit $F \in \mathbb{K}(X)$. Alors il existe un unique polynôme $E \in \mathbb{K}[X]$ et une unique fraction rationnelle $G \in \mathbb{K}(X)$ tel que :

(i) $\deg(G) < 0$;

(ii) $F = E + G$.

Le polynôme E est appelé **partie entière** de F.

Notation. $E(F)$

Démonstration. **Existence.** Posons $F = \dfrac{A}{B}$; alors par division euclidienne on a l'existence d'un couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $A = BQ+R$ et $\deg(R) < \deg(B)$. Ainsi, $F = Q + \dfrac{R}{B}$ avec $\deg\left(\dfrac{R}{B}\right) < 0$.

Unicité. Si il existe deux couples (E, G) et (E', G') vérifiant les conditions voulues, alors $E_1 - E_2 = G_2 - G_1$ ce qui n'est possible (car $deg(G_1 - G_2) < 0$ et $E_1, E_2 \in \mathbb{K}[X]$) que si les deux différences sont nulles.

□

Exemple XV.4.

— $\dfrac{X+1}{X} = 1 + \dfrac{1}{X}$ donc $E\left(\dfrac{X+1}{X}\right) = 1$;

— $\dfrac{X}{X^2+1} = 0 + \dfrac{X}{X^2+1}$ donc $E\left(\dfrac{X}{X^2+1}\right) = 0$;

— Par division euclidienne, $2X^2 + 1 = (2X-2)(X+1) + 3$ donc

$$E\left(\frac{2X^2+1}{X+1}\right) = 2(X-1)\,.$$

Remarque XV.5. $E(F) = 0$ si et seulement si $\deg(F) < 0$.

c) Décomposition en éléments simples

◇ Le cas complexe

Théorème XV.4 (Décomposition en éléments simples (cas complexe))**.**
Soit $F \in \mathbb{C}(X)$ admettant n exactement n pôles $a_1, \dots, a_n$ de multiplicités respectives $k_1, \dots, k_n$. Alors il existe une unique famille $\alpha_{1,1}, \dots, \alpha_{k_1,1}, \alpha_{1,2}, \dots, \alpha_{k_n,n}$ de nombres complexes telle que :

$$F = E(F) + \sum_{j=1}^{n} \sum_{\ell=1}^{k_j} \frac{\alpha_{\ell,j}}{(X-a_j)^\ell}\,.$$

Démonstration. Admis. □

Et en pratique ? La première étape est dégager la partie entière, ce qui nous permet de partir du principe que notre fraction $F \in \mathbb{C}(X)$ est de degré strictement négatif.

Si les pôles sont simples : F est donc de la forme $\dfrac{A}{\prod_{i=1}^{n}(X-a_i)}$ avec $A \in \mathbb{C}_{n-1}[X]$.

On fixe alors $j_0 \in [\![1, n]\!]$ et on remarque que $G = (X - a_{j_0})F$ n'a plus de pôle en a_{j_0} et

$$G(a_{j_0}) = \frac{A(a_{j_0})}{\prod_{j \neq j_0}(X-a_j)}\,.$$

Par unicité dans la DES, on obtient que si

$$F = \sum_{j=0} \frac{\alpha_j}{(X - a_j)}$$

alors

$$\alpha_{jj_0} = \frac{A(a_{j_0})}{\prod\limits_{j \neq j_0} (X - a_j)} \, .$$

Cette formule étant au programme, il est admissible de l'utiliser directement.

➠ **Exemple XV.5.** La DES de $\dfrac{X}{(X-1)(X-2)}$ est

$$\frac{X}{(X-1)(X-2)} = \frac{\lambda}{X-1} + \frac{\mu}{X-2} \, ,$$

avec $\lambda = -1$ et $\mu = 2$.

Dans le cas général : on utilise les dérivées successives de la fraction rationnelle pour déterminer les coefficients du DES.

➠ **Exemple XV.6.** Considèrons la fraction rationnelle

$$F = \frac{X}{(X-1)(X-2)^2} \, .$$

Cette fraction est de degré -2 avec un pôle simple et un pôle double. Sa DES doit donc être de la forme :

$$F = \frac{\lambda}{X-1} + \frac{\mu}{X-2} + \frac{\nu}{(X-2)^2} \, .$$

Usant de la méthode vue *supra* relativement aux pôles simples, on trouve que $\lambda = 1$. Ensuite, en multipliant l'expression ci–dessus par $(X-2)^2$ et évaluant en "$X = 2$", on trouve :

$$\frac{2}{(2-1)} = \nu$$

et donc $\nu = 2$. Pour obtenir μ, on dérive l'expression ci dessus, puis on évalue en "$X = 2$", ce qui donne $\mu = -1$.

◇ **Le cas réel**

Théorème XV.5 (Décomposition en éléments simples (cas réel))**.**
Soit $F = \frac{P}{Q} \in \mathbb{R}(X)$ une fraction irréductible et soit

$$Q = \prod_{i=1}^{n}(X - a_i)^{\alpha_i} \prod_{i=1}^{m}(X^2 + p_i X + q_i)^{\beta_i}$$

la décomposition en produit de facteurs irréductibles de Q sur $\mathbb{R}$, avec :
— les $\alpha_i, \beta_i \in \mathbb{N}^*$;
— les $a_i, p_i, q_i \in \mathbb{R}$ vérifiant $p_i^2 - 4q_i < 0$.
Alors il existe une unique famille de réels $\lambda_{i,j}, \mu_{i,j}$ et $\nu_{i,j}$ telle que :

$$F = E(F) + \sum_{i=1}^{n}\sum_{j=1}^{\alpha_i} \frac{\lambda_{i,j}}{(X - a_i)^j} + \sum_{i=1}^{m}\sum_{j=1}^{\beta_i} \frac{\mu_{i,j} X + \nu_{i,j}}{(X^2 + p_i X + q_i)^j} \ .$$

Démonstration. Admis. □

En pratique, il est souvent efficace de décomposer en éléments sur simples sur $\mathbb{C}$ puis de regrouper les pôles conjugués. On peut aussi, se ramener à un système linéaire, comme illustré *infra.*

➠ **Exemple XV.7.** Pour déterminer la DES de $F = \frac{1}{X^3 - 1} = \frac{1}{(X-1)(X^2 + X + 1)}$, on part du théorème qui nous dit que cette dernière sera de la forme :

$$\frac{1}{(X-1)(X^2 + X + 1)} = \frac{\lambda}{X - 1} + \frac{\mu X + \nu}{X^2 + X + 1} \ .$$

Usant de la méthode usuelle, on trouve $\lambda = \frac{1}{3}$. De plus, on pose :

$$G = (X^2 + X + 1)F = \frac{1}{X - 1} = \lambda \frac{X^2 + X + 1}{X - 1} + \mu X + \nu$$

et on a, en évaluant G en 0 et 2 :

$$\begin{cases} -1 = -\lambda + \nu \\ 1 = 7\lambda + 2\mu + \nu \end{cases} ,$$

ce qui donne $\mu = -\frac{1}{3}$ et $\nu = -\frac{2}{3}$.

d) Dérivée logarithmique

Terminons ce chapitre par un exemple fondamental et fort utile. Si $P \in \mathbb{K}[X]$ est un polynôme non constant, alors il peut s'écrire (sur $\mathbb{C}$) sous la forme :

$$P = c \prod_{i=1}^{n} (X - a_i)^{k_i} ,$$

avec $c \in \mathbb{K}$, les $a_i \in \mathbb{C}$ et les $k_i \in \mathbb{N}^*$. De fait, si nous étions complètement malades, nous pourrions écrire la formule suivante :

$$\ln(P) = \ln(c) + \sum_{i=1}^{n} k_i \ln(X - a_i)$$

et "donc", en "dérivant" :

$$\frac{P'}{P} = \sum_{i=1}^{n} \frac{k_i}{X - a_i}\,.$$

Évidemment, on peut démontrer (et on doit savoir le faire !) cette formule proprement en utilisant les méthodes de calcul de DES vues précédemment, mais cette recette de cuisine impie a l'avantage de rester en mémoire.

➠ **Exemple XV.8.**

— $\dfrac{2X+4}{(X+2)^2} = \dfrac{2}{(X+2)}$;

— $\dfrac{nX^{n-1}}{X^n - 1} = \sum\limits_{k=1}^{n} \dfrac{1}{X - e^{\frac{2ik\pi}{n}}}$ pour $n \geq 1$.

Addendum : calcul de primitives

Les résultats vus dans ce chapitre nous permettent de calculer efficacement les primitives de fonctions rationnelles ; il nous suffit en effet de savoir le faire pour les éléments simples. Bien que les résultats de ce paragraphe soient *stricto sensu* hors programme, ils pourront être utile au lecteur avide d'approfondissement calculatoire et fournissent des techniques fort utiles au demeurant.

◇ Éléments simples de première espèce

On entend par la les éléments simples de la forme

$$f : x \mapsto \frac{1}{(x-a)^n}$$

avec $n \geq 1$ et $a \in \mathbb{C}$.

Cas 1 : $n \geq 2$. Une primitive de f est aisée à trouver :

$$F : x \mapsto \frac{-1}{(n-1)(x-a)^{n-1}}\,.$$

Cas 2 : $n = 1$. Si $a \in \mathbb{R}$, une primitive de f est $F : x \mapsto \ln(|x-a|)$. Sinon, posons $a = p + iq$ et remarquons que, pour tout x raisonnable :

$$\begin{aligned} f(x) &= \frac{1}{(x-p) - iq} \\ &= \frac{(x-p) + iq}{(x-p)^2 + q^2} \end{aligned}$$

et donc une primitive de f est donnée par

$$F : x \mapsto \frac{1}{2}\ln((x-p)^2 + q^2) + i\arctan\left(\frac{x-p}{q}\right).$$

◇ Éléments simples de deuxième espèce

On entend par la les éléments simples de la forme

$$f : x \mapsto \frac{\alpha x + \beta}{x^2 + px + q}$$

avec $\alpha, \beta, p, q \in \mathbb{R}$ et $p^2 - 4q < 0$. En posant, pour $x \in \mathbb{R}$, $t = x + \frac{p}{2}$, on obtient que $f(x) = g(t)$, où g est de la forme :

$$g : t \mapsto \frac{ut + v}{t^2 + a^2}$$

avec $u, v, a \in \mathbb{R}$ et $a \neq 0$. En effet :

$$\begin{aligned} x^2 + px + q &= \left(t - \frac{p}{2}\right)^2 + p\left(t - \frac{p}{2}\right) + q \\ &= t^2 - pt + \frac{p^2}{4} + pt - \frac{p^2}{2} + q \\ &= t^2 - \frac{p^2 - 4q}{4} \end{aligned}$$

et donc $a = \sqrt{-\frac{p^2 - 4q}{4}}$ est bien défini et non nul car $p^2 - 4q < 0$. Une primitive de g est donc donnée par :

$$G : t \mapsto \frac{u}{2} \ln(t^2 + a^2) + \frac{v}{a} \arctan\left(\frac{t}{a}\right) .$$

◇ Éléments simples de deuxième espèce, mais en différent

Le dernier type d'éléments simples dont nous avons besoin de déterminer une primitive est celui représenté (modulo translation similaire à ce qui a été fait dans le paragraphe *supra* par les deux intégrales suivantes (pour x réel) :

$$I_n = \int_0^x \frac{t}{(t^2 + a^2)^n} \, \mathrm{d}t \quad \text{et} \quad J_n = \int_0^x \frac{1}{(t^2 + a^2)^n} \, \mathrm{d}t$$

avec $a \in \mathbb{R}^*$ et $n \geq 2$. Remarquons dans un premier temps que, par forme composée usuelle :

$$I_n = \frac{-1}{2(n-1)(x^2 + a^2)^{n-1}}$$

et tentons de calculer J_n par IPP, appliquée aux fonctions $t :\mapsto t$ et $t \mapsto (t^2 + a^2)^{-n}$, de classes $\mathscr{C}^1$. On a alors :

$$\begin{aligned} J_n =& x(x^2 + a^2)^{-n} - n \int_0^x t \frac{-2t}{(t^2 + a^2)^{n+1}} \, \mathrm{d}t \\ &= x(x^2 + a^2)^{-n} + n \int_0^x \frac{2t^2}{(t^2 + a^2)^{n+1}} \, \mathrm{d}t \, . \end{aligned}$$

Or, pour tout $t \in [0, x]$:

$$\begin{aligned} \frac{t^2}{(t^2 + a^2)^{n+1}} &= \frac{t^2 + a^2}{(t^2 + a^2)^{n+1}} - \frac{a^2}{(t^2 + a^2)^{n+1}} \\ &= \frac{1}{(t^2 + a^2)^n} - \frac{a^2}{(t^2 + a^2)^{n+1}} \end{aligned}$$

et donc

$$J_n = x(x^2 + a^2)^{-n} + 2nJ_n - 2a^2nJ_{n+1}$$

i.e

$$J_{n+1} = \frac{x(x^2 + a^2)^{-n} + (2n-1)J_n}{2a^2n}$$

ce qui permet un calcul itératif de J_n.

Second semestre

Chapitre XVI

Dénombrement, combinatoire

1.⁻ Ensembles finis

a) Cardinal

On présente dans ce chapitre une version naïve de la théorie des ensembles finis. En particulier, la définition suivante est introduite sans vérifier que le cardinal est défini de façon unique. De façon générale, on passera sous silence toute démonstration technique afin d'alléger l'exposé et de rester dans le cadre du programme de MPSI.

Définition XVI.1. Soit E un ensemble. Alors, on dit que E est **fini** si il existe $n \geq 0$ et $f : E \to [\![1, n]\!]$ bijective. L'entier n est alors unique et appelé **cardinal** de E.

Notation. Le cardinal sera noté indifféremment $|E|$, $\mathrm{card}(E)$ ou parfois $\#E$.

✌ **Remarque XVI.1.** La bijection f représente (heuristiquement) une "façon d'étiqueter" les éléments de E par n entiers successifs.

➠ **Exemple XVI.1.**
— L'ensemble vide est fini de cardinal 0.
— L'ensemble $\{\spadesuit, \pitchfork, \clubsuit\}$ est fini de cardinal 3.

✌ **Remarque XVI.2.** Avec cette définition, il est rapide de vérifier que si E et F sont finis alors :
— il existe une bijection entre E et $F \Leftrightarrow \mathrm{card}(E) = \mathrm{card}(F)$;
— il existe une injection entre E et $F \Leftrightarrow \mathrm{card}(E) \leq \mathrm{card}(F)$;
— il existe une surjection entre E et $F \Leftrightarrow \mathrm{card}(E) \geq \mathrm{card}(F)$.

Proposition XVI.1. Soit E un ensemble fini et soit $E' \subset E$. Alors :
(i) E' est fini ;
(ii) $\mathrm{card}(E') \leq \mathrm{card}(E)$;
(iii) $E = E' \Leftrightarrow \mathrm{card}(E) = \mathrm{card}(E')$.

Démonstration. Les points (i) et (ii) découlent du fait que $x \mapsto x$ réalise une injection de E' dans E. Pour le cas d'égalité, procédons en deux temps.

(⇒) ¯_(ツ)_/¯

(⇐) Par contraposée, supposons que $E \neq E'$. Ceci signifie qu'il existe $e \in E \setminus E'$ et donc, en posant $n = \mathrm{card}(E')$ on a :

$$\mathrm{card}(E' \cup \{a\}) = n + 1$$

et, comme $E \cup \{a\} \subset E$:

$$n = \mathrm{card}(E') < n + 1 \leq \mathrm{card}(E)$$

d'où le résultat.

□

La proposition suivante est au cœur de bien de ce chapitre et de plusieurs de ses applications ultérieures. Il peut donc être utile d'y accorder quelque attention.

Proposition XVI.2. Soient E, F deux ensembles finis **de même cardinal** et soit $f : E \to F$ une application. Alors, les propriétés suivantes sont équivalentes :

(i) f est bijective ;

(ii) f est injective ;

(iii) f est surjective.

Démonstration. On procède de façon circulaire.

(i)⇒(ii) Trivial.

(ii)⇒(iii) Supposons f injective ; il en découle que $\mathrm{card}(f(E)) = \mathrm{card}(E)$. Par hypothèse, $\mathrm{card}(E) = \mathrm{card}(F)$ et donc $f(E)$ est une partie de F de cardinal égal à celui de F. *Ipso facto*, $f(E) = F$ et donc f est surjective.

(iii)⇒(i) Supposons f surjective ; alors si $x, y \in E$ sont deux éléments distincts tels que $f(x) = f(y)$, on aurait $\mathrm{card}(f(E)) < \mathrm{card}(E)$, ce qui est absurde car $f(E) = F$ est de même cardinal que E. La fonction f est donc bijective car injective et surjective.

□

✍ **Exercice XVI.1.** Démontrer que tout anneau commutatif intègre fini est un corps.

➥ **Correction :** *Soit $\mathbb{A}$ un anneau intègre fini et soit $a \in \mathbb{A} \setminus \{0\}$. Alors l'application*

$$\begin{aligned} f_a : \mathbb{A} &\to \mathbb{A} \\ x &\mapsto ax \end{aligned}$$

est injective (par intégrité) et donc surjective. De fait, il existe $x \in \mathbb{A}$ tel que $ax = 1$, d'où le résultat.

b) Opérations sur les ensembles finis

Proposition XVI.3. Soient $E_1, \dots, E_n$ des ensembles finis **deux à deux disjoints**. Alors, la réunion de ces ensembles est finie et

$$\operatorname{card}\left(\bigsqcup_{k=1}^{n} E_k\right) = \sum_{k=1}^{n} \operatorname{card}(E_k)\,.$$

✖ **Attention :** évidemment, ceci n'est vrai que pour les ensembles disjoints : le cardinal de la réunion $\{0,1\} \cup \{0,2\}$ n'est pas égal à 4.

Démonstration. Admise pour éviter tout technicité excessive. □

Remarque XVI.3. Si les ensembles ne sont pas supposés disjoints, on démontre par récurrence que :

$$\operatorname{card}\left(\bigcup_{k=1}^{n} E_k\right) \leq \sum_{k=1}^{n} \operatorname{card}(E_k)\,.$$

✍ **Exercice XVI.2.** Soit G un groupe fini (noté multiplicativement) et soit H un sous–groupe de G.

1. Justifier que H est fini.
2. (a) Vérifier que la relation

   $$x \sim y \Longleftrightarrow xy^{-1} \in H$$

   définit une relation d'équivalence sur G.

   (b) Démontrer que toutes les classes d'équivalences associées à la relation $\sim$ ont le même cardinal.
3. *Théorème de Lagrange.* Déduire de ce qui précède que $\operatorname{card}(H)$ divise $\operatorname{card}(G)$.

➥ **Correction :**

1. Immédiat par inclusion dans un ensemble fini.

2. (a) — Soit $x \in G$; alors $xx^{-1} = e \in H$, donc la relation est réflexive.

— Si $x, y \in G$ sont tels que $x \sim y$, i.e tels que $xy^{-1} \in H$, alors par stabilité $yx^{-1} = (xy^{-1})^{-1} \in H$. De fait, on a bien $y \sim x$ et donc la relation est symétrique.

— Si $x, y, z \in G$ sont tels que $x \sim y$ et $y \sim z$, alors par stabilité $xz^{-1} = (xy^{-1})(yz^{-1}) \in H$, d'où la transitivité.

(b) Soit $x \in H$; alors la classe d'équivalence de cet élément est donné par :

$$\bar{x} = \{y \in G \,|\, xy^{-1} \in H\}\,.$$

Ceci signifie que, pour tout $y \in G$, on a :

$$\begin{aligned} y \in \overline{x} &\Longleftrightarrow xy^{-1} \in H \\ &\Longleftrightarrow \exists\, h \in H,\ xy^{-1} = h \\ &\Longleftrightarrow \exists\, h \in H,\ y = h^{-1}x \end{aligned}$$

et donc

$$\overline{x} = Hx = \{hx \mid h \in H\} .$$

Il est ensuite aisé de démontrer que l'application suivante est une bijection :

$$\begin{aligned} \phi : H &\to Hx \\ h &\mapsto hx \end{aligned} \quad ,$$

ce qui implique que $\text{card}(\overline{x}) = \text{card}(H)$.

3. *On sait que les classes d'équivalences selon* $\sim$ *partitionnent l'ensemble* G *; ceci entraîne qu'il existe une famille* $C_1, \ldots, C_N$ *de telles classes* ***disjointes*** *telles que :*

$$G = \bigsqcup_{i=1}^{N} C_i$$

ergo :

$$\text{card}(G) = \sum_{i=1}^{N} \text{card}(C_i) = N\text{card}(H) ,$$

d'où le résultat.

Proposition XVI.4. Soient E et F deux ensembles finis. Alors :

(i) **si** $F \subset E$, $E \setminus F$ est fini et

$$\text{card}(E \setminus F) = \text{card}(E) - \text{card}(F) ;$$

(ii) $E \cup F$ et $E \cap F$ sont finis, avec :

$$\text{card}(E \cup F) = \text{card}(E) + \text{card}(F) - \text{card}(E \cap F) .$$

✌ **Remarque XVI.4.** La formule du crible de Poincaré, donnant le cardinal d'une réunion quelconque d'ensembles finis est hors programme. Le lecteur averti pourra se référer à la littérature, en prenant garde de porter des lunettes protectrices. En cas de contact direct avec la peau, consulter un médecin.

Démonstration. Il suffit de faire les deux remarques suivantes :

$$E = E \sqcup (E \setminus F)$$

et

$$E \cup F = (E \setminus (E \cap F)) \sqcup F .$$

□

✍ **Exercice XVI.3.** Soient E, F, G trois ensembles finis. Calculer $\text{card}(E \cup F \cup G)$.

➥ **Correction :** *On a :*

$$\begin{aligned}\operatorname{card}(E\cup F\cup G) &= \operatorname{card}(E\cup F)+\operatorname{card}(G)-\operatorname{card}((E\cup F)\cap G)\\ &= \operatorname{card}(E)+\operatorname{card}(F)+\operatorname{card}(G)-\operatorname{card}((E\cup F)\cap G)-\operatorname{card}(E\cap F)\\ &= \operatorname{card}(E)+\operatorname{card}(F)+\operatorname{card}(G)-\operatorname{card}((E\cap G)\cup(F\cap G))-\operatorname{card}(E\cap F)\\ &= \operatorname{card}(E)+\operatorname{card}(F)+\operatorname{card}(G)\\ &\quad -\operatorname{card}(E\cap G)-\operatorname{card}(F\cap G))-\operatorname{card}(E\cap F)\\ &\quad +\operatorname{card}(E\cap F\cap G)\,.\end{aligned}$$

Proposition XVI.5. Soient E, F des ensembles finis. Alors :
(i) $\operatorname{card}(E\times F)=\operatorname{card}(E)\operatorname{card}(F)$;
(ii) $\operatorname{card}(E^p)=\operatorname{card}(E)^p$ pour tout $p\in\mathbb{N}^*$.

Démonstration. Il suffit de remarquer pour le (i) que :

$$E\times F=\bigsqcup_{y\in F}E\times\{y\}\,.$$

Le point (ii) se traite ensuite par récurrence sur p. □

➠ **Exemple XVI.2.** Une expérience dans laquelle on a n choix puis m choix possède nm issues. Par exemple, un lancer de deux dés à 6 faces peut donner 36 résultats (pas somme) différents.

c) Parties d'un ensemble fini

Proposition XVI.6. Soit E un ensemble fini de cardinal n. Alors :

$$\operatorname{card}(\mathscr{P}(E))=2^n\,.$$

Démonstration. On procède par récurrence sur n. Le cas $n=0$ est trivial car $\mathscr{P}(\emptyset)=\{\emptyset\}$. Si la propriété est vraie au rang n et que E est un ensemble fini de cardinal n, on fixe $a\in E$ et $E'=E\setminus\{a\}$.

Soit $A\subset E$; alors :
— soit $a\notin A$ et dans ce cas $A\subset E'$. Par hypothèse de récurrence il existe 2^n telles parties ;
— soit $a\in A$ et alors $A\setminus\{a\}\subset E'$. Par hypothèse de récurrence il existe 2^n telles parties.

En conclusion, il existe $2^n+2^n=2^{n+1}$ parties distinctes de E. □

➠ **Exemple XVI.3.** $\operatorname{card}(\mathscr{P}([\![1,3]\!]))=8$.

d) Applications

Proposition XVI.7. Soient E et F deux ensembles finis. Alors :

$$\operatorname{card}(F^E) = \operatorname{card}(F)^{\operatorname{card}(E)} .$$

Démonstration. On procède par récurrence sur $p = \operatorname{card}(E)$.

— Si $p = 0$, E est vide et donc il existe une seule application dans F^E, donnée par le triplet $(\emptyset, F, \emptyset)$.

— Supposons la propriété vérifiée pour tous les ensembles de cardinal p, et fixons E un ensemble de cardinal $p+1$; on fixe $a \in E$ et $E' = E \setminus \{a\}$. Pour définir une application de E dans F il nous faut déterminer l'image de a ($\operatorname{card}(F)$) possibilités puis celles des éléments de E' ($\operatorname{card}(F)^p$ possibilités par hypothèse de récurrence). *In fine*,

$$\operatorname{card}(F^E) = \operatorname{card}(F) \times \operatorname{card}(F)^p = \operatorname{card}(F)^{\operatorname{card}(E)} .$$

□

➠ **Exemple XVI.4.** Il existe exactement 27 applications de $[\![1, 3]\!]$ dans lui–même, dont 6 sont bijectives (les éléments de $\mathfrak{S}_3$).

✍ **Exercice XVI.4.** Soit E un ensemble fini. Démontrer que l'application

$$\begin{aligned} \mathbb{1} : \mathscr{P}(E) &\to \{0,1\}^E \\ A &\mapsto \mathbb{1}_A \end{aligned}$$

est une bijection. Utiliser ce résultat pour retrouver la formule du cardinal de $\mathscr{P}(E)$.

2.– Un peu de combinatoire

a) Injections, bijections

Si E et F sont deux ensembles finis et que $f \in F^E$, on peut énoncer les reformulations suivantes relatives à l'inj/surj/bijectivité :

— f est **injective** $\Longleftrightarrow$ pour tout $y \in F$, $\operatorname{card}(f^{-1}(\{y\}) \leq 1$;

— f est **surjective** $\Longleftrightarrow$ pour tout $y \in F$, $\operatorname{card}(f^{-1}(\{y\}) \geq 1$;

— f est **bijective** $\Longleftrightarrow$ pour tout $y \in F$, $\operatorname{card}(f^{-1}(\{y\}) = 1$.

De plus, il nous est également possible de dénombrer les injections et bijections de E dans F *via* le résultat suivant. Un résultat (moche) relatif aux surjections existe, mais est hors–programme.

Proposition XVI.8. Soient E et F deux ensembles finis de cardinaux respectifs p et n. Alors :

(i) le nombre d'injections de E dans F est égal à $\dfrac{n!}{(n-p)!}$ si $n \geq p$ et 0 sinon ;

(ii) le nombre de bijections de E dans F est égal à $n!$ si $n = p$ et 0 sinon.

Démonstration. (i) Pour varier, procédons par récurrence sur $p = \text{card}(E)$. Si $p = 0$, on rigole, et si la propriété est vérifiée au rang p on fixe E un ensemble de cardinal $p+1$, $a \in E$ et $E' = E \setminus \{a\}$. Alors, pour définir une injection $f : E \hookrightarrow F$, il faut :
— choisir l'image de a (n possibilités) ;
— choisir (de façon injective) les images des éléments de E' dans $F \setminus \{f(a)\}$ $\left(\dfrac{(n-1)!}{(n-1-p)!} \text{ ou } 0 \text{ possibilité(s) par hypothèse de récurrence}\right)$.
Ainsi, dans le cas ou la deuxième quantité mentionnée est non nulle, on a le nombre d'injections suivant :

$$n \times \frac{(n-1)!}{(n-1-p)!} = \frac{n!}{(n-(p+1))!}$$

d'où le résultat.

(ii) Déjà traité au chapitre VIII lors de l'étude du groupe symétrique. On peut aussi utiliser la proposition XVI.2 et remarquer que si $n = p$ alors les injections de E dans F sont bijectives.

□

Notation. La quantité $\dfrac{n!}{(n-p)!}$ est notée $(n)_p$ et appelée **nombre d'arrangements** de p dans n.

✌ **Remarque XVI.5.** Notons que, si $n \geq p$:

$$(n)_p = n(n-1)\dots(n-p+1)\,.$$

Il s'agit du nombre de façon de classer p éléments parmi n.

➠ **Exemple XVI.5.** Il existe $\dfrac{9!}{2!} = 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 = 181\,440$ injections de $[\![1,7]\!]$ dans $[\![1,9]\!]$.

Corollaire XVI.8.a. Soit F un ensemble de cardinal n et soit $p \leq n$. Alors l'ensemble des p–listes ordonnées (suites finies d'éléments deux à deux distincts) d'éléments de F est fini de cardinal $(n)_p$.

Démonstration. Il s'agit en fait de dénombrer les injections de $[\![1,p]\!]$ dans $[\![1,n]\!]$. □

➠ **Exemple XVI.6.** Si on effectue 4 tirages **successifs** sans remise dans une urne contenant 10 objets distinguables, il existe $(10)_4 = 5040$ tirages possibles.

b) Parties de taille fixée

Nous venons de voir comment dénombrer les choix de p éléments parmi n **avec** un ordre fixé. Dans ce paragraphe, nous nous intéressons à la combinatoire des parties (**non ordonnées**, donc) de taille fixée d'un ensemble fini.

Notation. Si E est un ensemble fini et $k \in \mathbb{N}$, on note $\mathscr{P}_k(E)$ l'ensemble des parties de E de cardinal k.

Proposition XVI.9. Soient $n, k \in \mathbb{N}$ tels que $k \leq n$ et soit E un ensemble fini de cardinal n. Alors :
$$\operatorname{card}(\mathscr{P}_k(E)) = \binom{n}{k}.$$

Démonstration. Une récurrence sur n ? Joie !
- Si $n = 0$, la vie est belle.
- Supposons la propriété vérifiée pour $n \geq 0$. Soit E un ensemble de cardinal $n+1$, soit $A \in \mathscr{P}_k(E)$ et soit $a \in E$; on a alors deux possibilités : soit A ne contient pas a (et on dénombre par hypothèse de récurrence), soit A contient a et alors on dénombre les possibilités pour $A \setminus \{a\}$ via cette même, fort urbaine, hypothèse. *In fine* :
$$\operatorname{card}(\mathscr{P}_k(E)) = \binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$$
par formule de Pascal.

□

Exemple XVI.7. Si on tire 4 boules parmi 10 simultanément, il existe $\binom{10}{4} = 210$ issues possibles. Cela est très différent du tirage avec ordre vu précédemment.

Ces procédés combinatoires nous permettent de démontrer différemment certains résultats vus au chapitre II ; nous offrons gracieusement au lecteur un florilège de ceux–ci.

◇ Sommes des coefficients binomiaux

Si n est un entier naturel, on a :
$$\begin{aligned}\sum_{k=0}^{n} \binom{n}{k} &= \sum_{k=0}^{n} \operatorname{card}(\mathscr{P}_k(\llbracket 1, n \rrbracket)) \\ &= \operatorname{card}\left(\bigsqcup_{k=0}^{n} \mathscr{P}_k(\llbracket 1, n \rrbracket)\right) \\ &= \operatorname{card}(\mathscr{P}(\llbracket 1, n \rrbracket)) \\ &= 2^n.\end{aligned}$$

◇ Formule de Pascal

Soit E un ensemble de cardinal $n \geq 1$ et soit $k \leq n$. On fixe $a \in E$; alors pour construire une partie à k éléments de E, il faut :
- soit choisir k éléments parmi $E' = E \setminus \{a\}$;
- soit choisir $k-1$ éléments parmi E' et ajouter a.

De fait,
$$\operatorname{card}(\mathscr{P}_k(E)) = \operatorname{card}(\mathscr{P}_k(E')) + \operatorname{card}(\mathscr{P}_{k-1}(E'))$$
ce qui se traduit par :
$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

◇ **Binôme de Newton**

Soient $a, b \in \mathbb{C}$ et soit $n \geq 1$. Alors $(a+b)^n$ se développe en 2^n termes de la forme $a^k b^{n-k}$, où k est le nombre de facteurs dans lequel nous avons "choisi" a pour obtenir ce terme. Ce terme apparaîtra donc $\binom{n}{k}$ car ces k occurrences de a sont à "choisir" parmi n facteurs possibles.

$$(a+b)(a+b)(a+b)(a+b)$$

3 "choix" de a : $a^3 b^1$

Chapitre XVII

Analyse asymptotique

On fixe dans tout ce chapitre un corps $\mathbb{K}$ égal à $\mathbb{R}$ ou $\mathbb{C}$.

1.– Comparaison des fonctions

a) Négligeabilité, domination

Définition XVII.1. Soit $a \in \overline{\mathbb{R}}$ et soient f, g deux fonctions définies au voisinage de a (sauf peut–être en a) et telles que g ne s'annule pas au voisinage de a (sauf peut–être en a). On dira que :
- f est **dominée** par g au voisinage de a si la fonction $\frac{f}{g}$ est bornée au voisinage de a ;
- f est **négligeable** devant g au voisinage de a si $\frac{f(x)}{g(x)} \xrightarrow[x\to a]{} 0$.

Notation. La domination (resp. la négligeabilité) est notée $f(x) \underset{x\to a}{=} \mathcal{O}(g(x))$ (resp. $f(x) \underset{x\to a}{=} o(g(x))$) ou $f(x) \underset{x\to a}{=} \mathcal{O}(g(x))$ (resp. $f(x) \underset{x\to a}{=} o(g(x))$).

Exemple XVII.1.
- $x^2 \underset{x\to\infty}{=} o(x^4)$;
- $\frac{x^2}{2+x} \underset{x\to 0}{=} \mathcal{O}(x^2)$.

✖ **Attention :** le point où l'étude est effectuée est déterminant ; par exemple $x^2 \underset{x\to\infty}{=} o(x^3)$ mais $x^3 \underset{x\to 0}{=} o(x^2)$.

Remarque XVII.1.
- Négligeabilité implique domination ;
- les relations o et $\mathcal{O}$ sont transitives ;
- notons que les croissances comparées vues au chapitre II peuvent se traduire par les résultats suivants, si $\alpha, \beta, \gamma \in \mathbb{R}_+$:
  - $\ln(x)^\beta \underset{x\to\infty}{=} o(x^\alpha)$;
  - $|\ln(x)|^\beta \underset{x\to 0}{=} o(x^{-\alpha})$;

— $x^\alpha \underset{x\to\infty}{=} o(e^{\gamma x})$.

À ce stade, ceux d'entre vous qui ne sont pas recroquevillés en position fœtale se demandent probablement quel peut bien être l'usage de toutes ces comparaisons. En premier lieu et dans un premier temps, elles nous serviront à lever les indéterminations qui (facheusement) se produisent parfois lors de l'étude de limites.

Exemple XVII.2.
— $\dfrac{e^x}{x^3} \xrightarrow[x\to\infty]{} 0$ car $x^3 \underset{x\to\infty}{=} o(e^x)$.
— $x^2\ln(x)^7 \xrightarrow[x\to 0^+]{} 0$.

Proposition XVII.1. Soient f, g, h des fonctions définies au voisinage de $a \in \overline{\mathbb{R}}$ telles que $f(x) \underset{x\to a}{=} \mathcal{O}(h(x))$ et $g(x) \underset{x\to a}{=} \mathcal{O}(h(x))$. Alors :
(i) $f(x)+g(x) \underset{x\to a}{=} \mathcal{O}(h(x))$;
(ii) $f(x)g(x) \underset{x\to a}{=} \mathcal{O}(h(x)^2)$.

Remarque XVII.2. Ce résultat reste vrai en remplaçant "$\mathcal{O}$" par "o".

Démonstration. Immédiat par quotient. □

Remarque XVII.3. Cette proposition pourra être (abusivement) résumée par : "$\mathcal{O}(h(x)) + \mathcal{O}(h(x)) = \mathcal{O}(h(x))$ (et idem avec o et le produit).

b) Équivalence de fonctions

Définition XVII.2. Soient f, g deux fonctions définies au voisinage de a (sauf peut–être en a) et telles que g ne s'annule pas au voisinage de a (sauf peut–être en a). On dit que f est **équivalente** à g en a si $\dfrac{f(x)}{g(x)} \xrightarrow[x\to a]{} 1$.

Notation. $f(x) \underset{x\to a}{\sim} g(x)$ ou $f(x) \underset{x\to a}{\sim} g(x)$.

Exemple XVII.3. $x^3+x^2+x+1 \underset{x\to\infty}{\sim} x^3$.

Remarque XVII.4.
— Si f admet une limite **finie non nulle** ℓ en a, alors $\dfrac{f(x)}{\ell} \to 1$ et donc $f(x) \underset{x\to a}{\sim} \ell$.
— Seule les fonctions localement nulles sont équivalentes à 0.
— l'équivalence de fonctions en un point est une relation ...d'équivalence.

La propositions qui suit est une application directe de la définition d'équivalence des fonctions, dont la démonstrations est laissée en exercice au lecteur habité d'une motivation à l'épreuve des obus.

Proposition XVII.2. Soient f, g deux fonctions définies au voisinage de $a \in \overline{\mathbb{R}}$ (sauf peut–être en a) telles que $f(x) \underset{x\to a}{\sim} g(x)$. Alors :

(i) si $g(x) \xrightarrow[x\to a]{} \ell \in \overline{\mathbb{R}}$, alors $f(x) \xrightarrow[x\to a]{} \ell$;

(ii) si le signe de g est constant au voisinage de a, f vérifie la même propriété (avec un signe identique).

✖ **Attention :** la réciproque est **fausse** : il suffit de considérer $x \mapsto x$ et $x \mapsto x^2$ au voisinage de 0 pour s'en convaincre (j'espère !).

Démonstration. Découle trivialement de la définition d'équivalence. □

➠ **Exemple XVII.4.** $\dfrac{x^2+x}{x^3+x^2} \underset{x\to\infty}{\sim} \dfrac{1}{x}$ donc $\dfrac{x^2+x}{x^3+x^2} \xrightarrow[x\to\infty]{} 0$.

Proposition XVII.3. Soient f, g deux fonctions définies au voisinage de $a \in \overline{\mathbb{R}}$ (sauf peut–être en a). Alors :

$$f(x) \underset{x\to a}{\sim} g(x)$$
$$\Leftrightarrow$$
$$f(x) - g(x) \underset{x\to a}{=} o(g(x)).$$

✌ **Remarque XVII.5.** Cela nous permet de traduire le fait que $f(x) \underset{x\to a}{\sim} g(x)$ par l'égalité $f(x) \underset{x\to a}{=} g(x) + o(g(x))$ au voisinage de a. Ceci sera très utile en pratique.

Démonstration.

($\Rightarrow$) En posant $h = \dfrac{f}{g}$, on a $h(x) \xrightarrow[x\to a]{} 1$ et :

$$f(x) = h(x)g(x) \text{ au voisinage de } a.$$

On a donc, au voisinage de a :

$$f(x) - g(x) = (\underbrace{h(x) - 1}_{\to 0})g(x)$$

d'où le résultat.

($\Leftarrow$) En posant $h = \dfrac{f}{g}$, on a $h(x) \xrightarrow[x\to a]{} 0$ et :

$$f(x) - g(x) = h(x)g(x) \text{ au voisinage de } a.$$

De fait, toujours au voisinage de a, on a :

$$f(x) = (\underbrace{h(x) + 1}_{\to 1})g(x)$$

d'où le résultat.

□

Proposition XVII.4. Soit $a \in \overline{\mathbb{R}}$ et f, g, h définies au voisinage de a (sauf peut–être en a) telles que (toujours au voisinage de a) on ait :
— $f(x) \leq g(x) \leq h(x)$;
— $f(x) \underset{x \to a}{\sim} h(x)$.
Alors $f(x) \underset{x \to a}{\sim} g(x)$.

Démonstration. Immédiat par quotient. □

Proposition XVII.5. Soient f_1, f_2, g_1, g_2 des fonctions définies au voisinage de $a \in \overline{\mathbb{R}}$ telles que $f_1(x) \underset{x \to a}{\sim} f_2(x)$ et $g_1(x) \underset{x \to a}{\sim} g_2(x)$. Alors :

(i) $f_1(x)g_1(x) \underset{x \to a}{\sim} f_2(x)g_2(x)$;

(ii) **SI** g_1 ne s'annule pas au voisinage de a, c'est également le cas de g_2 et

$$\frac{f_1(x)}{g_1(x)} \underset{x \to a}{\sim} \frac{f_2(x)}{g_2(x)}.$$

✖ **ATTENTION :** on ne somme **PAS** les équivalents : $x \underset{x \to \infty}{\sim} x+1$ et $-x \underset{x \to \infty}{\sim} -x+1$ et pourtant $0 \underset{x \to \infty}{\not\sim} 2 \ldots$

Démonstration. Quitte à yada yada, il existe deux fonctions h, k ayant pour limite 1 en a telles que, au voisinage de a :

$$f_1(x) = h(x)f_2(x) \text{ et } g_1(x) = k(x)g_2(x)$$

et donc :

$$f_1(x)g_1(x) = (\underbrace{h(x)k(x)}_{\to 1})f_2(x)g_2(x)$$

d'où le résultat pour le produit. Le reste se démontre de façon analogue. □

➠ **Exemple XVII.5.** $\dfrac{x^2+x}{x^3+x^2} \underset{x \to \infty}{\sim} \dfrac{1}{x}$ car $x^2 + x \underset{x \to \infty}{\sim} x^2$ et $x^3 + x^2 \underset{x \to \infty}{\sim} x^3$.

c) Zoologie zérocentrique des équivalents usuels

Proposition XVII.6. On dispose des équivalents suivants en 0 :

(i) $e^x - 1 \underset{x\to 0}{\sim} x$;

(ii) $\ln(1+x) \underset{x\to 0}{\sim} x$;

(iii) $(1+x)^\alpha - 1 \underset{x\to 0}{\sim} \alpha x$, pour $\alpha \in \mathbb{R}^*$;

(iv) $\sin(x) \underset{x\to 0}{\sim} x$;

(v) $\tan(x) \underset{x\to 0}{\sim} x$;

(vi) $1 - \cos(x) \underset{x\to 0}{\sim} \dfrac{x^2}{2}$;

(vii) $\mathrm{sh}(x) \underset{x\to 0}{\sim} x$;

(viii) $\mathrm{ch}(x) - 1 \underset{x\to 0}{\sim} \dfrac{x^2}{2}$;

(ix) $\mathrm{th}(x) \underset{x\to 0}{\sim} x$;

(x) $\arcsin(x) \underset{x\to 0}{\sim} x$;

(xi) $\arctan(x) \underset{x\to 0}{\sim} x$.

Démonstration. Cela découle dans presque tous les cas de la limite du taux d'accroissement des fonctions étudiées en 0 ; par exemple

$$\frac{e^x - 1}{x} = \frac{e^x - e^0}{x - 0} \xrightarrow[x\to 0]{} 1 = e^0 .$$

Le point (vi) provient de l'égalité, pour $x \neq 0$:

$$\begin{aligned} 1 - \cos(x) &= 2\sin(x/2)^2 \\ &\underset{x\to 0}{\sim} 2\frac{x^2}{4} \\ &= \frac{x^2}{2} . \end{aligned}$$

On déduit le point (viii) d'un calcul similaire. □

d) Comparaison des suites numériques

Nous le savons désormais (*cf.* chapitre V), les suites numériques sont des applications de $\mathbb{N}$ dans $\mathbb{R}$ ou $\mathbb{C}$. Nous pouvons donc leur étendre les notions vues *supra*, via la définition suivante.

Définition XVII.3. Soient $u, v \in \mathbb{K}^{\mathbb{N}}$ telle que v ne s'annule pas. On dit que :
- u est **dominée** par v, noté $u_n = \mathcal{O}(v_n)$, si la suite $\left(\frac{u_n}{v_n}\right)_n$ est bornée ;
- u est **négligeable** devant v, noté $u_n = o(v_n)$, si $\frac{u_n}{v_n} \to 0$;
- u est **équivalente** à v, noté $u_n \sim v_n$, s$u_n = o(v_n)$, si $\frac{u_n}{v_n} \to 1$.-

Toutes les propositions vues précédemment se généralisent, en n'oubliant pas que les choses sont ici bien plus simples car les suites ont la politesse de n'avoir qu'une seule limite !

2.– Développements limités

a) Quoi ?

Définition XVII.4. Soit $n \in \mathbb{N}$, $a \in \mathbb{R}$ et soit f une fonction définie au voisinage de a. On dira que f admet un **développement limité d'ordre** n **en** a (DL_n(a)) si il existe une famille $a_0, \ldots, a_n$ d'éléments de $\mathbb{K}$ telle que :

$$f(x) \underset{x \to a}{=} \sum_{k=0}^{n} a_k (x-a)^k + o((x-a)^n)$$

au voisinage de a.

Vocabulaire. La somme apparaissant dans le membre de droite de cette égalité est appelée **partie régulière** du DL. Le reste est appelé **partie négligeable** de celui–ci.

✌ **Remarque XVII.6.**
- Une fonction admettant un DL_n(a) peut donc être approximée au voisinage de a par une fonction polynomiale de degré n.
- On démontre aisément que si f est (im)paire et admet un $\mathrm{DL}_n(0)$, celui–ci ne peut contenir que des puissances (im)paires.
- Quitte à poser $h = x-a$, on peut écrire tout DL_n(a) sous **forme normalisée** :

  $$f(a+h) \underset{h \to 0}{=} \sum_{k=0}^{n} a_k h^k + o(h^n)$$

  soit, si $p = \min\{k \in \mathbb{N} \,|\, a_k \neq 0\}$:

  $$f(a+h) \underset{h \to 0}{=} h^p(a_p + a_{p+1}h + \ldots + a_n h^{n-p} + o(h^{n-p})) .$$

  Ceci nous permet de démontrer que $f(a+h) \underset{h \to 0}{\sim} a_p h^p$ et, par conséquent, d'étudier le signe de f au voisinage de a.

➠ **Exemple XVII.6.**

— $e^x \underset{x\to 0}{=} 1+x+o(x)$; notons que tous les équivalents usuels vus précédemment nous livrent des DL d'ordre 1 ou 2.
— $\cos(x) \underset{x\to 0}{=} 1 - \dfrac{x^2}{2} + o(x^2)$.
— Un exemple fondamental est celui des sommes géométriques ; si $x \in]-1,1[$ et $n \geq 0$, on a :

$$\begin{aligned}\sum_{k=0}^{n} x^k &= \frac{1-x^{n+1}}{1-x}\\ &= \frac{1}{1-x} + \frac{x^{n+1}}{x-1}\\ &\underset{x\to 0}{=} \frac{1}{1-x} + o(x^n)\ .\end{aligned}$$

— Pour obtenir un DL d'un polynôme, il suffit de tronquer le degré à l'ordre voulu.

Proposition XVII.7. Si une fonction f admet un $\mathrm{DL}_n(\mathrm{a})$ pour $a \in \mathbb{R}$, alors ce dernier est unique.

Démonstration. Supposons qu'il existe deux familles $a_0, \dots a_n$ et $b_0, \dots, b_n$ de réels telles que :

$$f(x) \underset{x\to a}{=} \sum_{k=0}^{n} a_k (x-a)^k + o((x-a)^n) \underset{x\to a}{=} \sum_{k=0}^{n} b_k (x-a)^k + o((x-a)^n)\ .$$

Alors, par soustraction, on a :

$$\sum_{k=0}^{n} (a_k - b_k)(x-a)^k \underset{x\to a}{=} o((x-a)^n)\ .$$

Si il existe $k \in [\![0,n]\!]$ tel que $a_k \neq b_k$, on peut poser $k_0 = \min\{k \in [\![0,n]\!] \mid a_k \neq b_k\}$ et vérifier que

$$\frac{\sum\limits_{k=0}^{n} (a_k - b_k)(x-a)^k}{(a_{k_0} - b_{k_0})(x-a)^{k_0}} \underset{x\to a}{\longrightarrow} 1$$

i.e

$$\sum_{k=0}^{n} (a_k - b_k)(x-a)^k \underset{x\to a}{\sim} (a_{k_0} - b_{k_0})(x-a)^{k_0}\ .$$

Ceci contredit le fait que cette somme soit un $o_a((x-a)^n)$ car $k_0 \leq n$, d'où le résultat. ☐

Proposition XVII.8. Soit f une fonction définie au voisinage de $a \in \mathbb{R}$. Alors :
(i) f admet un $\mathrm{DL}_0(a) \Leftrightarrow f$ est continue en a ;
(ii) f admet un $\mathrm{DL}_1(a) \Leftrightarrow f$ est dérivable en a.

Démonstration. Le (i) découle de la définition de continuité et le (ii) a été démontré dans le chapitre XI (proposition XI.1). □

✖ **Attention :** ce résultat ne se généralise **pas** aux ordres supérieurs.

b) Formule de Taylor–Young

Ce résultat découle de la formule établie par Brook Taylor (anglais, 1685—1731) pour les polynômes (et vue au chapitre XIV) et affinée par William Henry Young (anglais, 1863—1942). La démonstration de ce résultat est hors–programme. Il peut toutefois être vu comme une conséquence de la proposition XX.19.

Théorème XVII.9 (Taylor–Young)**.**
Soit f une fonction de classe $\mathscr{C}^n$ au voisinage de $a \in \mathbb{R}$. Alors admet un DL_n(a) donné par la formule :

$$f(a+h) \underset{h\to 0}{=} \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!} h^k + o(h^n)\ .$$

Remarque XVII.7. Ceci entraîne qu'il y a existence et unicité du DL_npour les fonctions de classe $\mathscr{C}^n$.

◇ Développements limités usuels en 0

La formule de Taylor–Young permet de démontrer les DL suivants en 0, qui nous seront utiles par la suite.

$$\begin{aligned}\frac{1}{1-x} &\underset{x\to 0}{=} \sum_{k=0}^{n} x^k + o(x^n)\\ &\underset{x\to 0}{=} 1 + x + x^2 + \ldots + x^n + o(x^n)\end{aligned}$$

$$\begin{aligned}\ln(1+x) &\underset{x\to 0}{=} \sum_{k=1}^{n} (-1)^{k+1} \frac{x^k}{k} + o(x^n)\\ &\underset{x\to 0}{=} x - \frac{x^2}{2} + \frac{x^3}{3} + \ldots + (-1)^{n+1}\frac{x^n}{n} + o(x^n)\end{aligned}$$

$$\begin{aligned}(1+x)^\alpha &\underset{x\to 0}{=} 1 + \sum_{k=1}^{n} \left(\prod_{i=0}^{k-1} (\alpha - i)\right) \frac{x^k}{k!} + o(x^n)\\ &\underset{x\to 0}{=} 1 + \alpha x + \frac{\alpha(\alpha-1)}{2} x^2 + \frac{\alpha(\alpha-1)(\alpha-2)}{6} x^3 + \ldots\\ &\qquad \ldots + \frac{\alpha(\alpha-1)\ldots(\alpha-n+1)}{n!} x^n + o(x^n)\end{aligned}$$

$$\begin{aligned} e^x &\underset{x\to 0}{=} \sum_{k=0}^{n} \frac{x^k}{k!} + o(x^n) \\ &\underset{x\to 0}{=} 1 + x + \frac{x^2}{2} + \ldots + \frac{x^n}{n!} + o(x^n) \end{aligned}$$

$$\begin{aligned} \cos(x) &\underset{x\to 0}{=} \sum_{k=0}^{n} (-1)^k \frac{x^{2k}}{(2k)!} + o(x^{2n+1}) \\ &\underset{x\to 0}{=} 1 - \frac{x^2}{2} + \frac{x^4}{24} + \ldots + (-1)^n \frac{x^{2n}}{(2n)!} + o(x^{2n+1}) \end{aligned}$$

$$\begin{aligned} \sin(x) &\underset{x\to 0}{=} \sum_{k=0}^{n} (-1)^k \frac{x^{2k+1}}{(2k+1)!} + o(x^{2n+2}) \\ &\underset{x\to 0}{=} x - \frac{x^3}{6} + \frac{x^5}{120} + \ldots + (-1)^n \frac{x^{2n+1}}{(2n+1)!} + o(x^{2n+2}) \end{aligned}$$

$$\begin{aligned} \mathrm{ch}(x) &\underset{x\to 0}{=} \sum_{k=0}^{n} \frac{x^{2k}}{(2k)!} + o(x^{2n+1}) \\ &\underset{x\to 0}{=} 1 + \frac{x^2}{2} + \frac{x^4}{24} + \ldots + \frac{x^{2n}}{(2n)!} + o(x^{2n+1}) \end{aligned}$$

$$\begin{aligned} \mathrm{sh}(x) &\underset{x\to 0}{=} \sum_{k=0}^{n} \frac{x^{2k+1}}{(2k+1)!} + o(x^{2n+2}) \\ &\underset{x\to 0}{=} x + \frac{x^3}{6} + \frac{x^5}{120} + \ldots + \frac{x^{2n+1}}{(2n+1)!} + o(x^{2n+2}) \end{aligned}$$

$$\begin{aligned} \arctan(x) &\underset{x\to 0}{=} \sum_{k=0}^{n} (-1)^k \frac{x^{2k+1}}{2k+1} + o(x^{2n+2}) \\ &\underset{x\to 0}{=} x - \frac{x^3}{3} + \ldots + (-1)^n \frac{x^{2n+1}}{2n+1} + o(x^{2n+2}) \end{aligned}$$

$$\tan(x) \underset{x\to 0}{=} x + \frac{x^3}{3} + o(x^3)$$

c) Pourquoi ?

En pratique, les DL ont de nombreux usages, outre celui de générer de charmantes sessions de calcul. D'une façon générale, ils permettes d'étudier en finesse le comportement d'une fonction au voisinage d'un point donné.

◇ Limites

Une fonction est équivalente à la partie régulière de son DL : cela permet souvent de lever des indéterminations. Par exemple :

$$\frac{\sin(x)}{x} \underset{x\to 0}{\sim} \frac{x}{x} = 1 \xrightarrow[x\to 0]{} 1\,.$$

De même, certains taux d'accroissements voient leur vie considérablement simplifiée (d'aucun diraient limitée) par ce type d'étude.

$$\begin{aligned}\forall x \neq 0,\ \frac{\frac{\sin(x)}{x}-1}{x-0} &= \frac{\sin(x)}{x^2} - \frac{1}{x}\\ &\underset{x\to 0}{=} \frac{x - \frac{x^3}{6} + o(x^3)}{x^2} - \frac{1}{x}\\ &\underset{x\to 0}{=} -\frac{x}{6} + o(x)\\ &\xrightarrow[x\to 0]{} 0\end{aligned}$$

et donc le sinus cardinal (*cf.* chapitre XI) est dérivable en 0 de dérivée nulle. En réalité, on peut itérer ce procédé et démontrer que cette fonction est de classe $\mathscr{C}^\infty$ sur $\mathbb{R}$.

◇ Extrema locaux

Nous avons vu dans le chapitre XI que toute fonction f dérivable admettant un extremum local en un point $a \in \mathbb{R}$ vérifiait $f'(a) = 0$ (on dit que a est un **point critique** pour f). La notion de développement limité nous permet d'affiner quelque peu cette étude et d'en obtenir une réciproque partielle via la proposition suivante.

Proposition XVII.10. Soit f une fonction **à valeurs réelles** admettant un développement limité d'ordre 2 en un point $a \in \mathbb{R}$ et vérifiant que $f'(a) = 0$. On a de fait l'existence de $\lambda \in \mathbb{R}$:

$$f(x) = f(a) + \lambda(x-a)^2 + o((x-a)^2)\,.$$

Alors :

(i) si $\lambda > 0$, f admet un minimum local en a ;

(ii) si $\lambda < 0$, f admet un maximum local en a.

Démonstration. Immédiat : au voisinage de a, $f(x) - f(a)$ est du signe de λ si ce dernier est non nul. □

➠ **Exemple XVII.7.** Ceci nous permet de vérifier que cos admet un maximum local en 0.

✌ **Remarque XVII.8.**

— Dans le cas où $\lambda = 0$, on ne peut conclure. Étudier le cas des fonctions $x \mapsto x^3$ et $x \mapsto x^2$ en 0.

— Si f est de classe $\mathscr{C}^2$, on a $\lambda = \dfrac{f''(a)}{2}$.

d) Opérations sur les développements limités

Dans ce paragraphe, nous nous attachons à donner une série de "recettes" permettant de calculer efficacement avec les développements limités. L'objectif est ici presque purement opérationnel : nous ne nous attarderons pas plus que nécessaire sur le caractère général des résultats énoncé.

◇ Troncature

Pour le moment tout va bien : si une fonction admet un DL_n(a), on peut lui trouver des DL à des ordres inférieurs quitte à tronquer la partie régulière.

◇ Combinaison linéaire

Si $a \in \mathbb{R}$ et f et g sont deux fonctions admettant des DL_n(a), alors pour tout $\lambda \in \mathbb{R}$, $f + \lambda g$ admet un DL_n(a) obtenu en combinant linéairement les parties régulières de ceux de f et g.

➠ **Exemple XVII.8.** On retrouve de cette façon les DL de ch et sh à partir de celui de exp.

◇ Produit

Soit $a \in \mathbb{R}$ et soient f, g admettant les DL_n(a) suivants :

$$f(x) \underset{x\to a}{=} \sum_{k=0}^{n} a_k(x-a)^k + o((x-a)^n) \quad \text{et} \quad g(x) \underset{x\to a}{=} \sum_{k=0}^{n} b_k(x-a)^k + o((x-a)^n)\,.$$

Alors, par relation sur les "o" et produit de polynômes, fg admet le DL_n(a) suivant :

$$f(x)g(x) \underset{x\to a}{=} \sum_{k=0}^{n} \left(\sum_{j=0}^{k} a_j b_{k-j} \right) (x-a)^k + o((x-a)^n)\,.$$

En pratique, il s'agit ici de faire le produit des parties régulières en ne conservant que les puissances inférieures ou égales à n.

➠ **Exemple XVII.9.** Cherchons à obtenir un $\mathrm{DL}_3(0)$ de $x \mapsto e^x \sin(x)$. Pour cela, notons dans un premier temps que :

$$e^x \underset{x\to 0}{=} 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + o(x^3)$$

et

$$\sin(x) \underset{x\to 0}{=} x - \frac{x^3}{6} + o(x^3)$$

et que, pour tout $x \in \mathbb{R}$:

$$\begin{aligned}(1 + x + \frac{x^2}{2} + \frac{x^3}{6})(x - \frac{x^3}{6}) &\underset{x\to 0}{=} x - \frac{x^3}{6} + x^2 + \frac{x^3}{2} + o(x^3) \\ &\underset{x\to 0}{=} x + x^2 + \frac{x^3}{3} + o(x^3)\,.\end{aligned}$$

In fine, on a donc :

$$e^x \sin(x) \underset{x\to 0}{=} x + x^2 + \frac{x^3}{3} + o(x^3)\,.$$

◇ **Composition**

Aucun résultat général n'est au programme : il s'agit ici de chercher à faire simple et efficace. Si f et g admettent un $\mathrm{DL}_n(0)$ (quitte à se ramener en ce point par un changement de variable) **et** que $g(0) = 0$ (ou *a minima* $g(x) \underset{x\to 0}{\longrightarrow} 0$, mais je chipote) alors la composée $f \circ g$ admet un $\mathrm{DL}_n(0)$ (pour peu qu'elle soit bien définie). On trouve la partie régulière de ce dernier en priant très fort.

➠ **Exemple XVII.10.** Au voisinage de 0, on a :

$$\ln(\cos(x)) = \ln(1 + \underbrace{\cos(x) - 1}_{\text{vaut 0 en 0}}) .$$

Or :

$$\ln(1+u) \underset{u\to 0}{=} u - \frac{u^2}{2} + o(u^2)$$

et

$$\cos(x) - 1 \underset{x\to 0}{=} -\frac{x^2}{2} + o(x^2)$$

ce qui permet de conclure que :

$$\ln(\cos(x)) \underset{x\to 0}{=} -\frac{x^2}{2} + o(x^2)$$

car $(\cos(x) - 1)^2 \underset{x\to 0}{=} o(x^2)$.

✖ **Attention :** si il est vrai que l'on peut composer les DL, il ne faut **surtout pas** se laisser aller à composer les équivalents. En effet, $x \underset{x\to\infty}{\sim} x+1$ et pourtant $e^x \underset{x\to\infty}{\not\sim} e^{x+1}$.

◇ **Inverse**

L'idée est ici de composer le DL par celui de $x \mapsto \dfrac{1}{1-x}$. Une fois de plus, un peu de courage et (éventuellement) un sac à vomi sont des atouts précieux.

➠ **Exemple XVII.11.** Développons $x \mapsto \dfrac{1}{\cos(x)}$ à l'ordre 4 en 0. Faites comme on vous dit et il n'y aura pas de blessé. Commençons par remarquer que :

$$\frac{1}{\cos(x)} = \frac{1}{1 - \underbrace{(1-\cos(x))}_{\text{vaut 0 en 0}}} .$$

On sait de plus que :

$$\frac{1}{1-u} \underset{u\to 0}{=} 1 + u + u^2 + u^3 + u^4 + o(u^4) .$$

En posant, au voisinage de 0, $u = 1 - \cos(x)$ (oui, je sais...), on obtient :

$$u \underset{x\to 0}{=} \frac{x^2}{2} - \frac{x^4}{24} + o(x^4) ;$$

$$u^2 \underset{x\to 0}{=} \frac{x^4}{4} + o(x^4)$$

et

$$u^3,\ u^4 \underset{x\to 0}{=} o(x^4)\ .$$

Au final, on obtient :

$$\frac{1}{\cos(x)} \underset{x\to 0}{=} 1 + \frac{x^2}{2} + \frac{5x^4}{24} + o(x^4)\ .$$

Évidemment, pour obtenir le DL d'un quotient, nous passons par le produit de l'inverse. Le lecteur audacieux pourra utiliser l'exemple *supra* pour retrouver le DL de tan en 0.

◇ Primitives

Proposition XVII.11. Soit $a \in \mathbb{R}$ et soit f une fonction admettant un DL_n(a) donné par

$$f(x) \underset{x\to a}{=} \sum_{k=0}^{n} a_k(x-a)^k + o((x-a)^n)\ .$$

Alors toute primitive F de f admet un $\mathrm{DL}_{n+1}(a)$ donné par la formule :

$$F(x) \underset{x\to a}{=} F(a) + \sum_{k=0}^{n} \frac{a_k}{k+1}(x-a)^{k+1} + o((x-a)^{n+1})\ .$$

Démonstration. Immédiat. □

✌ **Remarque XVII.9.** Ceci nous permet de retrouver très rapidement les DL de arctan et $x \mapsto \ln(1+x)$.

✍ **Exercice XVII.1.** Déterminer un DL d'ordre 5 de arcsin en 0.

➥ **Correction :** *On sait que, pour tout* $x \in]-1,1[$ *:*

$$\arcsin'(x) = \frac{1}{\sqrt{1-x^2}}$$

et que :

$$\begin{aligned}\frac{1}{\sqrt{1-x^2}} &= (1+(-x^2))^{-1/2}\\ &\underset{x\to 0}{=} 1 + \frac{x^2}{2} + \frac{3x^4}{8} + o(x^4)\ .\end{aligned}$$

On en déduit que :

$$\arcsin(x) \underset{x\to 0}{=} x + \frac{x^3}{6} + \frac{3x^5}{40} + o(x^5)\ .$$

3.⁻ Développements asymptotiques

a) Quoi maintenant ?

Jusque ici, nous avons fait des développements limités, à savoir des approximations de fonction en un point **réel** par un **polynôme**. Un peu contraignant n'est–il pas ? L'objectif de ce paragraphe est d'en finir avec ces limitations et de déverrouiller notre plein potentiel calculatoire. Ou quelque chose de ce genre. Nous nous contenterons de donner quelques exemples afin de nourrir la réflexion (et/ou les cauchemars) de notre lecteur.

➠ **Exemple XVII.12.** Développons la fonction $f : x \mapsto x^x$ en 0. Ne mentez pas, je sais que vous en avez toujours rêvé. On a, au voisinage de 0 :

$$\begin{aligned} f(x) &= e^{x\ln(x)} \\ &\underset{x\to 0}{=} 1 + x\ln(x) + \frac{x^2\ln(x)^2}{2} + o(x^2\ln(x)^2)\,. \end{aligned}$$

Notons que la composée de DL ci–dessus est valable car $x\ln(x) \xrightarrow[x\to 0]{} 0$. Ce résultat ne constitue pas un DL *stricto sensu*, mais nous apporte des informations assez précises sur le comportement asymptotique de f, ce qui est fort sympathique au demeurant : on parle de **développement asymptotique (DA) d'ordre** 2 **en** $x\ln(x)$ **au voisinage de** 0.

✍ **Exercice XVII.2.** Déterminer la limite en $+\infty$ de $x \mapsto \sqrt{x^2+1} - \sqrt{x^2-1}$.

➥ **Correction :** *Posons, pour $x > 0$, $t = \dfrac{1}{x}$. Alors on a :*

$$\begin{aligned} \sqrt{x^2-1} &= \sqrt{\frac{1}{t^2} - 1} \\ &= \sqrt{\frac{1-t^2}{t^2}} \\ &= \frac{1}{t}\sqrt{1-t^2} \end{aligned}$$

et, de façon analogue :

$$\sqrt{x^2+1} = \frac{1}{t}\sqrt{1+t^2}\,.$$

En faisant en DL (en t) à l'ordre 4 en 0, nous obtenons que :

$$\sqrt{1 \pm t^2} \underset{t\to 0}{=} 1 \pm \frac{t^2}{2} - \frac{t^4}{8} + o(t^4)$$

ce qui entraîne que :

$$\begin{aligned} \frac{1}{t}\sqrt{1+t^2} - \frac{1}{t}\sqrt{1-t^2} &\underset{t\to 0}{=} \frac{1}{t} + \frac{t}{2} - \frac{t^3}{8} - \left(\frac{1}{t} - \frac{t}{2} - \frac{t^3}{8}\right) + o(t^3) \\ &\underset{t\to 0}{=} t + o(t^3)\,. \end{aligned}$$

En conclusion, nous pouvons écrire (en repassant à la variable x) :

$$\sqrt{x^2+1} - \sqrt{x^2-1} \underset{x\to\infty}{=} \frac{1}{x} + o\left(\frac{1}{x^3}\right) \xrightarrow[x\to\infty]{} 0\,.$$

Notons qu'un DL à l'ordre 1 suffisait (peut–être...). Mais bon, quand on aime, on ne compte pas.

Exemple XVII.13. Souvenons nous que, pour tout $x > 0$:

$$\arctan(x) = \frac{\pi}{2} - \arctan\left(\frac{1}{x}\right)$$

et donc, on peut établir que :

$$\arctan(x) \underset{x\to\infty}{=} \frac{\pi}{2} - \frac{1}{x} + \frac{1}{3x^3} + o\left(\frac{1}{x^3}\right) .$$

L'usage des développements asymptotiques permet une flexibilité que n'autorisent pas les DL. On se retrouve donc souvent, dans les sciences fondamentales et appliquées, à en faire usage pour résoudre divers problèmes.

Exercice XVII.3. Soit $n \in \mathbb{N}$. On pose :

$$I_n = \int_0^1 \frac{\mathrm{d}t}{1+t^n} .$$

1. Démontrer que $I_n = 1 + \mathscr{O}\left(\frac{1}{n}\right)$.
2. À l'aide d'une intégration par parties, montrer que :

$$I_n = 1 - \frac{\ln(2)}{n} + o\left(\frac{1}{n}\right) .$$

Correction :

1. *On vérifie rapidement que, pour tout $n \in \mathbb{N}$ on a :*

$$0 \leq 1 - I_n = \int_0^1 \frac{t^n}{1+t^n}\,\mathrm{d}t \leq \int_0^1 t^n\,\mathrm{d}t = \frac{1}{n+1} .$$

Ainsi, par encadrement, on a le résultat voulu.

2. *Les fonctions $t \mapsto t$ et $t \mapsto \frac{\ln(1+t^n)}{n}$ étant de classe $\mathscr{C}^1$ sur $[0,1]$, une IPP nous livre :*

$$\begin{aligned}\forall n \in \mathbb{N}^*,\ \int_0^1 \frac{t^n}{1+t^n}\,\mathrm{d}t &= \int_0^1 t \times \frac{t^{n-1}}{1+t^n}\,\mathrm{d}t\\ &= \left[\frac{t}{n}\ln(1+t^n)\right]_0^1 - \int_0^1 \frac{1}{n}\ln(1+t^n)\,\mathrm{d}t\\ &= \frac{\ln(2)}{n} - \frac{1}{n}\int_0^1 \ln(1+t^n)\,\mathrm{d}t .\end{aligned}$$

Or, par concavité du logarithme, on a vu dans le chapitre XI que $\ln(1+u) \leq u$ pour $u \in]-1,\infty[$. De fait et par croissance de l'intégrale (que nous reverrons dans le chapitre XX), on a :

$$\frac{1}{n}\int_0^1 \ln(1+t^n)\,\mathrm{d}t \leq \int_0^1 t^n\,\mathrm{d}t = \frac{1}{n+1}$$

ce qui entraîne que :

$$\int_0^1 \ln(1+t^n)\,\mathrm{d}t \xrightarrow[n\to\infty]{} 0$$

et donc que :

$$\begin{aligned} I_n - 1 &= -\frac{\ln(2)}{n} + \frac{1}{n}\int_0^1 \ln(1+t^n)\,\mathrm{d}t \\ &= -\frac{\ln(2)}{n} + o\left(\frac{1}{n}\right) \end{aligned}$$

d'où le résultat.

b) Tangentes, asymptotes

Comme nous l'avons évoqué dans le chapitre XI, le calcul du DL à l'ordre 1 d'une fonction nous livre directement une équation des tangentes à sa courbe représentative. Plus précisément, si une fonction f admet en un point a de son ensemble de définition un DL de la forme

$$f(x) \underset{x\to a}{=} \beta + \alpha(x-a) + o((x-a))$$

alors la droite d'équation $y = \alpha(x-a) + \beta$ est tangente à la courbe de f au point $(a, f(a))$ et la position relative de ces deux objets géométriques peut être déterminée à l'aide du terme suivant (selon les puissances croissantes de $(x-a)$) du DL (si il existe). Tout lien avec la convexité est évidemment non fortuit...

Similairement, si une fonction f admet un DA de la forme

$$f(x) \underset{x\to\infty}{=} ax + b + o(1)\,,$$

alors on peut dire que la droite d'équation $y = ax+b$ est une **asymptote** à la courbe représentative de f au voisinage de l'infini (on peut évidemment faire la même chose en $-\infty$). La aussi, le terme suivant du DA (selon les puissances **décroissantes** de x) nous livrera la position de la courbe relativement à son asymptote.

✍ **Exercice XVII.4.** Étudier tangentes et asymptotes de la fonction $f : x \mapsto \sqrt{1+x+x^2}$.

c) Formule de Stirling

Achevons ce chapitre (et le lecteur) en énonçant la formule suivante, du à Abraham de Moivre (français, 1667—1754) et James Stirling (écossais, 1692—1770). Le premier démontra la formule sans calculer la constante apparaissant dans l'équivalent, injustice réparée par le second.

Théorème XVII.12 (Stirling)**.**

$$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}\,.$$

Démonstration. Admis. □

✌ **Remarque XVII.10.** Cette formule peut être interpretée comme un développement asymptotique. En effet, si

$$n! = \left(\frac{n}{e}\right)^n \sqrt{2\pi n} + o\left(\left(\frac{n}{e}\right)^n \sqrt{n}\right)$$

alors on a :

$$\ln(n!) = n\ln(n) - n + \frac{1}{2}\ln(2\pi n) + o(\ln(n))\,.$$

✍ **Exercice XVII.5.** Déterminer la limite de $\left(\dfrac{e^n}{n!}\right)_n$.

Chapitre XVIII

Espaces vectoriels

On fixe dans tout ce chapitre un corps $\mathbb{K}$ égal à $\mathbb{R}$ ou $\mathbb{C}$.

1.⁻ Structures linéaires

a) C'est quoi ?

Définition XVIII.1. Soit E un ensemble muni d'un loi de composition interne $+ : E \times E \to E$ et d'une loi de composition externe $\cdot : \mathbb{K} \times E \to E$. On dit que le triplet $(E, +, \cdot)$ est un $\mathbb{K}$–**espace vectoriel** (abrégé $\mathbb{K}$–e.v) si :

(A) $(E, +)$ est un groupe abélien ;

(B) $\forall x \in E$, $1_{\mathbb{K}} \cdot x = x$;

(C) $\forall \lambda \in \mathbb{K}$, $\forall x, y \in E$, $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$;

(D) $\forall \lambda, \mu \in \mathbb{K}$, $\forall x \in E$, $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$;

(E) $\forall \lambda, \mu \in \mathbb{K}$, $\forall x \in E$, $(\lambda\mu) \cdot x = \lambda \cdot (\mu \cdot x)$.

Vocabulaire. Les éléments de E sont appelés **vecteurs**, ceux de $\mathbb{K}$ **scalaires**.

✌ **Remarque XVIII.1.** La donnée des lois de composition pourra être sous entendue, tout comme la notation "$\cdot$" pour la multiplication externe.

➠ **Exemple XVIII.1.**
- $\mathbb{K}$ est un $\mathbb{K}$–e.v ; la multiplication externe est alors interne ;
- l'ensemble $\mathscr{F}(\mathbb{K}, \mathbb{K}) = \mathbb{K}^{\mathbb{K}}$ est un $\mathbb{K}$–e.v pour l'addition des fonctions et leur multiplication par une constante ;
- $\{0_{\mathbb{K}}\}$ est un $\mathbb{K}$–e.v, appelé **espace nul** ;
- l'ensemble $\mathbb{K}^2$ muni de l'addition coordonnée par coordonnée et de la multiplication par un scalaire est un $\mathbb{K}$–e.v ;
- $\mathbb{K}[X]$ est un $\mathbb{K}$–e.v pour l'addition des polynômes et la multiplication par une constante. Il en va similairement de $\mathbb{K}(X)$.

Proposition XVIII.1. Soit E un $\mathbb{K}$–e.v et soient $\lambda \in \mathbb{K}$ et $x \in E$. Alors :

$$(\lambda \cdot x = 0) \Leftrightarrow (\lambda = 0) \vee (x = 0) \,.$$

✖ **Attention :** il y a deux zéros différents dans la proposition *supra* : le premier est celui de $\mathbb{K}$, le second celui de E.

Démonstration. ($\Leftarrow$) Cela découle du fait que $\lambda \cdot 0 = \lambda \cdot (0+0)$ et donc $\lambda \cdot 0 = -\lambda \cdot 0$. De même, $(0+0) \cdot x = 0 \cdot x \ldots$

($\Rightarrow$) Supposons $\lambda \cdot x = 0$ et $\lambda \neq 0$. Alors, quitte à multiplier des deux côtés par $\dfrac{1}{\lambda}$ on obtient que $1 \cdot x = 0$, *i.e* $x = 0$.

□

Proposition XVIII.2. Soit E un $\mathbb{K}$–e.v et soit $x \in E$. Alors $(-1) \cdot x = -x$.

✖ **Attention :** "$-x$" représente ici l'inverse de x pour "+".

Démonstration. On a $1 \cdot x + (-1) \cdot x = (1 + (-1)) \cdot x = 0 \cdot x = 0$ d'où le résultat. □

b) Exemples fondamentaux

◇ $\mathbb{K}^n$

L'espace $\mathbb{K}^n$ est un $\mathbb{K}$–e.v pour l'addition terme à terme et la multiplication par un scalaire, *i.e* si $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in E$ et $\lambda \in \mathbb{K}$ on pose :

$$(x_1, \ldots x_n) + \lambda \cdot (y_1, \ldots, y_n) = (x_1 + \lambda y_1, \ldots, x_n + \lambda y_n) .$$

✖ **Attention :** le corps de base est évidemment fondamental : $\mathbb{R}^2$ est un $\mathbb{R}$–e.v et $\mathbb{C} = \mathbb{C}^1$ un $\mathbb{C}$–e.v et pourtant leurs structures sont différentes. En particulier, on ne multiplie pas par i dans $\mathbb{R}^2$……

◇ **Fonctions**

Soit X un ensemble et E un $\mathbb{K}$–e.v ; alors l'ensemble $\mathscr{F}(X, E) = E^X$ est un $\mathbb{K}$–e.v pour les opérations suivantes : si $f, g \in E^X$ et $\lambda \in \mathbb{K}$ alors

$$(f + \lambda g) : x \mapsto f(x) + \lambda g(x) .$$

En particulier, l'ensemble $E^{\mathbb{N}}$ des suites à valeurs dans E est un $\mathbb{K}$–e.v.

◇ **Produits**

Soient $E_1, \ldots, E_n$ des $\mathbb{K}$–e.v ; alors le produit $E_1 \times E_n$ est un $\mathbb{K}$–e.v pour l'addition terme à terme et la multiplication scalaire. On retrouve la structure vue sur $\mathbb{K}^n$ comme cas particulier.

◇ **Matrices**

Pour $n, p \in \mathbb{N}^*$, l'espace $\mathscr{M}_{n,p}(\mathbb{K})$ des matrices à n lignes et p colonnes est $\mathbb{K}$–e.v pour les opérations linéaires décrites dans le chapitre XII, à savoir : :

— la somme de deux matrices $M = (m_{i,j})_{i,j}$ et $N = (n_{i,j})_{i,j}$ de $\mathscr{M}_{n,p}(\mathbb{K})$ est définie comme étant la matrice $M + N = (a_{i,j})_{i,j}$ telle que :

$$\forall (i,j) \in [\![1,n]\!] \times [\![1,p]\!], \quad a_{i,j} = m_{i,j} + n_{i,j} \,.$$

Ceci définit une loi de composition interne commutative sur $\mathscr{M}_{n,m}(\mathbb{K})$;

— si $M = (m_{i,j})_{i,j} \in \mathscr{M}_{n,p}(\mathbb{K})$ et $\lambda \in \mathbb{K}$, on définit la matrice $\lambda M = (a_{i,j})_{i,j}$ *via*

$$\forall (i,j) \in [\![1,n]\!] \times [\![1,p]\!], \quad a_{i,j} = \lambda m_{i,j} \,.$$

c) Combinaisons linéaires

Définition XVIII.2. Soit E un $\mathbb{K}$–e.v ; on appelle **combinaison linéaire sur** E toute expression de la forme

$$\sum_{i=1}^{n} \lambda_i x_i$$

avec les $\lambda_i \in \mathbb{K}$ (appelés **coefficients**) et les $x_i \in E$.

Exemple XVIII.2.

— Dans $\mathbb{K}^2$, tout élément est combinaison linéaire de $(0,1)$ et $(1,0)$.

— Dans $\mathbb{K}^3$, posons $e_1 = (1,2,1)$, $e_2 = (2,-1,0)$ et $e_3 = (3,1,1)$. Alors, $(x,y,z) \in \mathbb{K}^3$ est combinaison linéaire de e_1, e_2 et e_3 si et seulement si il existe λ, μ et ν tels que :

$$\lambda e_1 + \mu e_2 + \nu e_3 = (x,y,z)$$

i.e

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

Ce concept de combinaisons linéaires (finies) peut se reformuler pour accepter des familles de vecteurs potentiellement infinies à condition que seul un nombre fini de coefficients soient non nuls. Nous avons vu un procédé similaire lors de l'étude des polynômes au chapitre XIV.

Définition XVIII.3. Une famille $(\lambda_i)_{i\in I}$ de scalaires sera dite **presque nulle** (ou à support fini) si il existe $J \subset I$ fini tel que :

$$\forall i \in I \setminus J, \ \lambda_i = 0 \,.$$

Dans ce cas, l'ensemble (fini)

$$\operatorname{supp}((\lambda_i)_{i\in I}) = \{i \in I \,|\, \lambda_i \neq 0\}$$

est appelé **support** de la famille $(\lambda_i)_{i\in I}$.

Dans le cas où $(x_i)_{i\in I}$ est une famille de vecteurs et $(\lambda_i)_{i\in I}$ une famille presque nulle de scalaires de support J, on pourra noter :

$$\sum_{i\in I}\lambda_i x_i = \underbrace{\sum_{i\in J}\lambda_i x_i}_{\text{somme finie}}$$

et on parlera de "combinaison linéaire des x_i".

✖ **Attention :** une combinaison linéaire est donc **toujours** une somme **finie**.

➠ **Exemple XVIII.3.** Tout polynôme est combinaison linéaire de la famille $(X^n)_{n\in\mathbb{N}}$.

2.⁻ Applications linéaires

a) C'est quoi ?

Définition XVIII.4. Soient E et F deux $\mathbb{K}$–e.v ; une application $f : E \to F$ est dite **linéaire** si :
- $\forall x, y \in E,\ f(x+y) = f(x) + f(y)$;
- $\forall x \in E,\ \forall \lambda \in \mathbb{K},\ f(\lambda x) = \lambda f(x)$.

✌ **Remarque XVIII.2.**
- Une telle application est donc un morphisme de groupes de $(E, +)$ vers $(F, +)$ ce qui entraîne que $f(0_E) = 0_F$. **Il est donc inutile de démontrer cette propriété lors de l'étude.**
- Pour tout $\mathbb{K}$–e.v E, les applications $x \mapsto \lambda x$ (pour $\lambda \in \mathbb{K}$) sont des applications linéaires de E dans E, appelée **homothéties**. Si $\lambda = 1$ (resp. $\lambda = 0$) on parle d'application identité (resp. d'application nulle).

➠ **Exemple XVIII.4.** Les applications suivantes sont linéaires :
- $$f : \mathbb{K}^2 \longrightarrow \mathbb{K}^2 \quad (x,y) \mapsto (x-y, x+y) \quad ;$$
- $$g : \mathbb{K}^2 \longrightarrow \mathbb{K} \quad (x,y) \mapsto x - 14y \quad ;$$
- $$h : \mathbb{K}^{\mathbb{N}} \longrightarrow \mathbb{K}^{\mathbb{N}} \quad u \mapsto (3u_n - u_0)_n \quad ;$$
- $$\mathrm{d} : \mathbb{K}[X] \longrightarrow \mathbb{K}[X] \quad P \mapsto P' \quad ;$$

— pour $\lambda \in \mathbb{K}$, et E un $\mathbb{K}$–e.v l'homothétie de rapport λ sur E :

$$\begin{aligned} h_\lambda : E &\longrightarrow E \\ x &\mapsto \lambda x \end{aligned} \quad ;$$

— si $a \in \mathbb{K}$, l'évaluation en a :

$$\begin{aligned} \mathrm{eval}_a : \mathbb{K}[X] &\longrightarrow \mathbb{K} \\ P &\mapsto P(a) \end{aligned} \quad ;$$

— si E est l'ensemble des suites convergentes de $\mathbb{K}^{\mathbb{N}}$ (vérifier qu'il s'agit bien d'un $\mathbb{K}$–e.v .) :

$$\begin{aligned} \lim : E &\longrightarrow \mathbb{K} \\ u &\mapsto \lim u_n \end{aligned} \quad ;$$

— si I est un intervalle de $\mathbb{R}$, les espaces $\mathscr{C}(I, \mathbb{K})$ sont des $\mathbb{K}$–e.v et, pour tout $a \in I$,

$$\begin{aligned} I : \mathscr{C}^1(I, \mathbb{K}) &\longrightarrow \mathscr{C}^0(I, \mathbb{K}) \\ f &\mapsto \left(x \mapsto \int_a^x f(t)\,\mathrm{d}t \right) \end{aligned}$$

est linéaire.

✌ **Remarque XVIII.3.** Une application linéaire conserve les combinaisons linéaires : ceci est **fondamental**. Si f est linéaire, $(\lambda_i)_{i\in I}$ est une famille presque nulle de scalaires et $(x_i)_{i\in I}$ une famille de vecteurs, alors :

$$f\left(\sum_{i\in I} \lambda_i x_i \right) = \sum_{i\in I} \lambda_i f(x_i) \,.$$

Notation.
- L'ensemble des applications linéaires de E vers F est noté $\mathscr{L}(E, F)$.
- Les applications linéaires de E dans E sont appelées **endomorphismes** ; leur ensemble est noté $\mathscr{L}(E)$.
- Les applications linéaires bijectives de E dans F sont appelées **isomorphismes** ; leur ensemble est noté $GL(E, F)$.
- Les applications linéaires bijectives de E dans E sont appelées **automorphismes** ; leur ensemble est noté $GL(E)$ et appelé **groupe linéaire de** E.
- Les applications linéaires de E dans $\mathbb{K}$ sont appelées **formes linéaires** ; leur ensemble est noté E^* et appelé **dual de** E.

◇ Endomorphismes du plan

Posons $e_1 = (1, 0)$, $e_2 = (0, 1) \in \mathbb{K}^2$. Alors, tout élément $u = (x, y) \in \mathbb{K}^2$ s'écrit de façon unique comme combinaison linéaire de e_1 et e_2, en l'occurrence :

$$u = xe_1 + ye_2 \,.$$

Soit à présent $f \in \mathscr{L}(\mathbb{K}^2)$. Alors, pour tout $u = (x, y) \in \mathbb{K}^2$, on a :

$$f(u) = f(xe_1 + ye_2) = xf(e_1) + yf(e_2)$$

et donc l'application f est totalement déterminée par la donnée de $f(e_1)$ et $f(e_2)$. Plus précisément, si on pose $(a,c) = f(e_1)$ et $(b,d) = f(e_2)$ on a :

$$f(u) = (ax + by, cx + dy) \ : .$$

Réciproquement, les applications définies par ce type de formule sont bien des endomorphismes de $\mathbb{K}^2$, *ergo* :

$$\mathscr{L}(\mathbb{K}^2) = \{(x,y) \mapsto (ax + by, cx + dy) \,|\, a,b,c,d \in \mathbb{K}\} .$$

Ceci étant fait, intéressons nous au cas des automorphismes : si $f \in \mathscr{L}(\mathbb{K}^2)$ et que $u, u' \in \mathbb{K}^2$ vérifient $f(u) = f(u')$, on a :

$$f(u - u') = f(u) - f(u') = 0$$

et donc, on en déduit aisément que f est injective si et seulement si :

$$\{u \in \mathbb{K}^2 \,|\, f(u) = 0\} = \{0\} .$$

Si f est donnée par le mécanisme $f : (x,y) \mapsto (ax + by, cx + dy)$ avec $a,b,c,d \in \mathbb{K}$, alors :

$$\begin{aligned} \forall u = (x,y) \in \mathbb{K}^2,\ f(u) = 0 &\Leftrightarrow \left\{ \begin{array}{rcl} ax + by &=& 0 \\ cx + dy &=& 0 \end{array} \right. \\ &\Leftrightarrow \left\{ \begin{array}{rcl} (ad - bc)x &=& 0 \\ (ad - bc)y &=& 0 \end{array} \right. \end{aligned}$$

via les opérations élémentaires $L_1 \leftarrow dL_1 - bL_2$ et $L_2 \leftarrow aL_2 - cL_1$. Ce système n'admet de solution non nulle que si $ad - bc \neq 0$, ce qui nous livre une CNS d'injectivité pour les endomorphismes de $\mathbb{K}^2$. On peut adapter ce raisonnement pour démontrer que la même condition nous livre la surjectivité, ce qui entraîne que :

$$GL(\mathbb{K}^2) = \{(x,y) \mapsto (ax + by, cx + dy) \,|\, a,b,c,d \in \mathbb{K},\ ad - bc \neq 0\} .$$

b) Opérations sur les applications linéaires

Proposition XVIII.3. Soient E et F deux $\mathbb{K}$–e.v ; alors $\mathscr{L}(E,F)$ est un $\mathbb{K}$–e.v .

Démonstration. C'est essentiellement immédiat une fois les opérations posées : il s'agit de celles déjà définies sur les ensembles de fonctions. □

✌ **Remarque XVIII.4.** $\mathscr{L}(E,F) \subset F^E$: il s'agit donc d'un $\mathbb{K}$–e.v inclus dans un autre $\mathbb{K}$–e.v ; de là à parler de "sous–$\mathbb{K}$–e.v "...

Proposition XVIII.4. Soient E, F, G des $\mathbb{K}$–e.v et soient $f \in \mathscr{L}(E,F)$ et $g \in \mathscr{L}(F,G)$. Alors :

(i) $g \circ f \in \mathscr{L}(E,G)$;

(ii) si $f \in GL(E,F)$, alors sa réciproque est linéaire.

Démonstration. (i) Trivial.

(ii) Soient $X, Y \in F$; alors, comme f est bijective, il existe un unique couple $(x, y) \in E^2$ tel que $f(x) = X$ et $f(y) = Y$. Ainsi, pour tout $\lambda \in \mathbb{K}$:

$$\begin{aligned} f^{-1}(X + \lambda Y) &= f^{-1}(f(x) + \lambda f(y)) \\ &= f^{-1} \circ f(x + \lambda y) \text{ par linéarité de } f \\ &= x + \lambda y \\ &= f^{-1}(X) + \lambda f^{-1}(Y) . \end{aligned}$$

□

✌ **Remarque XVIII.5.** La composition des applications linéaires est **bilinéaire**, *i.e* si f, g, h sont des applications linéaires et $\lambda \in \mathbb{K}$ on a, sous réserve de la légalité des composées *infra* :

$$f \circ (g + \lambda h) = f \circ g + \lambda(f \circ h) \quad \text{et} \quad (f + \lambda g) \circ h = f \circ h + \lambda(f \circ g) .$$

Corollaire XVIII.4.a. Soit E un $\mathbb{K}$–e.v . Alors $(\mathscr{L}(E), +, \circ)$ est un anneau.

✌ **Remarque XVIII.6.** Cet anneau est non commutatif dés que $\dim(E) \geq 2$ (*cf.* chapitre XIX). On peut par exemple remarquer que $f : (x, y) \mapsto (0, y)$ et $g : (x, y) \mapsto (x+y, y)$ ne commutent pas car $g \circ f(0, 1) = (1, 1)$ et $f \circ g(0, 1) = (0, 1)$. Il est est également non intègre (même nonobstant la commutativité) et contient des éléments nilpotents ($(x, y) \mapsto (0, x)$ par exemple).

Corollaire XVIII.4.b. Soit E un $\mathbb{K}$–e.v . Alors $(GL(E), \circ)$ est un groupe.

✖ **Attention :** $GL(E)$ n'est **PAS** un $\mathbb{K}$–e.v : si $f \in GL(E)$, $f - f \notin GL(E)$ (si $E \neq \{0\}$)...

✌ **Remarque XVIII.7.** Ces résultats justifient le fait que nous noterons souvent, pour $k \in \mathbb{N}^*$ et $u \in \mathscr{L}(E)$, u^k la composée $\underbrace{u \circ \ldots \circ u}_{k \text{ fois}}$, avec la convention que $u^0 = \mathrm{id}_E$. Dans le cas où $u \in GL(E)$, on définira de façon analogue u^k, avec $k < 0$, comme une composée de u^{-1}. On notera aussi parfois, lorsque $u, v \in \mathscr{L}(E)$, uv la composée $u \circ v$.

3.⁻ Sous–espaces vectoriels

a) Quoi ?

Définition XVIII.5. Soit $(E, +, \cdot)$ un $\mathbb{K}$–e.v et soit $F \subset E$. On dit que F est un **sous–espace vectoriel** (s–e.v) de E si $(F, +, \cdot)$ est un $\mathbb{K}$–e.v .

Exemple XVIII.5.
- $\{0_E\}$ est un s–e.v de E pour tout $\mathbb{K}$–e.v E ;
- de même, tout $\mathbb{K}$–e.v est un s–e.v de lui–même ;
- si E et F sont deux $\mathbb{K}$–e.v , $\mathscr{L}(E,F)$ est un s–e.v de F^E ;
- pour tout $n \geq 0$, $\mathbb{K}_n[X]$ est un s–e.v de $\mathbb{K}[X]$;
- l'ensemble des suites convergentes sur $\mathbb{K}$ est un s–e.v de $\mathbb{K}^{\mathbb{N}}$;
- $\mathscr{C}^0(\mathbb{R})$ est un s–e.v de $\mathbb{R}^{\mathbb{R}}$;
- $\mathscr{C}^1(\mathbb{R})$ est un s–e.v de $\mathscr{C}^0(\mathbb{R})$ et donc de $\mathbb{R}^{\mathbb{R}}$.

Nous disposons, comme pour les sous–groupes/anneaux, d'une caractérisation des s–e.v qui nous sera précieuse en pratique. En l'occurrence, F est un s–e.v de E si et seulement si :

(i) $F \subset E$;

(ii) $0 \in F$;

(iii) $\forall x, y \in F$, $\forall \lambda \in \mathbb{K}$, $x + \lambda y \in F$.

Vocabulaire. Si F est un s–e.v de E, il est dit *strict* si $\{0\} \subsetneq F \subsetneq E$, et *trivial* sinon.

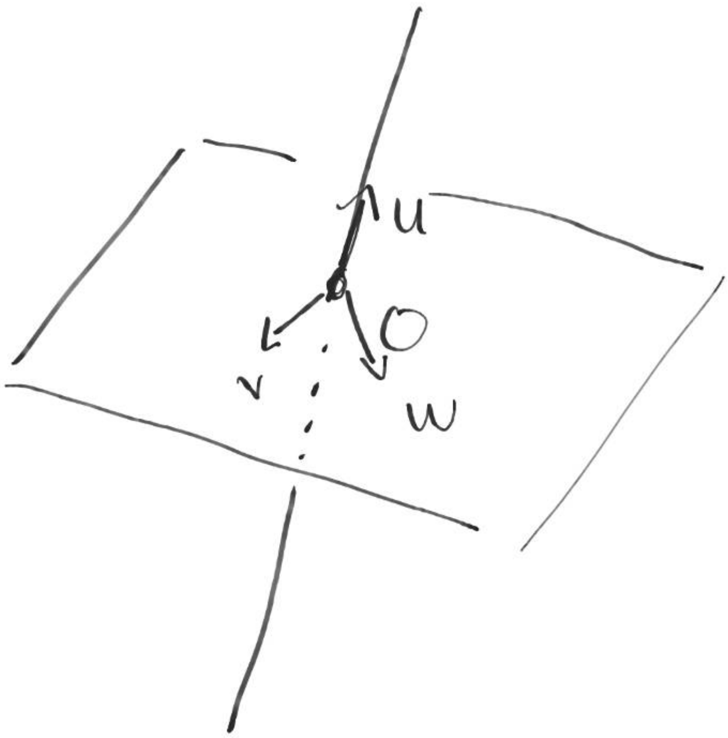
b) Exemples fondamentaux

◇ Objets "géométriques"

On fixe dans cette partie un $\mathbb{K}$–e.v E. On appelle **droite engendrée par un vecteur** $v \in E$ l'ensemble :

$$\mathscr{D}_v = \{\lambda v \mid \lambda \in \mathbb{K}\}.$$

Dans $\mathbb{R}^2$ et $\mathbb{R}^3$, on retrouve la notion de droite (vectorielle) vue dans les classes antérieures, ce qui est plutôt rassurant.



De la même façon, étant donné deux vecteurs $u, v \in E$ tels que $u \notin \mathscr{D}_v$ (on parle de vecteurs **non colinéaires**), on peut définir le **plan engendré par** u **et** v comme l'ensemble :

$$\mathscr{P}_{u,v} = \{\lambda u + \mu v \,|\, \lambda, \mu \in \mathbb{K}\} .$$

Il s'agit donc de l'ensemble des combinaisons linéaires de u et v ; ceci coïncide également avec la notion de plan vectoriel dans $\mathbb{R}^2$ et $\mathbb{R}^3$ avec laquelle nous nous permettons d'espérer que le lecteur soit familier. Dans le cas contraire, nous incluons un "joli" dessin.

✍ **Exercice XVIII.1.** Démontrer ("à la main") que le plan vectoriel d'équation $x + 2y - 3z = 0$ est un s–e.v de $\mathbb{R}^3$.

➠ **Exemple XVIII.6.** Pour tout $x \in \mathbb{R}$ et tout $\theta \in \mathbb{R}$, on a

$$\cos(x + \theta) = \cos(x)\cos(\theta) - \sin(x)\sin(\theta)$$

et donc $x \mapsto \cos(x + \theta)$ appartient au plan engendré par cos et sin.

Proposition XVIII.5. Droites et plans sont des s–e.v des espaces concernés.

Démonstration. Trivial via la caractérisation. □

◇ Image, image réciproque, noyau

Le paragraphe qui suit devra logiquement apparaître au lecteur attentif comme réminiscent du chapitre VIII. Ceci n'est pas fortuit.

Proposition XVIII.6. Soient E, F deux $\mathbb{K}$–e.v , E' (resp. F') un s–e.v de E (resp. F) et $f \in \mathscr{L}(E, F)$. Alors :

(i) $f(E')$ est un s–e.v de F ;

(ii) $f^{-1}(F')$ est un s–e.v de E.

Démonstration.

(i) Il est clair que $f(E') \subset F$; de plus $0 \in E'$ (car E' est un s–e.v de E) ce qui entraîne que $0 = f(0) \in f(E')$. Soient ensuite $X, Y \in f(E')$ et $\lambda \in \mathbb{K}$; alors il existe $x, y \in E'$ tels que $X = f(x)$ et $Y = f(y)$ donc :

$$\begin{aligned} X + \lambda Y &= f(x) + \lambda f(y) \\ &= f(\underbrace{x + \lambda y}_{\in E'}) \in f(E') . \end{aligned}$$

(ii) On sait que $f^{-1}(F') \subset E$; de plus $0 \in F'$ ce qui entraîne que $0 = f^{-1}(0) \in f^{-1}(F')$. Soient ensuite $x, y \in f^{-1}(F')$ et $\lambda \in \mathbb{K}$; alors :

$$f(x + \lambda y) = f(x) + \lambda f(y) \in F'$$

et donc $x + \lambda y \in f^{-1}(F')$.

$\square$

Proposition/définition XVIII.6. Soient E, F deux $\mathbb{K}$–e.v et soit $f \in \mathscr{L}(E, F)$. On appelle :

— **noyau** de f l'ensemble

$$\mathrm{Ker}(f) = \{x \in E \mid f(x) = 0\} ;$$

— **image** de f l'ensemble

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

Ces deux ensembles sont de plus des s–e.v de E et F respectivement.

Démonstration. Il suffit de remarquer que $\mathrm{Ker}(f) = f^{-1}(\{0\})$ et $\mathrm{Im}(f) = f(E)$. $\square$

Exemple XVIII.7.

— Pour tout $a \in \mathbb{K}$, le noyau de l'application $\mathrm{eval}_a \in \mathbb{K}[X]^*$ est l'ensemble des polynômes admettant a comme racine, *i.e* $(X - a)\mathbb{K}[X]$. Son image est $\mathbb{K}$ tout entier car, pour tout $x \in \mathbb{K}$, $x = \mathrm{eval}_a(x)$.

— Le noyau de l'application $\mathrm{d} \in \mathscr{L}(\mathscr{C}^1(\mathbb{R}), \mathscr{C}^0(\mathbb{R}))$ définie par $\mathrm{d} : f \mapsto f'$ est l'ensemble des fonctions constantes. Son image est l'ensemble des fonctions continues : en effet, si $f \in \mathscr{C}^0(\mathbb{R})$, alors

$$f = \mathrm{d}\left(x \mapsto \int_0^x f(t)\,\mathrm{d}t\right) .$$

— L'image de la fonction $x \mapsto (x, 2x)$ définie de $\mathbb{K}$ dans $\mathbb{K}^2$ est la droite engendrée par $(1, 2)$. Son noyau est nul.

Proposition XVIII.7. Soient E, F deux $\mathbb{K}$–e.v et soit $f \in \mathscr{L}(E, F)$. Alors :

(i) f est injective $\Leftrightarrow \mathrm{Ker}(f) = \{0\}$;

(ii) f est surjective $\Leftrightarrow \mathrm{Im}(f) = F$.

Démonstration. Une application linéaire est un morphisme de groupes, d'où le résultat. $\square$

Exemple XVIII.8. On peut déterminer le noyau de l'application

$$\begin{aligned} f : \mathbb{K}^2 &\to \mathbb{K}^2 \\ (x, y) &\mapsto (x + y, x - y) \end{aligned}$$

en résolvant le système

$$\begin{cases} x + y &= 0 \\ x - y &= 0 \end{cases} .$$

On trouve $\mathrm{Ker}(f) = \{0\}$: f est injective. Le lecteur intrigué pourra vérifier qu'elle est même surjective.

Proposition XVIII.8. Soit E un $\mathbb{K}$–e.v et soit $\varphi \in E^*$ **non nulle**. Alors $\mathrm{Im}(\varphi) = \mathbb{K}$.

Démonstration. Il suffit de remarquer que si $\lambda \in \mathbb{K}$ alors, si $a \in E \setminus \mathrm{Ker}(\varphi)$:

$$\lambda = \varphi\left(\frac{\lambda a}{\varphi(a)}\right).$$

□

c) Intersection, sous–espace engendré par une partie

On fixe dans cette partie un $\mathbb{K}$–e.v E.

Proposition XVIII.9. Soit $(F_i)_{i\in I}$ une famille (quelconque) de s–e.v de E. Alors :

$$\bigcap_{i\in I} F_i \text{ est un s–e.v de } E.$$

Démonstration. Immédiat via la caractérisation ; on rappelle que $x \in \bigcap_{i\in I} F_i$ si et seulement si $\forall i \in I$, $x \in F_i$. □

Exemple XVIII.9.
- L'intersection de deux droites est un s–e.v ; c'est même le sous–espace nul. Dans $\mathbb{R}^3$, on peut s'intéresser aux intersections de plans, qui sont des droites. Dans $\mathbb{R}^4$, deux plans peuvent ne s'intersecter qu'en 0, et cela peut causer des migraines. ;
- l'ensemble des solutions d'un système linéaire homogène à p équations et q inconnues est un s–e.v de $\mathbb{K}^q$, intersection des p s–e.v des solutions de chaque équation.

✖ **Attention :** la réunion de deux s–e.v n'est a priori **pas** un s–e.v : regarder $\mathscr{D}_{e_1} \cup \mathscr{D}_{e_2}$ dans $\mathbb{K}^2$ qui contient e_1 et e_2 mais pas $(1,1) = e_1 + e_2$.

Proposition/définition XVIII.7. Soit $A \subset E$. Alors l'intersection de tout les s–e.v de E contenant A est un s–e.v de E, appelé **espace engendré par** A.

Notation. $\mathrm{Vect}(A)$; lorsque le corps de base sera une donnée essentielle, on notera $\mathrm{Vect}_{\mathbb{K}}(A)$.Si la partie A est décrite comme une famille $(x_i)_{i\in I}$ de vecteurs, on pourra noter $\mathrm{Vect}(x_i)_{i\in I}$.

Démonstration. Il s'agit d'une intersection de s–e.v . □

✌ **Remarque XVIII.8.** Le sous–espace engendré par A est donc le plus petit s–e.v de E contenant A. Cela signifie que **tout s–e.v de E contenant A contient** $\mathrm{Vect}(A)$.

Exemple XVIII.10.
— $\text{Vect}(\emptyset) = \{0\}$;
— si F est un s–e.v de E, $\text{Vect}(F) = F$;
— si $e \in E \setminus \{0\}$, $\text{Vect}(e)$ est la droite $\mathscr{D}_e$;
— de même, si $u, v \in E$ sont non colinéaires, $\text{Vect}(u, v) = \mathscr{P}_{u,v}$.

Les deux derniers exemples se visualisent plus facilement une fois la proposition suivante démontrée.

Proposition XVIII.10. Soit $A \subset E$. Alors $\text{Vect}(A)$ est l'ensemble des combinaisons linéaires d'éléments de A.

Démonstration. Posons F l'ensemble des combinaisons linéaires d'éléments de A. Il s'agit naturellement d'un s–e.v de E contenant A et donc, par minimalité, $\text{Vect}(A) \subset F$. De plus, tout s–e.v de E contenant A doit contenir F par stabilité, *ergo* $F \subset \text{Vect}(A)$. □

Exercice XVIII.2. Soient $u = (1, 1)$ et $v = (2, 2)$ deux vecteurs de $\mathbb{K}^2$. Déterminer l'espace $\text{Vect}(u, v)$.

Correction : *u et v sont colinéaires, donc* $\text{Vect}(u, v) = \text{Vect}(u) = \mathscr{D}_u$.

Proposition XVIII.11. Soient $A, B \subset E$. Alors :
(i) $A \subset \text{Vect}(A)$ avec égalité si et seulement si A est un s–e.v de E ;
(ii) $\text{Vect}(\text{Vect}(A)) = \text{Vect}(A)$;
(iii) $(A \subset B) \Rightarrow (\text{Vect}(A) \subset \text{Vect}(B))$;
(iv) $\text{Vect}(A \cap B) \subset \text{Vect}(A) \cap \text{Vect}(B)$.

Démonstration. (i) L'inclusion est immédiate ; le cas d'égalité se traite en remarquant que si A est $\mathbb{K}$–e.v , alors il s'agit bien du plus petit s–e.v de E contenant A.
(ii) Trivial.
(iii) Si $A \subset B$, alors tout s–e.v de E contenant B contient A et donc $\text{Vect}(A)$, d'où le résultat.
(iv) $A\cap B \subset A$ et donc $\text{Vect}(A\cap B) \subset \text{Vect}(A)$ par (iii). On procède symétriquement avec B.

□

✖ **Attention :** on n'a pas l'égalité $\text{Vect}(A\cap B) = \text{Vect}(A)\cap\text{Vect}(B)$ dans le cas général. Prendre comme contre–exemple $A = \{(1, 2)\}$ et $B = \{(2, 4)\}$ dans $\mathbb{R}^2$: on a $\text{Vect}(A) = \text{Vect}(B)$ et $\text{Vect}(A \cap B) = \text{Vect}(\emptyset) = \{0\}$.

4.⁻ Familles remarquables de vecteurs

On fixe dans cette partie un $\mathbb{K}$–e.v E.

a) Familles libres, familles génératrices, bases

Définition XVIII.8. Soit $\mathscr{F} = (e_i)_i i \in I$ une famille de vecteurs de E. On dit que $\mathscr{F}$ est :
- **libre** si pour tout élément de E s'écrivant comme combinaison linéaire des vecteurs de $\mathscr{F}$, cette écriture est unique ;
- **génératrice** si tout élément de E s'écrit d'**au moins** une façon comme combinaison linéaire des vecteurs de $\mathscr{F}$;
- une **base** de E si elle est libre et génératrice.

✌ **Remarque XVIII.9.** $\mathscr{F}$ est une base si et seulement si tout vecteur de E s'écrit d'une unique façon comme combinaison linéaire des e_i.

➠ **Exemple XVIII.11.**
- La famille vide $\mathscr{F} = ()$ est libre.
- Si $u \in E$, alors $((u)$ est libre$) \Leftrightarrow (u \neq 0)$.
- Si $u, v \in E$ sont non colinéaires, alors (u, v) est libre.
- Pour tout $A \subset E$, $(a)_{a\in A}$ est génératrice de $\mathrm{Vect}(A)$.
- Dans $\mathbb{K}^n$, la famille $(\varepsilon_i)_{1\leq i\leq n}$, où
$$\varepsilon_i = (\delta_{i,j})_{j\in[\![1,n]\!]} = (0, \dots, 0, \underbrace{1}_{i}, 0 \dots, 0)$$
est une base, appelée **base canonique** de $\mathbb{K}^n$.
- Par construction, la famille $(X^n)_{n\in\mathbb{N}}$ est une base de $\mathbb{K}[X]$, également appelée **base canonique** de cet ensemble.
- Vous l'aurez deviné, $\mathbb{K}_n[X]$ a aussi une base canonique (pas de jaloux) : la famille $(1, X, X^2, \dots, X^n)$.
- *Quid* de la décomposition en éléments simples, cher lecteur ?
- Nous verrons dans le chapitre XIX que les matrices élémentaires forment une base de $\mathscr{M}_{n,p}(\mathbb{K})$.

Vocabulaire. Une famille non libre est dite **liée**. De plus, on parle parfois de vecteurs **linéairement indépendants** lorsque l'on considère une famille libre. Enfin, si $(e_i)_{i\in I}$ est une base de E et que $x \in E$ s'y décompose comme :
$$x = \sum_{i\in I} x_i e_i$$
alors les x_i sont appelés **coordonnées** de x dans cette base.

✌ **Remarque XVIII.10.** Rappelons au passage que la somme *supra* est en fait finie.

Proposition XVIII.12. Soit $\mathscr{F} = (e_i)_{i\in I}$ une famille de vecteurs de E. Alors :

$\mathscr{F}$ est libre
$$\Leftrightarrow$$
pour toute famille $(\lambda_i)_{i\in I}$ presque nulle de scalaires,
$$\left(\sum_{i\in I} \lambda_i e_i = 0\right) \Rightarrow (\forall i \in I,\ \lambda_i = 0)\,.$$

Démonstration.

($\Downarrow$) Découle de l'unicité de la décomposition de 0 selon $\mathscr{F}$.

($\Uparrow$) Supposons que $x \in E$ admette deux décompositions selon $\mathscr{F}$: $x = \sum_{i \in I} \lambda_i e_i$ et $x = \sum_{i \in I} \mu_i e_i$. Alors :

$$0 = x - x = \sum_{i \in I} (\lambda_i - \mu_i) e_i$$

et donc, pour tout $i \in I$, $\lambda_i = \mu_i$.

□

Par conséquent, pour démontrer qu'une famille $(e_i)_{i \in I}$ est libre, on procède comme suit :

— on se donne une famille $(\lambda_i)_i$ de scalaires presque nulle telle que $\sum_{i \in I} \lambda_i e_i = 0$;

— on démontrer que $\forall i \in I,\ \lambda_i = 0$.

➠ **Exemple XVIII.12.** La famille $(\cos, \sin)$ est libre dans $\mathbb{R}^{\mathbb{R}}$. En effet, si $\lambda, \mu \in \mathbb{R}$ sont tels que $\lambda \cos + \mu \sin = 0$, alors on a :

$$\forall x \in \mathbb{R},\ \lambda \cos(x) + \mu \sin(x) = 0$$

et donc, en évaluant en 0 (resp. $\frac{\pi}{2}$) on obtient que $\lambda = 0$ (resp. $\mu = 0$).

✌ **Remarque XVIII.11.** Il découle de la proposition XVIII.12 qu'une famille $\mathscr{F} = (e_i)_{i \in I}$ de vecteurs de E est liée si et seulement si il existe une famille presque nulle de scalaires $(\lambda_i)_i$ telle que :

— il existe $i_0 \in I$ tel que $\lambda_{i_0} \neq 0$;

— $\sum_{i \in I} \lambda_i e_i = 0$.

Ceci est équivalent au fait que :

$$e_{i_0} = \frac{-1}{\lambda_{i_0}} \sum_{i \neq i_0} \lambda_i e_i .$$

Une famille est donc liée si et seulement si l'un de ses vecteurs s'exprime en tant que combinaison linéaire des autres.

➠ **Exemple XVIII.13.** La famille $((1,0,0),(0,2,0),(1,1,0))$ est liée dans $\mathbb{K}^3$.

✖ **Attention :** ne pas confondre famille liée (non libre) et famille génératrice.

Proposition XVIII.13. Toute famille de polynômes non nuls de degrés deux à deux distincts est libre.

Démonstration. Si on se donne une telle famille $(P_i)_{i \in I}$ et que l'on suppose qu'il existe une famille presque nulle $(\lambda_i)_{i \in I}$ de scalaires dont au moins l'un des membres est non nul et telle que

$$\sum_{i \in I} \lambda_i P_i = 0$$

alors, en posant $d = \max\{\deg(P_j) \mid \lambda_j \neq 0\}$ on a, par somme de polynômes de degrés distincts que

$$\deg\left(\sum_{i\in I} \lambda_i P_i\right) = d\,,$$

ce qui est absurde. □

Vocabulaire. Une telle famille est dite "de degrés échelonnés".

✖ **Attention :** la réciproque est **fausse** : la famille (X^2, X^2+2) est libre sans être de degrés échelonnés.

b) Maximalité, minimalité

Proposition XVIII.14.
(i) Toute sous–famille d'une famille libre est libre ;
(ii) toute sur–famille d'une famille liée est liée ;
(iii) toute sur–famille d'une famille génératrice est génératrice.

Démonstration. Trivial. □

Proposition XVIII.15. Soit $\mathscr{F}$ une famille de vecteurs de E. Les trois propriétés suivantes sont alors équivalentes :
(i) $\mathscr{F}$ est libre et toutes ses sur–familles sont liées ;
(ii) $\mathscr{F}$ est génératrice et toutes ses sous–familles ne sont pas génératrices ;
(iii) $\mathscr{F}$ est une base de E.

✌ **Remarque XVIII.12.** Ceci signifie que les bases sont exactement les familles libres maximales et les familles génératrices minimales. Ceci sera très important dans le chapitre XIX.

Démonstration.

(i)⇒(ii) Si $\mathscr{F}$ est libre maximale, alors pour tout $e \in E$, $\mathscr{F} \cup \{e\}$ est liée et donc e s'écrit comme combinaison linéaire des autres vecteurs de $\mathscr{F} \cup \{e\}$, *i.e* des vecteurs de $\mathscr{F}$. La famille est donc génératrice. Pour montrer que $\mathscr{F}$ est génératrice minimale, il nous suffit de remarquer qu'aucun des vecteurs de $\mathscr{F}$ ne peut s'exprimer en fonction des autres (par liberté). De fait, aucune sous–famille de $\mathscr{F}$ ne peut être génératrice.

(ii)⇒(iii) Supposons $\mathscr{F}$ génératrice minimale. Alors, si $\mathscr{F}$ était liée, l'un de ses vecteurs serait combinaison linéaire des autres et donc $\mathscr{F}$ privée de celui–ci serait génératrice, ce qui est absurde. $\mathscr{F}$ est donc une base de E.

(iii)⇒(i) Si $\mathscr{F}$ est une base, elle est libre. De plus, tout vecteur $e \in E$ s'exprime dans $\mathscr{F}$ (elle est génératrice), donc $\mathscr{F} \cup \{e\}$ est liée, ce qui assure la maximalité.

□

c) Lien aux applications linéaires

Proposition XVIII.16. Soit F un $\mathbb{K}$–e.v et soit $f \in \mathscr{L}(E, F)$. Soit $\mathscr{F}$ une famille de vecteurs de E. Alors :

(i) $f(\mathrm{Vect}(\mathscr{F})) = \mathrm{Vect}(f(\mathscr{F}))$;

(ii) $(f \text{ injective }) \wedge (\mathscr{F} \text{ libre}) \Rightarrow (f(\mathscr{F}) \text{ libre})$;

(iii) $(f \text{ surjective }) \wedge (\mathscr{F} \text{ génératrice}) \Rightarrow (f(\mathscr{F}) \text{ génératrice})$.

Démonstration. On pose $\mathscr{F} = (e_i)_{i\in I}$. Dans ce cas, on a naturellement $f(\mathscr{F}) = (f(e_i))_{i\in I}$.

(i) Soit $y \in F$. Alors :

$$\begin{aligned} y \in f(\mathrm{Vect}(\mathscr{F})) &\Leftrightarrow \exists\,(\lambda_i)_i \in \mathbb{K}^I \text{ presque nulle telle que } y = f\left(\sum_{i\in I}\lambda_i e_i\right) \\ &\Leftrightarrow \exists\,(\lambda_i)_i \in \mathbb{K}^I \text{ presque nulle telle que } y = \sum_{i\in I}\lambda_i f(e_i) \\ &\Leftrightarrow y \in \mathrm{Vect}(f(\mathscr{F}))\,. \end{aligned}$$

(ii) Supposons que $\mathscr{F}$ soit libre et f injective. Si $(\lambda_i)_i$ est une famille presque nulle de scalaires telle que $\sum\limits_{i\in I}\lambda_i f(e_i) = 0$ alors

$$0 = f\left(\sum_{i\in I}\lambda_i e_i\right)$$

et donc, par injectivité :

$$\sum_{i\in I}\lambda_i e_i = 0\,.$$

De plus, $\mathscr{F}$ est libre, donc on peut conclure que les λ_i sont tous nuls.

(iii) Supposons $\mathscr{F}$ génératrice et f surjective. Alors :

$$\begin{aligned} \mathrm{Vect}(f(\mathscr{F})) &= f(\mathrm{Vect}(\mathscr{F})) \text{ par (i)} \\ &= f(E) \text{ car } \mathscr{F} \text{ est génératrice} \\ &= F \text{ car } f \text{ est surjective} \end{aligned}$$

et donc $f(\mathscr{F})$ est génératrice dans F.

□

✌ **Remarque XVIII.13.** Cela signifie que si $(x_i)_{i\in I}$ est une famille génératrice de E et que f est une application linéaire, la famille $(f(x_i))_{i\in I}$ engendre $\mathrm{Im}(f)$, *i.e*

$$\mathrm{Im}(f) = \mathrm{Vect}(f(x_i))_{i\in I}\,.$$

Corollaire XVIII.16.a. Soit $\mathscr{B}$ une base de E, F un $\mathbb{K}$–e.v et $f \in \mathscr{L}(E, F)$. Alors :

(i) f est injective $\Leftrightarrow f(\mathscr{B})$ est libre ;

(ii) f est surjective $\Leftrightarrow f(\mathscr{B})$ est génératrice ;

(iii) f est bijective $\Leftrightarrow f(\mathscr{B})$ est une base.

Tout ceci nous permet de démontrer ce qui est sans doute le résultat élémentaire le plus important de la théorie des applications linéaires.

Proposition XVIII.17. Soit F un $\mathbb{K}$–e.v , soit $\mathscr{B} = (e_i)_{i\in I}$ une base de E et $\mathscr{F} = (f_i)_{i\in I}$ une famille de vecteurs de F indexée par le même ensemble que $\mathscr{B}$. Alors :

$$\exists!\, f \in \mathscr{L}(E,F), \quad \forall i \in I,\ f(e_i) = f_j\,.$$

✌ **Remarque XVIII.14.** Une conséquence de ceci est qu'UNE APPLICATION LINÉAIRE EST TOTALEMENT DÉTERMINÉE PAR LA DONNÉE DE L'IMAGE D'UNE BASE DE SON ENSEMBLE DE DÉPART. Ceci est absolument fondamental, et nous permettra de définir de telles applications uniquement par la donnée de leurs valeurs sur les vecteurs d'une base.

Démonstration. Soit $x \in E$; alors x se décompose dans la base $\mathscr{B}$, disons par $x = \sum_{i\in I} x_i e_i$. De fait, si f est application linéaire vérifiant la condition donnée :

$$f(x) = f\left(\sum_{i\in I} x_i e_i\right) = \sum_{i\in I} x_i f(e_i) = \sum_{i\in I} x_i f_i$$

et donc f est entièrement déterminée par la donnée des f_i. Réciproquement, le mécanisme

$$\sum_{i\in I} x_i e_i \mapsto \sum_{i\in I} x_i f_i$$

définit bien une application linéaire (en exercice pour notre lecteur motivé). $\square$

➠ **Exemple XVIII.14.**

— L'application linéaire

$$\begin{aligned} f : \mathbb{R}^3 &\longrightarrow \mathbb{R}^2 \\ (1,0,0) &\mapsto (1,0) \\ (0,1,0) &\mapsto (0,1) \\ (0,0,1) &\mapsto (0,2) \end{aligned}$$

est bien définie. Plus précsiément, si $(x,y,z) \in \mathbb{R}^3$ on a :

$$\begin{aligned} f((x,,y,z)) &= xf((1,0,0)) + yf((0,1,0)) + zf((0,0,1)) \\ &= x\cdot(1,0) + y\cdot(0,1) + z\cdot(0,2) \\ &= (x, y+2z)\,. \end{aligned}$$

Cette application est surjective car l'image de la base canonique de $\mathbb{R}^3$ par f est génératrice de $\mathbb{R}^2$. Elle n'est pas injective car

$$\mathrm{Ker}(f) = \{(0,-2z,z) | z \in \mathbb{R}\} = \mathrm{Vect}((0,-2,1))\,.$$

— L'application linéaire

$$\begin{aligned} g : \mathbb{R}^2 &\longrightarrow \mathbb{R}^{\mathbb{R}} \\ (1,0) &\mapsto \cos \\ (0,1) &\mapsto \sin \end{aligned}$$

est bien définie et injective car l'image de la base canonique de $\mathbb{R}^2$ par g est $(\cos,\sin)$, qui est libre dans $\mathbb{R}^{\mathbb{R}}$.

5.⁻ Sous–espaces supplémentaires

On fixe dans cette partie un $\mathbb{K}$–e.v E.

a) Somme de deux s–e.v

Soient F et G deux s–e.v de E. Nous avons vu que l'ensemble $F \cup G$ n'était pas en général un s–e.v de E ; cependant l'espace engendré $\text{Vect}(F \cup G)$ en est bien un. La question à laquelle nous devons répondre à présent est : certes, mais qui est–il ?

Proposition XVIII.18. Soient F et G deux s–e.v de E. Alors l'espace $\text{Vect}(F \cup G)$ est égal à

$$F + G = \{x + y \,|\, (x, y) \in F \times G\} .$$

Démonstration. On procède par double inclusion pour montrer que $F+G = \text{Vect}(F \cup G)$.

($\supset$) Il est clair que $F \cup G \subset F + G$ car $0 \in F$ et $0 \in G$. Il est de plus aisé de vérifier que $F + G$ est un s–e.v de E, ce qui entraîne par minimalité que $\text{Vect}(F \cup G) \subset F + G$.

($\subset$) Soit H un s–e.v de E contenant $F \cup G$; alors pour tout $(x, y) \in F \times G$, $x, y \in F \cup G \subset H$ et donc $x+y \in H$. Ainsi $F+G \subset H$ et donc $F+G \subset \text{Vect}(F \cup G)$ par minimalité.

□

Exemple XVIII.15. Dans $\mathbb{K}^2$, $Vect((0, 1)) + \text{Vect}((1, 1)) = \mathbb{K}^2$ et

$$Vect((0, 1)) + \text{Vect}((0, -1)) = \mathscr{D}_{(0,1)} .$$

b) Somme directe

Définition XVIII.9. Soient F, G deux s–e.v de E. On dit que F et G sont en **somme directe** si :

$$\forall z \in F + G,\ \exists\, (x, y) \in F \times G,\ z = x + y .$$

Notation. L'ensemble $F + G$ est alors noté $F \oplus G$.

✌ **Remarque XVIII.15.** La nouveauté est ici l'unicité de la décomposition selon F et G.

Proposition XVIII.19. Soient F et G deux s–e.v de E. Alors :

$$F \text{ et } G \text{ sont en somme directe} \iff F \cap G = \{0\}.$$

Démonstration.

($\Downarrow$) Si $x \in F \cap G$, alors $x = 0 + x = x + 0$ et donc, par unicité de la décomposition, $x = 0$.

($\Uparrow$) Soit $z \in F + G$ que l'on suppose décomposable comme $z = x + y$ et $z = x' + y'$ avec $x, x' \in F$ et $y, y' \in G$. Alors $\underbrace{x - x'}_{\in F} = \underbrace{y' - y}_{\in G}$, ce qui entraîne que $x - x', y' - y \in F \cap G = \{0\}$ d'où le résultat.

□

Exemple XVIII.16.

— Si $u, v \in E$ sont non colinéaires, alors $\mathscr{D}_u$ et $\mathscr{D}_v$ sont en somme directe. De plus, $\mathscr{D}_u \oplus \mathscr{D}_v = \mathscr{P}_{u,v}$.

— Posons, dans $\mathbb{R}^{\mathbb{R}}$, $F = \text{Vect}(\cos)$ et $G = \text{Vect}(\sin)$. Alors, si $f \in F \cap G$, il existe $\lambda, \mu \in \mathbb{R}$ tels que $f = \lambda \cos = \mu \sin$. De fait, $f(0) = \lambda$ et $f(0) = 0$ donc $\lambda = 0$ *ergo* $f = 0$. On en déduit que F et G sont en somme directe.

Définition XVIII.10. Deux s–e.v F et G de E sont dit supplémentaires si $E = F \oplus G$.

Remarque XVIII.16. En pratique, il faut donc démontrer que :

— F et G sont en somme directe ;

— $E \subset F + G$.

Exemple XVIII.17. On vérifie aisément que $\mathbb{K}^2 = \text{Vect}((0,1)) \oplus \text{Vect}((1,0))$.

Exercice XVIII.3. Soit F l'ensemble des fonctions impaires de $\mathbb{R}$ dans $\mathbb{R}$ et G celui des fonctions paires.

(a) Démontrer que F et G sont des s–e.v de $\mathbb{R}^{\mathbb{R}}$.

(b) Montrer que
$$\mathbb{R}^{\mathbb{R}} = F \oplus G\,.$$

Correction :

(a) Immédiat via la caractérisation des s–e.v .

(b) Commençons par remarquer que si $f \in \mathbb{R}^{\mathbb{R}}$ alors $g : x \mapsto \dfrac{f(x) + f(-x)}{2}$ est paire et $h : x \mapsto \dfrac{f(x) - f(-x)}{2}$ est impaire. Ainsi, $f = h + g \in F + G$ et donc $\mathbb{R}^{\mathbb{R}} = F + G$. ***Cette décomposition est souvent utile ; elle est à retenir.*** *Pour conclure, il suffit de noter que si $f \in F \cap G$ alors pour tout $x \in \mathbb{R}$, $f(x) = f(-x) = -f(x)$ et donc $f = 0$.*

Remarque XVIII.17. Supposons trouvés F et G deux s–e.v supplémentaires de E. Alors, si l'on dispose d'une base $\mathscr{F}$ de F et d'une base $\mathscr{G}$ de G, on démontre aisément que $\mathscr{B} = \mathscr{F} \cup \mathscr{G}$ est une base de E. On parle de **base adaptée** aux sous–espaces F et G.

Proposition XVIII.20. Soient F et G deux s–e.v supplémentaires de E. Alors, pour tout couple $(u,v) \in \mathscr{L}(F) \times \mathscr{L}(G)$, il existe une unique application linéaire $f \in \mathscr{L}(E)$ telle que $f_{|_F} = u$ et $f_{|_G} = v$.

Démonstration. Ceci découle de la remarque *supra* et de la proposition XVIII.17. □

c) Projecteurs

Définition XVIII.11. Un endomorphisme $p \in \mathscr{L}(E)$ est appelé un **projecteur** si

$$p \circ p = p\,.$$

Exemple XVIII.18.
- id_E est un projecteur ;
- $(x,y) \mapsto (x,0)$ est un projecteur sur $\mathbb{K}^2$;
- de façon plus générale, pour tout $i \in [\![1,n]\!]$, l'application

$$\begin{aligned} \pi_i : \mathbb{K}^n &\longrightarrow \mathbb{K}^n \\ (x_1,\dots,x_n) &\mapsto (0,\dots,0,\underbrace{x_i}_{i},0,\dots,0) \end{aligned}$$

  est un projecteur.

Exercice XVIII.4. Soit p un projecteur et soit $\lambda \in \mathbb{K}$ tel qu'il existe $x \in E\backslash\{0\}$ vérifiant $p(x) = \lambda x$. Démontrer que $\lambda \in \{0,1\}$.

Proposition XVIII.21. Soit $p \in \mathscr{L}(E)$. Alors :

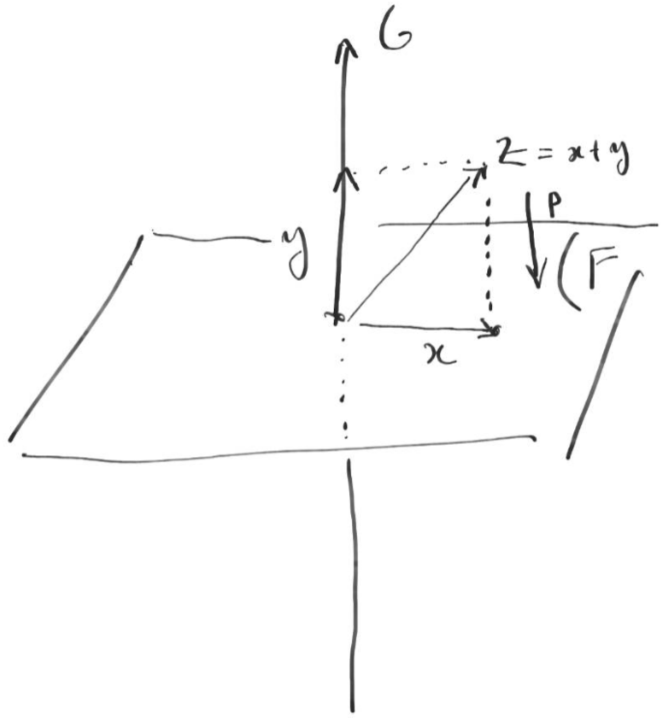
p est un projecteur
$\Longleftrightarrow$
il existe deux s–e.v F et G **supplémentaires** dans E tels que :

(i) $\forall x \in F$, $p(x) = x$;

(ii) $\forall x \in G$, $p(x) = 0$.

Dans ce cas, F et G sont de plus uniques.

Vocabulaire. On dit alors que p est **le projecteur sur F parallèlement à G.**



Démonstration.

($\Uparrow$) Soit $z \in E$, de décomposition $z = x+y \in F \oplus G$. Alors $p \circ p(z) = p(p(x)+p(y)) = p(x) = x$ et $p(z) = p(x) + p(y) = p(x) = x$, donc p est bien un projecteur.

($\Downarrow$) Supposons que p soit un projecteur et posons

$$G = \operatorname{Ker}(p) \quad \text{et} \quad F = \operatorname{Ker}(p - \mathrm{id}_E) = \{x \in E \,|\, p(x) = x\}\,.$$

Il est clair que F et G vérifient les conditions (i) et (ii) de la proposition. De plus, si $x \in F \cap G$ alors $p(x) = x$ et $p(x) = 0$, donc $F \cap G = \{0\}$ *ergo* F et G sont en somme directe. Pour conclure quant au caractère supplémentaire de F et G, fixons $z \in E$ et notons que :

$$p(z - p(z)) = p(z) - p \circ p(z) = p(z) - p(z) = 0$$

et donc :

$$z = \underbrace{z - p(z)}_{\in G} + \underbrace{p(z)}_{\in F} \in F \oplus G\,.$$

Pour démontrer, remarquons que si F et G sont deux s–e.v de E tels que soit p le projecteur sur F relativement à G, alors, pour tout $z \in E$, il existe un unique couple $(x, y) \in F \times G$ tel que $z = x + y$ et :

$$\begin{aligned} p(z) = 0 &\Leftrightarrow p(x+y) = 0 \\ &\Leftrightarrow p(x) + p(y) = 0 \\ &\Leftrightarrow x + 0 = 0 \\ &\Leftrightarrow z \in G\,. \end{aligned}$$

De plus, $p \circ p(z) = z$ donc p$p(z) = p(x + 0) = p(x) = x$. *In fine*, on a :

— $F = \operatorname{Im}(p) = \operatorname{Ker}(p - \mathrm{id}_E)$;

— $G = \mathrm{Ker}(p)$.

□

✌ **Remarque XVIII.18.** On déduit de tout ceci que si p est un projecteur alors $\mathrm{Im}(p) = \mathrm{Ker}(p - \mathrm{id}_E)$. De plus, si p est bijectif alors $\mathrm{Ker}(p) = \{0\}$ et donc $p = \mathrm{id}_E$.

✍ **Exercice XVIII.5.** Soient $u = (1, 1)$ et $v = (0, 1)$. Décrire le projecteur sur $\mathscr{D}_u$ parallèlement à $\mathscr{D}_v$ dans $\mathbb{K}^2$.

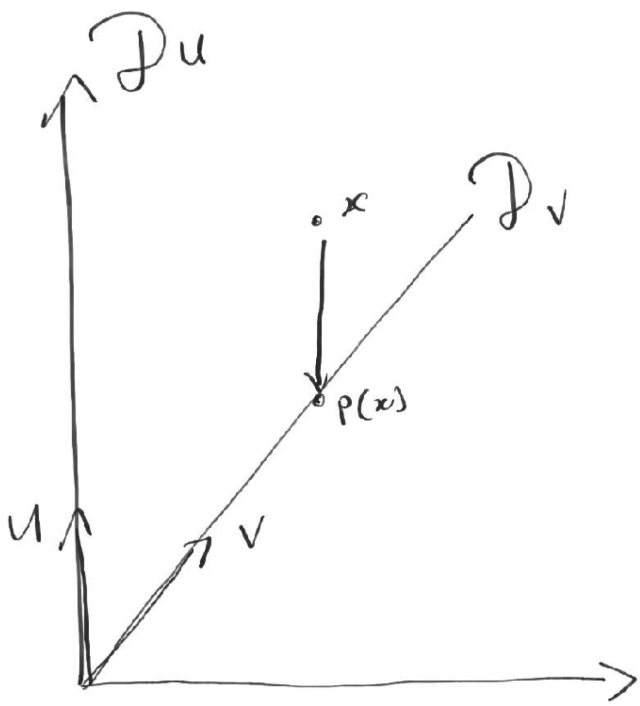
➥ **Correction :** *Commençons par remarquer que les deux droites en question sont bien supplémentaires : elles sont clairement en somme directe (leurs vecteurs directeurs sont non colinéaires) et, pour tout $(x, y) \in \mathbb{K}^2$ on a :*

$$(x, y) = x \cdot u + (y - x) \cdot v\,,$$

expression que le lecteur averti pourra retrouver à l'aide d'un système linéaire en cherchant $\lambda, \mu \in \mathbb{K}$ tels que $(x, y) = \lambda u + \mu v$. De fait, le projecteur p sur $\mathscr{D}_u$ parallèlement à $\mathscr{D}_v$ est donné par :

$$p : (x, y) \mapsto x \cdot (1, 1) = (x, x)\,.$$

Il "suffit" de conserver la "coordonnée" selon u.



✍ **Exercice XVIII.6.** De la même façon, déterminer le projecteur sur $\mathrm{Vect}((1, 0, 0), (0, 1, 0))$ parallèlement à $\mathrm{Vect}((0, 0, 1))$ dans $\mathbb{K}^3$.

d) Symétries

Définition XVIII.12. Une application $s \in \mathscr{L}(E)$ est appelée **symétrie** si $s \circ s = \mathrm{id}_E$.

✌ **Remarque XVIII.19.** Une symétrie est automatiquement un automorphisme. Il s'agit même d'une involution.

➟ **Exemple XVIII.19.**
— id_E est une symétrie ;
— $x \mapsto -x$ est une symétrie ;
— $(x, y) \mapsto (y, x)$ est une symétrie de $\mathbb{K}^2$;
— de façon plus générale, pour tout $i, j \in [\![1, n]\!]$, l'application

$$\begin{aligned} \sigma_{i,j} : \mathbb{K}^n &\longrightarrow \mathbb{K}^n \\ (x_1, \dots, x_n) &\mapsto (x_1, \dots, \underbrace{x_j}_{i}, \dots, \underbrace{x_i}_{j}, \dots, x_n) \end{aligned}$$

est une symétrie.

✍ **Exercice XVIII.7.** Soit s une symétrie et soit $\lambda \in \mathbb{K}$ tel qu'il existe $x \in E \setminus \{0\}$ vérifiant $s(x) = \lambda x$. Démontrer que $\lambda \in \{-1, 1\}$.

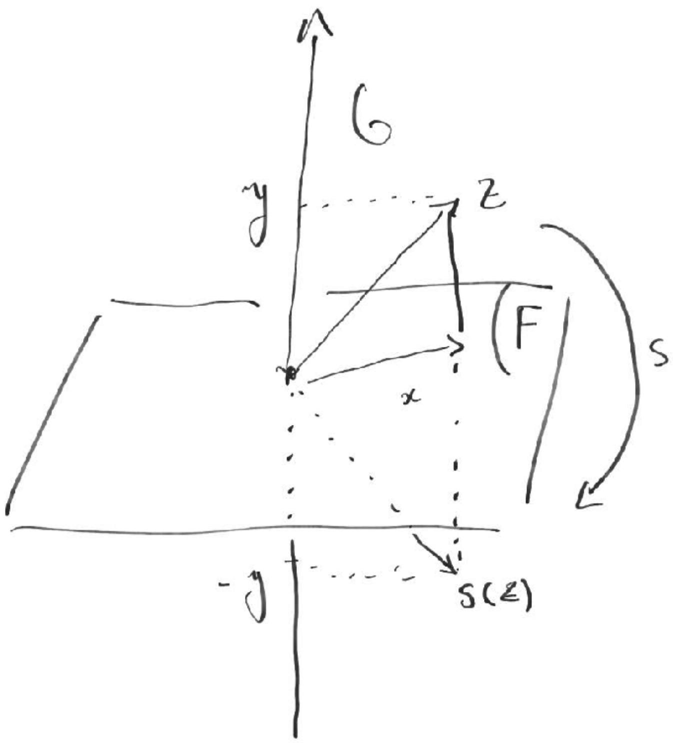
Proposition XVIII.22. Soit $s \in \mathscr{L}(E)$. Alors :

s est une symétrie
$\Longleftrightarrow$
il existe deux s–e.v F et G **supplémentaires** dans E tels que :

(i) $\forall x \in F$, $s(x) = x$;
(ii) $\forall x \in G$, $s(x) = -x$.

Dans ce cas, F et G sont de plus uniques.

Vocabulaire. On parle de **symétrie par rapport à** F **parallèlement à** G.



Démonstration. ($\Uparrow$) Soit $z \in E$, de décomposition $z = x + y \in F \oplus G$. Alors $s \circ s(z) = s(s(x) + s(y)) = s(x - y) = x + y = z$ donc s est bien une symétrie.

($\Downarrow$) Supposons que s soit une symétrie et posons

$$G = \operatorname{Ker}(s + \mathrm{id}_E) \quad \text{et} \quad F = \operatorname{Ker}(p - \mathrm{id}_E)\,.$$

Il est clair que F et G vérifient les conditions (i) et (ii) de la proposition. De plus, si $x \in F \cap G$ alors $s(x) = x$ et $s(x) = -x$, donc $F \cap G = \{0\}$ *ergo* F et G sont en somme directe. Pour conclure quant au caractère supplémentaire de F et G, fixons $z \in E$ et notons que :

$$z = \underbrace{\frac{z + s(z)}{2}}_{\in F} + \underbrace{\frac{z - s(z)}{2}}_{\in G} \in F + G\,.$$

L'unicité se traite de façon similaire au cas des projecteurs. □

Exemple XVIII.20. On retrouve dans $\mathbb{R}^2$, $\mathbb{R}^3$ des procédés vus au collège et au lycée. On peut également chercher à déterminer dans $\mathbb{K}^2$ la symétrie par rapport à $\operatorname{Vect}((1,1))$ parallèlement à $\operatorname{Vect}((0,1))$; on trouve

$$s : (x, y) \mapsto (x, y) = x \cdot (1, 1) - (y - x) \cdot (0, 1) = (x, 2x - y)\,.$$

e) Hyperplans

Définition XVIII.13. Soit E un $\mathbb{K}$–e.v et soit H un s–e.v de E. On dit que H est un **hyperplan** de E si il existe une forme linéaire **non nulle** φ sur E telle que :

$$H = \operatorname{Ker}(\varphi)\,.$$

Exemple XVIII.21.
— L'ensemble $\{(x, y, z) \in \mathbb{R}^3 \mid x + y + 2z = 0\}$ est un hyperplan de $\mathbb{R}^3$.
— L'ensemble $\{P \in \mathbb{K}[X] \mid P(\pi) = 0\}$ est un hyperplan de $\mathbb{K}[X]$, noyau de eval_π.

Proposition XVIII.23. Soit E un $\mathbb{K}$–e.v et soit H un s–e.v de E. Alors :

$$H \text{ est un hyperplan} \iff \forall a \notin H, \quad H \oplus \mathscr{D}_a = E.$$

Démonstration.

($\Downarrow$) Soit H un hyperplan ; il existe par définition une forme linéaire non nulle φ telle que $H = \operatorname{Ker}(\varphi)$. Notons que comme $\varphi \neq 0$, il existe $a \notin H$ et on a alors pour tout tel vecteur a :
— $H \cap \mathscr{D}_a = \{0\}$ car $\mathscr{D}_a$ est une droite non comprise dans H ;

— pour tout $x \in E$:

$$x = \underbrace{x - \frac{\varphi(x)}{\varphi(a)}a}_{\in H} + \frac{\varphi(x)}{\varphi(a)}a$$

et donc $E = H + \mathscr{D}_a$.

En conclusion, H et $\mathscr{D}_a$ sont supplémentaires, d'où le point (i).

($\Uparrow$) Soit $a \notin H$; alors $E = H \oplus \mathscr{D}_a$ et donc l'unique application linéaire envoyant H sur $0_{\mathbb{K}}$ et a sur $1_{\mathbb{K}}$ convient.

$\square$

Remarque XVIII.20.

— Si $H = \mathrm{Ker}(\varphi)$ alors $\{\phi \in E^* \mid H = \mathrm{Ker}(\phi)\}$ est la droite $\mathscr{D}_\varphi \subset E^*$.

— Il suffit de l'existence d'un seul vecteur $e \notin H$ tel que $H \oplus \mathscr{D}_e = E$ pour que H soit un hyperplan. En effet, dans ce cas pour tout $a \notin H$ il existe un unique couple $(h, \lambda) \in H \times \mathbb{K}$ tel que $a = h + \lambda e$. De plus, $\lambda \neq 0$ car $a \notin H$, ce qui permet d'écrire que :

$$e = \frac{1}{\lambda}(a - h)\ .$$

Soit $x \in E$: alors il existe un unique couple $(y, \mu) \in H \times \mathbb{K}$ tel que :

$$x = y + \mu e = \underbrace{y - \frac{\mu}{\lambda}h}_{\in H} + \frac{\mu}{\lambda}a$$

et donc $E = H + \mathscr{D}_a$. Or, $a \notin H$ dont $H \cap \mathscr{D}_a = \{0\}$ ce qui entraîne que $E = H \oplus \mathscr{D}_a$.

Chapitre XIX

Dimension finie

On fixe dans tout ce chapitre un corps $\mathbb{K}$ égal à $\mathbb{R}$ ou $\mathbb{C}$.

1.⁻ Notion de dimension

a) Espaces de dimension finie

On fixe dans cette partie un $\mathbb{K}$–e.v E.

Définition XIX.1. Un $\mathbb{K}$–e.v est dit **de dimension finie** si il admet une famille génératrice finie.

Exemple XIX.1. Les espaces $\mathbb{K}^n$, $\mathbb{K}_n[X]$ sont de dimension finie pour $n \geq 1$. L'espace $\mathbb{K}[X]$ ne l'est par contre pas car l'existence d'une famille génératrice finie entraînerait une borne sur le degré des polynômes.

Proposition XIX.1. Soit $n \geq 1$. Si E admet une famille génératrice de cardinal n, alors toutes les familles libres de E sont finies de cardinal inférieur ou égal à n.

Pour démontrer cette proposition, nous allons (une fois n'est pas coutume) avoir recours à un lemme.

Lemme XIX.1. Soit $\mathscr{F} = (e_i)_{1\leq i\leq n}$ et $\mathscr{F}' = (e'_i)_{1\leq i\leq n+1}$ deux familles de vecteurs de E vérifiant que :

$$\forall i \in [\![1, n+1]\!], \quad e'_i \in \mathrm{Vect}(\mathscr{F}) .$$

Alors $\mathscr{F}'$ est liée.

Démonstration. On démontre par récurrence sur $n \in \mathbb{N}^*$ la propriété suivante : pour tout $n \geq 1$, pour toutes familles $\mathscr{F} = (e_i)_{1\leq i\leq n}$ et $\mathscr{F}' = (e'_i)_{1\leq i\leq n+1}$ de vecteurs de E telles que $\forall i \in [\![1, n+1]\!]$, $e'_i \in \mathrm{Vect}(\mathscr{F})$, la famille $\mathscr{F}'$ est liée.

— $n = 1$: trivial.

— Supposons la propriété vraie au rang $n \geq 1$ et soit $\mathscr{F} = (e_i)_{1\leq i\leq n+1}$ et $\mathscr{F}' = (e'_i)_{1\leq i\leq n+2}$ deux familles de vecteurs de E telles que $\forall i \in [\![1, n+2]\!]$, $e'_i \in \mathrm{Vect}(\mathscr{F})$.

Ceci signifie qu'il existe une famille de scalaires $a_{i,j}$ telle que :

$$\forall i \in [\![1, n+2]\!], \quad e'_i = \sum_{j=1}^{n+1} a_{i,j} e_j \ .$$

Si tous les $a_{i,n+1}$ sont nuls, alors les vecteurs de $\mathscr{F}'$ sont dans l'espace engendré par $(e_1, \dots, e_n)$ et on peut conclure par hypothèse de récurrence. Dans le cas contraire, on peut supposer (quitte à réordonner les e_j) que $a_{n+2,n+1}$ est non nul.
Posons, pour $i \in [\![1, n+1]\!]$:

$$e''_i = e'_i - \frac{a_{i,n+1}}{a_{n+2,n+1}} e'_{n+2}$$

et remarquons que :

$$\begin{aligned}
e''_i &= \sum_{j=1}^{n+1} a_{i,j} e_j - \frac{a_{i,n+1}}{a_{n+2,n+1}} \sum_{j=1}^{n+1} a_{n+2,j} e_j \\
&= \sum_{j=1}^{n} a_{i,j} e_j + a_{i,n+1} e_{n+1} - \frac{a_{i,n+1}}{a_{n+2,n+1}} \sum_{j=1}^{n} a_{n+2,j} e_j - \frac{a_{i,n+1}}{a_{n+2,n+1}} a_{n+2,n+1} e_{n+1} \\
&= \sum_{j=1}^{n} \left(a_{i,j} - \frac{a_{i,n+1}}{a_{n+2,n+1}} \right) e_j \\
&\in \mathrm{Vect}(e_1, \dots, e_n) \ .
\end{aligned}$$

On peut ensuite conclure par hypothèse de récurrence que les e''_i sont liés, et en déduire que $\mathscr{F}'$ l'est également.

□

Nous sommes grâce à ce lemme en mesure de démontrer la proposition *supra.*

Démonstration. Soit $\mathscr{G}$ une famille génératrice de E de cardinal n et soit $\mathscr{F}$ une famille libre de cet espace. Si $\mathscr{F}$ admettait plus de n éléments, alors elle devrait être liée (en application du lemme) car $\mathrm{Vect}(\mathscr{G}) = E$. □

Corollaire XIX.1.a. Toutes les bases d'un $\mathbb{K}$–e.v de dimension finie sont finies de même cardinal.

Démonstration. Soient $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E. Comme ces deux familles sont libres, elles sont finies et comme $\mathscr{B}$ est libre et $\mathscr{B}'$ génératrice alors $\mathrm{card}(\mathscr{B}) \leq \mathrm{card}(\mathscr{B}')$. On conclut en échangeant les rôles de $\mathscr{B}$ et $\mathscr{B}'$. □

☞ Nous savons donc que si il y a existence de bases de E, elles sont de même cardinal. Mais existent–elles ?

b) Théorème de la base incomplète

Théorème XIX.2 (Base incomplète)**.**
On suppose que E est de **dimension finie**. Soit $\mathscr{F}$ une famille libre de E. Alors il existe une base de E contenant $\mathscr{F}$.

Démonstration. Fixons $\mathscr{G} = (e_1, \dots, e_n)$ une famille génératrice finie de E et posons $\mathscr{F}_0 = \mathscr{F}$. On définit ensuite par récurrence une famille $\mathscr{F}_k$, pour $k \in [\![1, n[\![$ par :
- si $e_k \in \text{Vect}(\mathscr{F}_{k-1})$ alors on pose $\mathscr{F}_k = \mathscr{F}_{k-1}$;
- sinon, on pose $\mathscr{F}_k = \mathscr{F}_{k-1} \cup \{e_k\}$.

Les familles $\mathscr{F}_k$ sont toutes libres par construction et on a, pour tout $k \in [\![1, n]\!]$:

$$\text{Vect}(\mathscr{F}_k) \supset \text{Vect}(e_1, \dots e_k)\,.$$

De fait, la famille $\mathscr{F}_n$ est libre et génératrice : c'est une base de E. □

✌ **Remarque XIX.1.** Ce résultat se généralise en dimension infinie, mais ceci est bien au delà de notre niveau technique à ce stade.

Corollaire XIX.2.a. Tout $\mathbb{K}$–e.v de dimension finie admet une base.

Démonstration. Appliquer le théorème XIX.2 à la famille vide. □

De façon analogue, on peut démontrer un théorème "miroir" au théorème de la base incomplète, permettant d'amaigrir une famille génératrice.

Théorème XIX.3 (Base extraite)**.**
On suppose que E est de **dimension finie**. Soit $\mathscr{G}$ une famille génératrice de E. Alors il existe une base de E contenue dans $\mathscr{G}$.

c) Bilan

Nous venons démontrer que tout espace de dimension finie admettait des bases, et que ces dernières étaient toutes de même cardinal. Ceci nous permet de poser sereinement la définition *infra*.

Définition XIX.2. Supposons E de dimension finie. On appelle **dimension** de E le cardinal commun à toutes ses bases.

Notation. On notera la dimension de E $\dim(E)$ (ou $\dim_{\mathbb{K}}(E)$ lorsqu'il sera nécessaire de préciser le corps de base).

➠ **Exemple XIX.2.** Les dimensions qui suivent découlent trivialement des exemples de bases vues dans le chapitre XVIII :
- $\dim(\{0\}) = 0$ (et il s'agit du seul espace vectoriel de dimension nulle) ;

— si $e \in E \setminus \{0\}$, $\dim(\mathscr{D}_e) = 1$;
— si $u, v \in E$ sont non colinéaires, $\dim(\mathscr{P}_{u,v}) = 2$;
— plus généralement, si $\mathscr{F}$ est une famille finie de E alors :

$$\dim(\mathrm{Vect}(\mathscr{F})) \leq \mathrm{card}(\mathscr{F}),$$

avec égalité si et seulement $\mathscr{F}$ est libre.
— $\dim(\mathbb{K}^n) = n$;
— $\dim(\mathbb{K}_n[X]) = n + 1$;

✖ **Attention :** $\dim_{\mathbb{C}}(\mathbb{C}) = 1$ mais $\dim_{\mathbb{R}}(\mathbb{C}) = 2$.

✍ **Exercice XIX.1.** Soit E un $\mathbb{C}$–e.v. de dimension finie. Démontrer que E est $\mathbb{R}$–e.v. de dimension finie et que :

$$\dim_{\mathbb{R}}(E) = 2\dim_{\mathbb{C}}(E).$$

Tous les $\mathbb{R}$–e.v. sont–ils des $\mathbb{C}$–e.v. ?

➠ **Exemple XIX.3.** L'espace des solutions d'une équation différentielle linéaire **homogène** d'ordre 1 (resp. 2) est de dimension 1 (resp. 2). Méditer quant à la possibilité d'en donner une base (indice : ce n'est pas très difficile)...Nous verrons par ailleurs dans le chapitre XXI un résultat plus précis concernant les systèmes linéaires.

✍ **Exercice XIX.2.** Soient $a, b \in \mathbb{C}$. Déterminer une base et la dimension de l'espace $E = \{u \in \mathbb{C}^{\mathbb{N}} \mid \forall n \in \mathbb{N},\ u_{n+2} = au_{n+1} + bu_n\}$.

✌ **Remarque XIX.2.** Si E est un $\mathbb{K}$–e.v de dimension finie de dimension n, on a donc naturellement que :
— les familles libres de E sont de cardinal inférieur ou égal à n ;
— tout famille de cardinal **strictement** supérieur à n est liée ;
— les familles génératrices de E sont de cardinal supérieur ou égal à n ou infinies.

On déduit de cette remarque et de la proposition XVIII.15 sur les familles libres maximales et génératrices minimales le résultat suivant, qui sauve bien des vies en pratique.

Proposition XIX.4. On suppose E de dimension finie $n \in \mathbb{N}$. Alors, pour toute famille $\mathscr{B}$ finie de vecteurs de E, les propriétés suivantes sont équivalentes :

(i) $\mathscr{B}$ est une base ;

(ii) $\mathscr{B}$ est libre de cardinal n ;

(iii) $\mathscr{B}$ est génératrice de cardinal n.

➠ **Exemple XIX.4.** La famille $((1,0,1),(1,0,0),(0,1,0))$ est une base de $\mathbb{K}^3$ car libre et de cardinal 3.

✌ **Remarque XIX.3.** Nous avons vu dans le chapitre XVIII que toute famille de polynômes non nuls de degrés distincts est libre dans $\mathbb{K}[X]$. On en déduit que toute famille de $n+1$ polynômes non nuls de degrés échelonnés est une base de $\mathbb{K}_n[X]$.

2.⁻ Zoologie dimensionnelle

On fixe dans cette partie un $\mathbb{K}$–e.v de dimension finie E de dimension $n \in \mathbb{N}$.

a) Dimension d'un s–e.v

Proposition XIX.5. Soit F un s–e.v de E. Alors :
(i) F est de dimension finie ;
(ii) $\dim(F) \leq \dim(E)$.
Il y a de plus égalité entre E et F si et seulement si leurs dimensions sont égales.

Démonstration. La démonstration est triviale dans le cas où $F = \{0\}$. Supposons donc $F \neq \{0\}$, ce qui entraîne *de facto* que $n \geq 1$. Soit x un élément non nul de F ; $\{x\}$ est une partie libre de F, donc F contient des parties libres. Toute partie libre d'éléments de F étant une partie libre d'éléments de E toutes les parties libres de F ont au plus n éléments. On considère l'ensemble $\mathscr{E}$ des entiers k tels qu'il existe une partie libre de F ayant k éléments. Cet ensemble est non vide ($1 \in \mathscr{E}$) et est un sous-ensemble borné de $\mathbb{N}$ donc il admet un maximum. Soit p ce maximum et soit $\{v_1, v_2, \ldots, v_p\}$ une partie libre de F ayant p éléments ; cette partie libre est donc une partie libre maximale de F et donc une base, d'où le résultat.

De plus, $\dim(E) = \dim(F)$ si et seulement si F possède une base $\mathscr{B}$ de cardinal n. Or, dans ce cas, $\mathscr{B}$ est libre dans E et de cardinal n : il s'agit donc d'une base de E *ergo* $E = \mathrm{Vect}(\mathscr{B}) = F$. □

➠ **Exemple XIX.5.** On retrouve le résultat "vu" au lycée concernant les dimensions possibles des sous–espaces vectoriels de $\mathbb{R}^2$ $(0, 1, 2)$ et $\mathbb{R}^3$ $(0, 1, 2, 3)$.

✌ **Remarque XIX.4.** Ceci nous permet de dire que deux sous–espaces F et G de E sont supplémentaires **si et seulement si** :
(i) $F \cap G = \{0\}$;
(ii) $\dim(F + G) = \dim(E)$.

Définition XIX.3. Si F est un s–e.v de E de dimension p, on appelle **base adaptée** à F toute base $(e_1, \ldots, e_n)$ de E telle que $(e_1, \ldots, e_p)$ soit une base de F.

➠ **Exemple XIX.6.** $((1, 0, 1), (0, 0, 1), (0, 1, 0))$ est une base de $\mathbb{R}^3$ adaptée à $\mathscr{D}_{(1,0,1)}$.

Vocabulaire.
— Tout sous–espace vectoriel de dimension 1 est appelé **droite** ;
— tout sous–espace vectoriel de dimension 2 est appelé **plan**.

✌ **Remarque XIX.5.** Les deux premiers points de vocabulaire *supra* correspondent aux définitions données pour ces objets dans le chapitre XVIII : un s–e.v de dimension p de E est en effet un espace vectoriel engendré par une famille **libre** à p éléments de E.

b) Supplémentaires, produits

Proposition XIX.6. Soit F un s–e.v de E de dimension p. Alors :

(i) F admet un supplémentaire ;

(ii) tous les supplémentaires de F sont de dimension $n-p$.

Démonstration.

(i) Soit $\mathscr{F}$ une base de F ; alors par théorème de la base incomplète (XIX.2), il existe une base $\mathscr{B} = (e_i)_{i \in [\![1,p]\!]}$ de E adaptée à F. Posons alors $G = \mathrm{Vect}(e_{p+1}, \dots, e_n)$: on a alors par définition $\dim(G) = n - p$ (la famille engendrant G est libre dans E) et $E = F \oplus G$ (car $(e_1, \dots, e_p)$ est une base de F.

(ii) Si H est un supplémentaire de F de base $\mathscr{H}$, alors $Fr \cup \mathscr{H}$ est de cardinal n par somme directe (il s'agit d'une base de E adaptée à F et H). Il est découle que $\dim(H) = \mathrm{card}(\mathscr{H}) = n - p$.

□

Exemple XIX.7. Dans $\mathbb{R}^3$, les supplémentaires de droites sont des plans. Dans $\mathbb{R}^2$, il s'agit de droites.

Corollaire XIX.6.a. Les hyperplans d'un $\mathbb{K}$–e.v de dimension finie de dimension $n \in \mathbb{N}^*$ sont exactement ses s–e.v de dimension $n-1$.

Démonstration. Ceci découle du fait qu'un hyperplan est supplémentaire à une droite. □

Corollaire XIX.6.b. Soient F, G deux s–e.v de E en somme directe. Alors :

$$\dim(F \oplus G) = \dim(F) + \dim(G)\,.$$

Démonstration. G est un supplémentaire de F dans $F \oplus G$. □

✌ **Remarque XIX.6.** Pour démontrer que deux s–e.v F et G de E sont supplémentaires, il suffit donc de vérifier que :

(i) $F \cap G = \{0\}$;

(ii) $\dim(F) + \dim(G) = \dim(E)$.

Proposition XIX.7. Soient E et F deux $\mathbb{K}$–e.v de dimension finie ; alors $\dim(E \times F) = \dim(E) + \dim(F)$.

Démonstration. Il suffit de vérifier que si $(e_1, \dots, e_p)$ et $(e'_1, \dots, e'_n)$ sont des bases respectives de E et F alors $((e_1, 0), \dots, (e_p, 0), (0, e'_1), \dots, (0, e'_n))$ est une base de $E \times F$. □

Remarque XIX.7. Ce résultat se généralise trivialement à un produit cartésien de n $\mathbb{K}$–e.v de dimension finie pour $n \geq 3$.

c) Applications linéaires

Proposition XIX.8. Soient E et F deux espaces vectoriels et soit $f \in \mathscr{L}(E, F)$. On se donne E' un s–e.v de E **de dimension finie**. Alors :

(i) $f(E')$ est de dimension finie ;

(ii) $\dim(f(E')) \leq \dim(E')$ avec égalité lorsque f est injective.

Démonstration. Fixons une base $\mathscr{B}$ de E'. $f(E') = \mathrm{Vect}(f(\mathscr{B}))$, ce qui entraîne que $\dim(f(E'))$ est finie ; de plus $\dim(f(E')) = \mathrm{card}(f(\mathscr{B})) \leq \mathrm{card}\mathscr{B} = \dim(E')$ avec égalité lorsque f est injective (*cf.* chapitre XVI). □

Exemple XIX.8.
- L'image d'une droite par $f \in \mathscr{L}(\mathbb{R}^2)$ est une droite ou un point ;
- il n'existe aucune surjection linéaire de $\mathbb{R}^2$ vers $\mathbb{R}^4$ (s'intéresser à la dimension de l'image pour obtenir une contradiction).

Remarque XIX.8. D'une façon générale, cette proposition entraîne que le passage "par" une application linéaire ne peut que **diminuer** la dimension d'un s–e.v, jamais l'augmenter.

Proposition XIX.9. Deux $\mathbb{K}$–e.v de dimension finie sont isomorphes **si et seulement si** leurs dimensions sont égales.

Démonstration. Soient E et F deux $\mathbb{K}$–e.v de dimension finie et soit $f \in GL(E, F)$; alors, $\dim(E) = \dim(f(E))$ car f est injective. Or, f est surjective donc $f(E) = F$, d'où le résultat.

Réciproquement, si E et F sont deux $\mathbb{K}$–e.v de dimension finie de même dimension et de bases respectives $\mathscr{B}$ et $\mathscr{B}'$ alors l'unique application linéaire envoyant $\mathscr{B}$ sur $\mathscr{B}'$ est bijective (car elle envoie une base sur une base), d'où le résultat. □

Corollaire XIX.9.a. Soit un E un $\mathbb{K}$–e.v de dimension finie et posons $n = \dim(E)$. Alors E est isomorphe à $\mathbb{K}^n$.

Ce résultat n'est pas anodin : il s'agit la d'une classification (à isomorphisme près) des $\mathbb{K}$–e.v de dimension finie par leur dimension : deux espaces vectoriels de même dimension sont de fait "fortement similaires", et l'espace $\mathbb{K}^n$ pourra être utilisé comme "prototype" de ces derniers.

Exemple XIX.9. $\mathbb{K}_n[X]$ est isomorphe à $\mathbb{K}^{n+1}$. Un isomorphisme explicite peut même être déterminé par la méthode désormais usuelle du "jetons une base sur son homologue et prions" :

$$\begin{aligned} \varphi : \mathbb{K}_n[X] &\to \mathbb{K}^{n+1} \\ X^k &\mapsto (\delta_{i,k+1})_{1\leq i\leq n} . \end{aligned}$$

Proposition XIX.10. Soient E et F deux $\mathbb{K}$–e.v de dimension finie. Alors :
(i) $\mathscr{L}(E,F)$ est de dimension finie ;
(ii) $\dim(\mathscr{L}(E,F)) = \dim(E) \times \dim(F)$.

Démonstration. Pour reprendre une expression tristement célèbre en politique, "il suffit de" construire une base de $\mathscr{L}(E,F)$. Le procédé est hélas relativement douloureux.

Commençons par fixer $\mathscr{B} = (e_1, \ldots, e_p)$ et $\mathscr{B}' = (e'_1, \ldots, e'_n)$ des bases respectives de E et F (et donc $p = \dim(E)$ et $n = \dim(F)$). Posons, pour $(i,j) \in [\![1,n]\!] \times [\![1,p]\!]$:

$$\begin{aligned} g_{i,j} : E &\to F \\ e_k &\mapsto \delta_{j,k} e'_i \end{aligned}$$

de façon à ce que $g_{i,j}(e_j) = e'_i$. Faites moi confiance, et il n'y aura pas de blessés. Posons $\mathscr{F} = (g_{i,j})_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]}$ et démontrons que cette famille constitue une base de $\mathscr{L}(E,F)$.

Soit $f \in \mathscr{L}(E,F)$ et soit $x = \sum\limits_{j=1}^{p} x_j e_j \in E$. Alors :

$$\begin{aligned} f(x) &= f\left(\sum_{j=1}^{p} x_j e_j\right) \\ &= \sum_{j=1}^{p} x_j f(e_j) . \end{aligned}$$

Pour tout $j \in [\![1,p]\!]$, $f(e_j) \in F$: il existe donc une unique famille $(a_{i,j})_{i\in[\![1,n]\!]}$ de scalaires telle que :

$$f(e_j) = \sum_{i=1}^{n} a_{i,j} e'_i$$

et donc

$$\begin{aligned} f(x) &= \sum_{j=1}^{p} x_j \sum_{i=1}^{n} a_{i,j} e'_i \\ &= \sum_{j=1}^{p} \sum_{i=1}^{n} a_{i,j} x_j e'_i . \end{aligned}$$

Gardons cela en tête le temps de remarquer que, pour $(i,j) \in [\![1,n]\!] \times [\![1,p]\!]$, on a :

$$\begin{aligned} g_{i,j}(x) &= g_{i,j}\left(\sum_{k=1}^{p} x_k e_k\right) \\ &= \sum_{k=1}^{p} x_k g_{i,j}(e_k) \\ &= \sum_{k=1}^{p} x_k \delta_{j,k} e'_i \\ &= x_j e'_i \end{aligned}$$

ce qui entraîne que :

$$f(x) = \sum_{j=1}^{p} \sum_{i=1}^{n} a_{i,j} g_{i,j}(x)$$

i.e

$$f = \sum_{j=1}^{p} \sum_{i=1}^{n} a_{i,j} g_{i,j} \in \operatorname{Vect}(\mathscr{F})\,.$$

On en déduit que $\mathscr{F}$ est génératrice dans $\mathscr{L}(E,F)$.

Donnons nous ensuite une famille $(\lambda_{i,j})_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]}$ de scalaires telle que

$$\sum_{i=1}^{n} \sum_{j=1}^{p} \lambda_{i,j} g_{i,j} = 0\,.$$

Alors, pour tout $k \in [\![1,p]\!]$, on a :

$$\begin{aligned} 0 &= \sum_{i=1}^{n} \sum_{j=1}^{p} \lambda_{i,j} g_{i,j}(e_k) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{p} \lambda_{i,j} \delta_{j,k} e'_i \\ &= \sum_{i=1}^{n} \lambda_{i,k} e'_i\,. \end{aligned}$$

Or, la famille $\mathscr{B}'$ est libre, ce qui entraîne que les $\lambda_{i,k}$ sont tous nuls. On en déduit que $\mathscr{F}$ est libre et donc une base, ce qui permet de conclure car $\operatorname{card}(\mathscr{F}) = p\times n = \dim(E)\times\dim(F)$.
□

✌ **Remarque XIX.9.** Soit E un $\mathbb{K}$–e.v de dimension $n \in \mathbb{N}$. Alors :
— $\dim(\mathscr{L}(E) = n^2$;
— $\dim(E^*) = n$ et donc E et E^* sont isomorphes.

➠ **Exemple XIX.10.** $\dim(\mathscr{L}(\mathbb{K}_n[X], \mathbb{K}^n)) = (n+1)n$.

d) Matrices

Proposition XIX.11. Soient $m, n \in \mathbb{N}^*$. Alors $\mathscr{M}_{n,m}(\mathbb{K})$ est un $\mathbb{K}$–e.v de dimension finie de dimension nm.

Démonstration. La structure d'espace vectoriel se vérifie dans la douleur. Concernant la dimension, rappelons la définition, pour $(i,j) \in [\![1,n]\!] \times [\![1,m]\!]$, de la matrice élémentaire :

$$E_{i,j} = (\delta_{i,k}\delta_{j,\ell})_{(k,\ell)\in[\![1,n]\!]\times[\![1,m]\!]} \,.$$

Ceci signifie que tous les coefficients de la matrice $E_{i,j}$ sont nuls, à l'exception de celui situé ligne i, colonne j, qui est égal à 1 ; *e.g* pour $n = m = 2$ nous avons :

$$E_{1,1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad E_{1,2} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$E_{2,1} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad E_{2,2} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} .$$

Cette famille est clairement génératrice : en effet, si $A = (a_{i,j})_{i,j} \in \mathscr{M}_{n,m}(\mathbb{K})$ on a :

$$A = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{i,j}E_{i,j} \,.$$

De plus, si l'on suppose trouvée une famille $(\lambda_{i,j})_{i,j}$ de scalaires telle que

$$\sum_{i=1}^{n}\sum_{j=1}^{m} \lambda_{i,j}E_{i,j} = 0$$

alors cela signifie que la matrice de coefficients $(\lambda_{i,j})_{(i,j)\in[\![1,n]\!]\times[\![1,m]\!]}$ est nulle, *i.e* que tous les $\lambda_{i,j}$ le sont : la famille $\mathscr{F} = (E_{i,j})_{(i,j)\in[\![1,n]\!]\times[\![1,m]\!]}$ est donc une base de $\mathscr{M}_{n,m}(\mathbb{K})$ *ergo* $\dim(\mathscr{M}_{n,m}(\mathbb{K})) = \mathrm{card}(\mathscr{F}) = nm$. □

✌ **Remarque XIX.10.** On peut établir un isomorphisme entre $\mathscr{M}_{n,m}(\mathbb{K})$ et $\mathscr{L}(\mathbb{K}^m, \mathbb{K}^n)$ en envoyant les $E_{i,j}$ sur les $g_{i,j}$ de la proposition XIX.10.

✍ **Exercice XIX.3.** Démontrer que les ensembles $S_n(\mathbb{K})$ et $A_n(\mathbb{K})$ sont des espaces vectoriels de dimensions respectives $\frac{n(n+1)}{2}$ et $\frac{n(n-1)}{2}$ et que l'on a :

$$\mathscr{M}_n(\mathbb{K}) = S_n(\mathbb{K}) \oplus A_n(\mathbb{K}) \,.$$

➥ **Correction :** *Considérons l'application*

$$\begin{aligned} \phi : \mathscr{M}_n(\mathbb{K}) &\to \mathscr{M}_n(\mathbb{K}) \\ A &\mapsto A^\top \,. \end{aligned}$$

Il s'agit (proposition XII.2) d'un endomorphisme de $\mathscr{M}_n(\mathbb{K})$ vérifiant la relation $\phi^2 = \mathrm{id}_{\mathscr{M}_n(\mathbb{K})}$: ϕ est donc une symétrie de $\mathscr{M}_n(\mathbb{K})$. De fait, par la proposition XVIII.22, on a :

$$\mathscr{M}_n(\mathbb{K}) = \mathrm{Ker}(\phi - \mathrm{id}_{\mathscr{M}_n(\mathbb{K})}) \oplus \mathrm{Ker}(\phi + \mathrm{id}_{\mathscr{M}_n(\mathbb{K})}) \,.$$

De plus, si $M \in \mathscr{M}_n(\mathbb{K})$ alors :

$$\begin{aligned} M \in \mathrm{Ker}(\phi - \mathrm{id}_{\mathscr{M}_n(\mathbb{K})}) &\Leftrightarrow (\phi - \mathrm{id}_{\mathscr{M}_n(\mathbb{K})})(M) = 0 \\ &\Leftrightarrow M^\top - M = 0 \\ &\Leftrightarrow M \in S_n(\mathbb{K}) \end{aligned}$$

et donc $\mathrm{Ker}(\phi - \mathrm{id}_{\mathscr{M}_n(\mathbb{K})}) = S_n(\mathbb{K})$*. Symétriquement, on vérifie que* $\mathrm{Ker}(\phi + \mathrm{id}_{\mathscr{M}_n(\mathbb{K})}) = A_n(\mathbb{K})$*. Concernant la dimension, il suffit de remarquer que* $S_n(\mathbb{K})$ *est engendré par les matrices* $E_{i,j} + E_{j,i}$ *pour* $i \leq j \in [\![1, n]\!]$ *et que cette famille est libre ; de fait* $\dim(S_n(\mathbb{K})) = \dfrac{n(n+1)}{2}$ *et* $\dim(A_n(\mathbb{K})) = \dim(\mathscr{M}_n(\mathbb{K})) - \dim(S_n(\mathbb{K})) = \dfrac{n(n-1)}{2}$.
Notons que, si $M \in \mathscr{M}_n(\mathbb{K})$, on a (comme évoqué dans le chapitre XII) :

$$M = \underbrace{\frac{M + M^\top}{2}}_{\in S_n(\mathbb{K})} + \underbrace{\frac{M - M^\top}{2}}_{\in A_n(\mathbb{K})} .$$

3.⁻ Rang

a) C'est quoi ?

Définition XIX.4. Soit E un $\mathbb{K}$–e.v et soit $\mathscr{F}$ une famille de vecteurs de E. On appelle **rang** de $\mathscr{F}$ la dimension (éventuellement infinie) de $\mathrm{Vect}(\mathscr{F})$.

Notation. $\mathrm{rg}(\mathscr{F})$

Exemple XIX.11. Dans $\mathbb{R}^2$, $\mathrm{rg}((0,1),(0,2)) = 1$. Dans $\mathbb{K}[X]$, $\mathrm{rg}(X, X^3+X) = 2$.

Remarque XIX.11. Si $\mathscr{F}$ est finie, alors $\mathrm{rg}(\mathscr{F}) \leq \mathrm{card}(\mathscr{F})$ avec égalité si et seulement si $\mathscr{F}$ est libre.

Définition XIX.5. Soient E et F deux $\mathbb{K}$–e.v avec E de dimension finie et soit $f \in \mathscr{L}(E, F)$. On appelle **rang** de f la dimension de $\mathrm{Im}(f)$.

Notation. $\mathrm{rg}(f)$

Remarque XIX.12. L'introduction simultanée de ces deux notions peut sembler étonnante et propice à confusion. Rassurons nous toutefois : si $\mathscr{B}$ est une base de E, alors on a, par définition(s) :

$$\mathrm{rg}(f) = \mathrm{rg}(f(\mathscr{B})) .$$

Je suis convaincu que le lecteur est désormais soulagé.

Exemple XIX.12.
— $\mathrm{rg}(\mathrm{id}_E) = \dim(E)$;

— plus généralement, toute bijection est de rang égal à la dimension de son espace de départ/arrivée ;
— si p est le projecteur sur F parallèlement à G (ces espaces étant de dimension finie), alors $\mathrm{rg}(p) = \dim(\mathrm{Im}(p)) = \dim(F)$.

✌ **Remarque XIX.13.** f est surjective si et seulement si $\mathrm{rg}(f) = \dim(F)$. En effet, $\mathrm{rg}(f) = \dim(f(E))$ ...

Proposition XIX.12. Soient E, F, G trois $\mathbb{K}$–e.v tels que E et F soient de dimension finies. Alors, si $u \in \mathscr{L}(E, F)$ et $v \in \mathscr{L}(F, G)$ on a :
(i) $\mathrm{rg}(v \circ u) \leq \min(\mathrm{rg}(u), \mathrm{rg}(v))$;
(ii) si u (resp. v) est un isomorphisme, $\mathrm{rg}(v \circ u) = \mathrm{rg}(v)$ (resp. $\mathrm{rg}(v \circ u) = \mathrm{rg}(u)$).

Démonstration.
(i) Comme $\mathrm{Im}(v\circ u) = v(u(E))$ et que $u(E) \subset F$, on a $\dim(v(u(E)) \leq \dim v(F) = \mathrm{rg}(v)$. De plus, par image, $\dim v(u(E)) \leq \dim u(E) = \mathrm{rg}(u)$, d'où le résultat.
(ii) Si u est bijective, alors $u(E) = F$ et donc $\mathrm{rg}(v \circ u) = \dim v(F) = \mathrm{rg}(v)$. On procède symétriquement dans le cas où v est bijective.

□

◇ Calcul pratique du rang d'une famille de vecteurs

Soit E un $\mathbb{K}$–e.v de dimension $p \in \mathbb{N}$ et soit $\mathscr{B} = (e_1, \dots, e_p)$ une base de E. On fixe une famille $\mathscr{F} = (u_1, \dots, u_n)$ de vecteurs de E s'écrivant, pour tout $j \in [\![1, n]\!]$:

$$u_j = \sum_{i=1}^{p} a_{i,j} e_i$$

dans la base $\mathscr{B}$.

Afin d'aider au calcul du rang de $\mathscr{F}$, nous énonçons les faits suivants, qui seront démontrés au chapitre XXI : on ne modifie pas le rang de $\mathscr{F}$ si on...
(A) ...on échange la position de deux vecteurs dans la famille ($u_i \leftrightarrow u_j$) ;
(B) ...on multiplie un vecteur par un scalaire **non nul** ($u_i \leftarrow \lambda u_j$) ;
(C) ...on ajoute à un vecteur une combinaison linéaire des **autres** $\left(u_i \leftarrow u_i + \sum_{j\neq i} \lambda_j u_j\right)$.

➠ **Exemple XIX.13.** Pour déterminer le rang de la famille $((1, 2, 5), (2, 1, 4), (1, -1, -1))$ dans $\mathbb{K}^3$, on effectue les opérations élémentaires suivantes : partant de

$$\begin{array}{c|c|c} 1 & 2 & 1 \\ 2 & 1 & -1 \\ 5 & 4 & -1 \end{array}$$

on soustrait à la deuxième colonne deux fois la première ($C_2 \leftarrow C_2 - 2C_1$) et à la troisième la première ($C_3 \leftarrow C_3 - C_1$), obtenant

$$\begin{array}{c|c|c} 1 & 0 & 0 \\ 2 & -3 & -3 \\ 5 & -6 & -6 \end{array}$$

puis on effectue $C_3 \leftarrow C_3 - C_2$

$$\begin{array}{c|c|c} 1 & 0 & 0 \\ 2 & -3 & 0 \\ 5 & -6 & 0 \end{array}$$

ce qui permet de conclure que le rang de notre famille est égal à celui de $((1,2,5),(0,-3,-6),(0,0,0))$, à savoir 2.

b) Théorème du rang

Proposition XIX.13 (Théorème "géométrique" du rang)**.** Soient E et F deux $\mathbb{K}$–e.v et soit $f \in \mathscr{L}(E,F)$. Alors, pour tout supplémentaire G de $\mathrm{Ker}(f)$, l'application

$$\begin{aligned} \varphi : G &\to \mathrm{Im}(f) \\ x &\mapsto f(x) \end{aligned}$$

est un isomorphisme.

✌ **Remarque XIX.14.** Noter que ce résultat est valable en dimension infinie (il faut toutefois obtenir l'existence d'un supplémentaire de $\mathrm{Ker}(f)$, ce qui nécessite l'axiome du choix).

Démonstration. Remarquons tout d'abord que l'application φ est bien définie et linéaire par construction. De plus :

$$\begin{aligned} \mathrm{Ker}(\varphi) &= \{x \in G \mid f(x) = 0\} \\ &= G \cap \mathrm{Ker}(f) \\ &= \{0\} \end{aligned}$$

donc φ est injective. Enfin, notons que si $y \in \mathrm{Im}(f)$ alors $\exists x \in E$, $f(x) = y$ et, comme $E = \mathrm{Ker}(f) \oplus G$ il existe un unique couple $(u,v) \in \mathrm{Ker}(f) \times G$ tel que : $y = f(u+v) = f(v)$ et donc φ est surjective. □

Théorème XIX.14 (Théorème du rang)**.**
Soient E et F deux $\mathbb{K}$–e.v tels que E soit de dimension finie et soit $f \in \mathscr{L}(E,F)$. Alors :

$$\dim(E) = \dim(\mathrm{Ker}(f)) + \mathrm{rg}(f)\,.$$

Démonstration. Soit G un supplémentaire de $\mathrm{Ker}(f)$ (il existe sans râler par dimension finie de E) ; alors $\dim(E) = \dim(\mathrm{Ker}(f)) + \dim(G)$. Or, la proposition XIX.13 entraîne que $\dim(G) = \dim(\mathrm{Im}(f)) = \mathrm{rg}(f)$, d'où le résultat. □

✖ **Attention :** ce théorème, fort utile au demeurant, ne signifie pas que si $f \in \mathscr{L}(E)$ alors $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ sont supplémentaires. Prendre par exemple

$$\begin{aligned} f : \mathbb{K}^2 &\longrightarrow \mathbb{K}^2 \\ (x,y) &\mapsto (y,0) \end{aligned}$$

qui vérifie $\mathrm{Ker}(f) = \mathrm{Im}(f) = \{(x,0) \mid x \in \mathbb{K}\}$.

Proposition XIX.15. Soient E et F deux $\mathbb{K}$–e.v de dimension finie **de même dimension** et soit $f \in \mathscr{L}(E,F)$. Alors les trois propriétés suivantes sont équivalentes :

(i) f est injective ;

(ii) f est surjective ;

(iii) f est bijective.

Démonstration.

(i)⇒(ii) Si f est injective alors $\dim(E) = \mathrm{rg}(f)$ par théorème du rang (XIX.14) et comme $\dim(E) = \dim(F)$ on a bien f surjective.

(ii)⇒(iii) On a dans ce cas $\dim(\mathrm{Ker}(f)) = \dim(E) - \mathrm{rg}(f) = \dim(F) - \mathrm{rg}(f) = 0$, d'où f est injective donc bijective.

(iii)⇒(i) Trivial.

□

✌ **Remarque XIX.15.** Cela signifie qu'un endomorphisme est bijectif si et seulement si il est inversible à gauche ou à droite.

➠ **Exemple XIX.14.** Ce résultat facilite **considérablement** notre travail lorsque nous souhaitons démontrer le caractère bijectif d'une application linéaire pour peu que les étoiles (et les dimensions) soient alignées.

— l'application

$$\begin{aligned} f : \mathbb{K}^3 &\longrightarrow \mathbb{K}_2[X] \\ (a,b,c) &\mapsto aX^2 + bX + c \end{aligned}$$

est bijective : son noyau est aisé à déterminer et $\dim(\mathbb{K}_2[X]) = 3 = \dim(\mathbb{K}^3)$.

— De même, on montre aisément que l'application

$$\begin{aligned} \varphi : \mathbb{K}_n[X] &\longrightarrow \mathbb{K}^{n+1} \\ P &\mapsto (P(a_0), \ldots, P(a_n)) . \end{aligned}$$

est bijective pour $a_0, \ldots, a_n \in \mathbb{K}$ deux à deux distincts. Le lecteur avisé subira une impression massive de déjà vu.

La formule qui suit est attribuée à Hermann Günther Grassmann, mathématicien et indianiste (spécialiste des langues et civilisations du sous–continent indien) allemand (1809—1877).

Proposition XIX.16. Soient F et G deux s–e.v d'un $\mathbb{K}$–e.v de dimension finie E. Alors :

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

Démonstration. Il suffit de remarquer que l'application

$$\begin{aligned} f : F \times G &\to F + G \\ (x, y) &\mapsto x + y \end{aligned}$$

est surjective, de noyau

$$\operatorname{Ker}(f) = \{(x, -x) \,|\, x \in F \cap G\}$$

isomorphe à $F \cap G$ et d'appliquer le théorème du rang (XIX.14) en se rappelant que $\dim(F \times G) = \dim(F) + \dim(G)$. □

Exemple XIX.15. Soient $\mathscr{P}$ et $\mathscr{P}'$ deux plan de $\mathbb{R}^3$. Alors :

$$\dim(\mathscr{P} \cap \mathscr{P}') = \dim(\mathscr{P}) + \dim(\mathscr{P}') - \dim(\mathscr{P} + \mathscr{P}') = 4 - \dim(\mathscr{P} + \mathscr{P}') \,.$$

Or $\dim(\mathscr{P} + \mathscr{P}') = 3$ si les deux plans ne sont pas confondus et 2 sinon. Ceci entraîne que l'intersection de deux plans non confondus de $\mathbb{R}^3$ est une droite.

Exemple XIX.16. Deux droites sont en somme directe si et seulement si elles engendrent un plan. De même, un plan et une droite le sont à condition d'engendrer un espace de dimension 3.

4.– Formes linéaires et hyperplans

Rappelons avant de débuter ce paragraphe que si E est un $\mathbb{K}$–e.v, son **dual** E^* est l'ensemble

$$E^* = \mathscr{L}(E, \mathbb{K})$$

des **formes linéaires** sur E. Nous avons également vu que si E est de dimension finie, alors $\dim(E) = \dim(E^*)$, ce qui entraîne que E et E^* sont isomorphes.

On fixe dans ce paragraphe un $\mathbb{K}$–e.v de dimension finie E de dimension $n \in \mathbb{N}$.

a) Formes linéaires coordonnées

Définition XIX.6. Soit $\mathscr{B} = (e_i)_{i \in [\![1,n]\!]}$ une base de E. On appelle **formes coordonnées** relativement à la base $\mathscr{B}$ les formes linéaires suivantes :

$$\begin{aligned} e_i^* : E &\to \mathbb{K} \\ e_j &\mapsto \delta_{i,j} \end{aligned}$$

pour $i \in [\![1, n]\!]$.

Remarque XIX.16.

— Si $x = \sum_{i=1}^{n} x_i e_i \in E$, on a, pour $j \in [\![1, n]\!]$:

$$e_j^*(x) = \sum_{i=1} x_i \underbrace{e_j^*(e_i)}_{=\delta_{i,j}} = x_j \,.$$

Ces formes linéaires peuvent également être définies, *stricto sensu*, en dimension infinie (lorsque l'on dispose d'une base de E).

— On peut démontrer que la famille des formes linéaires coordonnées à une base donnée forme une base de E^*. Il suffit de montrer que cette famille est libre, étant donné l'égalité $\dim(E) = \dim(E^*)$. Si l'on suppose trouvée une famille $(\lambda_i)_{i\in[\![1,n]\!]}$ de scalaires telle que $\sum_{i=1}^{n} \lambda_i e_i^* = 0$ alors, pour tout $j \in [\![1,n]\!]$:

$$0 = \sum_{i=1}^{n} \lambda_i e_i^*(e_j) = \lambda_j$$

d'où le résultat.

— Le résultat précédent peut également être vu comme un corollaire de la proposition XIX.10 (fixer (1) comme base de $\mathbb{K}$).

Exemple XIX.17.

— Considérons la base $((1,1)(0,1))$ de $\mathbb{K}^2$; si $(x,y) \in \mathbb{K}^2$ alors

$$(x,y) = x \cdot (1,1) + (y-x) \cdot (0,1)$$

ce qui entraîne que les formes linéaires coordonnées associées à cette dernière sont $(x,y) \mapsto x$ et $(x,y) \mapsto y - x$.

— Soient $x_0, \dots, x_n \in \mathbb{K}$ deux à deux distincts : on dispose alors de la famille des polynômes de Lagrange associée à ceux ci, en l'occurrence, pour $i \in [\![0,n]\!]$:

$$L_i = \prod_{j\neq i} \frac{X - x_j}{x_i - x_j} \in \mathbb{K}_n[X]\,.$$

Par existence du polynôme interpolateur de Lagrange (*cf.* chapitre XIV), la famille $(L_0, \dots, L_n)$ est génératrice de $\mathbb{K}_n[X]$ et de cardinal égal à la dimension de cet espace : il s'agit donc d'une base. Pour déterminer les formes linéaires coordonnées associées à cette dernière sont, notons que pour tous $i, j \in [\![0,n]\!]$ nous devrions avoir :

$$L_i^*(L_j) = \delta_{i,j}$$

et donc, si $P \in \mathbb{K}_n[X]$ alors $P = \sum_{j=0}^{n} P(x_j) L_j$ ce qui entraîne que :

$$L_i^*(P) = \sum_{j=0}^{n} P(x_j) L_i^*(L_j) = P(x_i)\,.$$

Les L_i^* sont donc les morphismes d'évaluation en les x_i.

b) Lien aux hyperplans

Si H est un hyperplan de E, alors H est le noyau d'une forme linéaire non nulle $\varphi \in E^*$. Fixons $(e_i)_{i\in[\![1,n]\!]}$ une base de E : alors il existe une unique famille $(\lambda_i)_{i\in[\![1,n]\!]}$ de scalaires telle que :

$$\varphi = \sum_{i=1}^{n} \lambda_i e_i^*$$

avec de plus, pour tout $j \in [\![1,n]\!]$:

$$\varphi(e_j) = \sum_{i=1}^{n} \lambda_i \underbrace{e_i^*(e_j)}_{=\delta_{i,j}} = \lambda_j$$

ce qui permet d'écrire :

$$\varphi = \sum_{i=1}^{n} \varphi(e_i)e_i^* .$$

Soit $x = \sum_{i=1}^{n} x_i e_i \in E$; alors on a :

$$\begin{aligned} x \in H &\Leftrightarrow \varphi(x) = 0 \\ &\Leftrightarrow \sum_{i=1}^{n} \varphi(e_i)e_i^*(x) = 0 \\ &\Leftrightarrow \sum_{i=1}^{n} \varphi(e_i)x_i = 0 . \end{aligned}$$

Cette dernière égalité est appelée **équation cartésienne** de l'hyperplan $\mathscr{H}$.

➠ **Exemple XIX.18.** $x + y - 3z = 0$ est l'équation d'un plan dans $\mathbb{R}^3$, noyau de $(x, y, z) \mapsto x + y - 3z$. Une base en est (par exemple) $(1, 2, 1), (1, -1, 0))$.

De fait, un hyperplan dans E correspond à l'espace des solutions d'une équation **linéaire** à n inconnues. On en déduit que l'ensemble des solutions d'un système linéaire est une intersection d'hyperplans.

Proposition XIX.17. Soient $H_1, \dots, H_m$ des hyperplans de E. Alors :

$$\dim\left(\bigcap_{i=1}^{m} H_i\right) \geq n - m .$$

Réciproquement, si F est un s–e.v de E de dimension $n - m$, alors il existe m hyperplans $\mathscr{H}_1, \dots, \mathscr{H}_m$ de E tels que :

$$F = \bigcap_{k=1}^{m} \mathscr{H}_k .$$

Démonstration. Soient $\varphi_1, \dots, \varphi_m \in E^* \setminus \{0\}$ telles que pour tout $i \in [\![1, m]\!]$, $H_i = \mathrm{Ker}(\varphi)$. On obtient le premier point en appliquant le théorème du rang à l'application

$$\begin{aligned} f : E &\to \mathbb{K}^m \\ x &\mapsto (\varphi_1(x), \dots, \varphi_m(x)) \end{aligned}$$

dont le noyau est égal à l'intersection des H_i et qui est surjective. Pour la réciproque, fixons $\mathscr{B} = (e_1, \dots, e_n)$ une base de E adaptée à F et posons, pour $k \in [\![1, m]\!]$ φ_k comme étant l'unique forme linéaire envoyant e_{n-m+k} sur 0 est les autres e_i sur 1. Il suffit alors de poser $\mathscr{H}_k = \mathrm{Ker}(\varphi_k)$. □

✌ **Remarque XIX.17.** Tout ceci généralise les résultats vus en géométrie dans les classes antérieures sur les équations de droites et plans dans $\mathbb{R}^2$ et $\mathbb{R}^3$.

Chapitre XX

Intégration

0.⁻ Continuité uniforme

On fixe dans ce paragraphe un intervalle I d'intérieur non vide.

Définition XX.1. Une fonction $f : I \to \mathbb{R}$ est dite **uniformément continue** (u.c) si :

$$\forall \varepsilon > 0,\, \exists\, \delta > 0,\, \forall x, y \in I,\, (|x-y| \leq \delta) \Rightarrow (|f(x) - f(y)| \leq \varepsilon)\,.$$

Exemple XX.1. Si $a \in \mathbb{R}^*$, la fonction $x \mapsto ax$ est u.c : il suffit, à ε fixé de poser $\delta = \dfrac{\varepsilon}{|a|}$.

Remarque XX.1. Notons la différence avec la définition de continuité sur I, qui est (rappelons le) :

$$\forall x \in I,\, \forall \varepsilon > 0,\, \exists\, \delta > 0,\, \forall y \in I,\, (|x-y| \leq \delta) \Rightarrow (|f(x) - f(y)| \leq \varepsilon)\,.$$

Dans le cas de la continuité "simple", δ dépend du point x où l'on étudie la continuité. Dans le cas uniforme, il est. . .uniforme relativement à celui–ci.

Proposition XX.1. Toute fonction u.c sur I est continue sur cet intervalle.

Démonstration. Découle immédiatement de la remarque *supra*. □

✖ **Attention :** la réciproque est **fausse**. Pour un contre exemple, considérons la fonction (continue) $x \mapsto x^2$ sur $\mathbb{R}_+$ et fixons $\delta > 0$. Comme $(2x+\delta)\delta \xrightarrow[x \to \infty]{} \infty$, il existe $x \in \mathbb{R}_+$ tel que

$$(2x+\delta)\delta > 1\,.$$

En posant $y = x + \delta$ on a à la fois $|x-y| \leq \delta$ et

$$|x^2 - y^2| = |x^2 - x^2 - 2x\delta - \delta^2| = (2x+\delta)\delta > 1$$

ce qui contredit la définition de continuité uniforme pour $\varepsilon = 1$.

Proposition XX.2. Toute fonction lipschitzienne est u.c.

Démonstration. Soit f une fonction lipschitzienne : il existe donc $M \in \mathbb{R}_+^*$ tel que :

$$\forall x, y \in I,\ |f(x) - f(y)| \leq M|x - y| .$$

Soit $\varepsilon > 0$; alors, en posant $\delta = \dfrac{\varepsilon}{M}$ on a bien

$$\forall x, y \in I, (|x - y| \leq \delta) \Rightarrow (|f(x) - f(y)| \leq \varepsilon) .$$

□

✖ **Attention :** une fois encore, la réciproque est fumeuse. L'exercice *infra* fournit un contre exemple (presque) gratuit.

✍ **Exercice XX.1.** On considère la fonction

$$\begin{aligned} g : \mathbb{R}_+ &\to \mathbb{R} \\ x &\mapsto \sqrt{x} \end{aligned} \quad .$$

1. (a) Démontrer que pour tous $x, y \in \mathbb{R}_+$,

   $$|\sqrt{x} - \sqrt{y}| \leq \sqrt{|x - y|} .$$

   (b) En déduire que g est u.c. sur $\mathbb{R}_+$.
2. Démontrer g n'est pas lipschitzienne sur $\mathbb{R}_+$. On pourra considérer le taux d'accroissement de g en 0.

Le point culminant (et pertinent vis à vis du programme) est le résultat suivant, dont la démonstration est admise. Il est du au mathématicien allemand Eduard Heine (1821—1881).

Théorème XX.3 (Heine)**.**
Toute fonction continue sur un segment y est uniformément continue.

✍ **Exercice XX.2.** La démonstration de ce résultat est tout à fait abordable en MPSI. Le lecteur curieux pourra s'y essayer via cet exercice. Fixons deux réels a et b tels que $a < b$ et une fonction continue $f : [a, b] \to \mathbb{R}$ et procédons par l'absurde en supposant que f n'est pas u.c. sur $[a, b]$.

1. Démontrer qu'il existe dans ce cas un réel $\varepsilon > 0$ et deux suites $(x_n)_n, (y_n)_n$ d'éléments de $[a, b]$ tels que

   $$\forall n \geq 1, \qquad \left(|x_n - y_n| \leq \frac{1}{n}\right) \wedge (|f(x_n) - f(y_n)| > \varepsilon) .$$

2. (a) Montrer qu'il existe une fonction strictement croissante $\varphi : \mathbb{N} \to \mathbb{N}$ telle que $(x_{\varphi(n)})_n$ converge vers un nombre réel ℓ.

   (b) Justifier que $\ell \in [a, b]$.

   (c) Démontrer que la suite $(y_{\varphi(n)})_n$ converge également vers ℓ.

   (d) Déterminer la limite, quand n tend vers l'infini, de la quantité $|f(y_{\varphi(n)}) - f(x_{\varphi(n)})|$.
3. Conclure.

1.⁻ Intégrale des fonctions en escalier

On fixe dans ce paragraphe $a, b \in \mathbb{R}$ tels que $a < b$.

a) Subdivisions, fonctions en escalier

Définition XX.2. On appelle **subdivision** du segment $[a, b]$ toute famille $\sigma = (x_0, \ldots, x_n)$ de points de celui–ci tels que :

$$a = x_0 < x_1 < \ldots < x_{n-1} < x_n = b\,.$$

Remarque XX.2. Il s'agit donc de "délimiter" n sous–segments au segment $[a, b]$.

Notation. On notera $S(a, b)$ l'ensemble des subdivisions du segment $[a, b]$.

Exemple XX.2.
— $\left(0, \frac{1}{3}, \frac{1}{2}, 1\right)$ est une subdivision relativement aisée à visualiser du segment $[0, 1]$;
— pour $n \geq 1$, on appelle **subdivision régulière** du segment $[a, b]$ de rang n la subdivision

$$\sigma^n_{\mathscr{R}}(a, b) = \left(a + k\frac{b-a}{n}\right)_{k \in [\![0, n]\!]}\,.$$

Définition XX.3. Soit $\sigma = (x_0, \ldots, x_n) \in S(a, b)$. On appelle :
— **pas** de σ la quantité $\mu(\sigma) = \max\{x_{i+1} - x_i \,|\, i \in [\![0, n-1]\!]\}$;
— **support** de σ l'ensemble $\mathrm{supp}(\sigma) = \{x_i | i \in [\![0, n]\!]\}$.

Exemple XX.3. Le pas de $\sigma^n_{\mathscr{R}}(a, b)$ est $\frac{b-a}{n}$.

Définition XX.4. Soient $\sigma, \sigma' \in S(a, b)$. On dit que σ est **plus fine** que σ' si $\mathrm{supp}(\sigma') \subset \mathrm{supp}(\sigma)$.

Notation. $\sigma' \prec \sigma$

Remarque XX.3. Cela signifie que σ contient *a minima* tous les points de σ'.

Exemple XX.4. $\left(0, \frac{1}{2}, 1\right) \prec \sigma^4_{\mathscr{R}}(0, 1)$.

Remarque XX.4. Il s'agit d'un ordre non total sur $S(a, b)$.

Proposition XX.4. Soient $\sigma, \sigma' \in S(a, b)$. Alors il existe une subdivision σ'' telle que $\sigma \prec \sigma''$ et $\sigma' \prec \sigma''$.

Démonstration. Il suffit de choisir σ'' de façon à ce que $\mathrm{supp}(\sigma'') = \mathrm{supp}(\sigma) \cup \mathrm{supp}(\sigma')$. □

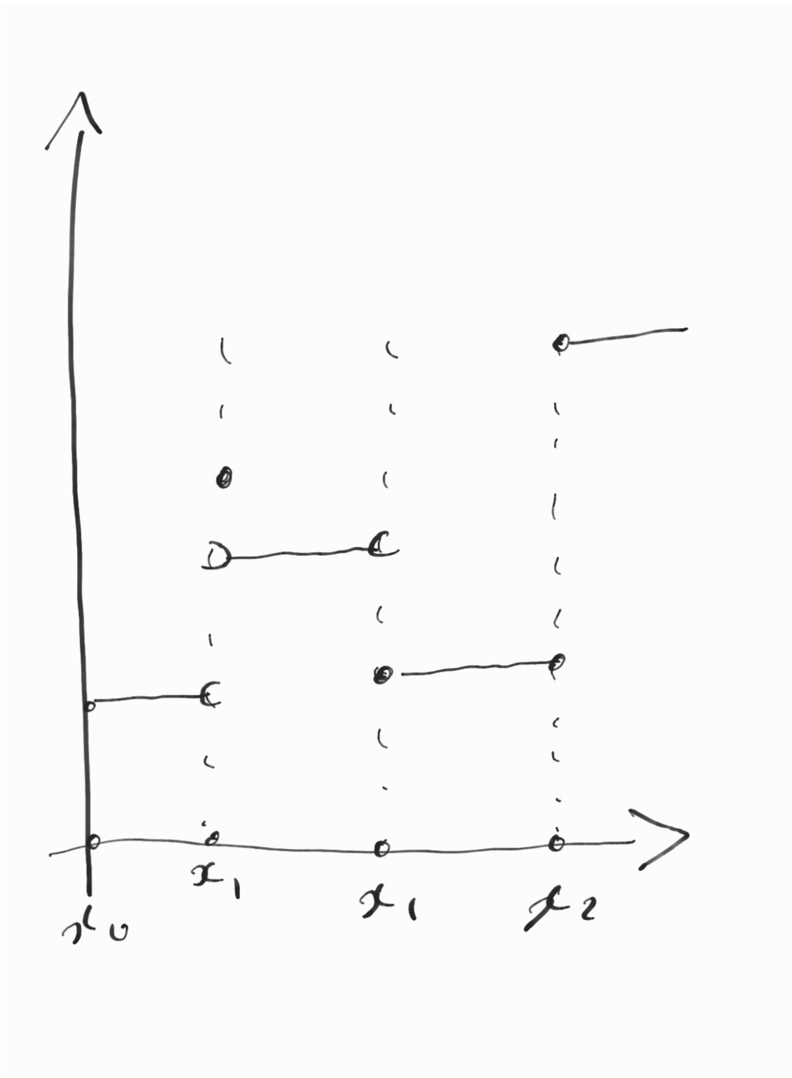
Ces définitions liminaires nous permettent (enfin) de rentrer dans le cœur de notre sujet à ce stade, en l'occurrence les fonctions en escalier.

Définition XX.5. Une fonction $\phi : [a,b] \to \mathbb{R}$ est dite **en escalier** si il existe une subdivision $\sigma = (x_0, \dots, x_n) \in S(a,b)$ telle que :

$$\forall i \in [\![0, n-1]\!], \text{ la fonction } \phi_{|]x_i, x_{i+1}[} \text{ est constante.}$$

Notation. On notera $\mathscr{E}(a,b)$ l'ensemble des fonctions en escalier sur $[a,b]$.

Vocabulaire. Une subdivision vérifiant les conditions de la définition XX.5 est dite **adaptée** à la fonction ϕ. Notons que si σ est adaptée, alors toute subdivision σ' plus fine que σ l'est également.



➠ **Exemple XX.5.** La fonction partie entière est en escalier sur $[-5, 12]$ (par exemple), relativement à toute subdivision dont le support contient $\mathbb{Z}$.

✌ **Remarque XX.5.**

— $(\mathscr{E}(a,b),+,.)$ (resp. $(\mathscr{E}(a,b),+,\times)$) est un s–e.v (resp. un sous–anneau) de $\mathbb{R}^{[a,b]}$. Lorsque ces deux structures sont présentes, on parle de **sous–algèbre**.
— Le seuls fonctions en escalier continues sont constantes.

b) Intégrale d'une fonction en escalier

Proposition/définition XX.6. Soit $\phi \in \mathscr{E}(a,b)$ et soit $\sigma \in S(a,b)$ une subdivision adaptée à ϕ. Pour $i \in [\![0,n-1]\!]$, on note y_i la valeur de la fonction (constante) $\phi_{|]x_i,x_{i+1}[}$. Alors la quantité

$$\sum_{i=0}^{n-1} y_i(x_{i+1}-x_i)$$

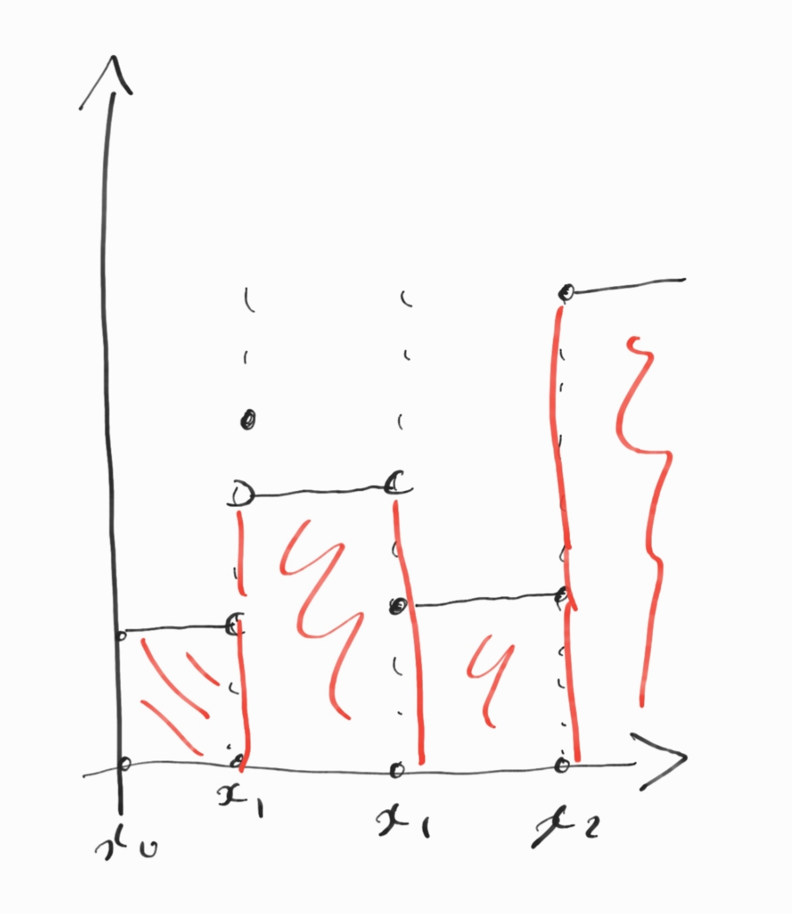
ne dépend pas de σ et est appelée **intégrale** de ϕ sur le segment $[a,b]$.

Démonstration. Il est clair que cette quantité est inchangée si l'on passe à une subdivision plus fine que σ. Si σ' est une autre subdivision adaptée à ϕ qui n'est pas plus fine que σ, on utilise la proposition XX.4 pour régler la question. □

Notation. Les **seules** notations tolérées par le programme de MPSI sont :

$$\int_{[a,b]} \phi, \quad \int_a^b \phi \quad \text{et} \quad \int_a^b \phi(t)\,\mathrm{d}t\,.$$

Géométriquement, l'intégrale d'une fonction en escalier correspond à l'aire (algébrique) délimitée par la courbe de f (ignorant les discontinuités) et l'axe des abscisses.



Exemple XX.6.

$$\int_{-1}^{7} \lfloor x \rfloor \, \mathrm{d}x = \sum_{i=-1}^{6} i(i+1-i) = -1+0+1+2+3+4+5+6 = 20\,.$$

Proposition XX.5. Soient $\phi, \psi \in \mathscr{E}(a,b)$ et soit $\lambda \in \mathbb{R}$. Alors :

(i)
$$\int_{[a,b]} \phi + \lambda\psi = \int_{[a,b]} \phi + \lambda \int_{[a,b]} \psi\ ; \qquad \textbf{[linéarité]}$$

(ii)
$$(\phi \leq \psi) \Rightarrow \left(\int_{[a,b]} \phi \leq \int_{[a,b]} \psi \right)\ ; \qquad \textbf{[croissance]}$$

(iii)
$$\left| \int_{[a,b]} \phi \right| \leq \int_{[a,b]} |\phi|\,. \qquad \textbf{[inégalité triangulaire]}$$

Démonstration.

(i) Trivial, quitte à utiliser la proposition XX.4 pour matérialiser une subdivision adaptée à ϕ **et** ψ.

(ii) Par définition de l'intégrale, on a que si $\phi - \psi \leq 0$ alors $\displaystyle\int_a^b \phi - \psi \leq 0$. On conclut par linéarité.

(iii) On sait que $\phi \leq |\phi|$ et $-\phi \leq |\phi|$. De fait, par croissance et linéarité :

$$\int_a^b \phi \leq \int_a^b |\phi| \quad \text{et} \quad -\int_a^b \phi = \int_a^b (-\phi) \leq \int_a^b |\phi|$$

d'où le résultat.

□

La proposition suivante est souvent appelée "formule de Chasles", de part sa similarité avec la relation vectorielle éponyme. Elle n'a cependant rien à voir avec Michel Chasles, mathématicien français (1793—1880) connu pour ses travaux en géométrie projective et analyse harmonique.

Proposition XX.6 ("Chasles")**.** Soit $c \in [a, b]$ et soit $\phi \in \mathscr{E}(a, b)$. Alors :

$$\int_a^b \phi = \int_a^c \phi + \int_c^b \phi\,.$$

Démonstration. Il suffit de fixer une subdivision adaptée à $[a, c]$ et $[c, b]$. □

Remarque XX.6. Il est possible d'assouplir quelque peu notre notation en posant (rappelons que $a < b$) :

$$\int_b^a \phi = -\int_a^b \phi\,.$$

Les propriétés vues précédemment, formule de "Chasles" comprise, se généralisent sans guère de soucis à la condition de **prendre garde au sens des inégalités** : l'intégrale "à l'envers" est décroissante et non croissante. Notons au passage que l'on obtient :

$$\int_a^a \phi = \int_a^b \phi + \int_b^a \phi = 0\,.$$

2.⁻ Intégrale de Riemann

On fixe dans ce paragraphe $a, b \in \mathbb{R}$ tels que $a < b$.

a) Fonctions continues par morceaux

Définition XX.7. Une fonction $f : [a, b] \to \mathbb{R}$ est dite **continue par morceaux** si il existe $\sigma = (x_0, \ldots, x_{n-1}) \in S(a, b)$ telle que :
— $\forall i \in [\![0, , n-1]\!]$, $f \in \mathscr{C}^0(]x_i, x_{i+1}[)$;
— f admet des limites **réelles** (non nécessairement égales) à gauche et à droite en $x_1, \ldots, x_{n-1}$;
— f admet une limite **réelle** à gauche en b et à droite en a.

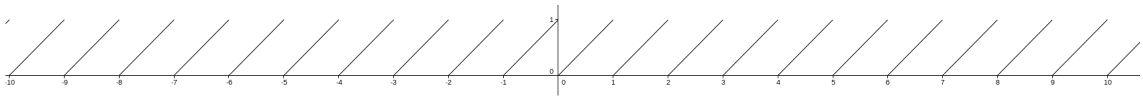
Vocabulaire. Toute subdivision satisfaisant ces propriétés est dite **adaptée** à f.

Notation. On note $\mathscr{C}_{\text{pm}}([a,b])$ l'ensembles des fonctions continue par morceaux sur $[a,b]$.

Exemple XX.7.
- les fonctions continues sont continue par morceaux ;
- les fonctions en escalier sont continue par morceaux ;
- la fonction

$$f : [-100, 100] \to \mathbb{R}$$
$$x \mapsto x - \lfloor x \rfloor$$

  est continue par morceaux .



- La fonction

$$x \mapsto \begin{cases} \sin\left(\dfrac{1}{x}\right) & \text{si } x \neq 0 \\ 0 \text{ sinon.} \end{cases}$$

  n'est **pas** continue par morceaux sur $[0,1]$ car elle n'admet pas de limite à droite en 0.

Remarque XX.7. $\mathscr{C}_{\text{pm}}([a,b])$ est une sous–algèbre de $\mathbb{R}^{[a,b]}$ contenant $\mathscr{E}(a,b)$ et $\mathscr{C}^0([a,b])$.

Définition XX.8. Une fonction est dite continue par morceaux sur I si elle l'est sur tout segment inclus dans I.

Exemple XX.8. La fonction f *supra* est en fait continue par morceaux sur $\mathbb{R}$.

Théorème XX.7 (Densité des fonctions en escalier)**.**
Soit $f \in \mathscr{C}_{\text{pm}}([a,b])$. Alors, pour tout $\varepsilon > 0$ il existe deux fonctions en escalier $\phi, \psi \in \mathscr{E}(a,b)$ telles que :

(i) $\phi \leq f \leq \psi$;

(ii) $0 \leq \psi - \phi \leq \varepsilon$.

Démonstration. Soit $\varepsilon > 0$. Commençons par remarquer qu'il nous suffit de définir ϕ et ψ sur chacun des intervalles de continuité de f : nous pouvons donc légitimement supposer f continue sur le segment $[a,b]$ et donc, par théorème de Heine (XX.3) uniformément continue sur ce dernier. Nous obtenons de fait l'existence de $\delta > 0$ tel que :

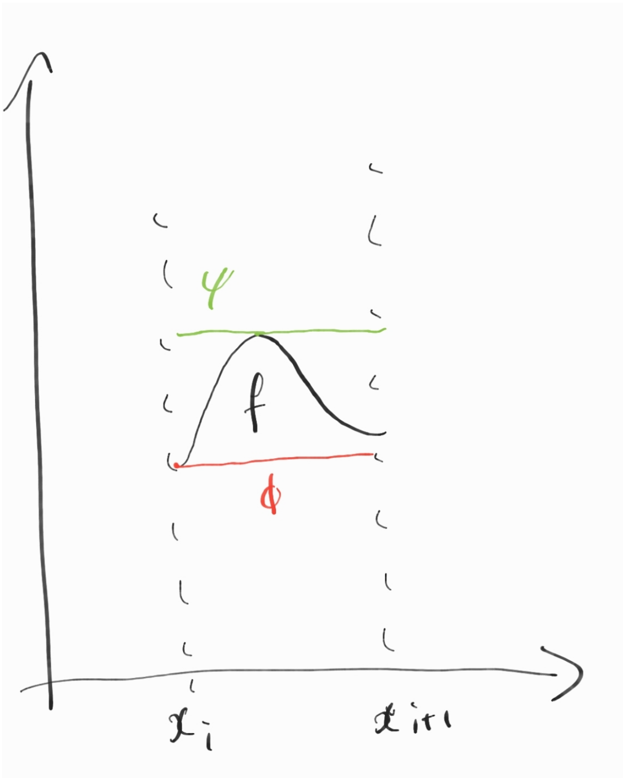
$$\forall x, y \in [a,b],\ (|x-y| \leq \delta) \Rightarrow (|f(x) - f(y)| \leq \varepsilon)\,.$$

Donnons nous à présent une subdivision $\sigma = (x_0, \dots, x_n) \in S(a,b)$ telle que $\mu(\sigma) \leq \delta$ et posons :

$$\begin{aligned} \phi : [a,b] &\longrightarrow \mathbb{R} \\ x &\mapsto \begin{cases} \min f_{[x_i,x_{i+1}[} \text{ si } x \in [x_i, x_{i+1}[\text{ avec } i \in [\![0, n-1]\!] \\ f(b) \text{ si } x = b \end{cases} \end{aligned}$$

ainsi que :

$$\begin{aligned} \psi : [a,b] &\longrightarrow \mathbb{R} \\ x &\mapsto \begin{cases} \max f_{[x_i,x_{i+1}[} \text{ si } x \in [x_i, x_{i+1}[\text{ avec } i \in [\![0, n-1]\!] \\ f(b) \text{ si } x = b \end{cases} \end{aligned}$$



Notons que ϕ (resp. ψ) constitue une approximation de f par défaut (resp. excès) sur les intervalles $[x_i, x_{i+1}[$. On a donc immédiatement que $\phi \leq f \leq \psi$ sur $[a,b]$ et, pour tout $i \in [\![0, n-1]\!]$ et $x \in [x_i, x_{i+1}[$:

$$\psi(x) - \phi(x) = \max f_{[x_i,x_{i+1}[} - \min f_{[x_i,x_{i+1}[} \leq \varepsilon$$

par continuité uniforme ($|x_{i+1} - x_i| \leq \delta$ par construction). L'inégalité étant triviale en $x = b$, on a bien $0 \leq \psi - \phi \leq \varepsilon$ sur $[a,b]$, d'où le résultat.

□

b) Intégrale d'une fonction continue par morceaux

Notation. Soit $f \in \mathscr{C}_{\text{pm}}([a,b])$. Comme f est bornée sur chacun des ses intervalles de continuité, elle l'est sur $[a,b]$; nous pouvons donc poser :

$$E_-(f) = \left\{ \int_{[a,b]} \phi \;\middle|\; \phi \in \mathscr{E}(a,b),\ \phi \leq f \right\}$$

et

$$E_+(f) = \left\{ \int_{[a,b]} \phi \,\middle|\, \phi \in \mathscr{E}(a,b),\ \phi \geq f \right\}.$$

Proposition XX.8. Soit $f \in \mathscr{C}_{\mathrm{pm}}([a,b])$; alors :

(i) $E_-(f)$ admet une borne supérieure ;

(ii) $E_+(f)$ admet une borne inférieure ;

(iii) $\sup(E_-(f)) = \inf(E_+(f))$.

Démonstration. Les deux ensembles $E_+(f)$ et $E_-(f)$ sont des parties de $\mathbb{R}$ non vides : en effet, f est bornée donc il existe $M \in \mathbb{R}_+$ tel que $\forall x \in [a,b]$, $|f(x)| \leq M$ et donc $E_-(f)$ resp. $(E_+(f))$ contient la fonction $x \mapsto -M$ (resp. $x \mapsto M$).

Soient à présent $x \in E_-(f)$ et $y \in E_+(f)$. Alors, il existe $\phi, \psi \in \mathscr{E}(a,b)$ telles que $\phi \leq f \leq \psi$, $x = \displaystyle\int_{[a,b]} \phi$ et $y = \displaystyle\int_{[a,b]} \psi$. De fait, par croissance de l'intégrale $x \leq y$ et donc les bornes voulues existent (tout élément de $E_-(f)$ minore $E_+(f)$ et tout élément de $E_+(f)$ majore $E_-(f)$) et $\sup(E_-(f)) \leq \inf(E_+(f))$.

Pour obtenir l'égalité, fixons $n \geq 1$ et notons que nous avons l'existence, par théorème XX.7, de deux fonctions en escalier $\phi, \psi \in \mathscr{E}(a,b)$ telles que $\phi \leq f \leq \psi$ et $\psi - \phi \leq \dfrac{1}{n(b-a)}$. On a, par croissance de l'intégrale sur les fonctions en escalier :

$$0 \leq \underbrace{\int_a^b \psi}_{\geq \inf(E_+(f))} - \underbrace{\int_a^b \phi}_{\leq \sup(E_-(f))} \leq \int_a^b \frac{1}{n(b-a)} = \frac{1}{n}$$

ce qui entraîne que :

$$\inf(E_+(f)) - \sup(E_-(f)) \leq \frac{1}{n}$$

et donc, en faisant tendre n vers l'infini, on obtient l'inégalité désirée. $\square$

Définition XX.9. Soit $f \in \mathscr{C}_{\mathrm{pm}}([a,b])$; la quantité $\sup(E_-(f)) = \inf(E_+(f))$ est appelée **intégrale** de f sur le segment $[a,b]$.

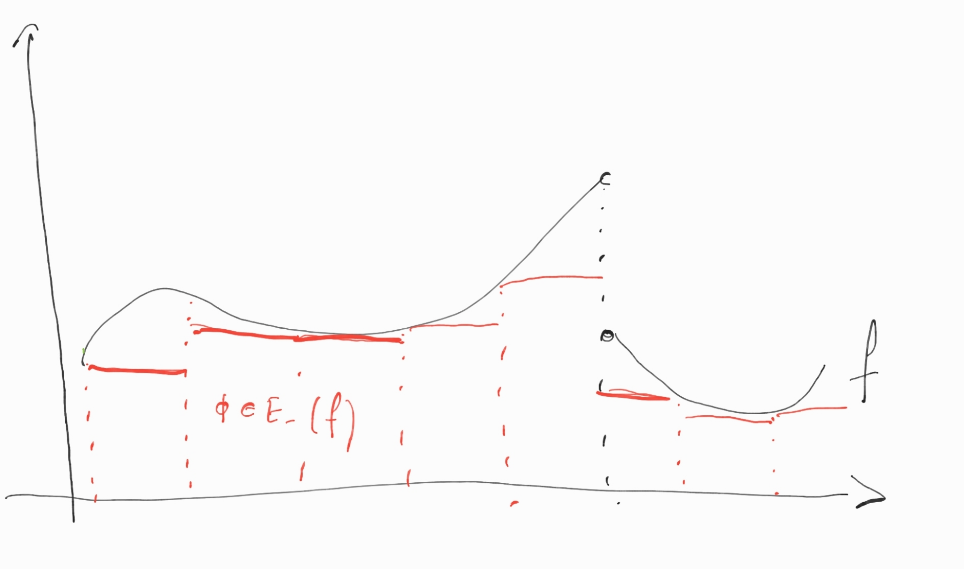
Notation. Une nouvelle fois, les **seules** notations tolérées par le programme de MPSI sont :

$$\int_{[a,b]} f, \quad \int_a^b f \quad \text{et} \quad \int_a^b f(t)\,\mathrm{d}t\,.$$

✌ **Remarque XX.8.**

— Notons que si f est en escalier, les bornes de $E_+(f)$ et $E_-(f)$ sont atteintes : nos deux définitions d'intégrales coïncident bien. Notre psychologue peut s'autoriser un soupir de soulagement.

— Une fonction "pas trop mal choisie" dans $E_-(f)$ est une fonction en escalier "aussi proche que possible" de f tout en restant au–dessous du point de vue des courbes : approcher l'intégrale de f par celle de cette fonction revient donc à appliquer à f une méthode des rectangles par défaut. Même chose avec $E_+(f)$ et la méthode par excès.



— On appelle **valeur moyenne** de f la quantité

$$\langle f \rangle = \frac{1}{b-a}\int_a^b f(t)\,\mathrm{d}t\,.$$

✍ **Exercice XX.3.** Déterminer $\displaystyle\int_0^1 x^2\,\mathrm{d}x$.

➥ **Correction :** *Soit $n \geq 1$; on pose $\sigma = \left(\frac{k}{n}\right)_{k\in[\![0,n]\!]}$ et*

$$\begin{aligned}\phi : [0,1] &\longrightarrow \mathbb{R}\\ x &\mapsto \begin{cases}\left(\frac{k}{n}\right)^2 \ \textit{si}\ x \in \left[\frac{k}{n},\frac{k+1}{n}\right[\ \textit{avec}\ k \in [\![0,n-1]\!]\\ 1 \ \textit{si}\ x = 1\end{cases}\end{aligned}$$

ainsi que :

$$\begin{aligned}\psi : [0,1] &\longrightarrow \mathbb{R}\\ x &\mapsto \begin{cases}\left(\frac{k+1}{n}\right)^2 \ \textit{si}\ x \in \left[\frac{k}{n},\frac{k+1}{n}\right[\ \textit{avec}\ k \in [\![0,n-1]\!]\\ 1 \ \textit{si}\ x = 1\end{cases}\end{aligned}\ .$$

On a alors clairement $\forall x \in [0,1],\ \phi(x) \leq x^2 \leq \psi(x)$ et :

$$\int_0^1 \phi(x)\,\mathrm{d}x = \frac{1}{n}\sum_{k=0}^{n-1}\left(\frac{k}{n}\right)^2 = \frac{(n-1)(2n-1)}{6n^2}$$

et

$$\int_0^1 \psi(x)\,\mathrm{d}x = \frac{1}{n}\sum_{k=0}^{n-1}\left(\frac{k+1}{n}\right)^2 = \frac{(n+1)(2n+1)}{6n^2}\,.$$

Ceci entraîne que

$$\frac{(n-1)(2n-1)}{6n^2} \leq \int_0^1 x^2 \,\mathrm{d}x \leq \frac{(n+1)(2n+1)}{6n^2}$$

et donc, par théorème d'encadrement des limites (VII.11) :

$$\int_0^1 x^2 \,\mathrm{d}x = \frac{1}{3}\,.$$

c) Propriétés de l'intégrale

Dans ce paragraphe, nous étendons à l'intégrale des fonctions continue par morceaux les propriétés observées dans le cas des fonctions en escalier. Sans surprise, tout ceci requiert un usage massif du théorème XX.7.

◇ Linéarité

Proposition XX.9. Soient $f, g \in \mathscr{C}_{\mathrm{pm}}([a,b]$ et soit $\lambda \in \mathbb{R}$. Alors :

$$\int_a^b (f(t) + \lambda g(t))\,\mathrm{d}t = \int_a^b f(t)\,\mathrm{d}t + \lambda \int_a^b g(t)\,\mathrm{d}t\,.$$

Démonstration. Traitons le cas $\lambda \geq 0$. Soit $n \geq 1$; alors, par théorème XX.7, il existe $\phi_1, \phi_2, \psi_1, \psi_2 \in \mathscr{E}(a,b)$ telles que $\phi_1 \leq f \leq \psi_1$, $\phi_2 \leq g \leq \psi_2$, $\psi_1 - \phi_1 \leq \frac{1}{n}$ et $\psi_2 - \phi_2 \leq \frac{1}{n}$. De fait, par croissance et linéarité de l'intégrale sur les fonctions en escalier, on a :

$$\begin{aligned}
\int_{[a,b]} (f + \lambda g) - \left(\int_{[a,b]} f + \lambda \int_{[a,b]} g\right) &\leq \int_{[a,b]} (\psi_1 + \lambda\psi_2) - \left(\int_{[a,b]} \phi_1 + \lambda \int_{[a,b]} \phi_2\right) \\
&= \int_{[a,b]} (\psi_1 - \phi_1) + \lambda \int_{[a,b]} (\psi_2 - \phi_2) \\
&\leq (b-a)\frac{2}{n}
\end{aligned}$$

et, de la même façon :

$$\begin{aligned}
\int_{[a,b]} (f + \lambda g) - \left(\int_{[a,b]} f + \lambda \int_{[a,b]} g\right) &\geq \int_{[a,b]} (\phi_1 + \lambda\phi_2) - \left(\int_{[a,b]} \psi_1 + \lambda \int_{[a,b]} \psi_2\right) \\
&\geq (a-b)\frac{2}{n}\,.
\end{aligned}$$

On obtient le résultat voulu en faisant tendre n vers l'infini via le théorème d'encadrement des limites (VII.11).

□

◇ Croissance, inégalité triangulaire

Proposition XX.10. Soit $f \in \mathscr{C}_{\mathrm{pm}}([a,b])$ une fonction **à valeurs positives**. Alors :

$$\int_a^b f(t)\,\mathrm{d}t \geq 0\,.$$

Démonstration. La fonction nulle est une fonction en escalier minorant f : elle appartient donc à $E_-(f)$. De fait :

$$\int_a^b f(t)\,\mathrm{d}t = \sup(E_+(f)) \geq \int_a^b 0\,\mathrm{d}t = 0\,.$$

□

✖ **Attention :** la réciproque est **fausse** : l'intégrale de $x \mapsto x$ entre -1 et 1 est positive sans que cette fonction ne le soit.

Corollaire XX.10.a. Soient $f, g \in \mathscr{C}_{\mathrm{pm}}([a,b])$. Alors :

$$(f \leq g) \Rightarrow \left(\int_{[a,b]} f \leq \int_{[a,b]} g\right)\,.$$

Démonstration. Appliquer la proposition *supra* à $g - f$. □

✌ **Remarque XX.9.** Cette proposition est apparente graphiquement : l'aire d'une fonction dont la courbe est située en permanence sous celle d'une autre risque de ne pas pouvoir excéder celle de son estimée collègue.

Proposition XX.11. Soit $f \in \mathscr{C}_{\mathrm{pm}}([a,b])$. Alors :

(i) $x \mapsto |f(x)| \in \mathscr{C}_{\mathrm{pm}}([a,b])$;

(ii)
$$\left|\int_a^b f(x)\,\mathrm{d}x\right| \leq \int_a^b |f(x)|\,\mathrm{d}x\,.$$

Démonstration. Identique à celle de l'inégalité triangulaire pour l'intégrale des fonctions en escalier. Pour le point(i), il suffit de remarquer que tout subdivision adaptée à f l'est aussi à $x \mapsto |f(x)|$. □

◇ **Relation de Chasles**

Proposition XX.12 (Chasles)**.** Soit $c \in [a, b]$ et soit $f : [a, b] \to \mathbb{R}$. Alors :

(i) $(f \in \mathscr{C}_{\text{pm}}([a, b])) \Leftrightarrow (f \in \mathscr{C}_{\text{pm}}([a, c] \cap \mathscr{C}_{\text{pm}}([c, b]))$;

(ii) dans ce cas,

$$\int_a^b f(t)\,\mathrm{d}t = \int_a^c f(t)\,\mathrm{d}t + \int_c^b f(t)\,\mathrm{d}t\,.$$

Démonstration. Il s'agit d'une abomination calculatoire que nous ferions mieux de laisser en paix. □

✌ **Remarque XX.10.** Il est possible, de la même façon et avec les **mêmes limites** que pour les fonctions en escalier, de généraliser l'intégrale ou cas où $a > b$.

◇ **Nullité**

Proposition XX.13 (Nullité de l'intégrale)**.** Soit $f : [a, b] \to \mathbb{R}$ une fonction **continue**, **positive** et telle que $\displaystyle\int_a^b f(t)\,\mathrm{d}t = 0$. Alors f est la fonction nulle.

✖ **Attention :** : ce théorème est bien entendu **faux** si on l'ampute d'une (ou plusieurs hypothèses) : l'indicatrice de $\mathbb{Z}$ sur $[0, 1]$ donne un contre–exemple discontinu, tandis que l'identité est d'intégrale nulle sur $[-1, 1]$ mais non nulle (elle n'est pas positive sur ce segment).

Démonstration. Supposons f non nulle : alors il existe $c \in [a, b]$ tel que $f(c) > 0$. Comme f est continue en c, il existe un voisinage $V \in \mathscr{V}(c)$ tel que $f > 0$ sur V ; de fait

$$\int_a^b f(t)\,\mathrm{d}t \geq \int_{[a,b]\cap V} f > 0$$

ce qui est absurde. □

✍ **Exercice XX.4.** Soit $P \in \mathbb{R}[x]$ tel que

$$\int_0^1 P^2(t)\,\mathrm{d}t = 0\,.$$

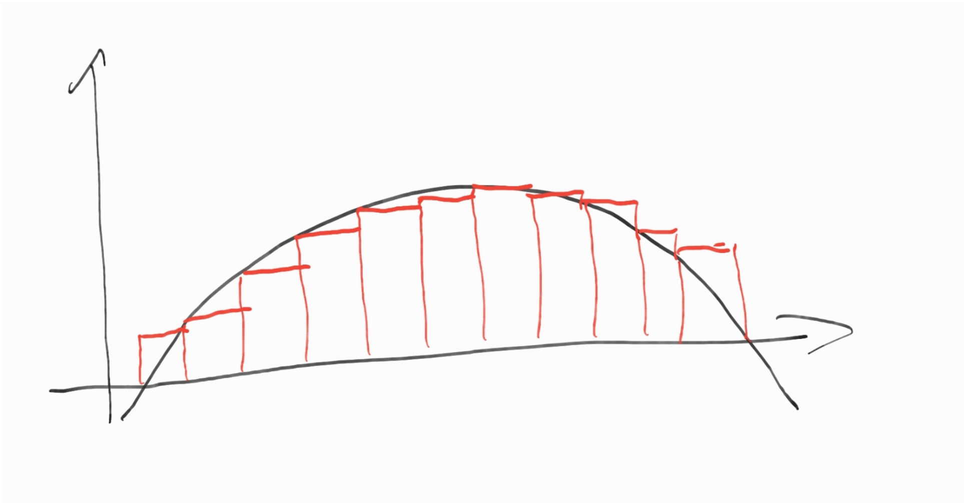
Montrer que $P = 0$.

d) Sommes de Riemann

Proposition XX.14. Soit $f \in \mathscr{C}_{\text{pm}}([a, b])$. Alors :

$$\frac{b-a}{n}\sum_{k=0}^{n-1} f\left(a + k\frac{b-a}{n}\right) \xrightarrow[n\to\infty]{} \int_a^b f(t)\,\mathrm{d}t\,.$$

✌ **Remarque XX.11.** Ce résultat est en fait une version séquentielle de la méthode des rectangles, appliquée aux subdivisions régulières $\sigma^n_{\mathscr{R}}(a,b)$.



Plus n sera "grand", plus nos rectangles seront "fins" et donc mieux l'intégrale sera approchée par la somme apparaissant dans la proposition, appelée **somme de Riemann**, du nom du mathématicien allemand Bernhard Riemann (1826—1866), que l'on ne présente plus.

Démonstration. **Nous nous limitons ici au cas où f est lipschitzienne de rapport $M > 0$.** Soit $n \geq 1$ et posons, pour $k \in [\![0,n]\!]$ $a_k = a + k\dfrac{b-a}{n}$; alors :

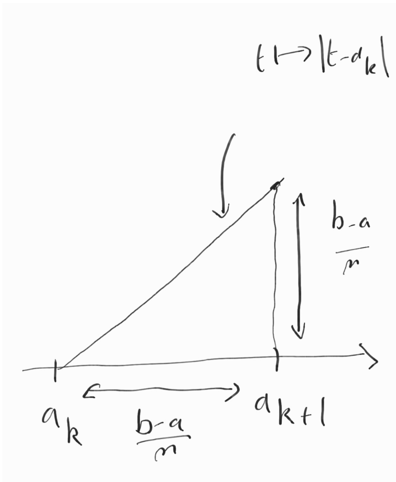
$$\begin{aligned}
\left|\int_a^b f(t)\,\mathrm{d}t - \frac{b-a}{n}\sum_{k=0}^{n-1} f\left(a+k\frac{b-a}{n}\right)\right| &= \left|\sum_{k=0}^{n-1}\int_{a_k}^{a_{k+1}} f(t)\,\mathrm{d}t - \frac{b-a}{n}\sum_{k=0}^{n-1} f(a_k)\right| \\
&= \left|\sum_{k=0}^{n-1}\int_{a_k}^{a_{k+1}} f(t)\,\mathrm{d}t - \frac{b-a}{n} f(a_k)\right| \\
&= \left|\sum_{k=0}^{n-1}\int_{a_k}^{a_{k+1}} f(t)\,\mathrm{d}t - (a_{k+1}-a_k) f(a_k)\right| \\
&= \left|\sum_{k=0}^{n-1}\int_{a_k}^{a_{k+1}} f(t)\,\mathrm{d}t - \int_{a_k}^{a_{k+1}} f(a_k)\,\mathrm{d}t\right| \\
&= \left|\sum_{k=0}^{n-1}\int_{a_k}^{a_{k+1}} f(t) - f(a_k)\,\mathrm{d}t\right| \\
&\leq \sum_{k=0}^{n-1}\left|\int_{a_k}^{a_{k+1}} f(t) - f(a_k)\,\mathrm{d}t\right| \\
&\leq \sum_{k=0}^{n-1}\int_{a_k}^{a_{k+1}} |f(t) - f(a_k)|\,\mathrm{d}t\,.
\end{aligned}$$

Or, comme f est M–lipschitzienne, on a :

$$\forall k \in [\![0, n-1]\!],\ \forall t \in [a_k, a_{k+1}]\ |f(t) - f(a_k)| \leq M|t - a_k|$$

ce qui entraîne que :

$$\sum_{k=0}^{n-1} \int_{a_k}^{a_{k+1}} |f(t) - f(a_k)| \, \mathrm{d}t \leq \sum_{k=0}^{n-1} \int_{a_k}^{a_{k+1}} M|t - a_k| \, \mathrm{d}t$$
$$= M \sum_{k=0}^{n-1} \int_{a_k}^{a_{k+1}} |t - a_k| \, \mathrm{d}t \, .$$



Or, l'intégrale de $t \mapsto |t - a_k|$ entre a_k et a_{k+1} correspond à l'aire du triangle rectangle de sommets $(a_k, 0)$, $(a_{k+1}, 0)$ et $(a_{k+1}, a_{k+1} - a_k)$. Un calcul d'aire nous livre alors que :

$$\int_{a_k}^{a_{k+1}} |t - a_k| \, \mathrm{d}t = \frac{1}{2} \left(\frac{b - a}{n} \right)^2$$

ce qui implique que :

$$M \sum_{k=0}^{n-1} \int_{a_k}^{a_{k+1}} |t - a_k| \, \mathrm{d}t = M \sum_{k=0}^{n-1} \frac{1}{2} \left(\frac{b - a}{n} \right)^2$$
$$= \frac{M}{2n} (b - a)^2$$
$$\xrightarrow[n \to \infty]{} 0$$

d'où le résultat.

□

➠ **Exemple XX.9.**

—
$$\frac{1}{n} \sum_{k=0}^{n-1} \cos\left(\frac{k}{n}\right) \xrightarrow[n \to \infty]{} \int_0^1 \cos(t) \, \mathrm{d}t \, ;$$

— si $n \geq 1$ alors :

$$n \sum_{k=0}^{n-1} \frac{1}{n^2 + k^2} = \frac{1}{n} \sum_{k=0}^{n-1} \frac{1}{1 + \left(\frac{k}{n}\right)^2}$$
$$\xrightarrow[n \to \infty]{} \int_0^1 \frac{1}{1 + t^2} \, \mathrm{d}t$$
$$= \frac{\pi}{4} \, .$$

3.‾ Primitives

On fixe dans ce paragraphe un intervalle I de $\mathbb{R}$ d'intérieur non vide.

On rappelle que si f est une fonction définie sur I, on appelle **primitive** de f toute fonction F **dérivable sur I** telle que $F' = f$. Nous reprenons (et démontrons) dans ce paragraphe plusieurs résultats évoqués au chapitre XIII.

a) Existence

Proposition XX.15. Soit $f \in \mathscr{C}^0(I)$ et soit $a \in I$. Alors la fonction

$$\begin{aligned} F : I &\to \mathbb{R} \\ x &\mapsto \int_a^x f(t)\,\mathrm{d}t \end{aligned}$$

est l'unique primitive de f telle que $F(a) = 0$.

✌ **Remarque XX.12.** La fonction F est alors automatiquement de classe $\mathscr{C}^1$.

Démonstration. La fonction F est bien définie car f est continue donc continue par morceaux. De plus si $x, y \in I$ sont tels que $x \neq y$ alors :

$$\begin{aligned} \frac{F(x) - F(y)}{x - y} &= \frac{1}{x-y}\left(\int_a^x f(t)\,\mathrm{d}t - \int_a^y f(t)\,\mathrm{d}t\right) \\ &= \frac{1}{x-y}\left(\int_a^x f(t)\,\mathrm{d}t + \int_y^a f(t)\,\mathrm{d}t\right) \\ &= \frac{1}{x-y}\int_y^x f(t)\,\mathrm{d}t\,. \end{aligned}$$

Nous savons en outre que f est continue en y ; ceci entraîne que :

$$\forall \varepsilon > 0,\ \exists\,\delta > 0, \forall t \in I\ (|t - y| \leq \delta) \Rightarrow (|f(t) - f(y)| \leq \varepsilon)\,.$$

De fait, si nous supposons $|x - y| \leq \delta$, on a :

$$\begin{aligned} \left|\frac{F(x) - F(y)}{x - y} - f(y)\right| &= \left|\frac{1}{x-y}\int_y^x f(t)\,\mathrm{d}t - f(y)\right| \\ &= \left|\frac{1}{x-y}\int_y^x f(t)\,\mathrm{d}t - \frac{1}{x-y}\int_y^x f(y)\,\mathrm{d}t\right| \\ &= \left|\frac{1}{x-y}\int_y^x f(t) - f(y)\,\mathrm{d}t\right| \\ &\leq \frac{1}{|x-y|}\int_{\underbrace{[x,y]}} |f(t) - f(y)|\,\mathrm{d}t \end{aligned}$$

où $\underbrace{[x,y]}$ désigne $[y,x]$ si $y<x$ et $[x,y]$ sinon. De fait, pour tout $t\in\underbrace{[x,y]}$, on a $|t-y|\leq\delta$ *ergo* :

$$\left|\frac{F(x)-F(y)}{x-y}-f(y)\right|\leq\frac{1}{|x-y|}\varepsilon|x-y|=\varepsilon$$

et donc

$$\frac{F(x)-F(y)}{x-y}\xrightarrow[x\to y]{}f(y)$$

d'où la dérivabilité de F sur I et le fait que $F'=f$.

Pour conclure, remarquons que si G est une primitive de f telle que $G(a)=0$ alors $F-G$ est constante car de dérivée nulle sur un intégrale et donc nulle car $(F-G)(a)=0$. □

Théorème XX.16 (Théorème fondamental du calcul intégral)**.**
Soit $f\in\mathscr{C}^0([a,b])$ et soit F une primitive de f sur $[a,b]$. Alors :

$$\int_a^b f(t)\,\mathrm{d}t=F(b)-F(a)\,.$$

Démonstration. La fonction $G:x\mapsto F(x)-F(a)$ est une primitive de f telle que $G(a)=0$ donc, d'après la proposition XX.15 on, pour tout $x\in[a,b]$:

$$F(x)-F(a)=\int_a^x f(t)\,\mathrm{d}t$$

d'où le résultat. □

✌ **Remarque XX.13.** Ce théorème a plusieurs conséquences fondamentales :

— les primitives de f sont exactement les fonctions de la forme

$$x\mapsto\int_a^x f(t)\,\mathrm{d}t+C$$

pour C parcourant $\mathbb{R}$;

— l'intégrale est une fonction continue de ses bornes, *i.e* pour tout $\alpha\in\mathbb{R}$ on a :

$$\int_a^x f(t)\,\mathrm{d}t\xrightarrow[x\to\alpha]{}\int_a^\alpha f(t)\,\mathrm{d}t\,;$$

— si f est de classe $\mathscr{C}^1$ sur $[a,b]$, on a :

$$f(b)-f(a)=\int_a^b f'(t)\,\mathrm{d}t\,.$$

b) Retour sur quelques méthodes de calcul intégral

Nous revenons brièvement dans ce paragraphe sur des résultats déjà démontrés au chapitre XIII, afin d'offrir à notre estimé lecteur le plaisir de s'immoler les rétines une fois de plus. Les remerciements sont superflus, je vous assure.

Proposition XX.17 (Intégration par parties)**.** Soient f et g deux fonctions **de classe** $\mathscr{C}^1$ sur I. Alors, pour tous $a, b \in I$:

$$\int_a^b f'(t)g(t)\,\mathrm{d}t = [f(t)g(t)]_a^b - \int_a^b f(t)g'(t)\,\mathrm{d}t\,,$$

avec

$$[f(t)g(t)]_a^b = f(b)g(b) - f(a)g(a)\,.$$

➠ **Exemple XX.10.** Soit $x \in [-1, 1]$; pour déterminer $\displaystyle\int_0^x \arcsin(t)\,\mathrm{d}t$ on applique l'IPP à $f : t \mapsto t$ et $g = \arcsin$, toutes deux de classe $\mathscr{C}^1$ sur $[0, x]$. On obtient :

$$\begin{aligned}\int_0^x \arcsin(t)\,\mathrm{d}t &= [t\arcsin(t)]_0^x - \int_0^x \frac{t}{\sqrt{1-t^2}}\,\mathrm{d}t\\ &= x\arcsin(x) - \sqrt{1-x^2} + 1\end{aligned}$$

car $t \mapsto \sqrt{1-t^2}$ est une primitive de $t \mapsto \dfrac{t}{\sqrt{1-t^2}}$.

Théorème XX.18 (Changement de variable)**.**
Soit $\varphi \in \mathscr{C}^1(I)$ et soit $f \in \mathscr{C}^0(\varphi(I))$. Alors, pour tous $a, b \in I$ on a :

$$\int_{\varphi(a)}^{\varphi(b)} f(x)\,\mathrm{d}x = \int_a^b f \circ \varphi(t)\varphi'(t)\,\mathrm{d}t\,.$$

Corollaire XX.18.a. Soit $fin\mathscr{C}^0([-a, a])$. Alors :

(i) si f est impaire, on a :

$$\int_{-a}^{a} f(t)\,\mathrm{d}t = 0\,.$$

(ii) si f est paire, on a :

$$\int_{-a}^{a} f(t)\,\mathrm{d}t = 2\int_0^a f(t)\,\mathrm{d}t\,.$$

Démonstration. On a, par changement de variable $u = -t$:

$$\int_0^a f(t)\,\mathrm{d}t = -\int_0^{-a} f(-u)\,\mathrm{d}u = -\int_{-a}^{0} f(u)\,\mathrm{d}u$$

et donc
$$\int_{-a}^{a} f(t)\,\mathrm{d}t = \int_{0}^{a} f(t)\,\mathrm{d}t + \int_{-a}^{0} f(t)\,\mathrm{d}t = 0\,.$$
Dans le cas où f est paire, un raisonnement similaire livre :
$$\int_{-a}^{a} f(t)\,\mathrm{d}t = 2\int_{0}^{a} f(t)\,\mathrm{d}t\,.$$

□

Corollaire XX.18.b. Soit $f \in \mathscr{C}^0(\mathbb{R})$ une fonction T–périodique (avec $T > 0$). Alors :
$$\forall a \in \mathbb{R},\qquad \int_{a}^{a+T} f(t)\,\mathrm{d}t = \int_{0}^{T} f(t)\,\mathrm{d}t\,.$$

Démonstration. Il convient dans un premier temps de remarquer que :
$$\forall a \in \mathbb{R},\qquad \int_{0}^{a} f(t)\,\mathrm{d}t = \int_{T}^{a+T} f(u)\,\mathrm{d}u$$
par changement de variable $u = t + T$. De fait, on a par la formule de "Chasles" :
$$\begin{aligned}\int_{0}^{T} f(t)\,\mathrm{d}t &= \int_{0}^{a} f(t)\,\mathrm{d}t + \int_{a}^{a+T} f(t)\,\mathrm{d}t + \int_{a+T}^{T} f(t)\,\mathrm{d}t\\ &= -\int_{a+T}^{T} f(t)\,\mathrm{d}t + \int_{a}^{a+T} f(t)\,\mathrm{d}t + \int_{a+T}^{T} f(t)\,\mathrm{d}t\\ &= \int_{a}^{a+T} f(t)\,\mathrm{d}t\,.\end{aligned}$$

□

4.– Formules de Taylor

On fixe dans ce paragraphe un intervalle I d'intérieur non vide.

Nous avons rencontré par le passé deux formules de Taylor : celle concernant les polynômes (proposition XIV.17) et la formule de Taylor–Young (théorème XVII.9). Ces deux formules avaient pour point commun l'expression de la valeur d'une fonction en un point à partir du polynôme de Taylor de f en un point a de son ensemble de définition, *i.e*
$$T_n = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!} X^k$$
et d'un éventuel reste négligeable (voire nul).

Nous donnons dans ce paragraphe une nouvelle formule de Taylor avec une expression explicite de ce reste, et étudions certaines conséquences d'un tel résultat.

a) Formule de Taylor avec reste intégral

Proposition XX.19. Soit $n \in \mathbb{N}$, $a, b \in I$ et $f \in \mathscr{C}^{n+1}(I)$. Alors :

$$f(b) = \sum_{k=0}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a) + \int_a^b \frac{(b-t)^n}{n!} f^{(n+1)}(t)\, \mathrm{d}t\,.$$

Démonstration. On le fait par récurrence (joie !) sur $n \geq 0$.

— Le cas $n = 0$ est trivial étant donné que l'on a :

$$f(b) = f(a) + \int_a^b f'(t)\, \mathrm{d}t$$

d'après le théorème XX.16.

— Si on suppose la propriété vraie au rang n et que $f \in \mathscr{C}^{n+2}([a, b])$ alors on a, comme f est automatiquement de classe $\mathscr{C}^{n+1}$ sur ce même intervalle :

$$f(b) = \sum_{k=0}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a) + \int_a^b \frac{(b-t)^n}{n!} f^{(n+1)}(t)\, \mathrm{d}t\,.$$

par hypothèse de récurrence. Les fonctions $f^{(n+1)}$ et $u : t \mapsto -\dfrac{(b-t)^{n+1}}{(n+1)!}$ sont de classes $\mathscr{C}^1$ sur I avec

$$\forall t \in I,\ u'(t) = \frac{(n+1)(b-t)^n}{(n+1)!} = \frac{(b-t)^n}{n!}$$

et donc, par intégration par parties (proposition XX.17) :

$$\begin{aligned}
\int_a^b \frac{(b-t)^n}{n!} f^{(n+1)}(t)\, \mathrm{d}t &= \left[-\frac{(b-t)^{n+1}}{(n+1)!} f^{(n+1)}(t) \right]_a^b - \int_a^b -\frac{(b-t)^{n+1}}{(n+1)!} f^{(n+2)}(t)\, \mathrm{d}t \\
&= \frac{(b-a)^{n+1}}{(n+1)!} f^{(n+1)}(a) + \int_a^b \frac{(b-t)^{n+1}}{(n+1)!} f^{(n+2)}(t)\, \mathrm{d}t\,.
\end{aligned}$$

En réinjectant, on obtient

$$\begin{aligned}
f(b) &= \sum_{k=0}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a) + \frac{(b-a)^{n+1}}{(n+1)!} f^{(n+1)}(a) + \int_a^b \frac{(b-t)^{n+1}}{(n+1)!} f^{(n+2)}(t)\, \mathrm{d}t \\
&= \sum_{k=0}^{n+1} \frac{(b-a)^k}{k!} f^{(k)}(a) + \int_a^b \frac{(b-t)^{n+1}}{(n+1)!} f^{(n+2)}(t)\, \mathrm{d}t
\end{aligned}$$

d'où le résultat.

□

Exemple XX.11. Si $x \in \mathbb{R}$ et $n \geq 0$, on a :

$$\begin{aligned}
e^x &= \sum_{k=0}^{n} \frac{x^k}{k!} \exp^{(k)}(0) + \int_0^x \frac{(x-t)^n}{n!} \exp^{(n+1)}(t)\, \mathrm{d}t \\
&= \sum_{k=0}^{n} \frac{x^k}{k!} + \int_0^x \frac{(x-t)^n}{n!} e^t\, \mathrm{d}t
\end{aligned}$$

l'intégrale pouvant se calculer par IPP (*cf.* chapitre XIII).

b) Inégalité de Taylor–Lagrange

Proposition XX.20. Soit $n \in \mathbb{N}$, $a, b \in I$ et $f \in \mathscr{C}^{n+1}(I)$. Alors :

$$f(b) = \sum_{k=0}^{n} \frac{(b-a)^k}{k!} f^{(k)}(a) + R_n$$

avec

$$|R_n| \leq \frac{|b-a|^{n+1}}{(n+1)!} \max_{\underbrace{[\,a, b\,]}} |f^{(n+1)}|$$

où $\underbrace{[\,a, b\,]}$ désigne le segment $[a, b]$ si $a \leq b$ et $[b, a]$ sinon.

Démonstration. D'après la formule de Taylor avec reste intégral (proposition XX.19), on a :

$$\begin{aligned}
|R_n| &= \left| \int_a^b \frac{(b-t)^n}{n!} f^{(n+1)}(t)\,\mathrm{d}t \right| \\
&\leq \int_a^b \left| \frac{(b-t)^n}{n!} f^{(n+1)}(t) \right| \mathrm{d}t \\
&\leq \int_a^b \left| \frac{(b-t)^n}{n!} \right| \sup_{\underbrace{[\,a, b\,]}} |f^{(n+1)}|\,\mathrm{d}t \\
&= \sup_{\underbrace{[\,a, b\,]}} |f^{(n+1)}| \int_a^b \left| \frac{(b-t)^n}{n!} \right| \mathrm{d}t \\
&= \sup_{\underbrace{[\,a, b\,]}} |f^{(n+1)}| \frac{|b-a|^{n+1}}{(n+1)!}
\end{aligned}$$

d'où le résultat, la borne supérieure étant un maximum car $f^{(n+1)}$ est continue sur le segment concerné. □

✌ **Remarque XX.14.**

➠ **Exemple XX.12.** En reprenant l'exemple précédent, nous avons, pour tout $n \in \mathbb{N}$ et $x \in \mathbb{R}$:

$$\left| e^x - \sum_{k=0}^{n} \frac{x^k}{k!} \right| \leq \frac{|x|^{n+1}}{(n+1)!} \sup_{\underbrace{[\,0, x\,]}} \exp$$

et donc on a, comme $\dfrac{|x|^{n+1}}{(n+1)!} \xrightarrow[n \to \infty]{} 0$, que :

$$\sum_{k=0}^{n} \frac{x^k}{k!} \xrightarrow[n \to \infty]{} e^x .$$

5.– Brève extension aux fonctions à valeurs complexes

Si $a, b \in \mathbb{R}$ sont tels que $a < b$ et $f : [a,b] \to \mathbb{C}$ est une fonction, on dira que f est continue par morceaux si et seulement si sa partie réelle et sa partie imaginaire le sont. De cette façon, on peut poser :

$$\int_a^b f(t)\,\mathrm{d}t = \int_a^b \mathrm{Re}(f(t))\,\mathrm{d}t + i\int_a^b \mathrm{Im}(f(t))\,\mathrm{d}t\,.$$

Toutes les propriétés vues dans ce chapitre se généralisent aux intégrales de fonctions continue par morceaux à valeurs complexes **sauf la croissance**. L'inégalité triangulaire reste vérifiée, quitte à remplacer la valeur absolue par le module.

Chapitre XXI

Algèbre linéaire matricielle

On fixe dans tout ce chapitre un corps $\mathbb{K}$ égal à $\mathbb{R}$ ou $\mathbb{C}$.

1.– Matrice(s) d'une application linéaire

a) Matrices et vecteurs

Soit E un $\mathbb{K}$–e.v de dimension finie de dimension n et soit $\mathscr{B} = (e_1, \ldots, e_n)$ une base de E. Fixons $x \in E$; alors il existe une unique famille $(x_1, \ldots, x_n)$ de scalaires telle que :

$$x = \sum_{i=1}^{n} x_i e_i \, .$$

Dans ces conditions, on appelle **matrice de x dans la base $\mathscr{B}$** la matrice

$$\mathrm{mat}_{\mathscr{B}}(x) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathscr{M}_{n,1}(\mathbb{K}) \, .$$

➠ **Exemple XXI.1.** Dans la base $\mathscr{B} = ((1,0),(1,1))$ de $\mathbb{R}^2$, on a, pour tous $x, y \in \mathbb{R}$:

$$(x,y) = (x-y) \cdot (1,0) + y \cdot (1,1)$$

et donc

$$\mathrm{mat}_{\mathscr{B}}((x,y)) = \begin{pmatrix} x-y \\ y \end{pmatrix} \, .$$

✌ **Remarque XXI.1.** On peut relier cette définition aux formes linéaires coordonnées en remarquant que :

$$\mathrm{mat}_{\mathscr{B}}(x) = \begin{pmatrix} e_1^*(x) \\ \vdots \\ e_n^*(x) \end{pmatrix} \, .$$

Proposition XXI.1. Soit E un $\mathbb{K}$–e.v de dimension finie de dimension $n \in \mathbb{N}$ et soit $\mathscr{B}$ une base de E. Alors l'application

$$\begin{aligned} \mathrm{mat}_{\mathscr{B}} : E &\to \mathscr{M}_{n,1}(\mathbb{K}) \\ x &\mapsto \mathrm{mat}_{\mathscr{B}}(x) \end{aligned}$$

est un isomorphisme.

Démonstration. La linéarité ne présente aucune difficulté. Notons ensuite que :

$$x \in \mathrm{Ker}(\mathrm{mat}_{\mathscr{B}}) \Leftrightarrow \forall i \in [\![1,n]\!],\ x_i = 0$$

ce qui entraîne l'injectivité. On conclut par égalité dimensionnelle. □

On définit de la même façon la matrice d'une famille de vecteurs $\mathscr{F} = (u_1, \ldots, u_k)$ dans une base $\mathscr{B}$ comme la matrice $\mathrm{mat}_{\mathscr{B}}(\mathscr{F}) \in \mathscr{M}_{n,k}(\mathbb{K})$ dont les colonnes sont les matrices des u_i dans la base $\mathscr{B}$.

➠ **Exemple XXI.2.** La matrice dans la base canonique de $\mathbb{R}^3$ de la famille $(1,0,1),(0,2,3))$ est

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

✌ **Remarque XXI.2.** On vérifie facilement que $\mathrm{mat}_{\mathscr{B}}(\mathscr{B}) = I_n$.

b) Matrices et applications linéaires

Définition XXI.1. Soit E (resp. F) un $\mathbb{K}$–e.v de dimension finie de dimension m (resp. n) et soit $\mathscr{B}$ (resp. $\mathscr{B}'$) une base de E (resp. de F). Alors, on appelle **matrice** d'une application linéaire $f \in \mathscr{L}(E,F)$ **dans les bases $\mathscr{B}$ et $\mathscr{B}'$** la matrice

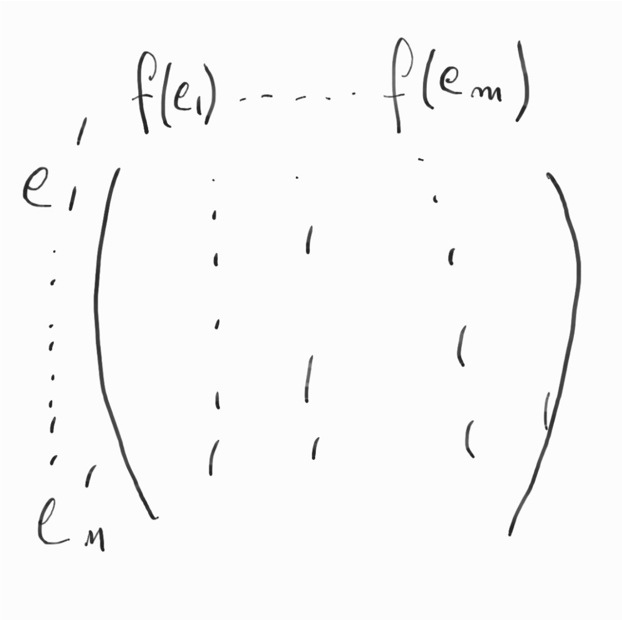
$$\mathrm{mat}_{\mathscr{B},\mathscr{B}'}(f) = \mathrm{mat}_{\mathscr{B}'}(f(\mathscr{B})) \in \mathscr{M}_{n,m}(\mathbb{K}) .$$

Notation. Si $f \in \mathscr{L}(E)$ et que $\mathscr{B} = \mathscr{B}'$, on notera $\mathrm{mat}_{\mathscr{B}}(f)$.

Concrètement, cela signifie que les colonnes de cette matrice sont les matrices des images par f des vecteurs de $\mathscr{B}$ dans la base $\mathscr{B}'$. Si on pose $\mathscr{B} = (e_1, \ldots, e_m)$ et $\mathscr{B}' = (e'_1, \ldots, e'_n)$, alors le coefficient en position (i,j) de la matrice $\mathrm{mat}_{\mathscr{B},\mathscr{B}'}(f)$ sera la coordonnée selon e'_i du vecteur $f(e_j)$; i.e en notant $m_{i,j}$ ces coefficients on aura :

$$\forall j \in [\![1,m]\!],\ f(e_j) = \sum_{i=1}^{n} m_{i,j} e'_i .$$

Ceci signifie que la matrice aura donc globalement la tronche suivante :



➠ **Exemple XXI.3.** On considère l'application suivante :

$$\begin{aligned} f : \mathbb{R}^2 &\to \mathbb{R}^3 \\ (x, y) &\mapsto (2x + y, x + y, 3y) . \end{aligned}$$

Il est clair que $f \in \mathscr{L}(\mathbb{R}^2, \mathbb{R}^3)$. Posons $\mathscr{B} = ((1, 0), (1, 1))$ et $\mathscr{B}' = ((1, 0, 0), (0, 1, 0), (0, 1, 1))$: il s'agit la de bases respectives de $\mathbb{R}^2$ et $\mathbb{R}^3$, avec :

$$f((1, 0)) = (2, 1, 0) = 2 \cdot (1, 0, 0) + 1 \cdot (0, 1, 0) + 0 \cdot (0, 1, 1)$$

et

$$f((1, 1)) = (3, 2, 3) = 3 \cdot (1, 0, 0) - 1 \cdot (0, 1, 0) + 3 \cdot (0, 1, 1) .$$

De fait, on a :

$$\mathrm{mat}_{\mathscr{B},\mathscr{B}'}(f) = \begin{pmatrix} 2 & 3 \\ 1 & -1 \\ 0 & 3 \end{pmatrix} .$$

✌ **Remarque XXI.3.** Si E est un $\mathbb{K}$–e.v de dimension finie de dimension n et que $\mathscr{B}$ est une base de E, alors $\mathrm{mat}_{\mathscr{B}}(\mathrm{id}_E) = I_n$.

✖ **Attention :** l'application identité ne donne pas toujours naissance à la matrice identité ; par exemple, si $\mathscr{B} = ((1, 0), (1, 1))$ et $\mathscr{B}' = ((1, 0), (0, 1))$ on a :

$$\mathrm{mat}_{\mathscr{B},\mathscr{B}'}(\mathrm{id}_{\mathbb{R}^2}) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} .$$

Proposition XXI.2. Soit E (resp. F) un $\mathbb{K}$–e.v de dimension finie de dimension m (resp. n) et soit $\mathscr{B} = (e_1, \dots, e_m)$ (resp. $\mathscr{B}' = (e'_1, \dots, e'_n)$) une base de E (resp. de F). Soit $f \in \mathscr{L}(E)$ et soit $M = (m_{i,j})_{i,j}$ sa matrice dans les bases $\mathscr{B}$ et $\mathscr{B}'$. Alors, si $x = \sum_{k=1}^{m} x_k e_k \in E$, on a :

$$f(x) = \sum_{i=1}^{n} m_{i,j} x_j e'_i .$$

Proposition XXI.3. Soient E, F deux $\mathbb{K}$–e.v de dimension finie de dimensions respectives m et n. Soient $\mathscr{B}$ et $\mathscr{B}'$ des bases respectives de E et F. Alors l'application

$$\varphi : \mathscr{L}(E, F) \to \mathscr{M}_{n,m}(\mathbb{K})$$
$$f \mapsto \mathrm{mat}_{\mathscr{B},\mathscr{B}'}(f)$$

est un isomorphisme.

Démonstration. La linéarité se démontre par un calcul rapide. De plus, cette application est bijective car toute application linéaire est totalement déterminée par la donnée de l'image d'une base de son ensemble de départ. □

✌ **Remarque XXI.4.** Soit $A \in \mathscr{M}_{n,m}(\mathbb{K})$; alors d'après la proposition *supra*, il existe une unique application $f \in \mathscr{L}(\mathbb{K}^m, \mathbb{K}^n)$ telle que A soit la matrice de f dans les bases canoniques respectives de $\mathbb{K}^m$ et $\mathbb{K}^n$. Il nous est donc possible de poser $\mathrm{Ker}(A) = \mathrm{Ker}(f)$, $\mathrm{Im}(A) = \mathrm{Im}(f)$ et $\mathrm{rg}(A) = \mathrm{rg}(f)$. Ce paradigme est régulièrement utilisé aux concours pour identifier matrices et applications linéaires : f est alors appelée **application linéaire canoniquement associée à la matrice** A.

Dans ces conditions, il est clair que les colonnes de A forment une famille génératrice de l'image de f et que ses lignes donnent un système d'équations du noyau (se référer à la vision matricielle d'un système linéaire vue au chapitre XII.

On notera également que, quitte à identifier les vecteurs à des matrices colonnes, on a, pour tout $x \in \mathbb{K}^m$:

$$f(x) = Ax\,.$$

✍ **Exercice XXI.1.** Déterminer l'endomorphisme canoniquement associé à la matrice

$$M = \begin{pmatrix} 1 & 0 & -1 & 2 \\ 0 & 2 & 2 & 2 \\ 1 & 2 & 3 & 4 \\ -1 & -2 & -3 & 0 \end{pmatrix},$$

ainsi que son image et son noyau.

c) Composition et produit

Donnons nous trois $\mathbb{K}$–e.v de dimension finie E, F et G, de dimensions respectives p, q et r et munis respectivement de bases $\mathscr{B} = (e_1, \ldots, e_p)$, $\mathscr{B}' = (e'_1, \ldots, e'_q)$ et $\mathscr{B}'' = (e''_1, \ldots, e''_r)$. Fixons ensuite $u \in \mathscr{L}(E, F)$ et $v \in \mathscr{L}(F, G)$ et posons $A = (a_{i,j})_{i,j} = \mathrm{mat}_{\mathscr{B}',\mathscr{B}''}(v)$ ainsi que $B = (b_{i,j})_{i,j} = \mathrm{mat}_{\mathscr{B},\mathscr{B}'}(u)$. On a alors, pour tout $j \in [\![1, p]\!]$:

$$\begin{aligned} v \circ u(e_j) &= v\left(\sum_{k=1}^{q} b_{k,j} e'_k\right) \\ &= \sum_{k=1}^{q} b_{k,j} v(e'_k) \\ &= \sum_{k=1}^{q} b_{k,j} \sum_{i=1}^{r} a_{i,k} e''_i \\ &= \sum_{i=1}^{r} \left(\sum_{k=1}^{q} a_{i,k} b_{k,j}\right) e''_i \,. \end{aligned}$$

Ceci signifie que la matrice de $v \circ u$ dans les bases $\mathscr{B}$ et $\mathscr{B}''$ admet pour coefficient en position (i, j), pour $i \in [\![1, r]\!]$ et $j \in [\![1, p]\!]$:

$$\sum_{k=1}^{q} a_{i,k} b_{k,j} \,,$$

et donc que :

$$\mathrm{mat}_{\mathscr{B},\mathscr{B}''}(v \circ u) = AB \,.$$

✌ **Remarque XXI.5.** Il découle de notre abominable laïus calculatoire que le produit matriciel présente de fortes similitudes avec la composition des applications linéaires. Plus précisément, et en conservant les notations *supra*, nous avons :

(i) $\mathrm{mat}_{\mathscr{B},\mathscr{B}''}(v \circ u) = \mathrm{mat}_{\mathscr{B}',\mathscr{B}''}(v) \times \mathrm{mat}_{\mathscr{B},\mathscr{B}'}(u)$;

(ii) $\forall x \in E$, $\mathrm{mat}_{\mathscr{B}'}(u(x)) = \mathrm{mat}_{\mathscr{B},\mathscr{B}'}(u) \times \mathrm{mat}_{\mathscr{B}}(x)$.

Ceci nous permet de retrouver que le produit matriciel est associatif et bilinéaire. Notons que le résultat du point (i) ne dépend pas du choix de la base $\mathscr{B}'$ et que le point (ii) sera **très** utile pour déterminer l'endomorphisme canoniquement associé à une matrice.

Proposition XXI.4. Soit $n \geq 0$. Alors $(\mathscr{M}_n(\mathbb{K}), +, \times, \cdot)$ est une algèbre. De plus, pour tout $\mathbb{K}$–e.v de dimension finie E de dimension n, l'algèbre $(\mathscr{L}(E), +, \circ, \cdot)$ est isomorphe (en tant qu'anneau et espace vectoriel) à $\mathscr{M}_n(\mathbb{K})$.

Démonstration. Il s'agit d'une synthèse des propriétés évoquées précédemment dans ce chapitre. Notons que le neutre pour le produit matriciel dans $\mathscr{M}_n(\mathbb{K})$ est la matrice identité I_n. □

✖ **Attention :** cette algèbre n'est évidemment **pas** commutative dés que $n \geq 2$: en effet

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

et

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \,.$$

d) Inversibilité

Proposition XXI.5. Soit $A \in \mathscr{M}_n(\mathbb{K})$; alors est inversible pour le produit matriciel à gauche si et seulement si elle est inversible à droite.

Démonstration. Soit $f \in \mathscr{L}(\mathbb{K}^n)$ l'application linéaire canoniquement associée à A. Alors, A est inversible à gauche si et seulement si il existe une matrice $B \in \mathscr{M}_n(\mathbb{K})$ telle que $BA = I_n$. Ceci signifie que si $g \in \mathscr{L}(\mathbb{K}^n)$ est l'application linéaire canoniquement associée à B on a $g \circ f = \mathrm{id}_{\mathbb{K}^n}$: f est donc injective et donc, par égalité de dimensions, surjective. Il en découle que $f \circ g = \mathrm{id}_{\mathbb{K}^n}$, *i.e* $AB = I_n$, d'où le résultat. □

Remarque XXI.6. Le groupe $(GL_n(\mathbb{K}), \times)$ est isomorphe au groupe $(GL(E), \circ)$ via restriction de l'isomorphisme entre $\mathscr{L}(E)$ et $\mathscr{M}_n(\mathbb{K})$. En particulier, si $f \in GL(E)$ et que $\mathscr{B}$ est une base de E on a $\mathrm{mat}_{\mathscr{B}}(f^{-1}) = \mathrm{mat}_{\mathscr{B}}(f)^{-1}$.

Exemple XXI.4. Soient $a, b, c, d \in \mathbb{R}$; alors on a vu dans le chapitre XVIII que l'application linéaire canoniquement associée à $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ étant dans $GL(E)$ si et seulement si $ad - bc \neq 0$. Il en va donc de même pour l'inversibilité de A.

Proposition XXI.6. Soit $A \in \mathscr{M}_n(\mathbb{K})$. Alors les propositions suivantes sont équivalentes :

(i) A est inversible ;

(ii) $\mathrm{Ker}(A) = \{0\}$;

(iii) les colonnes de A forment une base de $\mathbb{K}^n$.

Démonstration. Ceci découle de la proposition XIX.15. □

Remarque XXI.7. Ce résultat nous permet de retrouver la proposition XII.6 sur l'inversibilité des matrices triangulaires.

2.– Changements de base

a) Matrices de passage

On fixe dans ce paragraphe un $\mathbb{K}$–e.v de dimension finie E de dimension $n \in \mathbb{N}$.

Définition XXI.2. Soient $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E. On appelle **matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$** la matrice

$$P_{\mathscr{B}}^{\mathscr{B}'} = \mathrm{mat}_{\mathscr{B}}(\mathscr{B}')\,.$$

Remarque XXI.8. On a donc $P_{\mathscr{B}}^{\mathscr{B}'} = \mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\mathrm{id}_E)$.

Exemple XXI.5. La matrice de passage de $((1,0),(0,1))$ à $((1,0),(1,1))$ est

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

et celle de $((1,0),(1,1))$ à $((1,0),(0,1))$ est

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

Proposition XXI.7. Soient $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E ; alors :

(i) $P_{\mathscr{B}}^{\mathscr{B}'} \in GL_n(\mathbb{K})$;

(ii) $(P_{\mathscr{B}}^{\mathscr{B}'})^{-1} = P_{\mathscr{B}'}^{\mathscr{B}}$.

Démonstration. Nous savons que, d'après le lien produit–composition vu précédemment :

$$\begin{aligned} P_{\mathscr{B}}^{\mathscr{B}'} P_{\mathscr{B}'}^{\mathscr{B}} &= \mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\mathrm{id}_E)\mathrm{mat}_{\mathscr{B},\mathscr{B}'}(\mathrm{id}_E) \\ &= \mathrm{mat}_{\mathscr{B}}(\mathrm{id}_E \circ \mathrm{id}_E) \\ &= \mathrm{mat}_{\mathscr{B}}(\mathrm{id}_E) \\ &= I_n \end{aligned}$$

d'où le résultat. □

L'usage principal à ce stade des matrices de passage sera, pour nous, le **changement de base**, *i.e* le procédé permettant de passer des coordonnées ou de la matrice d'un vecteur ou d'une application linéaire dans la base $\mathscr{B}'$ à leur homologue dans $\mathscr{B}$. Ceci générera de nombreux calculs hilarants.

Proposition XXI.8. Soient $\mathscr{B}$ et $\mathscr{B}'$ deux bases de E et soit $x \in E$. Alors :

$$\mathrm{mat}_{\mathscr{B}}(x) = P_{\mathscr{B}}^{\mathscr{B}'} \mathrm{mat}_{\mathscr{B}'}(x).$$

Démonstration. Toujours d'après les propriétés élémentaires du produit matriciel, nous avons :

$$\begin{aligned} \mathrm{mat}_{\mathscr{B}}(x) &= \mathrm{mat}_{\mathscr{B}}(\mathrm{id}_E(x)) \\ &= \mathrm{mat}_{\mathscr{B}',\mathscr{B}}(\mathrm{id}_E)\mathrm{mat}_{\mathscr{B}'}(x) \\ &= P_{\mathscr{B}}^{\mathscr{B}'} \mathrm{mat}_{\mathscr{B}'}(x) \end{aligned}$$

d'où le résultat. □

Exemple XXI.6. Pour obtenir les coordonnées d'un vecteur $(x,y) \in \mathbb{R}^2$ dans la base $((1,0),(1,1))$ il nous suffit de calculer

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x-y \\ y \end{pmatrix}.$$

Proposition XXI.9. Soient E et F deux $\mathbb{K}$–e.v de dimension finie ; soient $\mathscr{B}_1$, $\mathscr{B}'_1$ deux bases de E et $\mathscr{B}_2$, $\mathscr{B}'_2$ deux bases de F. Alors, pour tout $f \in \mathscr{L}(E,F)$ on a :

$$\operatorname{mat}_{\mathscr{B}'_1,\mathscr{B}'_2}(f) = P_{\mathscr{B}'_2}^{\mathscr{B}_2} \operatorname{mat}_{\mathscr{B}_1,\mathscr{B}_2}(f) P_{\mathscr{B}_1}^{\mathscr{B}'_1}\,.$$

Démonstration. Commençons par noter que $f = \operatorname{id}_F \circ f \circ \operatorname{id}_E$; ainsi, on a :

$$\begin{aligned}\operatorname{mat}_{\mathscr{B}'_1,\mathscr{B}'_2}(f) =& \operatorname{mat}_{\mathscr{B}'_1,\mathscr{B}'_2}(\operatorname{id}_F \circ f \circ \operatorname{id}_E)\\ &= \operatorname{mat}_{\mathscr{B}_2,\mathscr{B}'_2}(\operatorname{id}_F)\operatorname{mat}_{\mathscr{B}_1,\mathscr{B}_2}(f)\operatorname{mat}_{\mathscr{B}'_1,\mathscr{B}_1}(\operatorname{id}_E)\\ &= P_{\mathscr{B}'_2}^{\mathscr{B}_2}\operatorname{mat}_{\mathscr{B}_1,\mathscr{B}_2}(f)P_{\mathscr{B}_1}^{\mathscr{B}'_1}\end{aligned}$$

d'où, pour changer, le résultat. □

✌ **Remarque XXI.9.** Si $E = F$, $\mathscr{B}_1 = \mathscr{B}_2$ et $\mathscr{B}'_1 = \mathscr{B}'_2$, on a alors, en posant $P = P_{\mathscr{B}_1}^{\mathscr{B}'_1}$:

$$\operatorname{mat}_{\mathscr{B}'_1}(f) = P^{-1}\operatorname{mat}_{\mathscr{B}_1}(f)P\,.$$

✍ **Exercice XXI.2.** Soit E un espace vectoriel de dimension 3 et soit f l'endomorphisme de E dont la matrice dans une base $\mathscr{B} = (e_1, e_2, e_3)$ de E est

$$A = \begin{pmatrix} 15 & -11 & 5 \\ 20 & -15 & 8 \\ 8 & -7 & 6 \end{pmatrix}.$$

Montrer que les vecteurs

$$e'_1 = 2e_1 + 3e_2 + e_3, \quad e'_2 = 3e_1 + 4e_2 + e_3, \quad e'_3 = e_1 + 2e_2 + 2e_3$$

forment une base $\mathscr{B}'$ de E et calculer la matrice de f dans celle–ci.

➥ **Correction :** *On vérifie rapidement que $\mathscr{B}'$ est libre et de cardinal 3 : il s'agit bien d'une base. Soit $P = P_{\mathscr{B}}^{\mathscr{B}'}$; alors :*

$$P = \begin{pmatrix} 2 & 3 & 1 \\ 3 & 4 & 2 \\ 1 & 1 & 2 \end{pmatrix}$$

Trouver P^{-1} est relativement rapide et donne :

$$P^{-1} = \begin{pmatrix} -6 & 5 & -2 \\ 4 & -3 & 1 \\ 1 & -1 & 1 \end{pmatrix}$$

Ne reste qu'à calculer

$$B = P^{-1}AP = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

qui est la matrice de f dans la base $\mathscr{B}'$.

b) Rang d'une matrice

Définition XXI.3. Soit $A \in \mathscr{M}_{n,m}(\mathbb{K})$. On appelle **rang** de A le rang de la famille de ses vecteurs colonnes.

Notation. $\mathrm{rg}(A)$

Remarque XXI.10. Il s'agit *de facto* également du rang de l'application linéaire canoniquement associée à A. Il en découle qu'une matrice de $\mathscr{M}_n(\mathbb{K})$ est inversible si et seulement si son rang est égal à n.

Exemple XXI.7. $\mathrm{rg}(I_n) = n$, $\mathrm{rg}\left(\begin{pmatrix} 1 & 2 \\ 4 & 8 \end{pmatrix}\right) = 1$.

Proposition/définition XXI.4 (Matrice canonique d'une application linéaire)**.** Soient E et F deux $\mathbb{K}$–e.v de dimension finie de dimensions respectives m et n. Soit $f \in \mathscr{L}(E, F)$ de rang $r \geq 0$; alors il existe une base $\mathscr{B}$ de E et une base $\mathscr{B}'$ de F telles que :

$$\mathrm{mat}_{\mathscr{B},\mathscr{B}'}(f) = J_r$$

où J_r est la **matrice canonique de rang** r donnée par :

$$J_r = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right).$$

✖ **Attention :** la matrice J_r dépend de n et m ...

Démonstration. D'après le théorème du rang, nous savons que $\dim(\mathrm{Ker}(f)) = m - r$; fixons nous donc un supplémentaire G de ce dernier et une base $\mathscr{B} = (e_1, \ldots, e_m)$ de E adaptée à la décomposition $E = G \oplus \mathrm{Ker}(f)$. La famille $\mathscr{F} = (e_1, \ldots, e_r)$ est donc libre et engendre G. De fait, elle n'intersecte pas $\mathrm{Ker}(f)$, ce qui entraîne que $f(\mathscr{F})$ est libre car $f_{|G}$ est injective.

La famille $f(\mathscr{F})$ étant libre dans F, on peut la prolonger en une base de $\mathscr{B}'$ de F. Il est alors aisé de vérifier que $\mathrm{mat}_{\mathscr{B},\mathscr{B}'}(f) = J_r$. □

c) Matrices équivalentes

Définition XXI.5. Deux matrices $A, B \in \mathscr{M}_{n,m}(\mathbb{K})$ sont dites **équivalentes** si il existe $P \in GL_n(\mathbb{K})$ et $Q \in GL_m(\mathbb{K})$ tel que :

$$B = P^{-1}AQ\,.$$

Exemple XXI.8. Soient $\mathscr{B}_1, \mathscr{B}_1'$ deux bases d'un $\mathbb{K}$–e.v de dimension finie E et $\mathscr{B}_2, \mathscr{B}_2'$ deux bases d'un $\mathbb{K}$–e.v de dimension finie F. Alors, pour tout $f \in \mathscr{L}(E, F)$ on a :

$$\mathrm{mat}_{\mathscr{B}_1',\mathscr{B}_2'}(f) = (P_{\mathscr{B}_2}^{\mathscr{B}_2'})^{-1}\mathrm{mat}_{\mathscr{B}_1,\mathscr{B}_2}(f)P_{\mathscr{B}_1}^{\mathscr{B}_1'}$$

et donc $\mathrm{mat}_{\mathscr{B}'_1,\mathscr{B}'_2}(f)$ et $\mathrm{mat}_{\mathscr{B}_1,\mathscr{B}_2}(f)$ sont équivalentes.

Proposition XXI.10. L'équivalence des matrices est une relation d'équivalence.

Démonstration. La démonstration de cette propriété fort surprenante est laissée en exercice au lecteur avide de savoir et d'eau fraîche. □

Proposition XXI.11. Soient $A, B \in \mathscr{M}_{n,m}(\mathbb{K})$. Alors les propriétés suivantes sont équivalentes :

(i) A est équivalente à B ;

(ii) A et B sont matrices d'une même application linéaire ;

(iii) $\mathrm{rg}(A) = \mathrm{rg}(B)$.

Démonstration.

(i)⇒(ii) Soit f l'application canoniquement associée à A et notons $\mathscr{B}$ la base canonique de $\mathbb{K}^m$ et $\mathscr{B}'$ celle de $\mathbb{K}^n$; nous avons donc $A = \mathrm{mat}_{\mathscr{B},\mathscr{B}'}(f)$. Comme B est équivalente à A, il existe $P \in GL_n(\mathbb{K})$ et $Q \in GL_m(\mathbb{K})$ telles que $A = P^{-1}BQ$. Or P (resp. Q) peut être vue comme la matrice de passage $P_{\mathscr{B}'}^{\mathscr{C}}$ (resp. $P_{\mathscr{B}}^{\mathscr{D}}$), où $\mathscr{C}$ (resp. $\mathscr{D}$) est la famille des colonnes de P (resp. Q), ces familles étant des bases de leurs espaces respectives par inversibilité de P et Q. Nous avons donc, *in fine* :

$$\begin{aligned} B &= P_{\mathscr{C}}^{\mathscr{B}'} \mathrm{mat}_{\mathscr{B},\mathscr{B}'}(f) P_{\mathscr{B}}^{\mathscr{D}} \\ &= \mathrm{mat}_{\mathscr{D},\mathscr{C}}(f) \end{aligned}$$

d'où le résultat souhaité.

(ii)⇒(iii) Soit f l'application canoniquement associée à A. Alors B est également matrice de f donc $\mathrm{rg}(A) = \mathrm{rg}(f) = \mathrm{rg}(B)$.

(iii)⇒(i) Soit f (resp. g) l'application linéaire canoniquement associée à A (resp. à B). Comme $\mathrm{rg}(A) = \mathrm{rg}(B)$, on a $\mathrm{rg}(f) = \mathrm{rg}(g)$ et donc f et g admettent pour matrice dans un certain couple de bases (potentiellement différentes pour l'une et l'autre) J_r avec $r = \mathrm{rg}(A)$. De fait, A et B sont équivalentes à Jr. Par transitivité, A est donc équivalente à B.

□

✌ **Remarque XXI.11.** Une conséquence importante de cette proposition est qu'une matrice est de rang r si et seulement si elle est équivalente à J_r. De plus, toute matrice inversible est une matrice de passage.

La vision matricielle des opérations élémentaires introduite au chapitre XII nous permet de plus de démontrer la proposition suivante.

Proposition XXI.12. Soient $A \in \mathscr{M}_{n,m}(\mathbb{K})$ la matrice d'une application linéaire f. Alors :

(i) les opérations élémentaires sur les colonnes de A préservent le rang et l'image de f ;

(ii) les opérations élémentaires sur les lignes de A préservent le rang et le noyau de f.

Démonstration. Ces propriétés découlent du fait que multiplier par une matrice inversible ne modifie pas le rang et du lien entre produit et composée (pour la partie "image/noyau"). $\square$

Proposition XXI.13. Soit $M \in \mathscr{M}_{n,m}(\mathbb{K})$. Alors $\mathrm{rg}(M^\top) = \mathrm{rg}(M)$.

Démonstration. Soit $r = \mathrm{rg}(M)$; alors on sait qu'il existe $P \in GL_n(\mathbb{K})$ et $Q \in GL_m(\mathbb{K})$ telles que $M = P^{-1}J_rQ$ et donc :

$$\begin{aligned} M^\top &= (P^{-1}J_rQ)^\top \\ &= Q^\top J_r^\top (P^{-1})^\top \\ &= Q^\top J_r^T (P^\top)^{-1} \end{aligned}$$

ce qui implique que $M^\top$ est équivalente à J_r^T (qui est elle même une "matrice J_r") et donc de rang r. $\square$

✌ **Remarque XXI.12.** Toute matrice est donc équivalente à sa transposée.

d) Matrices extraites

Définition XXI.6. Soit $M \in \mathscr{M}_{n,m}(\mathbb{K})$; on appelle **matrice extraite** toute restriction de M à un ensemble de la forme $I \times J$, avec $I \subset [\![1, n]\!]$ et $J \subset [\![1, m]\!]$ **non vides**.

➠ **Exemple XXI.9.** Il s'agit en pratique de ne conserver que certaines lignes et colonnes de la matrice en question : les matrices $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ et $\begin{pmatrix} 1 \\ 4 \end{pmatrix}$ sont par exemple extraites de $\begin{pmatrix} 1 & 2 & 5 \\ 3 & 4 & 2 \\ 4 & 0 & 0 \end{pmatrix}$.

✌ **Remarque XXI.13.** Dans la définition *supra*, nous disposons de $2^n - 1$ choix pour I et $2^m - 1$ choix pour J : toute matrice de $\mathscr{M}_{n,m}(\mathbb{K})$ admet donc $(2^n - 1)(2^m - 1)$ matrices extraites.

Proposition XXI.14. Soit $A \in \mathscr{M}_{n,m}(\mathbb{K})$ une matrice de rang $r \in \mathbb{N}^*$. Alors :

(i) il existe une matrice extraite de A appartenant à $GL_r(\mathbb{K})$;

(ii) toutes les matrices extraites de A sont de rang inférieur ou égal à r.

Démonstration.

(i) Par définition du rang, on peut trouver une famille libre de r vecteurs colonnes de la matrice A, ce qui permet d'extraire de A une matrice A' de taille $n \times r$ dont les colonnes forment une famille libre de r vecteurs de $\mathbb{K}^n$. Comme $\mathrm{rg}(A'^\top) = \mathrm{rg}(A') = r$, on peut extraire de A' r lignes formant une famille libre de $\mathbb{K}^r$, d'où le résultat.

(ii) Immédiat.

□

3.⁻ Similitude

a) Trace

Définition XXI.7. Soit $A = (a_{i,j})_{i,j} \in \mathscr{M}_n(\mathbb{K})$ une matrice **carrée**. On appelle **trace** de A la quantité :

$$\mathrm{Tr}(A) = \sum_{i=1}^{n} a_{i,i}\,.$$

➠ **Exemple XXI.10.** $\mathrm{Tr}(I_n) = n$, $\mathrm{Tr}\left(\begin{pmatrix} 1 & 0 \\ -12 & 3 \end{pmatrix}\right) = 4$.

Proposition XXI.15. Soient $A, B \in \mathscr{M}_n(\mathbb{K})$ et soit $\lambda \in \mathbb{K}$. Alors :

(i) $\mathrm{Tr}(A + \lambda B) = \mathrm{Tr}(A) + \lambda \mathrm{Tr}(B)$;

(ii) $\mathrm{Tr}(A^\top) = \mathrm{Tr}(A)$;

(iii) $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

Démonstration. Les point (i) et (ii) découlent directement de la définition. Pour le point (iii), remarquons que si on note $a_{i,j}$ (resp. $b_{i,j}$) les coefficients de A (resp. de B) on a :

$$\mathrm{Tr}(AB) = \sum_{i=1}^{n} \sum_{k=1}^{n} a_{i,k} b_{k,i}$$

et

$$\begin{aligned}\mathrm{Tr}(BA) &= \sum_{i=1}^{n}\sum_{k=1}^{n} b_{i,k}a_{k,i}\\ &= \sum_{k=1}^{n}\sum_{i=1}^{n} a_{k,i}b_{i,k}\\ &= \mathrm{Tr}(AB)\end{aligned}$$

ce qui constitue le résultat voulu. □

✌ **Remarque XXI.14.** La trace est donc une forme linéaire sur $\mathscr{M}_n(\mathbb{K})$.

Proposition/définition XXI.8. Soit E un $\mathbb{K}$–e.v de dimension finie et soit $\mathscr{B}$ une base de E. Alors, si $f \in \mathscr{L}(E)$, la quantité $\mathrm{Tr}(\mathrm{mat}_{\mathscr{B}}(f))$ est indépendante du choix de la base $\mathscr{B}$ et est appelée **trace** de f.

Notation. $\mathrm{Tr}(f)$

Démonstration. Fixons $\mathscr{B}'$ une base de E et posons $M = \mathrm{mat}_{\mathscr{B}}(f)$, $M' = \mathrm{mat}_{\mathscr{B}'}(f)$ et $P = P_{\mathscr{B}}^{\mathscr{B}'}$. Alors :

$$\begin{aligned}\mathrm{Tr}(M') &= \mathrm{Tr}(P^{-1}MP)\\ &= \mathrm{Tr}(PP^{-1}M)\\ &= \mathrm{Tr}(M)\,.\end{aligned}$$

□

Proposition XXI.16. On a les égalités suivantes :

(i) $\mathrm{Tr}(\mathrm{id}_E) = \dim(E)$;

(ii) si $u, v \in \mathscr{L}(E)$, $\mathrm{Tr}(u \circ v) = \mathrm{Tr}(v \circ u)$;

(iii) soit $p \in \mathscr{L}(E)$ un projecteur ; alors $\mathrm{Tr}(p) = \mathrm{rg}(p)$.

Démonstration.

(i) Si $\mathscr{B}$ est une base de E $\mathrm{mat}_{\mathscr{B}}(\mathrm{id}_{\mathrm{E}}) = I_n$, d'où le résultat.

(ii) Passer par les matrices.

(iii) Soit $\mathscr{B} = (e_1, \ldots, e_n)$ une base de E adaptée à la décomposition $E = \mathrm{Ker}(p) \oplus \mathrm{Im}(p)$. Alors, si $k = \dim(\mathrm{Ker}(p))$ on a :

 (i) $\forall i \in [\![1, k]\!]$, $p(e_i) = 0$;

 (ii) $\forall i \in [\![k+1, n]\!]$, $p(e_i) = e_i$.

 On a donc :

$$\mathrm{mat}_{\mathscr{B}}(p) = \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & I_{n-k}\end{array}\right)$$

 ce qui implique que $\mathrm{Tr}(p) = n - k = \mathrm{rg}(p)$.

□

✍ **Exercice XXI.3.** Que dire de la trace d'une symétrie ?

b) Matrices semblables

Définition XXI.9. Soient $A, B \in \mathscr{M}_n(\mathbb{K})$. On dit que A et B sont **semblables** si il existe $P \in GL_n(\mathbb{K})$ telle que :

$$B = P^{-1}AP\,.$$

✌ **Remarque XXI.15.** Deux matrices semblables sont équivalentes. La réciproque est évidemment fausse.

➠ **Exemple XXI.11.** Soient $\mathscr{B}$ et $\mathscr{B}'$ deux bases d'un $\mathbb{K}$–e.v de dimension finie E et soit $f \in \mathscr{L}(E)$. Alors, si on pose $P = P_{\mathscr{B}}^{\mathscr{B}'}$, on a :

$$\mathrm{mat}_{\mathscr{B}'}(f) = P^{-1}\mathrm{mat}_{\mathscr{B}}(f)P$$

et donc $\mathrm{mat}_{\mathscr{B}'}(f)$ et $\mathrm{mat}_{\mathscr{B}}(f)$ sont semblables. Réciproquement deux matrices semblables sont matrices d'un même **endomorphisme** dans deux bases (et non deux couples de bases, attention) différents.

Proposition XXI.17. La similitude des matrices est une relation d'équivalence.

Démonstration. Voici un fort bel exercice pour notre lecteur favori. Have fun. □

✌ **Remarque XXI.16.** Si A et B sont deux matrices semblables, alors leurs puissances le sont également (à vérifier par récurrence).

Proposition XXI.18. Soient $A, B \in \mathscr{M}_n(\mathbb{K})$ deux matrices semblables. Alors $\mathrm{Tr}(A) = \mathrm{Tr}(B)$.

Vocabulaire. On dit que la trace est un **invariant de similitude**.

Démonstration. Par similitude, il existe $P \in GL_n(\mathbb{K})$ telle que $B = P^{-1}AP$. On a donc :

$$\begin{aligned}\mathrm{Tr}(B) &= \mathrm{Tr}(P^{-1}AP)\\ &= \mathrm{Tr}(PP^{-1}A)\\ &= \mathrm{Tr}(A)\end{aligned}$$

youpi. □

✖ **Attention :** la réciproque est brutalement fausse : la matrice nulle et la matrice $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ ont la même trace sans être semblables.

4.– Compléments sur les systèmes linéaires

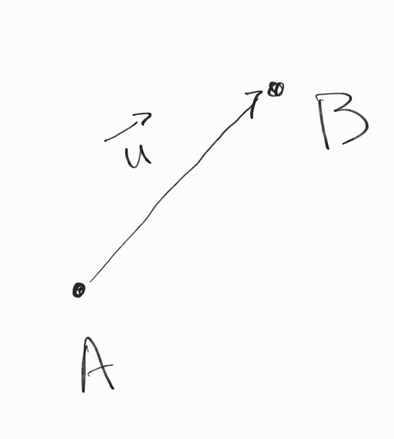
a) Sous–espaces affines d'un $\mathbb{K}$–e.v

L'objet de ce paragraphe est d'introduire, sans excès de technicité, la notion de sous–espace affine d'un $\mathbb{K}$–e.v. Nous fixons donc dans celui–ci un $\mathbb{K}$–e.v E.

La **structure affine d'un espace vectoriel** est, à notre niveau, un paradigme visant à distinguer au sein de celui–ci deux types d'objets essentiels : les **points** et les **vecteurs**. Nous appuyant sur les connaissances existantes du lecteur, nous noterons, pour $A, B \in E$

$$B = A + \vec{u}$$

pour signifier que l'objet $\vec{u}$ ainsi (informellement) défini est le vecteur (au sens vu dans l'enseignement secondaire) $\overrightarrow{AB}$. Notons que l'ensemble $\vec{E}$ des vecteurs (affines) de E peut être identifié à $\ldots E$. Nous conserverons toutefois une notation différente pour celui–ci, afin de préserver la santé mentale du lecteur.



Définition XXI.10. Soit $\vec{u}$ un vecteur (affine) de E. On appelle **translation** associée à $\vec{u}$ l'application

$$\begin{aligned} \tau_{\vec{u}} : E &\to E \\ A &\mapsto A + \vec{u}\,. \end{aligned}$$

Exemple XXI.12. Visualiser la translation de vecteur $\vec{u} = (1, 1)$ dans $\mathbb{R}^2$.

Définition XXI.11. Soit $\vec{F}$ un s–e.v de $\vec{E}$ et soit $A \in E$. On appelle **sous–espace affine de direction $\vec{F}$ passant par A** l'ensemble :

$$A + \vec{F} = \{A + \vec{u} \,|\, \vec{u} \in \vec{F}\}\,.$$

Remarque XXI.17. On a donc :

$$A + \vec{F} = \{\tau_{\vec{u}}(A) \,|\, \vec{u} \in \vec{F}\}\,.$$

Vocabulaire. Un sous–espace affine dirigé par une droite (resp. un plan, un hyperplan) est appelé droite (resp. plan, hyperplan) affine. De façon générale, on appelle **dimension** d'un tel espace la dimension (éventuellement infinie) de sa direction.

➠ **Exemple XXI.13.** Les sous–espaces affines de $\mathbb{R}^2$ et $\mathbb{R}^3$ ont été étudiés par le lecteur en terminale.

✌ **Remarque XXI.18.** L'intersection de deux sous–espaces affines est soit vide, soit un sous–espace affine.

Proposition XXI.19. Soit F un $\mathbb{K}$–e.v, $u \in \mathscr{L}(E, F)$ et soit $A \in F$. Alors l'ensemble

$$u^{-1}(\{A\}) = \{x \in E \mid u(x) = A\}$$

est soit vide, soit un sous–espace affine de E dirigé par $\mathrm{Ker}(u)$.

Démonstration. Supposons $u^{-1}(\{A\})$ non vide et fixons $x_0 \in u^{-1}(\{A\})$. Alors, pour tout $x \in E$:

$$\begin{aligned} x \in u^{-1}(\{A\}) &\Leftrightarrow u(x) = A \\ &\Leftrightarrow u(x) = u(x_0) \\ &\Leftrightarrow x - x_0 \in \mathrm{Ker}(u) \end{aligned}$$

d'où le résultat. □

✌ **Remarque XXI.19.** Ceci entraîne que si $(\mathscr{E})$ est une équation différentielle linéaire sur un intervalle I, alors $\mathrm{Sol}_{\mathscr{E}}$ est un sous–espace affine de $\mathbb{K}^I$ de direction $\mathrm{Sol}_{\mathscr{H}}$ (où $(\mathscr{H})$ est l'équation homogène associée à $(\mathscr{E})$), passant par une solution particulière de $(\mathscr{E})$. La dimension de $\mathrm{Sol}_{\mathscr{E}}$ est de plus égale à l'ordre de l'équation. Nous laissons le lecteur énoncer (et vérifier !) un résultat analogue relatif aux suites récurrentes linéaires.

b) Structure de l'espace des solutions d'un système linéaire

Avec le recul dont nous disposons désormais, la résolution d'un système linéaire à p équations et q inconnues peut être interprétée de quatre façons différentes :
- naïvement : on résout un paquet d'équations linéaires simultanément ;
- géométriquement : chaque équation du système décrit un hyperplan (éventuellement affine) de $\mathbb{K}^q$. Nous recherchons donc une intersection de p tels objets (voir aussi la proposition XIX.17).
- matriciellement : on résout une équation matricielle à une inconnue, elle aussi matricielle ;
- s'appuyant sur le point précédent, on peut voir que résoudre un tel système s'apparente à résoudre une équation du type $f(x) = b$ avec $b \in \mathbb{K}^p$ et $f \in \mathscr{L}(\mathbb{K}^q, \mathbb{K}^p)$.

Définition XXI.12. On considère un système linéaire $AX = B$. Alors on appelle **rang** du système la quantité $\mathrm{rg}(A)$.

✌ **Remarque XXI.20.** Si le système possède p équations et q inconnues, alors son rang est inférieur ou égal à $\min(p,q)$.

Proposition XXI.20. On considère un système linéaire homogène à p équations et q inconnues

$$(\mathscr{H}) \qquad AX = 0$$

de rang r. Alors l'espace $\mathrm{Sol}_{\mathscr{H}}$ des solutions de celui–ci est un s–e.v de $\mathbb{K}^q$ de dimension $q-r$.

Démonstration. Soit $f \in \mathscr{L}(\mathbb{K}^q, \mathbb{K}^p)$ l'application linéaire canoniquement associée à A. Alors $\mathrm{rg}(f) = \mathrm{rg}(A) = r$ et l'ensemble des solutions de $(\mathscr{H})$ est isomorphe (*via* l'application associant à un vecteur sa matrice dans la base canonique de $\mathbb{K}^q$) à $\mathrm{Ker}(f)$. Le résultat suit par théorème du rang (XIX.14). □

✌ **Remarque XXI.21.**
— On a naturellement $\mathrm{Sol}_{\mathscr{H}} = \mathrm{Ker}(A)$.
— Si $p < q$ (moins d'équations que d'inconnues), alors $r \leq p < q$ et donc $\dim(\mathrm{Sol}_{\mathscr{H}}) > 0$. Le système $(\mathscr{H})$ admet donc automatiquement une infinité de solutions non triviales.

Proposition XXI.21. On considère un système linéaire à p équations et q inconnues

$$(\mathscr{S}) \qquad AX = B$$

de rang r que l'on suppose **compatible**. Alors, l'espace $\mathrm{Sol}_{\mathscr{S}}$ des solutions de $(\mathscr{S})$ est un un sous–espace affine de dimension $q-r$ de $\mathbb{K}^q$ dirigé par $\mathrm{Sol}_{\mathscr{H}}$. Plus précisément, si $X_0 \in \mathrm{Sol}_{\mathscr{S}}$, on a :

$$\mathrm{Sol}_{\mathscr{S}} = X_0 + \mathrm{Sol}_{\mathscr{H}}\,.$$

Démonstration. Ceci découle de la proposition XXI.19 appliquée à l'application canoniquement associée à A. □

✌ **Remarque XXI.22.** Le système $AX = B$ est compatible si et seulement si $B \in \mathrm{Im}(A)$.

c) Systèmes de Cramer

Rappelons (*cf.* chapitre XII) qu'un système de Cramer est un système linéaire de la forme $AX = B$ avec $A \in GL_p(\mathbb{K})$. Reprenant les notations du paragraphe précédent, nous avons donc $p = q = r$. Un tel système admet toujours une unique solution, donnée par $X = A^{-1}B$.

Proposition XXI.22. Soit $A \in \mathscr{M}_n(\mathbb{K})$. Alors les propriétés suivantes sont équivalentes :

(i) $A \in GL_n(\mathbb{K})$;

(ii) $\forall B \in \mathscr{M}_{n,1}(\mathbb{K})$, le système $AX = B$ est compatible ;

(iii) $\forall B \in \mathscr{M}_{n,1}(\mathbb{K})$, le système $AX = B$ admet une unique solution ;

(iv) $\forall B \in \mathscr{M}_{n,1}(\mathbb{K})$, si le système $AX = B$ admet un solution, celle–ci est unique ;

(v) l'ensemble des solutions du système $AX = 0$ est réduit à $\{0\}$.

Démonstration. Soit f l'application canoniquement associée à A ; on peut alors traduire les propriétés énoncées comme suit :

(i) f est bijective ;

(ii) f est surjective ;

(iii) f est bijective ;

(iv) f est injective ;

(v) $\mathrm{Ker}(f) = \{0\}$.

Or, nous avons que ces propriétés sont équivalentes car f est un endomorphisme de $\mathbb{K}^n$, d'où le résultat. □

Chapitre XXII

Séries numériques

On fixe dans tout ce chapitre un corps $\mathbb{K}$ égal à $\mathbb{R}$ ou $\mathbb{C}$.

1.– Qu'est–ce ?

a) Notion de série

Définition XXII.1. Soit $u \in \mathbb{K}^{\mathbb{N}}$. On appelle **série de terme général** u_n la suite

$$\left(\sum_{n=0}^{N} u_n\right)_{N\in\mathbb{N}}.$$

Pour $N \in \mathbb{N}$ fixé, on appelle **somme partielle de rang** N de la série la quantité

$$S_N = \sum_{n=0}^{N} u_n \,.$$

✌ **Remarque XXII.1.** La somme partielle de rang N d'une série est donc le N-ième terme de la suite sous–jacente à celle–ci.

Notation. On note $\sum u_n$ la série de terme général u_n. **Ceci n'est PAS une somme**, mais une suite de sommes.

✌ **Remarque XXII.2.** Il est possible de considérer des séries dont le terme général n'est défini qu'à partir d'un rang $n_0 \in \mathbb{N}$. On noter alors $\sum\limits_{(n\geq n_0)} u_n$. Les résultats énoncés dans ce chapitre se généralisent aisément à ce type de séries.

➠ **Exemple XXII.1.** $\sum \cos(n)$ est une série définie à partir du rang 0 ; $\sum\limits_{(n\geq 1)} \frac{1}{n}$ est définie à partir du rang 1.

◇ **Exemples fondamentaux**

Définition XXII.2. Soit $q \in \mathbb{C}$. On appelle **série géométrique de raison** q la série $\sum q^n$.

Remarque XXII.3. Il est aisé de déterminer les sommes partielles d'une série géométrique ; si $N \in \mathbb{N}$ et $q \in \mathbb{C}$ on a :

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

Définition XXII.3. Soit $\alpha \in \mathbb{C}$. On appelle **série de Riemann de paramètre** α la série $\sum\limits_{(n \geq 1)} \frac{1}{n^\alpha}$.

Exemple XXII.2. La série de Riemann de paramètre 1 est la série $\sum\limits_{(n \geq 1)} \frac{1}{n}$. On l'appelle **série harmonique**.

b) Somme, restes

Définition XXII.4. Une série $\sum u_n$ est dite **convergente** si la suite de ses sommes partielles converge. Dans le cas contraire, on dit que la série est **divergente**.

Notation. **Si** la série $\sum u_n$ est convergente, on pose :

$$\sum_{n=0}^{\infty} u_n = \lim_{N \to \infty} \sum_{n=0}^{N} u_n \,.$$

Cette quantité, que l'on appelle **somme** de la série $\sum u_n$, n'est **toujours pas** une somme : il s'agit de la limite d'une suite de sommes ...

Exemple XXII.3.

— La série $\sum n$ diverge ; en effet, pour $N \geq 0$:

$$\sum_{n=0}^{N} n = \frac{N(N+1)}{2} \xrightarrow[N \to \infty]{} \infty \,.$$

— À l'inverse, la série $\sum\limits_{(n \geq 1)} \frac{1}{n(n+1)}$ converge. En effet, pour $N \geq 1$ on a :

$$\begin{aligned} \sum_{n=1}^{N} \frac{1}{n(n+1)} &= \sum_{n=1}^{N} \frac{1}{n} - \frac{1}{n+1} \\ &= \sum_{n=1}^{N} \frac{1}{n} - \sum_{n=1}^{N} \frac{1}{n+1} \\ &= \sum_{n=1}^{N} \frac{1}{n} - \sum_{n=2}^{N+1} \frac{1}{n} \\ &= 1 - \frac{1}{N+1} \\ &\xrightarrow[N \to \infty]{} 1 \end{aligned}$$

et donc
$$\sum_{n=1}^{\infty} \frac{1}{n(n+1)} = 1\,.$$

Proposition XXII.1. Soit $\sum u_n$ une série convergente. Alors la suite $(u_n)_n$ converge vers 0.

Démonstration. Il suffit de remarque que, si on note $(S_N)_N$ la suite des sommes partielles de $\sum u_n$, on a, pour tout $N \geq 1$:
$$\begin{aligned} u_N &= S_N - S_{N-1} \\ &\xrightarrow[N\to\infty]{} \sum_{n=0}^{\infty} u_n - \sum_{n=0}^{\infty} u_n \\ &= 0 \end{aligned}$$
d'où le résultat. □

✖ **Attention :** la réciproque est **fausse**. Pour un contre–exemple, considérer la série $\sum \sqrt{n+1} - \sqrt{n}$: on vérifie (faire un DL) que $\sqrt{n+1} - \sqrt{n} \to 0$ et pourtant, pour tout $N \geq 0$ on a :
$$\sum_{n=0}^{N} \sqrt{n+1} - \sqrt{n} = \sqrt{N+1} \to \infty\,.$$

✌ **Remarque XXII.4.** Ce résultat sera toutefois fort utile pour démontrer la **divergence** d'une série : si la suite $(u_n)_n$ ne converge pas vers 0, alors la suite $\sum u_n$ diverge automatiquement : on parle alors de **divergence grossière**.

➠ **Exemple XXII.4.** Les séries $\sum \cos(n)$ et $\sum n^3 + \frac{2}{n+1}$ divergent grossièrement.

✍ **Exercice XXII.1.** Déterminer pour quelles valeurs de x la série $\sum_{(n\geq 1)} \frac{(-1)^n x^n}{n}$ est convergente et établir que dans ce cas :
$$\sum_{n=1}^{\infty} \frac{(-1)^n x^n}{n} = -\ln(1+x)\,.$$

➥ **Correction :** *Pour obtenir la somme, utiliser l'inégalité de Taylor–Lagrange (proposition XX.20) en s'inspirant du développement limité de* $\ln(1+x)$ *en* 0.

Proposition XXII.2. Soient $\sum u_n$ et $\sum v_n$ deux séries **convergentes** et soit $\lambda \in \mathbb{K}$. Alors :

(i) la série $\sum u_n + \lambda v_n$ converge ;

(ii)
$$\sum_{n=0}^{\infty} u_n + \lambda v_n = \sum_{n=0}^{\infty} u_n + \lambda \sum_{n=0}^{\infty} v_n\,.$$

Démonstration. Appliquer les opérations sur les limites vues dans le chapitre VII aux sommes partielles. □

✖ **Attention :** ce type d'opérations ne saurait être effectué que lorsque les **deux** séries considérées convergent.

Définition XXII.5. Soit $\sum u_n$ une série **convergente** de somme S. Pour $N \in \mathbb{N}$, on appelle **reste d'ordre** N de la série $\sum u_n$ la quantité $R_N = S - S_N$, où S_N est la somme partielle de rang N de celle–ci.

Notation. Le reste d'ordre N de $\sum u_n$ est noté

$$R_N = \sum_{n=N+1}^{\infty} u_n \,.$$

✌ **Remarque XXII.5.** Il est aisé de vérifier que, comme $\sum u_n$ converge, $R_N \xrightarrow[N\to\infty]{} 0$.

➠ **Exemple XXII.5.** Soit $q \in \mathbb{C}$ tel que $|q| < 1$ et soit $N \in \mathbb{N}$. Alors :

$$\sum_{n=N+1}^{\infty} q^n = \frac{q^{N+1}}{1-q} \,.$$

c) Lien suite–série

Proposition XXII.3. Soit $u \in \mathbb{K}^{\mathbb{N}}$. Alors :

$$\text{la suite } (u_n)_n \text{ converge} \iff \text{la série } \sum u_{n+1} - u_n \text{ est convergente.}$$

Dans ce cas, on a de plus :

$$\sum_{n=0}^{\infty} u_{n+1} - u_n = \lim u_n - u_0 \,.$$

Démonstration. Soit $N \in \mathbb{N}$. Alors :

$$\begin{aligned}
\sum_{n=0}^{N} u_{n+1} - u_n &= \sum_{n=0}^{N} u_{n+1} - \sum_{n=0}^{N} u_n \\
&= \sum_{n=1}^{N+1} u_n - \sum_{n=0}^{N} u_n \\
&= u_{N+1} - u_0
\end{aligned}$$

d'où le résultat. □

Vocabulaire. Les séries du type $\sum u_{n+1} - u_n$ sont appelées **séries télescopiques**.

➠ **Exemple XXII.6.** La série $\sum\limits_{(n\geq 1)} \ln\left(\dfrac{n+1}{n}\right)$ diverge. En effet, son terme général est égal, pour $n \geq 1$, à $\ln(n+1) - \ln(n)$ et $\ln(n) \to \infty$.

✌ **Remarque XXII.6.** Ce résultat implique que toute suite qui tend vers 0 peut être interprétée comme la suite des restes d'une série convergente.

d) Exemples fondamentaux

◇ **Séries géométriques**

Proposition XXII.4. Soit $q \in \mathbb{C}$. Alors :

$$\text{la série géométrique } \sum q^n \text{ converge} \iff |q| < 1.$$

Dans ce cas, on a de plus :

$$\sum_{n=0}^{\infty} q^n = \frac{1}{1-q}.$$

Démonstration. **Cas 1 : $|q| < 1$.** Comme nous le savons, si $N \geq 0$ on a :

$$\sum_{n=0}^{N} q^n = \frac{1-q^{N+1}}{1-q}.$$

Il est alors clair que la suite des sommes partielles de $\sum q^n$ converge vers $\dfrac{1}{1-q}$.

Cas 2 : $|q| \geq 1$. La suite $(q^n)_n$ ne convergeant pas vers 0, on a divergence grossière (proposition XXII.1) de la série $\sum q^n$.

□

◇ **Séries exponentielles**

Proposition XXII.5. Soit $z \in \mathbb{C}$. Alors :

(i) la série $\sum \dfrac{z^n}{n!}$ converge ;

(ii)
$$\sum_{n=0}^{\infty} \frac{z^n}{n!} = e^z.$$

Démonstration. Soit $z \in \mathbb{C}$; on pose alors, pour tout $t \in \mathbb{R}_+$:

$$f_z(t) = e^{zt}.$$

La fonction f_z est de classe $\mathscr{C}^\infty$ sur $\mathbb{R}$ et on démontre aisément par récurrence que

$$\forall k \in \mathbb{N},\ \forall t \in \mathbb{R}, \quad f_z^{(k)}(t) = z^k e^{zt}\,.$$

L'inégalité de Taylor–Lagrange (proposition XX.20) entre 0 et 1 nous permet alors d'écrire que :

$$f_z(1) = \sum_{k=0}^{n} \frac{f_z^{(k)}(0)}{k!} + R_n$$

avec

$$|R_n| \leq \frac{1}{(n+1)!} \max_{x\in[0,1]} |z^{n+1}e^{zx}|\,.$$

On démontre (utiliser la formule de Stirling) que $R_n \xrightarrow[n\to\infty]{} 0$, ce qui implique que l'on a convergence de la série de Taylor associée à $f_z(1)$ et

$$f_z(1) = \sum_{n=0}^{\infty} \frac{f_z^{(n)}(0)}{n!} = \sum_{n=0}^{\infty} \frac{z^n}{n!}\,,$$

ce qui nous livre bien

$$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}\,.$$

□

✌ **Remarque XXII.7.** On déduit de ce résultat que, pour tout $x \in \mathbb{R}$, on a les formules suivantes :

$$\cos(x) = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!}\,;$$

$$\sin(x) = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}\,;$$

$$\mathrm{ch}(x) = \sum_{n=0}^{\infty} \frac{x^{2n}}{(2n)!}\,;$$

$$\mathrm{sh}(x) = \sum_{n=0}^{\infty} \frac{x^{2n+1}}{(2n+1)!}\,.$$

◇ Séries alternées

Proposition XXII.6. [Critère spécial des séries alternées] Soit $(u_n)_n$ une suite **décroissante** de nombres **réels positifs**. Alors :

(i) la série $\sum(-1)^n u_n$ converge si et seulement si $u_n \to 0$;

(ii) dans ce cas on a, pour tout $N \geq 0$:

$$S_{2N+1} \leq \sum_{n=0}^{\infty} (-1)^n u_n \leq S_{2N} \quad \text{et} \quad 0 \leq |R_N| \leq u_{N+1}$$

si $(S_N)_N$ (resp. $(R_N)_N$) est la suite des sommes partielles (resp. des restes) de la série $\sum(-1)^n u_n$. R_N est par ailleurs du signe du terme de $(-1)^{N+1}$.

Démonstration. Notons tout d'abord que si $u_n \not\to 0$, la série $\sum(-1)^n u_n$ diverge grossièrement. Inversement, si $u_n \to 0$, posons, pour $N \in \mathbb{N}$, $A_N = S_{2N}$ et $B_N = S_{2N+1}$; on a alors, pour tout $N \geq 0$:

$$\begin{aligned} A_{N+1} - A_N &= \sum_{n=0}^{2(N+1)} (-1)^n u_n - \sum_{n=0}^{2N} (-1)^n u_n \\ &= u_{2N+2} - u_{2N+1} \\ &\leq 0 \quad \text{par décroissance de } (u_n)_n. \end{aligned}$$

La suite $(A_N)_n$ est donc décroissante ; on vérifie de façon similaire que (B_N) est croissante. De plus :

$$\forall N \in \mathbb{N},\ A_N - B_N = \sum_{n=0}^{2N} (-1)^n u_n - \sum_{n=0}^{2N+1} (-1)^n u_n = u_{2N+1} \xrightarrow[N\to\infty]{} 0$$

et donc les suites $(A_N)_N$ et $(B_N)_N$ sont adjacentes et donc convergent vers une même limite ℓ (*cf.* proposition VII.16) vérifiant :

$$\forall N \geq 0, \quad S_{2N+1} \leq \ell \leq S_{2N}\,.$$

Les suites $(S_{2N})_N$ et $(S_{2N+1})_N$ convergeant toutes les deux vers ℓ, on a par la proposition VII.14 que la suite $(S_N)_N$ converge vers ℓ. On a donc bien convergence de la série $\sum(-1)^n u_n$ et l'inégalité voulue sur les sommes partielles. Il suffit ensuite de remarquer que pour si on soustrait S_{2N} à cette dernière on obtient :

$$-u_{2N+1} \leq R_{2N} \leq 0\,.$$

On a donc bien $|R_{2N}| \leq u_{2N+1}$ et :

$$0 \leq R_{2N+1} = \sum_{n=0}^{\infty} (-1)^n u_n - S_{2N+1} \leq S_{2N+2} - S_{2N+1} = u_{2N+2}$$

car $S_{2N+1} \leq \sum_{n=0}^{\infty} (-1)^n u_n \leq S_{2N+2}$, d'où le résultat. □

➠ **Exemple XXII.7.** Les séries de Riemann alternées $\sum_{(n\geq 1)} \frac{(-1)^n}{n^\alpha}$ convergent pour $\alpha \in \mathbb{R}_+^*$.

2.⁻ Séries à termes positifs

On s'intéresse dans ce paragraphe à une famille particulière de séries, en l'occurrence celles dont le terme général ne prend que des valeurs réelles positives.

Définition XXII.6. Une **série à termes positifs** est une série $\sum u_n$ telle que :

$$\forall n \geq 0,\ u_n \in \mathbb{R}_+\,.$$

a) Critère de convergence

Proposition XXII.7. Une série à termes positifs converge si et seulement si la suite de ses sommes partielles est majorée.

Démonstration. Ceci est immédiat car la suite des sommes partielles d'une série à termes positifs est une suite réelle croissante. □

✖ **Attention :** ce résultat est bien entendu faux lorsque la série n'est pas à termes positifs. La suite $\sum(-1)^n$ diverge grossièrement et pourtant ses sommes partielles sont comprises entre 0 et 1.

✌ **Remarque XXII.8.** Si $\sum u_n$ est une série à termes positives divergente alors on a

$$S_N = \sum_{n=0}^{N} u_n \xrightarrow[N\to\infty]{} +\infty\,.$$

b) Comparaison des séries à termes positifs

Proposition XXII.8. Soient $\sum u_n$ et $\sum v_n$ deux séries à termes positifs telles que, $\exists\, N \in \mathbb{N},\ \forall n \geq N,\ 0 \leq u_n \leq v_n$. Alors :

(i) la convergence de $\sum v_n$ implique celle de $\sum u_n$;

(ii) la divergence de $\sum u_n$ implique celle de $\sum v_n$.

✌ **Remarque XXII.9.** Par passage à la limite dans le cas (i), on a également, si l'inégalité $u_n \leq v_n$ est vérifiée pour tout n :

$$\sum_{n=0}^{\infty} u_n \leq \sum_{n=0}^{\infty} v_n\,.$$

Démonstration. Ceci découle du critère de convergence des séries à termes positifs (proposition XXII.6). □

De fait, ce résultat nous permet de déduire la convergence (ou divergence) de nombreuses séries à termes positifs en les comparant à des exemples connus (comme les séries géométriques de ce type) : nous nous constituons ainsi un "catalogue" de séries à termes positifs "témoins" pour établir la nature de leurs consœurs.

➠ **Exemple XXII.8.** La série de terme général $\dfrac{e^{-n!}}{2^n}$ converge par comparaison avec $\sum \frac{1}{2^n}$.

Proposition XXII.9. Soient $\sum u_n$ et $\sum v_n$ deux séries à termes positifs telles que $u_n \sim v_n$. Alors $\sum u_n$ et $\sum v_n$ sont de même nature.

Démonstration. Par équivalence, il existe une suite $(h_n)_n$ convergeant vers 1 et un entier $N \geq 0$ tel que :

$$\forall n \geq N,\ u_n = h_n v_n\,.$$

On obtient l'existence d'un entier $N' \geq 0$ tel que pour $n \geq N'$, $h_n \leq \pi$ et donc, pour tout $n \geq \max(N, N')$ $u_n \leq \pi v_n$. Ceci entraîne que, par comparaison (proposition XXII.8) que la convergence de $\sum v_n$ entraîne celle de $\sum u_n$. On conclut en observant que les rôles de $(u_n)_n$ et $(v_n)_n$ sont symétriques. □

➠ **Exemple XXII.9.** La série $\sum \frac{n^2+1}{3n^2+2} e^{-n}$ est convergente car son terme général est équivalent à $\dfrac{1}{3}\left(\dfrac{1}{e}\right)^n$, ce dernier étant le terme général d'une série géométrique convergente (à facteur multiplicatif près).

✖ **Attention :** il n'y a pas en général égalité des sommes dans le cas convergent. Des résultats de sommation plus précis seront étudiés en MP.

c) Critère de d'Alembert

Proposition XXII.10 (Critère de d'Alembert)**.** Soit $\sum u_n$ une série à termes positifs telle que :

$$\forall n \geq 0,\ u_n > 0\,.$$

On suppose que $\dfrac{u_{n+1}}{u_n} \xrightarrow[n\to\infty]{} \ell \in [0, +\infty]$. Alors :

(i) si $\ell < 1$, la série $\sum u_n$ converge ;

(ii) si $\ell > 1$, la série $\sum u_n$ diverge grossièrement ;

(iii) si $\ell = 1$, on ne peut conclure.

Démonstration.

(i) Si $\ell < 1$ alors il existe $q < 1$ tel que :

$$\exists\, N \in \mathbb{N},\ \forall n \geq N,\ \frac{u_{n+1}}{u_n} \leq q$$

et donc, pour $n \geq N$:

$$\begin{aligned} u_{n+1} &\leq q u_n \\ &\leq q^2 u_{n-1} \\ &\ \ \vdots \\ &\leq q^{n+1-N} u_N \end{aligned}$$

et donc, par comparaison (proposition XXII.8) avec la série géométrique $\sum q^n$, la série $\sum u_n$ converge.

(ii) Si $\ell > 1$, la suite $(u_n)_n$ est strictement croissante et donc ne peut converger vers 0, d'où le résultat.

(iii) Dans le cas $\ell = 1$, considérer les séries $\sum 1$ et $\sum\limits_{(n\geq 1)} \frac{1}{n} - \frac{1}{n+1}$ pour mesurer la futilité de la chose.

□

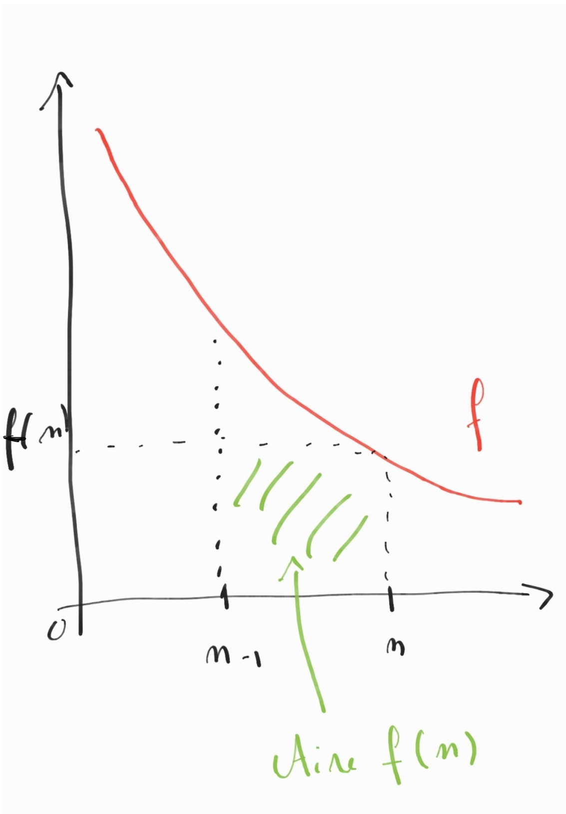
➠ **Exemple XXII.10.** La série à termes positifs $\sum \frac{n!}{n^n}$ converge car :

$$\begin{aligned}\frac{(n+1)!n^n}{n!(n+1)^{n+1}} &= \left(\frac{n}{n+1}\right)^n \\ &= \exp\left(-n\ln\left(1+\frac{1}{n}\right)\right) \\ &\xrightarrow[n\to\infty]{} \frac{1}{e} < 1\,.\end{aligned}$$

d) Comparaison série–intégrale

Considérons une fonction $f : \mathbb{R}_+ \to \mathbb{R}_+$ continue par morceaux et **décroissante**. Alors, on vérifie par méthode des rectangles que :

$$\forall n \geq 1,\ f(n) \leq \int_{n-1}^{n} f(t)\,\mathrm{d}t\,.$$



Ceci nous permet, pour $M, N \in \mathbb{N}$ tels que $M \leq N$ de vérifier que :

$$\begin{aligned}\sum_{n=M}^{N} f(n) &= f(M) + \sum_{n=M+1}^{N} f(n)\\ &\leq f(M) + \sum_{n=M+1}^{N} \int_{n-1}^{n} f(t)\,\mathrm{d}t\\ &= f(M) + \int_{M}^{N} f(t)\,\mathrm{d}t\,.\end{aligned}$$

Ce résultat nous laisse entrevoir un encadrement possible des sommes partielles de la série $\sum f(n)$ par des intégrales, que nous formalisons *infra*.

Proposition XXII.11 (Comparaison série–intégrale)**.** Soit $f \in \mathscr{C}_{\mathrm{pm}}(\mathbb{R}_+)$ une fonction **décroissante à valeurs positives**. Alors, pour tout $M, N \in \mathbb{N}$ tels que $M \leq N$ on a :

$$\int_{M}^{N+1} f(t)\,\mathrm{d}t \leq \sum_{n=M}^{N} f(n) \leq f(M) + \int_{M}^{N} f(t)\,\mathrm{d}t\,.$$

Démonstration. Nous avons déjà démontré l'inégalité de droite. Pour celle de gauche, appliquer une heuristique analogue en remarquant que, pour $n \in \mathbb{N}$:

$$f(n) \geq \int_{n}^{n+1} f(t)\,\mathrm{d}t\,.$$

□

✌ **Remarque XXII.10.** Un résultat analogue peut évidemment être obtenu pour les fonctions croissantes, quitte à changer le sens des inégalités.

Ce résultat a de nombreuses conséquences, dont nous étudierons certaines dans la suite de ce paragraphe. Dans un premier temps, intéressons nous aux séries de Riemann **de paramètre réel**.

Proposition XXII.12. Soit $\alpha \in \mathbb{R}$. Alors :

(i) si $\alpha \leq 0$, la série $\sum\limits_{(n\geq 1)} \frac{1}{n^\alpha}$ diverge grossièrement ;

(ii) si $\alpha \in]0, 1]$, la série $\sum\limits_{(n\geq 1)} \frac{1}{n^\alpha}$ diverge ;

(iii) si $\alpha > 1$, la série $\sum\limits_{(n\geq 1)} \frac{1}{n^\alpha}$ converge.

Démonstration. Commençons par remarquer que, pour $\alpha \in \mathbb{R}$, la fonction $f : x \mapsto x^{-\alpha}$ est continue sur $\mathbb{R}_+^*$.

(i) Trivial.

(ii) **Cas 1 : $0 < \alpha < 1$.** Dans ce cas, une primitive de f est :

$$x \mapsto \frac{x^{1-\alpha}}{1-\alpha}$$

et donc, par comparaison série–intégrale (proposition XXII.11), on a pour $N \geq 1$:

$$\begin{aligned}\sum_{n=1}^{N} \frac{1}{n^\alpha} &\geq \int_1^{N+1} \frac{\mathrm{d}t}{t^\alpha} \\ &= \frac{(N+1)^{1-\alpha}}{1-\alpha} - \frac{1}{1-\alpha} \\ &\xrightarrow[N\to\infty]{} \infty\end{aligned}$$

d'où le résultat.

Cas 2 : $\alpha = 1$. Une primitive de $f : x \mapsto \frac{1}{x}$ est :

$$x \mapsto \ln(x)$$

et donc, par comparaison série–intégrale, on a pour $N \geq 1$:

$$\begin{aligned}\sum_{n=1}^{N} \frac{1}{n} &\geq \int_1^{N+1} \frac{\mathrm{d}t}{t} \\ &= \ln(N+1) \\ &\xrightarrow[N\to\infty]{} \infty\end{aligned}$$

ce qui entraîne la divergence annoncée.

(iii) Dans ce cas, une primitive de f est donnée par

$$x \mapsto \frac{x^{1-\alpha}}{1-\alpha} = -\frac{1}{(\alpha-1)x^{\alpha-1}} .$$

De fait, par comparaison série–intégrale :

$$\begin{aligned}\forall N \geq 1, \sum_{n=1}^{N} \frac{1}{n^\alpha} &\leq 1 + \int_1^{N} \frac{\mathrm{d}t}{t^\alpha} \\ &= 1 + \frac{1}{\alpha-1} - \frac{1}{(\alpha-1)N^{\alpha-1}} \\ &\leq 1 + \frac{1}{\alpha-1}\end{aligned}$$

et donc, par critère de convergence des séries à termes positifs (proposition XXII.6), la série $\sum\limits_{(n\geq 1)} \frac{1}{n^\alpha}$ converge.

□

✍ **Exercice XXII.2.** Donner un équivalent du reste de la série $\sum\limits_{(n\geq 1)} \frac{1}{n^2}$.

➥ **Correction :** *On applique une comparaison série–intégrale (proposition XXII.11) pour $M, N \geq 1$ tels que $M \leq N$, obtenant :*

$$\int_M^{N+1} \frac{\mathrm{d}t}{t^2} \leq \sum_{n=M}^{N} \frac{1}{n^2} \leq \frac{1}{M^2} + \int_M^N \frac{\mathrm{d}t}{t^2}$$

i.e :

$$\frac{1}{M} - \frac{1}{N+1} \leq \sum_{n=M}^{N} \frac{1}{n^2} \leq \frac{1}{M^2} + \frac{1}{M} - \frac{1}{N}$$

et donc, en faisant tendre N vers $+\infty$ on obtient :

$$\frac{1}{M} \leq R_{M-1} \leq \frac{1}{M^2} + \frac{1}{M}\,.$$

Une application du théorème d'encadrement des limites (théorème VII.11) permet ensuite aisément de déduire que $R_M \sim \dfrac{1}{M}$.

◇ Étude asymptotique de la série harmonique

Nous avons démontré plus haut que la série harmonique $\sum\limits_{(n\geq 1)} \frac{1}{n}$ diverge. Mais encore ? Nous nous attachons dans ce paragraphe à offrir à notre lecteur une vision plus raffinée de la situation. Commençons par poser, pour $N \geq 1$:

$$S_N = \sum_{n=1}^{N} \frac{1}{n}$$

et remarquer que, par comparaison série–intégrale (proposition XXII.11)

$$\ln(N+1) \leq S_N \leq 1 + \ln(N)$$

ce qui permet de démontrer, *via* le théorème d'encadrement des limites (théorème VII.11) que :

$$S_N \sim \ln(N)\,.$$

Ce premier résultat étant acquis, affinons cette approximation. Pour ce faire, posons, pour $n \geq 1$, $u_n = S_n - \ln(n)$. Alors :

$$\begin{aligned}
u_{n+1} - u_n &= \sum_{k=1}^{n+1} \frac{1}{k} - \ln(n+1) - \sum_{k=1}^{n} \frac{1}{k} + \ln(n) \\
&= \frac{1}{n+1} - \ln\left(\frac{n+1}{n}\right) \\
&= \frac{1}{n+1} - \ln\left(1 + \frac{1}{n}\right) \\
&= \frac{1}{n+1} - \left(\frac{1}{n} - \frac{1}{2n^2} + o\left(\frac{1}{n^2}\right)\right)\,.
\end{aligned}$$

Or :

$$\begin{aligned}\frac{1}{n+1} &= \frac{1}{n}\frac{1}{1+\frac{1}{n}} \\ &= \frac{1}{n}\left(1-\frac{1}{n}+o\left(\frac{1}{n}\right)\right) \\ &= \frac{1}{n}-\frac{1}{n^2}+o\left(\frac{1}{n^2}\right)\end{aligned}$$

et donc, en réinjectant :

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

Ceci nous permet de conclure que $u_n - u_{n+1} \sim \dfrac{1}{2n^2}$ et donc, par comparaison des séries à termes positifs avec la série de Riemann convergente $\sum\limits_{(n\geq 1)} \frac{1}{n^2}$, la série $\sum\limits_{(n\geq 1)} u_n - u_{n+1}$ converge. Par lien suite–série (proposition XXII.3), la suite $(u_n)_n$ converge vers un réel γ, appelée constante d'Euler—Mascheroni (le second, de son prénom Lorenzo, ayant été un mathématicien et abbé cisalpin ; 1750—1800). Obtenir une valeur approchée de cette constante est aisé à l'aide de (par exemple) `python`. On obtient, en un temps raisonnable, $\gamma \approx 0,5772156649$.

```
from numpy import log

def approx_gamma(N):
    S=-log(N)
    for i in range(N):
        S+=1/(i+1)
    return S
```

On obtient donc, *in fine*, le développement asymptotique suivant :

$$\sum_{n=1}^{N} \frac{1}{n} = \ln(N) + \gamma + o(1)\,. \qquad \textbf{(E :XXII.1)}$$

3.– Convergence absolue

a) What ?

Définition XXII.7. On dit qu'une série $\sum u_n$ **converge absolument** si la série à termes positifs $\sum |u_n|$ est convergente.

Exemple XXII.11.

— Les séries à termes positifs convergentes sont absolument convergentes. . .

- La série $\sum\limits_{(n\geq 1)} \frac{(-1)^n}{n^2}$ converge absolument.
- La série $\sum \frac{z^n}{n!}$ est absolument convergente.
- Soit $\alpha = a + ib \in \mathbb{C}$ et soit $n \geq 1$. Alors :

$$\begin{aligned}\left|\frac{1}{n^\alpha}\right| &= \frac{1}{|n^a n^{ib}|} \\ &= \frac{1}{n^a|e^{ib\ln(n)}|} \\ &= \frac{1}{n^a}.\end{aligned}$$

On en déduit que **la série de Riemann** $\sum\limits_{(n\geq 1)} \frac{1}{n^\alpha}$ **converge absolument si et seulement si** $\mathrm{Re}(\alpha) > 1$.

b) Lien à la convergence

Dans le chapitre VII, nous avons démontré que la convergence d'une suite $(u_n)_n$ entraînait celle de $(|u_n|)_n$ avec réciproque fausse. Ce résultat ne se généralise pas aux séries, comme nous le démontrons avec le contre–exemple suivant.

Intéressons nous à la **série harmonique alternée** $\sum\limits_{(n\geq 1)} \frac{(-1)^n}{n}$, dont nous savons qu'elle converge par le critère spécial des séries alternées (propostion XXII.6). Or, elle ne converge pas absolument : la série de ses valeurs absolues est la série harmonique. **Convergence n'implique donc pas PAS convergence absolue pour les séries.**

Histoire de compliquer un peu plus les choses, la réciproque est, quant à elle, vraie. . .

Proposition XXII.13. Toute série absolument convergente est convergente.

Avant de démontrer ce résultat, introduisons une notion dont nous ferons également usage au chapitre XXVIII.

Définition XXII.8. Soit $x \in \mathbb{R}$. On appelle :

- **partie positive** de x le réel
$$x^+ = \begin{cases} x & \text{si } x \in \mathbb{R}_+^* \\ 0 & \text{sinon} \end{cases} \quad ;$$
- **partie négative** de x le réel
$$x^- = \begin{cases} -x & \text{si } x \in \mathbb{R}_-^* \\ 0 & \text{sinon} \end{cases} \quad .$$

Exemple XXII.12. $2^+ = 2$, $(-15)^- = 15$.

Remarque XXII.11. Si $x \in \mathbb{R}$, alors $x = x^+ - x^-$ et $|x| = x^+ + x^-$.

Démonstration. Dans le cas réel, nous avons, pour tout $n \in \mathbb{N}$, $|u_n| = u_n^+ + u_n^-$ et $u_n = u_n^+ - u_n^-$. De fait, les séries $\sum u_n^+$ et $\sum u_n^-$ sont à termes positifs et, pour tout $n \geq 0$, $u_n^{\pm} \leq |u_n|$: par comparaison des séries à termes positifs (proposition XXII.8), ces deux séries convergent si $\sum u_n$ converge absolument, ce qui entraîne la convergence de cette dernière par linéarité.

Dans le cas complexe, on procède de façon similaire avec les séries des parties réelles et imaginaires. □

Exemple XXII.13. Si $\alpha \in \mathbb{C}$ est tel que $\mathrm{Re}(\alpha) > 1$, alors la série de Riemann $\sum\limits_{(n\geq 1)} \frac{1}{n^\alpha}$ converge. Ceci permet de définir la **fonction zêta de Riemann** :

$$\begin{aligned} \zeta : \{z \in \mathbb{C} \,|\, \mathrm{Re}(z) > 1\} &\longrightarrow \mathbb{C} \\ z &\mapsto \sum_{n=1}^{\infty} \frac{1}{n^z}. \end{aligned}$$

Proposition XXII.14. Soit $\sum u_n$ une série absolument convergente. Alors :

$$\left| \sum_{n=0}^{\infty} u_n \right| \leq \sum_{n=0}^{\infty} |u_n|.$$

Démonstration. Passer à la limite dans l'inégalité triangulaire appliquée aux sommes partielles. □

Proposition XXII.15. Soit $u \in \mathbb{C}^{\mathbb{N}}$ et soit $v \in (\mathbb{R}_+)^{\mathbb{N}}$ telles que :
- $u_n = \mathcal{O}(v_n)$;
- $\sum v_n$ converge.

Alors $\sum u_n$ converge absolument.

Démonstration. Par domination, il existe une suite $(h_n)_n$ positive, bornée par $M \in \mathbb{R}_+$ telle que :

$$\exists\, N \in \mathbb{N},\ \forall n \geq N,\ |u_n| \leq h_n v_n$$

et donc, pour $n \geq N$, $|u_n| \leq M v_n$. Par comparaison des séries à termes positifs (proposition XXII.8), on obtient la convergence annoncée. □

Exemple XXII.14. La série $\sum\limits_{(n\geq 1)} \frac{\sin(n)}{n^3}$ converge absolument.

Chapitre XXIII

Groupe symétrique, déterminant

On fixe dans tout ce chapitre un corps $\mathbb{K}$ égal à $\mathbb{R}$ ou $\mathbb{C}$.

1.⁻ Permutations d'un ensemble fini

a) Rappels et compléments

Nous avons eu l'occasion d'évoquer le **groupe symétrique** $(\mathfrak{S}_n, \circ)$ (aussi noté S_n), pour $n \geq 1$, dans le chapitre VIII. Rappelons ici qu'il s'agit du groupe $\mathfrak{S}([\![1,n]\!],[\![1,n]\!])$ des bijections de l'ensemble $[\![1,n]\!]$ vers lui–même (appelées **permutations**). Il s'agit d'un groupe fini possédant $n!$ éléments.

Notation. Soit $\sigma \in \mathfrak{S}_n$; nous utiliserons (temporairement) pour σ la notation "raccourcie" suivante :

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

➠ **Exemple XXIII.1.**

— $\mathfrak{S}_2$ est constitué des permutations $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ et $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$.

— De son côté, $\mathfrak{S}_3$ contient exactement 6 éléments, qui sont $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ et $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

Notation. Pour alléger les calculs, nous nous autoriserons à noter, pour $\sigma, \tau \in \mathfrak{S}_n$, la composition $\sigma \circ \tau$ simplement $\sigma\tau$.

➠ **Exemple XXIII.2.**

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

✖ **Attention :** attention à l'ordre ; une composition se lit de droite à gauche.

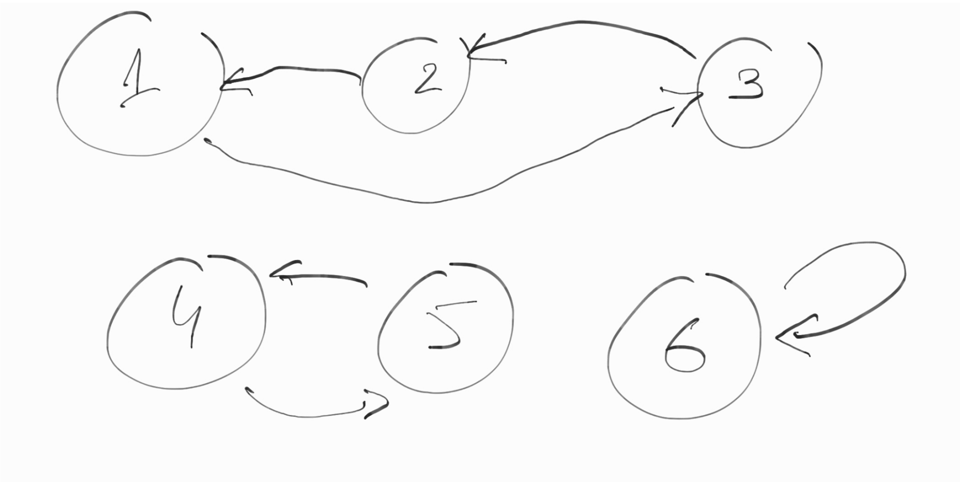
b) Cycles

Vocabulaire. Soit $\sigma \in \mathfrak{S}_n$ et soit $a \in [\![1, n]\!]$; on appelle **orbite de a selon σ** l'ensemble :

$$\{\sigma^k(a) \mid k \in \mathbb{Z}\}$$

où σ^k désigne la composée $\underbrace{\sigma \circ \ldots \circ \sigma}_{k \text{ fois}}$.

➠ **Exemple XXIII.3.** L'orbite d'un point est donc l'ensemble des points atteignables en partant de ce dernier *via* itérations de la permutation σ. Nous représentons ci–dessous les différentes orbites de la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 4 & 6 \end{pmatrix}$.



✌ **Remarque XXIII.1.** Les orbites disjointes selon une permutation $\sigma \in \mathfrak{S}_n$ partitionnent l'ensemble $[\![1, n]\!]$: il s'agit donc de classes d'équivalences.

Notation. La remarque *supra* nous autorise à envisager de noter une permutation comme la liste de ses orbites. Pour calculer l'image d'un point, il nous "suffira" alors de "retracer son chemin" parmi ces dernières. Par exemple, la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 4 & 6 \end{pmatrix}$ se notera :

$$\sigma = (1\ 3\ 2)(4\ 5)(6)\,.$$

Il est aussi conventionnel d'éliminer les orbites triviales de cette notation pour gagner en place et en efficacité. Dans le cas présent, nous noterions :

$$\sigma = (1\ 3\ 2)(4\ 5)\,.$$

➠ **Exemple XXIII.4.** $(1\ 3\ 2)(3\ 2) = (1\ 3)\,.$

Définition XXIII.1. On appelle **cycle** toute permutation admettant une unique orbite non triviale. Cette orbite est alors appelée **support** du cycle et son cardinal **longueur** de celui–ci.

➠ **Exemple XXIII.5.** Le cycle $(1\ 3\ 4) \in \mathfrak{S}_5$ est en fait la permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}.$$

✌ **Remarque XXIII.2.**
— Cette notation est ...cyclique ; par exemple $(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2)$.
— Si σ est un cycle de longueur k dans $\mathfrak{S}_n$ et que a est dans le support de σ, on a :

$$\sigma = (a\ \sigma(a)\ \sigma^2(a)\ \dots\ \sigma^{k-1}(a)).$$

Proposition XXIII.1. Deux cycles de supports disjoints commutent.

Démonstration. Ces deux cycles agissent (non trivialement) sur des ensembles disjoints : l'ordre de composition ne revêt donc aucune importance. □

Théorème XXIII.2.
Toute permutation différente de l'identité peut s'écrire de façon unique (à l'ordre près des facteurs) comme produit de cycles de supports disjoints.

Démonstration. Ce résultat est admis. □

➠ **Exemple XXIII.6.** Pour déterminer la décomposition d'une permutation, il suffit de recopier ses orbites "dans l'ordre". Par exemple :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 5).$$

c) Signature

Définition XXIII.2. On appelle **transposition** tout cycle de longueur 2.

✌ **Remarque XXIII.3.**
— Les permutations sont donc exactement les $(i\ j) \in \mathfrak{S}_n$ avec $i < j$.
— Si $i, j \in [\![1, n]\!]$, alors $(i\ j)^{-1} = (j\ i) = (i\ j)$.

Proposition XXIII.3. Toute permutation de $\mathfrak{S}_n$ peut s'écrire sous la forme d'un produit de transpositions.

Démonstration. Faisons le par récurrence sur $n \geq 1$.
— Pour $n = 1$, c'est trivial : tout élément de $\mathfrak{S}_1$ est produit d'exactement 0 transposition(s). Oui, nous en sommes toujours la après 387 pages de cours...

— Supposons la propriété vérifiée au rang n et soit $\sigma \in \mathfrak{S}_n$; alors on a :

$$\sigma = (n+1\ \sigma(n+1))\sigma'$$

avec $\sigma' \in \mathfrak{S}_n$. Ne reste alors qu'à appliquer l'hypothèse de récurrence.

□

✖ **Attention :** il n'y a pas unicité. En effet, $(1\ 2\ 3) = (1\ 2)(2\ 3) = (2\ 3)(3\ 1)$. La parité du nombre de facteurs reste, par contre, constante pour une permutation donnée (cela est aisé à démontrer par l'absurde).

➠ **Exemple XXIII.7.** Si $a_1, \dots a_k \in [\![1, n]\!]$, on a :

$$(a_1\ a_2\ \dots\ a_k) = (a_1\ a_2)(a_2\ a_3)\dots(a_{k-1}\ a_k)\,.$$

✖ **Attention :** si les orbites se lisent de gauche à droite, la composée, elle, se lit toujours de droite à gauche.

Théorème XXIII.4.
Il existe une unique application $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ telle que :

(i) pour toute transposition τ, $\varepsilon(\tau) = -1$;

(ii) ε est un morphisme de groupes de $(\mathfrak{S}_n, \circ)$ vers $(\{-1, 1\}, \times)$.

Ce morphisme est appelé **signature** sur $\mathfrak{S}_n$.

Démonstration. Admis. □

➠ **Exemple XXIII.8.** Pour calculer la signature de $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$, on la décompose sous forme de produit de transpositions :

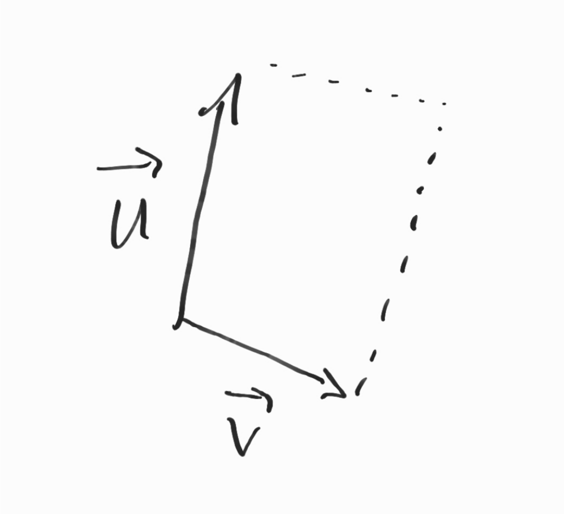
$$\begin{aligned} \varepsilon(\sigma) &= \varepsilon((1\ 2)(3\,5)) \\ &= \varepsilon((1\ 2))\varepsilon((3\,5)) \\ &= (-1)^2 \\ &= 1\,. \end{aligned}$$

✌ **Remarque XXIII.4.** Le noyau de ε est appelé **groupe alterné** et noté $\mathfrak{A}_n$. Il s'agit d'un sous–groupe de $\mathfrak{S}_n$ de cardinal $\dfrac{n!}{2}$ si $n \geq 2$.

2.⁻ Formes multilinéaires alternées

a) Laïus géométrique et définition

Étant donné deux vecteurs $\vec{u}$ et $\vec{v}$ dans $\mathbb{R}^2$, nous pouvons considérer l'aire **algébrique** $\mathscr{A}(\vec{u}, \vec{v})$ du parallélogramme engendré par ceux–ci.



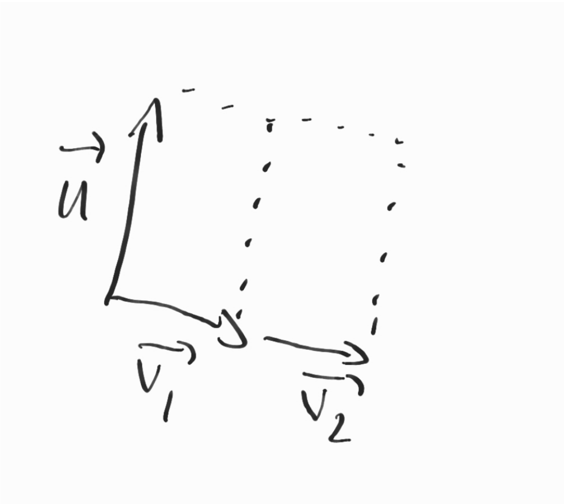
Si $\vec{u} = (a, b)$ et $\vec{v} = (c, d)$, nous avons la formule $\mathscr{A}(\vec{u}, \vec{v}) = ad - bc$. Les propriétés suivantes sont de plus vérifiées :

(i) $\mathscr{A}(\vec{v}, \vec{u}) = -\mathscr{A}(\vec{u}, \vec{v})$;

(ii) pour tout $\lambda \in \mathbb{R}$, $\mathscr{A}(\vec{u}, \lambda\vec{u}) = 0$;

(iii) pour tous vecteurs $\vec{v_1}$ et $\vec{v_2}$, on a

$$\mathscr{A}(\vec{u}, \vec{v_1} + \vec{v_2}) = \mathscr{A}(\vec{u}, \vec{v_1}) + \mathscr{A}(\vec{u}, \vec{v_2}) .$$



Nous pouvons développer la même théorie dans $\mathbb{R}^3$ via la notion de volume algébrique engendré par trois vecteurs. La définition suivante a pour but de proposer une généralisation de ces objets en dimension (éventuellement infinie) quelconque.

Définition XXIII.3. Soient E un $\mathbb{K}$–e.v ; on appelle **forme n–linéaire** sur ces espaces toute application $f : E^n \to \mathbb{K}$ telle que pour tout $i \in [\![1, \ldots, n]\!]$, pour tout $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \in E^n$, l'application

$$\begin{aligned} f_i : E &\longrightarrow \mathbb{K} \\ u &\mapsto f(x_1, \ldots, x_{i-1}, u, x_{i+1}, \ldots, x_n) \end{aligned}$$

est une forme linéaire sur E.

Remarque XXIII.5. Une forme n–linéaire est donc linéaire selon chacune des coordonnées (au sens du produit cartésien) des vecteurs de son ensemble de départ.

Exemple XXIII.9.

— $(x, y) \mapsto xy \in \mathscr{L}_2(\mathbb{K}, \mathbb{K})$;
— le produit scalaire (au sens vu en physique) est une forme 2–linéaire (on dit **bilinéaire**) sur $\mathbb{R}^2$, $\mathbb{R}^3$;
— l'aire et le volume algébriques évoqués dans le laïus géométrique *supra* sont des formes bilinéaire et trilinéaire respectivement.

Définition XXIII.4. Soit E un $\mathbb{K}$–e.v et soit f une forme n–linéaire sur E. On dit que f est **alternée** si pour tout $(x_1, \dots, x_n) \in E^n$ et tout couple $(i, j) \in [\![1, n]\!]$ tel que $i \neq j$ on a :

$$(x_i = x_j) \Rightarrow (f(x_1, \dots, x_n) = 0)\,.$$

b) Quelques propriétés élémentaires

Proposition XXIII.5. Soit E un $\mathbb{K}$–e.v et soit f une forme n–linéaire alternée. Alors pour tout $(x_1, \dots, x_n) \in E^n$ et tout couple $(i, j) \in [\![1, n]\!]$ tel que $i \neq j$ on a :

$$f(x_1, \dots, \underbrace{x_i}_{i}, \dots, \underbrace{x_j}_{j}, \dots, x_n) = -f(x_1, \dots, \underbrace{x_j}_{i}, \dots, \underbrace{x_i}_{j}, \dots, x_n)\,.$$

Démonstration. Pour tout $x_1, \dots, x_n \in E$ et $i \neq j$ dans $[\![1, n]\!]$ on a :

$$\begin{aligned}
0 &= f(x_1, \dots, \underbrace{x_i + x_j}_{i}, \dots, \underbrace{x_i + x_j}_{j}, \dots, x_n)\\
&= f(x_1, \dots, \underbrace{x_i}_{i}, \dots, \underbrace{x_i + x_j}_{j}, \dots, x_n) + f(x_1, \dots, \underbrace{x_j}_{i}, \dots, \underbrace{x_i + x_j}_{j}, \dots, x_n)\\
&= f(x_1, \dots, \underbrace{x_i}_{i}, \dots, \underbrace{x_i}_{j}, \dots, x_n) + f(x_1, \dots, \underbrace{x_i}_{i}, \dots, \underbrace{x_j}_{j}, \dots, x_n)\\
&\quad + f(x_1, \dots, \underbrace{x_j}_{i}, \dots, \underbrace{x_i}_{j}, \dots, x_n) + f(x_1, \dots, \underbrace{x_j}_{i}, \dots, \underbrace{x_j}_{j}, \dots, x_n)\\
&= f(x_1, \dots, \underbrace{x_i}_{i}, \dots, \underbrace{x_j}_{j}, \dots, x_n) + f(x_1, \dots, \underbrace{x_j}_{i}, \dots, \underbrace{x_i}_{j}, \dots, x_n)
\end{aligned}$$

par alternance, d'où le résultat.

□

Remarque XXIII.6. La réciproque est vraie : en effet, pour tout $x_1, \dots, x_n \in E$ et $i \neq j$ dans $[\![1, n]\!]$ on a :

$$f(x_1, \dots, \underbrace{x_i}_{i}, \dots, \underbrace{x_j}_{j}, \dots, x_n) = -f(x_1, \dots, \underbrace{x_j}_{i}, \dots, \underbrace{x_i}_{j}, \dots, x_n)$$

ce qui entraîne que si $x_i = x_j$

$$f(x_1, \dots, x_n) = -f(x_1, \dots, x_n)$$

et donc $f(x_1, \dots, x_n) = 0$.

Notation. On notera $\Lambda_n(E)$ l'ensemble des formes n–linéaires alternées/antisymétriques sur E.

✌ **Remarque XXIII.7.** On peut vérifier que $\Lambda_n(E)$ est un $\mathbb{K}$–e.v.

Proposition XXIII.6. Soit E un $\mathbb{K}$–e.v et soit $f \in \Lambda_n(E)$. Alors, pour toute famille **liée** $(x_1, \dots, x_n) \in E^n$ on a $f(x_1, \dots, x_n) = 0$.

Démonstration. Si la famille est liée, cela signifie que, quitte à modifier l'ordre des x_i (ce qui changera éventuellement le signe de $f(x_1, \dots, x_n)$) il existe $\lambda_1, \dots, \lambda_{n-1} \in \mathbb{K}$ tels que

$$x_n = \sum_{k=1}^{n-1} \lambda_k x_k$$

et donc :

$$\begin{aligned} f(x_1, \dots, x_n) &= f\left(x_1, \dots, x_{n-1}, \sum_{k=1}^{n-1} \lambda_k x_k\right) \\ &= \sum_{k=1}^{n-1} \lambda_k f(x_1, \dots, x_k, , \dots, x_{n-1}, x_k) \\ &= 0\,. \end{aligned}$$

□

Proposition XXIII.7. Soit E un $\mathbb{K}$–e.v et soit $f \in \Lambda_n(E)$. Alors, pour tout $\sigma \in \mathfrak{S}_n$ et tous $x_1, \dots, x_n \in E$, on a :

$$f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \varepsilon(\sigma) f(x_1, \dots, x_n)\,.$$

Démonstration. Écrire σ sous forme de produit de transpositions et développer. □

3.⁻ Déterminant

On fixe dans ce paragraphe un $\mathbb{K}$–e.v de dimension finie E de dimension $n \geq 1$ et une base $\mathscr{B} = (e_1, \dots, e_n)$ de celui–ci.

a) Déterminant d'une famille de vecteurs

Théorème XXIII.8.
Il existe une unique forme $f \in \Lambda_n(E)$ telle que $f(\mathscr{B}) = 1$.

Démonstration. La démonstration de l'existence n'est pas exigible. Pour l'unicité, fixons $f \in \Lambda_n(E)$ et $x_1, \dots, x_n \in E$. Alors, il existe une unique famille $(x_{1,1}, \dots, x_{n,1}, x_{1,2} \dots, x_{n,n})$ de scalaires telle que pour tout $j \in [\![1, n]\!]$ on ait

$$x_j = \sum_{i=1}^{n} x_{i,j} e_i \, .$$

et alors :

$$f(x_1, \dots, x_n) = f\left(\sum_{i=1}^{n} x_{i,1} e_i, \dots, \sum_{i=1}^{n} x_{i,n} e_i\right) .$$

Pour obtenir une intuition du résultat de cette horreur, plaçons nous temporairement dans le cas $n = 2$:

$$\begin{aligned} f(x_1, x_2) &= f(x_{1,1}e_1 + x_{2,1}e_2, x_{1,2}e_1 + x_{2,2}e_2) \\ &= x_{1,1} f(e_1, x_{1,2}e_1 + x_{2,2}e_2) + x_{2,1} f(e_2, x_{1,2}e_1 + x_{2,2}e_2) \\ &= x_{1,1}x_{1,2}(fe_1, e_1) + x_{1,1}x_{2,2} f(e_1, e2) + x_{2,1}x_{1,2} f(e_2, e_1) + x_{2,1}x_{2,2} f(e_2, e_2) \\ &= (x_{1,1}x_{1,2} - x_{2,1}x_{1,2}) f(e_1, e_2) \, . \end{aligned}$$

En développant l'expression multilinéaire de $f(x_1, \dots, x_n))$, nous "intuitons" que tous les termes contenant l'image d'une famille liée seront annulés : ceci entraîne que chaque terme sera de la forme :

$$\prod_{i=1}^{n} x_{\sigma(i),i} f(e_{\sigma(1)}, \dots, e_{\sigma(n)})$$

pour un certain $\sigma \in \mathfrak{S}_n$. Nous démontrons donc, par récurrence sur $n \in \mathbb{N}^*$, que :

$$\begin{aligned} f(x_1, \dots, x_n) &= \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^{n} x_{\sigma(i),i} f(e_{\sigma(1)}, \dots, e_{\sigma(n)}) \\ &= \left(\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} x_{\sigma(i),i}\right) f(e_1, \dots, e_n) \end{aligned}$$

la dernière égalité provenant de la proposition XXIII.7. Ceci entraîne le résultat voulu. □

Définition XXIII.5. L'unique forme $f \in \Lambda_n(E)$ telle que $f(\mathscr{B}) = 1$ est appelée **déterminant dans la base $\mathscr{B}$.**

Notation. $\det_{\mathscr{B}}$

Remarque XXIII.8. On a donc, pour tout $x_1, \dots, x_n \in E$:

$$\det_{\mathscr{B}}(x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} x_{\sigma(i),i}$$

avec les décompositions initales

$$x_j = \sum_{i=1}^{n} x_{i,j} e_i$$

pour $j \in [\![1, n]\!]$. De plus, il est immédiat que :

$$\det_{\mathscr{B}}(e_1, \dots, e_n) = 1$$

par définition.

Exemple XXIII.10. Si $x = (x_1, x_2)$ et $y = (y_1, y_2)$ sont deux vecteurs de $\mathbb{R}^2$ alors leur déterminant dans la bases canonique est :

$$\det(x, y) = x_1 y_2 - x_2 y_1 ,$$

ce qui correspond à la quantité $\mathscr{A}(x, y)$ décrite au début de ce chapitre.

Exercice XXIII.1. Donner une expression du déterminant dans la base canonique de trois vecteurs de $\mathbb{R}^3$. Interprétation géométrique ?

Remarque XXIII.9. La déterminant est une somme de $n!$ produits, dont exactement la moitié sont porteurs d'une signature négative.

Proposition XXIII.9. Soit $f \in \Lambda_n(E)$. Alors il existe un unique $\lambda \in \mathbb{K}$ tel que $f = \lambda \det_{\mathscr{B}}$.

Démonstration. Cela découle du calcul mené dans la démonstration du théorème XXIII.8. Le scalaire λ est en fait égal à $f(e_1, \dots, e_n)$. □

Remarque XXIII.10. Cela signifie que l'espace vectoriel $\Lambda_n(E)$ est de dimension 1 : il s'agit d'une droite.

Proposition XXIII.10. Soit $\mathscr{F} = (x_1, \dots, x_n)$ une famille de vecteurs de E. Alors :

$$\mathscr{F} \text{ est une base de } E \\ \Leftrightarrow \\ \det_{\mathscr{B}}(\mathscr{F}) \neq 0.$$

Démonstration.

($\Downarrow$) Supposons que $\mathscr{F}$ est une base de E. Dans ce cas, on a $\det_{\mathscr{B}}, \det_{\mathscr{F}} \in \Lambda_n(E)$. Ce dernier ensemble étant une droite, il existe $\lambda \in \mathbb{K}$ tel que $\det_{\mathscr{B}} = \lambda \det_{\mathscr{F}}$. Ainsi :

$$\det_{\mathscr{B}}(\mathscr{F}) = \lambda \det_{\mathscr{F}}(\mathscr{F}) = \lambda\,.$$

De plus, $\lambda \neq 0$ car $\det_{\mathscr{B}}(\mathscr{B}) = 1 = \lambda \det_{\mathscr{F}}(\mathscr{B})$.

($\Uparrow$) Supposons désormais que la famille $\mathscr{F}$ ne soit pas une base de E. Comme $\mathrm{card}(\mathscr{F}) = \dim(E)$, elle ne peut donc pas être libre et donc $\det_{\mathscr{B}}(\mathscr{F}) = 0$ par la proposition XXIII.6.

□

Remarque XXIII.11. En "bonus", nous tirons de la démonstration *supra* que pour toute base $\mathscr{B}'$ de E on a :

$$\det_{\mathscr{B}} = \det_{\mathscr{B}}(\mathscr{B}') \det_{\mathscr{B}'}$$

et

$$\det_{\mathscr{B}}(\mathscr{B}') = \frac{1}{\det_{\mathscr{B}'}(\mathscr{B})}\,.$$

b) Déterminant d'une matrice carrée

Définition XXIII.6. Soit $M \in \mathscr{M}_n(\mathbb{K})$. On appelle **déterminant** de M le déterminant de la famille de ses colonnes dans la base canonique de $\mathbb{K}^n$.

Notation. Le déterminant d'une matrice $M = (m_{i,j})_{i,j}$ sera noté $\det(M)$ ou

$$\begin{vmatrix} m_{1,1} & \dots & m_{1,n} \\ \vdots & \ddots & \vdots \\ m_{n,1} & \dots & m_{n,n} \end{vmatrix}.$$

Remarque XXIII.12. Cette définition entraîne que si $A = (a_{i,j})_{i,j} \in \mathscr{M}_n(\mathbb{K})$ on a :

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i}\,.$$

Il en découle, entre autres, que det est une application n–linéaire par rapport aux colonnes de la matrice concernée.

Exemple XXIII.11.
— $\det(I_n) = 1$;
— si $a, b, c, d \in \mathbb{K}$, on a :

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc\,.$$

Exercice XXIII.2. Déterminer une formule explicite pour le déterminant sur $\mathscr{M}_3(\mathbb{K})$.

Proposition XXIII.11. Soit $A, B \in \mathscr{M}_n(\mathbb{K})$ et soit $\lambda \in \mathbb{K}$. Alors :

(i) $\det(A^\top) = \det(A)$;

(ii) $A \in GL_n(\mathbb{K}) \Leftrightarrow \det(A) \neq 0$;

(iii) $\det(AB) = \det(A)\det(B)$;

(iv) $\det(\lambda A) = \lambda^n \det(A)$.

Démonstration.

(i)

$$\begin{aligned}\det(A) &= \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i} \\ &= \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),\sigma^{-1}(\sigma(i))} \\ &= \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{j=1}^{n} a_{j,\sigma^{-1}(j)}\end{aligned}$$

via le changement d'indice $j = \sigma^{-1}(i)$ dans les produits. De plus, $\mathfrak{S}_n$ étant un groupe, on a :

$$\{\sigma^{-1} \mid \sigma \in \mathfrak{S}_n\} = \mathfrak{S}_n \, .$$

Enfin, comme ε est un morphisme de groupes à valeurs dans $\{-1, 1\}$ on obtient l'egalité :

$$\forall \sigma \in \mathfrak{S}_n, \quad \varepsilon(\sigma^{-1}) = \varepsilon(\sigma)^{-1} = \varepsilon(\sigma) \, .$$

et donc :

$$\begin{aligned}\det(A) &= \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{j=1}^{n} a_{j,\sigma(j)} \\ &= \det(A^\top) \, .\end{aligned}$$

(ii) Une matrice est inversible si et seulement si la famille de ses colonnes forme une base de $\mathbb{K}^n$. Ce fait est équivalent à la non–nullité du déterminant de cette famille dans la base mentionnée, d'où le résultat.

(iii) L'application

$$\begin{aligned}\phi : \mathscr{M}_n(\mathbb{K}) &\longrightarrow \mathbb{K} \\ M &\mapsto \det(AM) \, ,\end{aligned}$$

vue comme fonction des colonnes de M, est une forme n–linéaire alternée. De fait, elle est multiple du déterminant dans la base canonique, *i.e* il existe $\lambda \in \mathbb{K}$ tel que :

$$\forall M \in \mathscr{M}_n(\mathbb{K}), \; \det(AM) = \lambda \det(M)$$

En évaluant en $M = I_n$, on trouve que $\lambda = \det(A)$, d'où le résultat.

(iv) L'application det, vue comme fonction des colonnes de la matrice concernée, est n–linéaire.

□

✌ **Remarque XXIII.13.** — Le déterminant réalise donc un morphisme de groupes de $GL_n(\mathbb{K})$ vers $\mathbb{K}^*$.
— Le point (i) implique que, pour tout $n \geq 0$:

$$A_{2n+1}(\mathbb{K}) \cap GL_{2n+1}(\mathbb{K}) = \emptyset\,.$$

Corollaire XXIII.11.a. Soit $A \in GL_n(\mathbb{K})$. Alors $\det(A^{-1}) = \dfrac{1}{\det(A)}$.

Corollaire XXIII.11.b. Le déterminant est un invariant de similitude.

c) Déterminant d'un endomorphisme

Proposition/définition XXIII.7. Soit $f \in \mathscr{L}(E)$. Alors la quantité $\det(\mathrm{mat}_{\mathscr{B}}(f))$ ne dépend pas du choix de la base $\mathscr{B}$ et est appelé **déterminant** de l'endomorphisme f.

Notation. $\det(f)$

Démonstration. Soit $\mathscr{B}'$ une base de E. Alors, en posant $P = P_{\mathscr{B}}^{\mathscr{B}'}$ on a

$$\mathrm{mat}_{\mathscr{B}'}(f) = P^{-1}\mathrm{mat}_{\mathscr{B}}(f)P$$

ergo

$$\begin{aligned}\det(\mathrm{mat}_{\mathscr{B}'}(f)) &= \det(P^{-1}\mathrm{mat}_{\mathscr{B}}(f)P)\\ &= \det(P^{-1})\det(\mathrm{mat}_{\mathscr{B}}(f))\det(P)\\ &= \frac{1}{\det(P)}\det(\mathrm{mat}_{\mathscr{B}}(f))\det(P)\\ &= \det(\mathrm{mat}_{\mathscr{B}}(f))\,.\end{aligned}$$

□

Proposition XXIII.12. Soient $f, g \in \mathscr{L}(E)$ et $\lambda \in \mathbb{K}$. Alors :

(i) $\det(g \circ f) = \det(g)\det(f)$;

(ii) $\det(\lambda f) = \lambda^n \det(f)$;

(iii) $f \in GL(E) \Leftrightarrow \det(f) \neq 0$.

Démonstration. Il s'agit d'un analogue de la proposition XXIII.11. □

✌ **Remarque XXIII.14.** Le déterminant réalise ici un morphisme de groupes de $GL(E)$ vers $\mathbb{K}^*$.

4.⁻ Calculs

Savoir définir un déterminant, c'est bien. Savoir le calculer, c'est...mieux ? Nous laissons le lecteur juge de ce fait.

a) Matrices triangulaires

Proposition XXIII.13. Soit $A = (a_{i,j})_{i,j} \in \mathscr{M}_n(\mathbb{K})$ une matrice **triangulaire**. Alors :

$$\det(A) = \prod_{i=1}^{n} a_{i,i}\,.$$

Démonstration. Supposons, pour fixer les idées, que $A \in T_n^+(\mathbb{K})$. Soit $\sigma \in \mathfrak{S}_n$ différente de l'identité. Alors, il existe nécessairement $i \in [\![1, n]\!]$ tel que $\sigma(i) > i$ et donc $a_{\sigma(i),i} = 0$, ce qui entraîne que :

$$\begin{aligned}\det(A) &= \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \underbrace{\prod_{i=1}^{n} a_{\sigma(i),i}}_{=0 \text{ si } \sigma\neq \mathrm{id}} \\ &= \prod_{i=1}^{n} a_{i,i}\,.\end{aligned}$$

□

Exemple XXIII.12.

— pour tous $d_1, \dots, d_n \in \mathbb{K}$, $\det(\mathrm{diag}(d_1, \dots, d_n)) = d_1 \dots d_n$;

—

$$\begin{vmatrix} 1 & 2 & 51 & 22 & -\pi \\ 0 & 2 & 3 & 6 & 0 \\ 0 & 0 & -1 & 0 & 2 \\ 0 & 0 & 0 & -1 & 42 \\ 0 & 0 & 0 & 0 & 8 \end{vmatrix} = 16\,.$$

Remarque XXIII.15. Ceci se généralise aux matrices triangulaires par blocs **carrés** : si A, B, C sont des matrices alors

$$\det\left(\left(\begin{array}{c|c} A & B \\ \hline 0 & C \end{array}\right)\right) = \det(A)\det(C)$$

et même chose avec les matrices triangulaires par blocs admettant un plus grand nombre de blocs.

b) Impact des opérations élémentaires

Nous avions listé dans le chapitre XII une liste d'opérations élémentaires sur les lignes et colonnes des matrices. Appliquer celles–ci aux **colonnes** d'un déterminant modifie celui–ci de la façon suivante :

(A) échanger la position de deux colonnes ($C_i \leftrightarrow C_j$) multiplie le déterminant par -1 (*antisymétrie*) ;

(B) multiplier une colonne par un scalaire **non nul** ($C_i \leftarrow \lambda C_i$) multiplie le déterminant par ce dernier (*n–linéarité*) ;

(C) ajouter à une colonne une combinaison linéaire des **autres** $\left(C_i \leftarrow C_i + \sum_{j\neq i} \lambda_j C_j\right)$ ne modifie pas le déterminant (*caractère alterné*).

Il est également possible d'agir sur les **lignes** d'un déterminant de la même façon et avec les mêmes effets. Appliquer l'algorithme du pivot de Gauss (*cf.* chapitre XII) pour obtenir un déterminant triangulaire est généralement une bonne idée.

✍ **Exercice XXIII.3.** Soit $x \in \mathbb{C}$. Calculer le déterminant suivant :

$$D_n(x) = \begin{vmatrix} x & 1 & \dots & 1 \\ 1 & x & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \dots & 1 & x \end{vmatrix}.$$

➥ **Correction :** *Commençons par effectuer l'opération $C_1 \leftarrow C_1 + \ldots + C_n$; on obtient*

$$\begin{aligned} D_n(x) &= \begin{vmatrix} x+n-1 & 1 & \dots & \dots & 1 \\ x+n-1 & x & \ddots & & \vdots \\ \vdots & 1 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 1 \\ x+n-1 & 1 & \dots & 1 & x \end{vmatrix} \\ &= (x+n-1) \begin{vmatrix} 1 & 1 & \dots & \dots & 1 \\ 1 & x & \ddots & & \vdots \\ \vdots & 1 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 1 \\ 1 & 1 & \dots & 1 & x \end{vmatrix}. \end{aligned}$$

Nous appliquons ensuite, pour tout $i \geq 2$, $L_i \leftarrow L_i - L_1$, ce qui donne :

$$\begin{aligned} D_n(x) &= (x+n-1) \begin{vmatrix} 1 & 1 & \dots & \dots & 1 \\ 0 & x-1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \dots & 0 & x-1 \end{vmatrix} \\ &= (x+n-1)(x-1)^{n-1}. \end{aligned}$$

c) Développement suivant une ligne ou une colonne

Définition XXIII.8. Soit $A \in \mathscr{M}_n(\mathbb{K})$ et soient $i, j \in [\![1, n]\!]$. On appelle :
- **mineur** d'indices i et j le déterminant de la matrice $\mathrm{Min}_{i,j}(A)$ extraite de A suivant l'ensemble $([\![1, n]\!] \setminus \{i\}) \times ([\![1, n]\!] \setminus \{j\})$;
- **cofacteur** d'indices i et j la quantité $\mathrm{Cof}_{i,j}(A) = (-1)^{i+j}\mathrm{Min}_{i,j}(A)$.

✌ **Remarque XXIII.16.** Le mineur d'indices i et j est donc la matrice obtenue en "rayant" la ligne i et la colonne j de la matrice A.

➠ **Exemple XXIII.13.** Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathscr{M}_2(\mathbb{K})$. Ses mineurs et cofacteurs sont donnés par le tableau récapitulatif *infra*.

i	j	$\mathrm{Min}_{i,j}(A)$	$\mathrm{Cof}_{i,j}(A)$
1	1	d	d
1	2	c	-c
2	1	b	-b
2	2	a	a

✍ **Exercice XXIII.4.** Lister les mineurs et les cofacteurs de la matrice $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$.

◇ Petit calcul sympathique

Soit $A = (a_{i,j})_{i,j} \in \mathscr{M}_n(\mathbb{K})$ et soient $A_1, \ldots, A_n \in \mathbb{K}^n$ ses colonnes (on aura donc $A = (A_1 \,|\, \ldots \,|\, A_n)$). On notera également $\mathscr{B} = (e_1, \ldots, e_n)$ la base canonique de $\mathbb{K}^n$, de façon à avoir, pour tout $j \in [\![1, n]\!]$

$$A_j = \sum_{i=1}^{n} a_{i,j} e_i \,.$$

De fait, à $j \in [\![1, n]\!]$ fixé, on a :

$$\begin{aligned} \det(A) &= \det_{\mathscr{B}}(A_1, \ldots, A_{j-1}, A_j, A_{j+1}, \ldots, A_n) \\ &= \det_{\mathscr{B}}\left(A_1, \ldots, A_{j-1}, \sum_{i=1}^{n} a_{i,j} e_i, A_{j+1}, \ldots, A_n\right) \\ &= \sum_{i=1}^{n} a_{i,j} \det_{\mathscr{B}}\left(A_1, \ldots, A_{j-1}, e_i, A_{j+1}, \ldots, A_n\right) \end{aligned}$$

par n–linéarité du déterminant dans la base $\mathscr{B}$. Dit autrement, cela signifie que nous avons

$$\begin{vmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \ldots & a_{n,n} \end{vmatrix} = \sum_{i=1}^{n} a_{i,j} D_{i,j}$$

avec

$$D_{i,j} = \begin{vmatrix} a_{1,1} & \dots & a_{1,j-1} & 0 & a_{1,j+1} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots & \vdots & & & \vdots \\ \vdots & & a_{i-1,j-1} & 0 & & & \vdots \\ a_{i,1} & \dots & a_{i,j-1} & 1 & a_{i,j+1} & \dots & a_{i,n} \\ \vdots & & \vdots & 0 & \vdots & \ddots & \vdots \\ \vdots & & \vdots & \vdots & \vdots & & a_{n-1,n} \\ a_{n,1} & \dots & a_{n,j-1} & 0 & a_{n,j+1} & \dots & a_{n,n} \end{vmatrix}$$

la colonne "modifiée" étant en j–ième position.

Tout ceci est bien sympathique, mais sommes nous seulement capables de calculer les $D_{i,j}$? Bien entendu, mais rien n'est gratuit...Calculons (avec entrain) ! Quitte à effecteurs les opérations $C_j \leftrightarrow C_{j+1}$, ..., $C_{n-1} \leftrightarrow C_n$ (dans cet ordre), on a :

$$D_{i,j} = (-1)^{n-j} \begin{vmatrix} a_{1,1} & \dots & a_{1,j-1} & a_{1,j+1} & \dots & a_{1,n} & 0 \\ \vdots & \ddots & \vdots & & & \vdots & \vdots \\ \vdots & & a_{i-1,j-1} & & & \vdots & 0 \\ a_{i,1} & \dots & a_{i,j-1} & a_{i,j+1} & \dots & a_{i,n} & 1 \\ \vdots & & \vdots & \vdots & \ddots & \vdots & 0 \\ \vdots & & \vdots & \vdots & & a_{n-1,n} & \vdots \\ a_{n,1} & \dots & a_{n,j-1} & a_{n,j+1} & \dots & a_{n,n} & 0 \end{vmatrix}.$$

Nous opérons ensuite les échanges (ordonnés) suivants : $L_i \leftrightarrow L_{i+1}$, $L_{i+1} \leftrightarrow L_{i+2}$, ..., $L_{n-1} \leftrightarrow L_n$. On a *in fine* :

$$D_{i,j} = \underbrace{(-1)^{2n-(i+j)}}_{} = (-1)^{i+j} \begin{vmatrix} a_{1,1} & \dots & a_{1,j-1} & a_{1,j+1} & \dots & a_{1,n} & 0 \\ \vdots & \ddots & \vdots & & & \vdots & \vdots \\ \vdots & & a_{i-1,j-1} & & & \vdots & 0 \\ \vdots & & \vdots & a_{j+1,j+1} & & \vdots & 0 \\ \vdots & & \vdots & \vdots & \ddots & & \vdots \\ a_{n,1} & \dots & a_{n,j-1} & a_{n,j+1} & \dots & a_{n,n} & 0 \\ a_{i,1} & \dots & a_{i,j-1} & a_{i,j+1} & \dots & a_{i,n} & 1 \end{vmatrix}.$$

Ce déterminant étant triangulaire par blocs, on a immédiatement :

$$D_{i,j} = (-1)^{i+j} \det(\mathrm{Min}_{i,j}(A)) = \mathrm{Cof}_{i,j}(A).$$

Nous déduisons de cette plongée dans le stupre calculatoire, la proposition suivante, fort utile en pratique.

Proposition XXIII.14. Soit $A \in \mathscr{M}_n(\mathbb{K})$ et soit $j \in [\![1, n]\!]$. Alors :

$$\det(A) = \sum_{i=1}^{n} a_{i,j} \mathrm{Cof}_{i,j}(A).$$

Remarque XXIII.17. Ce procédé, appelé **développement selon une colonne** de A admet un pendant relatif aux lignes de celles ci, dont la démonstration est analogue :

$$\forall i \in [\![1,n]\!],\ \det(A) = \sum_{j=1}^{n} a_{i,j}\mathrm{Cof}_{i,j}(A)\,.$$

Exemple XXIII.14. On retrouve aisément de cette façon la formule, pour $a,b,c,d \in \mathbb{K}$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$. Le lecteur audacieux pourra également s'en servir pour obtenir une formule explicite pour le déterminant dans $\mathscr{M}_3(\mathbb{K})$.

Exercice XXIII.5. Soit $x \in \mathbb{C}$ et $n \geq 0$. Calculer le déterminant :

$$D_n = \begin{vmatrix} 1+x^2 & x & 0 & \dots & \dots & 0 \\ x & 1+x^2 & x & 0 & \dots & 0 \\ 0 & x & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & \ddots & x \\ 0 & \dots & \dots & 0 & x & 1+x^2 \end{vmatrix}.$$

Correction : *Soit $n \geq 2$; on commence par opérer un développement par rapport à la première colonne, qui donne :*

$$D_n = (1+x^2)D_{n-1} - x\Delta_{n-1}$$

où

$$\Delta_{n-1} = \begin{vmatrix} x & 0 & 0 & \dots & \dots & 0 \\ x & 1+x^2 & x & 0 & \dots & 0 \\ 0 & x & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & \ddots & x \\ 0 & \dots & \dots & 0 & x & 1+x^2 \end{vmatrix}.$$

En développant Δ_{n-1} par rapport à sa première ligne, on trouve :

$$\Delta_{n-1} = xD_{n-2}$$

ce qui permet in fine d'écrire :

$$D_n = (1+x^2)D_{n-1} - x^2 D_{n-2}\,.$$

On reconnaît une relation de récurrence linéaire d'ordre 2 (cf. chapitre VII). Plus précisément, on a :

$$\begin{aligned} D_n - D_{n-1} &= x^2(D_{n-1} - D_{n-2}) \\ &\ \vdots \\ &= x^{2(n-1)}(D_1 - D_0) \end{aligned}$$

avec $D_0 = 1$ et $D_1 = 1 + x^2$ (en prenant la convention qu'un produit sans terme est égal à 1). Nous terminons donc avec :

$$D_n = D_{n-1} + x^{2n}$$

i.e

$$\begin{aligned} D_n &= \sum_{k=0}^{n} x^{2k} \\ &= \begin{cases} n+1 \text{ si } x = \pm 1 \\ \dfrac{1 - x^{2(n+1)}}{1 - x^2} \text{ sinon.} \end{cases} \end{aligned}$$

◇ **Déterminant de Vandermonde**

Le déterminant suivant est appelé **déterminant de Vandermonde** (en l'honneur d'Alexandre–Théophile Vandermonde, mathématicien, économiste, musicien et chimiste français, 1735—1796).

Proposition XXIII.15. Soit $n \geq 2$ et soient $a_0, \ldots, a_{n-1} \in \mathbb{K}$. Alors :

$$\det((a_i^j)_{i,j \in [\![0,n-1]\!]}) = \prod_{k=1}^{n-1} \prod_{j=0}^{k-1} (a_k - a_j) \,.$$

Démonstration. Posons :

$$\begin{aligned} V_n(a_0, \ldots, a_{n-1}) &= \det((a_i^j)_{i,j \in [\![0,n-1]\!]}) \\ &= \begin{vmatrix} 1 & a_0 & a_0^2 & \ldots & a_0^{n-1} \\ 1 & a_1 & a_1^2 & \ldots & a_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_{n-1} & a_{n-1}^2 & \ldots & a_{n-1}^{n-1} \end{vmatrix} . \end{aligned}$$

Pour calculer ce déterminant, nous effectuons, dans l'ordre **décroissant** de l'indice $k \in [\![2, n]\!]$, l'opération $C_k \leftarrow C_k - a_{n-1} C_{k-1}$, ce qui donne :

$$V_n(a_0, \ldots, a_{n-1}) = \begin{vmatrix} 1 & a_0 - a_{n-1} & a_0(a_0 - a_{n-1}) & \ldots & a_0^{n-2}(a_0 - a_{n-1}) \\ 1 & a_1 - a_{n-1} & a_1(a_1 - a_{n-1}) & \ldots & a_1^{n-2}(a_1 - a_{n-1}) \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_{n-2} - a_{n-1} & a_{n-2}(a_{n-2} - a_{n-1}) & \ldots & a_{n-2}^{n-2}(a_{n-2} - a_{n-1}) \\ 1 & 0 & 0 & \ldots & 0 \end{vmatrix} .$$

Ce déterminant se développe relativement à sa dernière ligne, livrant :

$$V_n(a_0, \ldots, a_{n-1}) = (-1)^{n+1} \begin{vmatrix} a_0 - a_{n-1} & a_0(a_0 - a_{n-1}) & \ldots & a_0^{n-2}(a_0 - a_{n-1}) \\ a_1 - a_{n-1} & a_1(a_1 - a_{n-1}) & \ldots & a_1^{n-2}(a_1 - a_{n-1}) \\ \vdots & \vdots & & \vdots \\ a_{n-2} - a_{n-1} & a_{n-2}(a_{n-2} - a_{n-1}) & \ldots & a_{n-2}^{n-2}(a_{n-2} - a_{n-1}) \end{vmatrix}$$

puis, nous pouvons factoriser, pour tout $k \in [\![1, n-1]\!]$, $a_{k-1} - a_{n-1}$ dans la ligne k, ce qui donne :

$$\begin{aligned} V_n(a_0, \dots, a_{n-1}) &= (-1)^{n+1} \prod_{k=0}^{n-2} (a_k - a_{n-1}) \begin{vmatrix} 1 & a_0 & \dots & a_0^{n-2} \\ 1 & a_1 & \dots & a_1^{n-2} \\ \vdots & \vdots & & \vdots \\ 1 & a_{n-2} & \dots & a_{n-2}^{n-2} \end{vmatrix} \\ &= (-1)^{n-1} \prod_{k=0}^{n-2} (a_k - a_{n-1}) V_{n-1}(a_0, \dots, a_{n-2}) \\ &= \prod_{k=0}^{n-2} (a_{n-1} - a_k) V_{n-1}(a_0, \dots, a_{n-2}) \,. \end{aligned}$$

On obtient donc, par récurrence que :

$$V_n(a_0, \dots, a_{n-1}) = \prod_{k=1}^{n-1} \prod_{j=0}^{k-1} (a_k - a_j) \,.$$

□

✌ **Remarque XXIII.18.**

— On a donc :

$$V_n(a_0, \dots, a_{n-1}) \neq 0$$
$$\Leftrightarrow$$
les a_i sont deux à deux distincts.

— On peut établir un parallèle entre la matrice associée au determinant de Vandermonde et l'interpolation polynomiale. En effet, si $x_0, \dots, x_{n-1}$ et $y_0, \dots, y_{n-1}$ sont des scalaires, trouver un polynôme $P = \sum_{k=0}^{n-1} a_k X^k \in \mathbb{K}_{n-1}[X]$ vérifiant, pour tout $k \in [\![0, n-1]\!]$, $P(x_k) = y_k$ revient à trouver $a_0, \dots, a_{n-1} \in \mathbb{K}$ tels que :

$$\begin{pmatrix} 1 & x_0 & x_0^2 & \dots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \dots & x_{n-1}^{n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ \vdots \\ y_{n-1} \end{pmatrix} .$$

Ce système linéaire est de Cramer si et seulement si $V_n(x_0, \dots, x_{n-1}) \neq 0$, *i.e* si et seulement si les x_k sont deux à deux distincts. Toute ressemblance avec la proposition XIV.22 et les polynômes interpolateurs de Lagrange est non fortuite…

d) Inversion de matrices

Définition XXIII.9. Soit $A \in \mathscr{M}_n(\mathbb{K})$. On appelle **comatrice** de A la matrice de $\mathscr{M}_n(\mathbb{K})$ dont le coefficient en position $(i,j) \in [\![1, n]\!]^2$ est le cofacteur $\mathrm{Cof}_{i,j}(A)$.

Notation. $\mathrm{Com}(A)$

Vocabulaire. La transposée de la comatrice de A est appelée **transcomatrice** de A. On la note $\mathrm{Com}(A)^\top$ ou $\tilde{A}$.

Exemple XXIII.15. Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathscr{M}_2(\mathbb{K})$. Alors :

$$\mathrm{Com}(A)^\top = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Proposition XXIII.16. Soit $A \in \mathscr{M}_n(\mathbb{K})$. Alors :

$$A\mathrm{Com}(A)^\top = \mathrm{Com}(A)^\top A = \det(A) I_n.$$

Démonstration. Notons $a_{i,j}$ les coefficients de A et $b_{i,j}$ ceux de sa transcomatrice. Alors, pour $i \in [\![1, n]\!]$, le coefficient en position (i, i) de la matrice $A\mathrm{Com}(A)^\top$ est :

$$\begin{aligned} \sum_{k=1}^n a_{i,k} b_{k,i} &= \sum_{k=1}^n a_{i,k} \mathrm{Cof}_{i,k}(A) \\ &= \det(A) \end{aligned}$$

via développement selon la ligne i. Si on fixe à présent $j \neq i$, le coefficient en position (i, j) de $A\mathrm{Com}(A)^\top$ est :

$$\sum_{k=1}^n a_{i,k} b_{k,j} = \sum_{k=1}^n a_{i,k} \mathrm{Cof}_{j,k}(A)$$

Il s'agit du déterminant de la matrice B définie comme suit : les lignes de B sont identigues à celles de A, à l'exception de la ligne j que l'on fixe égale à la ligne i de A. Cette matrice ayant deux lignes identiques, elle ne peut être inversible. De fait :

$$\sum_{k=1}^n a_{i,k} \mathrm{Cof}_{j,k}(A) = 0$$

d'où le résultat, quitte à raisonner similairement pour $\mathrm{Com}(A)^\top A$. □

Remarque XXIII.19. Si $A \notin GL_n(\mathbb{K})$, alors $A\mathrm{Com}(A)^\top = 0$. Toute matrice non inversible est donc un diviseur de zéro dans l'anneau $\mathscr{M}_n(\mathbb{K})$.

Corollaire XXIII.16.a. Soit $A \in GL_n(\mathbb{K})$. Alors :

$$A^{-1} = \frac{1}{\det(A)} \mathrm{Com}(A)^\top.$$

➠ **Exemple XXIII.16.** Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{K})$. Alors :

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

✌ **Remarque XXIII.20.** Calculer l'inverse d'une matrice $n \times n$ de cette façon demande de calculer n^2 déterminants de taille $(n-1) \times (n-1)$, soit $n \times n!$ multiplications. Ceci est déraisonnable : le calcul d'un inverse 20×20 demanderait plus de 150 ans sur une machine décente. De son côté, une application de l'algorithme du pivot de Gauss à un système de rang r nécessitera r étapes d'élimination. Dans chacune d'entre elles, nous devons normaliser une ligne ($\approx q$ divisions) et la soustraire à au plus p autres ($\approx q$ multiplications à chaque fois). Dans le cas d'un système de Cramer, avec $A \in GL_n(\mathbb{K})$, nous avons affaire à un nombre d'opérations en $\mathscr{O}(n^3)$. Ceci est **bien plus efficace** : nous donnons, à titre d'illustration, quelques exemples de temps de calcul approximatifs sur une machine effectuant *grosso modo* 10^{10} opérations par seconde (ce qui est raisonnable).

n	Comatrice	Gauss
3	2.10^{-9}s	5.10^{-9}s
5	7.10^{-8}s	2.10^{-8}s
10	4.10^{-3}s	2.10^{-7}s
20	160 ans	2.10^{-6}s
25	10^9 ans	3.10^{-6}s
100	3.10^{142} ans	2.10^{-4}s
1000	10^{2553} ans	$0,2$s

Chapitre XXIV

Probabilités

1.⁻ Notions liminaires

a) Univers

Ce cours sera axé autour de la notion d'**expérience aléatoire**, que nous définissons (informellement) comme une *expérience dont l'issue n'est pas déterminée à l'avance*. On pourra citer comme exemple le classique jet de dé(s), le remplissage d'un QCM, ...

Définition XXIV.1. On appelle **univers** d'une expérience aléatoire l'ensemble, traditionnellement noté Ω, de ses issues possibles.

✖ **ATTENTION :** nous nous limiterons cette année aux cas d'univers **finis**. Notons que cela ne signifie pas "petits"...

➠ **Exemple XXIV.1.**
- Dans le cas d'un jet de dé à 6 faces, l'univers est $\Omega = [\![1, 6]\!]$;
- si on en lance deux, l'univers devient $\Omega = [\![1, 6]\!]^2$;
- l'univers associé à un lancer de pièce ("pile ou face") est $\Omega = \{\text{pile}, \text{face}\}$;
- l'univers associé à une étape d'un jeu de chaises musicales à n personnes est $\Omega = [\![1, n]\!] \times \mathfrak{S}_{n-1}$: il faut "choisir" le perdant, puis placer ses $n-1$ congénères sur les chaises restantes.

b) Événements

On fixe dans ce paragraphe un univers Ω **fini**.

Définition XXIV.2. On appelle **événement** toute partie de l'univers Ω.

➠ **Exemple XXIV.2.** Dans le cas de deux lancers "pile ou face" successifs, $\Omega = \{\text{pile}, \text{face}\}^2$ et l'événement "obtenir au moins une fois 'pile' " correspond à l'ensemble $\{(\text{pile}, \text{pile}), (\text{pile}, \text{face}), (\text{face}, \text{pile})\}$.

Vocabulaire. Plusieurs notions vues dans le chapitre ont un pendant probabiliste rendu explicite par la définition *supra*. Nous les résumons dans le tableau suivant, en fixant deux parties $A, B \subset \Omega$ et un élément $\omega \in \Omega$.

Objet ou propriété	**Nom ensembliste**	**Nom probabiliste**
A	partie	événement
ω	élément	issue
$\{\omega\}$	singleton	événement élémentaire
$\Omega \setminus A$	complémentaire de A	événement contraire de A
$A \cup B$	réunion de A et B	A ou B
$A \cap B$	intersection de A et B	A et B
$\emptyset$	ensemble vide	événement impossible
Ω	tout	événement certain
$A \cap B = \emptyset$	ensembles disjoints	événements incompatibles

➠ **Exemple XXIV.3.** Dans le cas de deux lancers "pile ou face" successifs, l'événement "obtenir au moins une fois 'pile' " est incompatible avec "n'obtenir que 'face' ".

Notation. Dans le cas des probabilités, il est courant et sans ambiguïté de noter $\bar{A}$ l'événement contraire $\Omega \setminus A$.

Définition XXIV.3. On appelle **système complet d'événements** dans Ω toute famille $(A_1, \ldots, A_n)$ d'événements telle que :
- les A_i sont non impossibles (*i.e* non vides) ;
- les A_i sont deux à deux incompatibles (*i.e* deux à deux disjoints) ;
- $$\Omega = \bigsqcup_{i=1}^{n} A_i \,.$$

✌ **Remarque XXIV.1.** Cela signifie que les parties $(A_i)_{i \in [\![1,n]\!]}$ partitionnent (*cf.* chapitre V) l'ensemble Ω. En particulier, on a :

$$\forall \omega \in \Omega, \quad \exists!\, i,\ \omega \in A_i \,.$$

➠ **Exemple XXIV.4.**
- Si A est un événement différent de $\emptyset$ et Ω, alors $(A, \bar{A})$ est un système complet d'événements.
- Dans le cas du lancer successif de 14 dés à 6 faces, les événements $A_i =$"obtenir exactement i fois 1", pour $i \in [\![0, 14]\!]$, forment un système complet d'événements.

c) Variables aléatoires

Nous cherchons dans ce chapitre à modéliser une "quantité" X prenant des valeurs aléatoires, dépendant des événements d'un univers Ω. Mathématiquement parlant, nous formalisons ceci par la définition *infra*.

Définition XXIV.4. On appelle **variable aléatoire** sur Ω toute application $X : \Omega \to E$, avec E un ensemble. Si $E = \mathbb{R}$, on parle de **variable aléatoire réelle ou complexe**.

Remarque XXIV.2. L'ensemble $X(\Omega)$ des valeurs prises par la variable aléatoire X est fini car Ω l'est.

Exemple XXIV.5. Lançons deux dés à 6 faces ; l'univers nous intéressant est alors $\Omega = [\![1, 6]\!]^2$. L'application

$$\begin{aligned} X : \Omega &\to \mathbb{N} \\ (x, y) &\mapsto x + y \end{aligned}$$

est alors une variable aléatoire sur Ω vérifiant $X(\Omega) = [\![2, 12]\!]$.

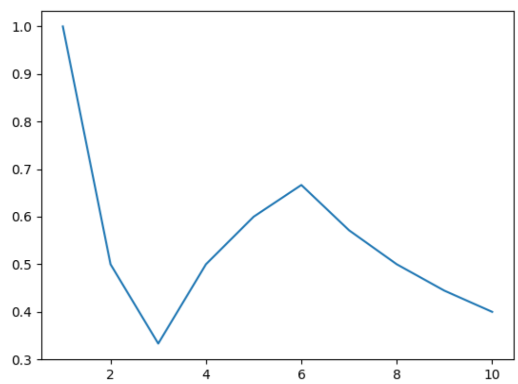
2.– Espaces probabilisés finis

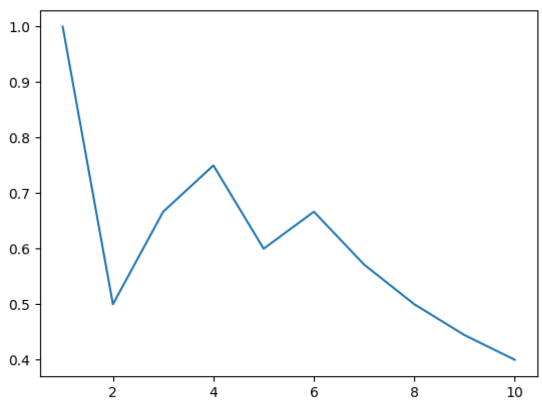
On fixe dans ce paragraphe un univers Ω **fini**.

Considérons l'experience aléatoire suivante : on lance une pièce de monnaie N fois (avec N "grand" et, n'en déplaise à H.P. Lovecraft, entier) et compte le nombre de fois où elle tombe sur "pile", que nous notons N_p. Intuitivement, il nous semble que le quotient $\frac{N_p}{N}$ (correspondant à la fréquence d'apparition de "pile") devrait, pour N suffisamment grand, être proche de $\frac{1}{2}$. Vérifions ceci en pratique, à l'aide du code `python` *infra*.

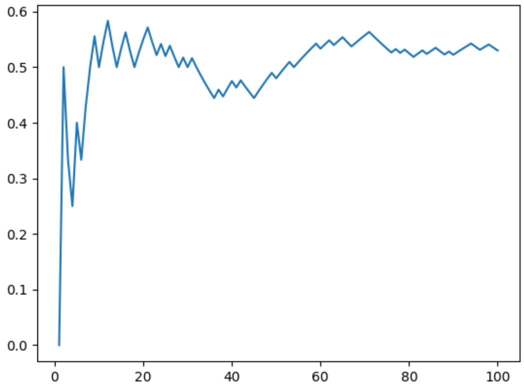
```
from numpy import *
from random import randint
from matplotlib.pyplot import *

def taux(N):
    S=0
    Y=[]
    for k in range(N):
        S+=randint(0,1)
        Y+=[S/(k+1)]
    plot(list(range(1,N+1)), Y)
    show()
```

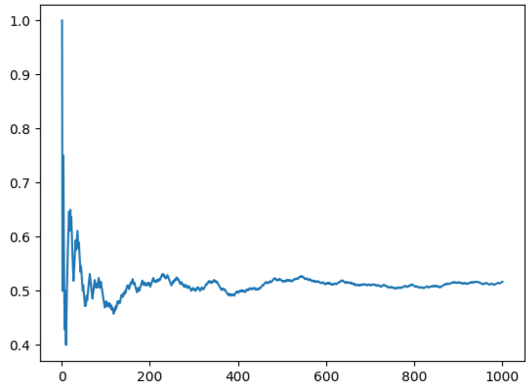
On remarque que les tracés obtenus pour de petits nombres de répétitions de l'expérience accusent une grande variabilité entre deux réalisations ; par exemple pour $N = 10$ on peut obtenir les deux graphes suivants :

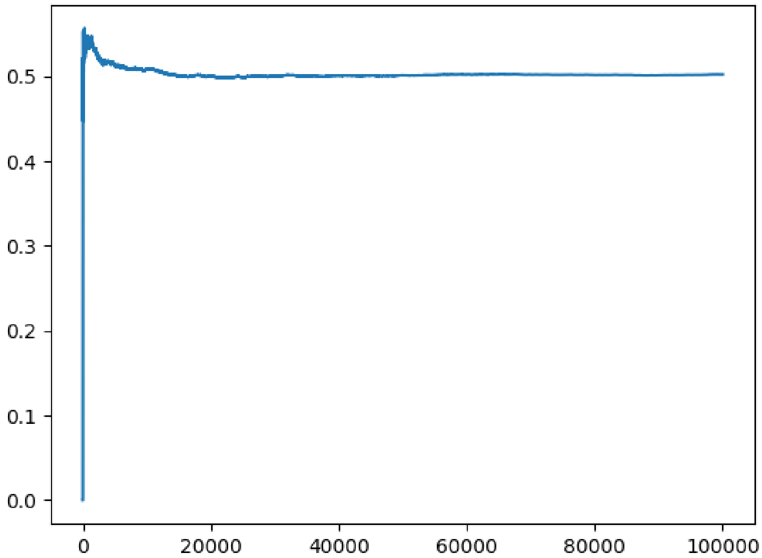




tandis qu'un grand nombre de répétitions a tendance à "lisser" le résultat, comme illustré *infra*.







Il semble donc en effet que la fréquence d'apparition de "pile" se stabilise, lorsque N tend vers l'infini, autour de la valeur $\frac{1}{2}$. Heuristiquement, nous avons la tentation d'avancer que la "chance" d'obtenir "pile" lors d'un tel lancer est de $\frac{1}{2}$; tentation à laquelle nous aller céder, non sans formaliser quelque peu notre cadre d'étude.

a) Notion de probabilité

Définition XXIV.5. On appelle **probabilité** sur l'univers Ω toute application $\mathbb{P} : \mathscr{P}(\Omega) \to [0,1]$ telle que :
- $\mathbb{P}(\Omega) = 1$;
- pour tous événements **incompatibles** A et B on a :

$$\mathbb{P}(A \sqcup B) = \mathbb{P}(A) + \mathbb{P}(B)\,.$$

Le couple $(\Omega, \mathbb{P})$ est alors appelé **espace probabilisé** (fini).

✌ **Remarque XXIV.3.**

— Si $A_1, \dots, A_n$ sont des événements deux à deux incompatibles, on a (par récurrence) :

$$\mathbb{P}\left(\bigsqcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} \mathbb{P}(A_i)\,.$$

— Une probabilité est caractérisée par ses valeurs en chaque événement élémentaire de Ω. En effet, si A est un événement, on a :

$$\begin{aligned}\mathbb{P}(A) &= \mathbb{P}\left(\bigsqcup_{\omega\in A} \{\omega\}\right)\\ &= \sum_{\omega\in A} \mathbb{P}(\{\omega\})\,.\end{aligned}$$

✖ **Attention :** ce raisonnement ne peut en aucun cas être généralisé au cas d'un univers infini.

Définition XXIV.6. On appelle **distribution de probabilités** sur un ensemble I toute famille **presque nulle** $(\lambda_i)_{i\in I}$ **de réels positifs** telle que :

$$\sum_{i\in I} \lambda_i = 1\,.$$

✌ **Remarque XXIV.4.**
— Notons que la somme *supra* est une somme finie.
— Ceci signifie qu'une probabilité $\mathbb{P}$ sur Ω est totalement déterminée par la donnée de la distribution de probabilités $(\mathbb{P}(\{\omega\}))_{\omega\in\Omega}$, et réciproquement.

➠ **Exemple XXIV.6.**
— La probabilité régissant un lancer de pièce de monnaie est caractérisée par $\mathbb{P}(\{\text{pile}\}) = \mathbb{P}(\{\text{face}\}) = \frac{1}{2}$;
— pour un lancer de dé à 6 faces, on a, pour $i \in [\![1, 6]\!]$:

$$\mathbb{P}(\text{obtenir } i) = \frac{1}{6}\,;$$

— le lecteur amateur de magouilles pourra se pencher sur le cas d'un dé pipé.

Proposition XXIV.1. Soit $\mathbb{P}$ une probabilité sur Ω. Alors $\mathbb{P}(\emptyset) = 0$.

Démonstration. L'événement impossible étant incompatible avec lui même (la chance ...), on a :

$$\mathbb{P}(\emptyset) = \mathbb{P}(\emptyset \sqcup \emptyset) = 2\mathbb{P}(\emptyset)$$

d'où le résultat. □

✌ **Remarque XXIV.5.** Il est possible d'avoir un événement A tel que $\mathbb{P}(A) = 1$ et $A \neq \Omega$. Prenons par exemple un pièce truquée pour toujours tomber sur "pile" et A l'événement "obtenir pile". De même, $\mathbb{P}(\text{"obtenir face"}) = 0$ et pourtant l'événement mentionné n'est pas impossible.

Proposition/définition XXIV.7. Il existe une unique probabilité $\mathbb{P}$ sur Ω telle que :

$$\forall \omega, \omega' \in \Omega,\ \mathbb{P}(\{\omega\}) = \mathbb{P}(\{\omega'\})\,.$$

Celle–ci est alors appelée **probabilité uniforme** sur l'univers Ω.

Démonstration. Procédons par analyse–synthèse : si $\mathbb{P}$ est une telle probabilité alors, pour tout $\omega_0 \in \Omega$:

$$\begin{aligned} 1 &= \mathbb{P}(\Omega) \\ &= \sum_{\omega \in \Omega} \mathbb{P}(\{\omega\}) \\ &= \operatorname{card}(\Omega)\mathbb{P}(\{\omega_0\}) \end{aligned}$$

ergo

$$\mathbb{P}(\{\omega_0\}) = \frac{1}{\operatorname{card}(\Omega)}\,.$$

En guise de synthèse, il nous suffit de vérifier que ceci caractérise bien une probabilité sur Ω. □

✌ **Remarque XXIV.6.** Si $\mathbb{P}$ est la probabilité uniforme sur Ω et A est un événement, il est aisé de vérifier que :

$$\mathbb{P}(A) = \frac{\operatorname{card}(A)}{\operatorname{card}(\Omega)}\,.$$

✍ **Exercice XXIV.1.** Quelle est la probabilité d'obtenir au moins un 4 en lançant 3 dés à 6 faces ?

➥ **Correction :** *Cette expérience est régie par la probabilité uniforme $\mathbb{P}$ sur $\Omega = [\![1,6]\!]^3$ car toutes ses issues sont équiprobables. Posons, pour $i \in [\![1,2,3]\!]$ l'événement $A_i =$"obtenir exactement i 4"; alors :*

$$\mathbb{P}(A_i) = \frac{\binom{3}{i}5^{3-i}}{6^3}$$

le coefficient binomial correspondant au choix des jets où le 4 est obtenu et le 5^{3-i} aux choix des valeurs affichées par les autres dés. Par incompatibilité on a alors :

$$\begin{aligned} \mathbb{P}(A_1 \sqcup A_2 \sqcup A_3) &= \frac{\binom{3}{1}5^2}{6^3} + \frac{\binom{3}{2}5}{6^3} + \frac{\binom{3}{3}}{6^3} \\ &= \frac{3 \times 25 + 3 \times 5 + 1}{216} \\ &= \frac{91}{216}\,. \end{aligned}$$

On fixe dans toute la suite de ce chapitre un espace probabilisé $(\Omega, \mathbb{P})$ **fini**.

b) Propriétés générales

Proposition XXIV.2 (Croissance)**.** Soient A, B deux événements tels que $A \subset B$. Alors :

(i) $\mathbb{P}(A) \leq \mathbb{P}(B)$;

(ii) $\mathbb{P}(B \setminus A) = \mathbb{P}(B) - \mathbb{P}(A)$.

Démonstration. Découle trivialement du fait que $B = A \sqcup (B \setminus A)$. □

Corollaire XXIV.2.a. Soit A un événement. Alors $\mathbb{P}(\bar{A}) = 1 - \mathbb{P}(A)$.

✍ **Exercice XXIV.2.** Refaire l'exercice XXIV.1 en utilisant le corollaire XXIV.2.a.

Proposition XXIV.3. Soient A, B deux événements. Alors :

$$\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)\,.$$

Démonstration. Découle, similairement au cas vu pour les cardinaux dans le chapitre XVI, du fait que $A \cup B = (A \setminus A \cap B) \sqcup B$. □

✌ **Remarque XXIV.7.** De façon analogue à ce qui a été fait au chapitre XVI, si A, B et C sont trois événements on a :

$$\begin{aligned}\mathbb{P}(A \cup B \cup C) =& \mathbb{P}(A) + \mathbb{P}(B) + \mathbb{P}(C)\\ & - \mathbb{P}(A \cap B) - \mathbb{P}(A \cap C) - \mathbb{P}(B \cap C)\\ & + \mathbb{P}(A \cap B \cap C)\end{aligned}$$

et on obtient, dans le cas de n événements, un analogue à la formule du crible de Poincaré évoquée dans ce même chapitre.

✌ **Remarque XXIV.8.** On peut, similairement encore une fois à ce qui a été vu au chapitre XVI, démontrer par une récurrence immédiate que pour tous événements $A_1, \ldots, A_n$ on a :

$$\mathbb{P}\left(\bigcup_{i=1}^{n} A_i\right) \leq \sum_{i=1}^{n} \mathbb{P}(A_i)\,.$$

✍ **Exercice XXIV.3.** On lance 3 dés à 6 faces. Déterminer la probabilité que l'on obtienne au moins un 6 ou que la somme des résultats obtenus soit supérieure ou égale à 14.

3.⁻ Probabilités conditionnelles

On fixe dans ce paragraphe un espace probabilisé $(\Omega, \mathbb{P})$ **fini**.

a) Qu'est–ce ?

Définition XXIV.8. Soient A, B deux événements tels que $\mathbb{P}(B) > 0$. On appelle **probabilité (conditionnelle) de** A **sachant** B la quantité

$$\frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)}.$$

Notation. $\mathbb{P}(A|B)$, $\mathbb{P}_B(A)$.

Remarque XXIV.9. Heuristiquement, cette quantité peut être interprétée comme une fréquence : on "compte" le "taux" de cas d'apparition de A et B parmi ceux de B.

Convention. Si A et B sont deux événements tels que $\mathbb{P}(B) = 0$, on s'autorisera à écrire $\mathbb{P}_B(A)\mathbb{P}(B) = 0$.

Exemple XXIV.7. Pour citer une blague connue (parmi les mathématiciens, au moins) : *alors qu'un statisticien passe un contrôle de sécurité dans un aéroport, on découvre une bombe dans sa valise. En garde à vue, il s'explique : "La probabilité d'avoir une bombe dans un avion est certes faible, mais la chance d'avoir deux bombes dans un même avion est infime. Ainsi, je fais ma part pour la sécurité de tous."* Ce statisticien confond probabilité et probabilité conditionnelle.

Proposition XXIV.4. Soit B un événement tel que $\mathbb{P}(B) > 0$. Alors l'application

$$\begin{aligned} \mathbb{P}_B : \mathscr{P}(\Omega) &\to [0,1] \\ A &\mapsto \mathbb{P}_B(A) \end{aligned}$$

est une probabilité.

Démonstration. Laissée en exercice à notre lecteur favori. □

Exercice XXIV.4. On considère une urne contenant r balles de couleur rouge, v balles de couleur verte et rien d'autre. On effectue deux tirages sans remise dans cette urne ; quelle est la probabilité de tirer deux balles vertes ?

Correction : *Notons $N = r + v$ le nombre de balles initialement dans l'urne et A_i (pour $i = 1, 2$) l'événement "le i–ième tirage est une balle verte". Il est clair, par uniformité de la situation que*

$$\mathbb{P}(A_1) = \frac{v}{N}$$

et

$$\mathbb{P}_{A_1}(A_2) = \frac{v-1}{N-1}$$

ce qui entraîne que :

$$\mathbb{P}(A_1 \cap A_2) = \mathbb{P}(A_1)\mathbb{P}_{A_1}(A_2) = \frac{v(v-1)}{N(N-1)}.$$

b) Probabilités composées, probabilités totales

Théorème XXIV.5 (Formules des probabilités composées)**.**
Soient $A_1, \dots, A_n$ des événements tels que $\mathbb{P}\left(\bigcap_{i=1}^{n} A_i\right) > 0$. Alors :

$$\begin{aligned}\mathbb{P}\left(\bigcap_{i=1}^{n} A_i\right) &= \mathbb{P}(A_1)\mathbb{P}_{A_1}(A_2)\mathbb{P}_{A_1\cap A_2}(A_3)\dots\mathbb{P}_{A_1\cap\dots\cap A_{n-1}}(A_n)\\ &= \prod_{i=1}^{n} \mathbb{P}\left(A_i \,\middle|\, \bigcap_{j=1}^{i-1} A_j\right).\end{aligned}$$

Démonstration. Il suffit de remplacer chaque probabilité conditionnelle par leur définition et de simplifier le produit. Le lecteur masochiste trouvera sans doute également plaisant de le démontrer par récurrence sur n (prendre garde à bien quantifier les événements dans l'hypothèse de récurrence dans ce cas). □

✌ **Remarque XXIV.10.** Le lecteur se souvenant encore de sa terminale aura sans doute des flash–backs avec des arbres n'ayant rien à voir avec le Vietnam. Ceci est non fortuit.

✍ **Exercice XXIV.5.** Reprenons l'urne de l'exercice XXIV.4 ; quelle est la probabilité de tirer les r balles rouges à la suite ?

Théorème XXIV.6 (Formules des probabilités totales)**.**
Soit $(A_1, \dots, A_n)$ un système complet d'événements et soit B un événement. Alors :

$$\mathbb{P}(B) = \sum_{i=1}^{n} \mathbb{P}_{A_i}(B)\mathbb{P}(A_i).$$

✌ **Remarque XXIV.11.** On rappelle que si $\mathbb{P}(A_i) = 0$, on s'autorise à écrire $\mathbb{P}_{A_i}(B)\mathbb{P}(A_i) = 0$. Youpi, c'est la fête.

Démonstration. Remarquons que :

$$\begin{aligned}B &= B \cap \Omega\\ &= B \cap \left(\bigsqcup_{i=1}^{n} A_i\right)\\ &= \bigsqcup_{i=1}^{n} A_i \cap B\end{aligned}$$

et donc

$$\begin{aligned}\mathbb{P}(B) &= \mathbb{P}\left(\bigsqcup_{i=1}^{n} A_i \cap B\right) \\ &= \sum_{i=1}^{n} \mathbb{P}(A_i \cap B) \\ &= \sum_{i=1}^{n} \mathbb{P}_{A_i}(B)\mathbb{P}(A_i)\,.\end{aligned}$$

□

✍ **Exercice XXIV.6.** On considère trois usines fabriquant des boulons destiné à un usage bien précis, comme par exemple boulonner des trucs :

— l'usine 1 fournit 10% de la production et accuse un taux de boulons défectueux de 3% ;

— l'usine 2 fournit 50% de la production et accuse un taux de boulons défectueux de 12% ;

— l'usine 3 fournit 40% de la production et accuse un taux de boulons défectueux de 5%.

Démontrer que $8,3\%$ des boulons produits seront au final défectueux.

c) Formules de Bayes

Les résultats exposés dans ce paragraphe ont été formulés (sous une forme plus limitée) par le révérend anglais Thomas Bayes (∼1702—1761) et retrouvés indépendamment par Pierre-Simon de Laplace (français, 1749—1827), mathématicien, astronome, physicien et homme politique de son (ses ?) état(s).

Théorème XXIV.7 (Bayes)**.**
Soient A, B deux événements et soit $(A_1, \dots, A_n)$ un système complet d'événements. On suppose que $\mathbb{P}(A)$, $\mathbb{P}(B)$ et les $\mathbb{P}(A_i)$ sont non nuls. Alors :

(i)
$$\mathbb{P}_B(A) = \frac{\mathbb{P}_A(B)\mathbb{P}(A)}{\mathbb{P}(B)}\ ;$$

(ii)
$$\forall j \in [\![1, n]\!]\ ,\ \mathbb{P}_B(A_j) = \frac{\mathbb{P}_{A_j}(B)\mathbb{P}(A_j)}{\sum\limits_{i=1}^{n} \mathbb{P}_{A_i}(B)\mathbb{P}(A_i)}\,.$$

Démonstration.

(i) On a

$$\mathbb{P}(A \cap B) = \mathbb{P}_B(A)\mathbb{P}(B) = \mathbb{P}_A(B)\mathbb{P}(A)$$

d'où le résultat.

(ii) Soit $j \in [\![1, n]\!]$; alors, d'après le point (i), on a :

$$\mathbb{P}_B(A_j) = \frac{\mathbb{P}_{A_j}(B)\mathbb{P}(A_j)}{\mathbb{P}(B)}.$$

Or, d'après la formule des probabilités totales (théorème XXIV.6) :

$$\mathbb{P}(B) = \sum_{i=1}^{n} \mathbb{P}_{A_i}(B)\mathbb{P}(A_i).$$

ce qui permet de conclure.

□

✍ **Exercice XXIV.7.** En reprenant le cadre de l'exercice XXIV.6, démontrer qu'environ 72% des boulons défectueux proviennent de l'usine 2. *Quid* des usines 1 et 3 ?

4.– Loi d'une variable aléatoire

a) La loi, c'est quoi ?

Commettons quelques crimes contre la rigueur ; pour $X : \Omega \to E$ une variable aléatoire, $x \in E$ et $A \subset E$ on notera :
- $\{X \in A\}$ ou $(X \in A)$ l'événement $X^{-1}(A) = \{\omega \in \Omega \,|\, X(\omega) \in A\}$;
- $\{X = x\}$ ou $(X = x)$ l'événement $X^{-1}(\{x\}) = \{\omega \in \Omega \,|\, X(\omega) = x\}$;
- $\{X \leq x\}$ ou $(X \leq x)$ l'événement $\{\omega \in \Omega \,|\, X(\omega) \leq x\}$ si "$\leq$" est une relation sur E.

Ceci signifie que nous pourrons par exemple chercher à calculer la probabilité $\mathbb{P}(X \in A)$ de l'événement $X^{-1}(A)$; ces notations existent pour mettre l'accent que la partie intéressante de l'étude d'une variable aléatoire n'est pas celle de son mécanisme mais celle des valeurs qu'elle peut prendre, et avec quelle probabilité.

Définition XXIV.9. Soit $X : \Omega \to E$ une variable aléatoire ; on appelle **loi de** X l'application

$$\begin{aligned} \mathbb{P}_X : \mathscr{P}(E) &\to [0, 1] \\ A &\mapsto \mathbb{P}(X \in A). \end{aligned}$$

Notation. Si X, Y sont deux variables aléatoires telles que $\mathbb{P}_X = \mathbb{P}_Y$, on notera $X \sim Y$.

✌ **Remarque XXIV.12.** La loi $\mathbb{P}_X$ est caractérisée par la donnée de la distribution de probabilités $(\mathbb{P}_X(\{x\}))_{x \in E} = (\mathbb{P}(X = x))_{x \in E}$. Si l'on a peur des ensembles infinis (ce qui est triste), on peut remarquer que x parcoure en fait $X(\Omega)$.

➠ **Exemple XXIV.8.** La loi de la somme X des résultats de deux dés à 6 faces est donnée par la tableau suivant.

x	2	3	4	5	6	7	8	9	10	11	12
$\mathbb{P}(X=x)$	$\frac{1}{36}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{9}$	$\frac{5}{36}$	$\frac{1}{6}$	$\frac{5}{36}$	$\frac{1}{9}$	$\frac{1}{12}$	$\frac{1}{18}$	$\frac{1}{36}$

Proposition XXIV.8. Soit X une variable aléatoire ; alors $\mathbb{P}_X$ est une probabilité sur $X(\Omega)$.

Démonstration. Il est rapide de vérifier que $\mathbb{P}_X(X(\Omega)) = \mathbb{P}(X \in X(\Omega)) = 1$. De plus, si A et B sont deux événements incompatibles de $X(\Omega)$, alors :

$$\begin{aligned}\mathbb{P}_X(A \sqcup B) &= \mathbb{P}(X \in A \sqcup B)\\ &= \mathbb{P}(X^{-1}(A \sqcup B))\\ &= \mathbb{P}(X^{-1}(A) \sqcup X^{-1}(B))\\ &= \mathbb{P}(X^{-1}(A)) + \mathbb{P}(X^{-1}(B))\\ &= \mathbb{P}_X(A) + \mathbb{P}_X(B)\end{aligned}$$

d'où le résultat. □

Remarque XXIV.13.
- $X(\Omega)$ est donc lui aussi un univers (fini).
- Par définition de probabilité, si $A \subset E$ on a :

$$\mathbb{P}_X(A) = \sum_{x \in A} \mathbb{P}(X = x)\,.$$

◇ Image d'une variable aléatoire par une application

Fixons une variable aléatoire $X : \Omega \to E$ et une application $f : E \to F$, E et F étant deux ensembles quelconques. Alors l'application $f \circ X : \Omega \to F$ est elle aussi une variable aléatoire ; on la note (malheureusement) $f(X)$. Oui, je sais, nous avons affaire ici à une véritable hérésie notatoire.

Si $A \in \mathscr{P}(F)$ on a par ailleurs :

$$\begin{aligned}\mathbb{P}_{f(X)}(A) &= \mathbb{P}(f(X) \in A)\\ &= \mathbb{P}(X \in f^{-1}(A))\\ &= \mathbb{P}_X(f^{-1}(A))\,.\end{aligned}$$

Proposition XXIV.9. Soient$X, Y : \Omega \to E$ deux variables aléatoires et soit $f : E \to F$ une application. Alors :

$$(X \sim Y) \Rightarrow (f(X) \sim f(Y))\,.$$

Démonstration. Immédiat d'après le calcul *supra.* □

Exercice XXIV.8. Soit X la variable aléatoire correspondant à la somme des résultats d'un lancer de deux dés à 6 faces. Déterminer la loi de $X^2 - X$.

b) Zoologie des lois usuelles

◇ Loi uniforme

Définition XXIV.10. Soit E un ensemble **fini** non vide. On dit qu'une variable aléatoire $X : \Omega \to E$ suit une **loi uniforme** si :

$$\forall x \in E, \quad \mathbb{P}(X = x) = \frac{1}{\text{card}(E)}.$$

Notation. La loi $\mathbb{P}_X$ sera notée $\mathscr{U}(E)$ et on écrira $X \sim \mathscr{U}(E)$ pour indiquer que X suit une loi uniforme. Si $E = [\![1, n]\!]$, on écrira parfois $\mathscr{U}(n)$ au lieu de $\mathscr{U}(E)$.

✌ **Remarque XXIV.14.** Si $X \sim \mathscr{U}(E)$, on a, pour tout $A \subset E$,

$$\mathbb{P}_X(A) = \frac{\text{card}(A)}{\text{card}(E)}.$$

$\mathbb{P}_X$ est donc une probabilité uniforme[1] sur E.

➠ **Exemple XXIV.9.** Un lancer de dé équilibré à 6 faces suit la loi $\mathscr{U}(6)$.

✍ **Exercice XXIV.9.** Soit $X \sim \mathscr{U}(n)$ pour $n \geq 0$. Démontrer que X^2 suit une loi uniforme sur un ensemble que l'on précisera.

◇ Loi de Bernoulli

La loi décrite dans ce paragraphe est nommée en l'honneur du mathématicien suisse Jacques (ou Jakob selon son humeur) Bernoulli (1654—1705), qu'il ne faut pas confondre avec son frère Jean (1667—1748, mathématicien et physicien) ou ses neveux Daniel (1700—1782, médecin, physicien et mathématicien), Nicolas (1695–1726, mathématicien) et (encore) Jean (1710—1790, mathématicien). La prochaine fois que l'un de vos enseignants vous cite un "résultat de Bernoulli", demandez lui "lequel ?" ; effet (et représailles) assuré(es).

Définition XXIV.11. Soit $p \in [0, 1]$. On dit qu'une variable aléatoire $X : \Omega \to \{0, 1\}$ suit une **loi de Bernoulli** de paramètre p si

$$\mathbb{P}(X = 1) = p.$$

Notation. $X \sim \mathscr{B}(p)$

➠ **Exemple XXIV.10.**
- un lancer de pièce équilibrée suit une loi $\mathscr{B}\left(\frac{1}{2}\right)$ (reste à décider qui de pile ou face correspond à 1 et qui correspond à 0) ;
- tirer une balle dans une urne en espérant qu'elle ait une couleur particulière suit une loi de Bernoulli.
- répondre à une question de QCM au hasard suit une loi de Bernoulli.

1. Surprenant, non ?

Remarque XXIV.15.

- Si $X \sim \mathscr{B}(p)$, comme $X(\Omega) \subset \{0,1\}$ alors on a nécessairement $\mathbb{P}(X=0) = 1-p$.
- Les lois de Bernoulli servent à modéliser les expériences aléatoires ayant exactement deux issues (on parle souvent, arbitrairement, de "succès" et "échec", mais cela reste une question de point de vue). Le paramètre p est alors la probabilité de "succès" de notre expérience. Encore une fois, avoir un flash–back arboricole ne semble pas déplacé.

Exercice XXIV.10. Soit $A \subset \Omega$; démontrer que $\mathbb{1}_A$ est variable aléatoire de loi $\mathscr{B}(\mathbb{P}(A))$.

◇ Loi binomiale

Définition XXIV.12. Soit $p \in [0,1]$ et $n \in \mathbb{N}^*$. On dit qu'un variable aléatoire $X : \Omega \to [\![0,n]\!]$ suit une **loi binomiale** de paramètres n et p si :

$$\forall k \in [\![0,n]\!], \quad \mathbb{P}(X=k) = \binom{n}{k} p^k (1-p)^{n-k} .$$

Notation. $X \sim \mathscr{B}(n,p)$

Remarque XXIV.16. La formule *supra* définit bien une probabilité sur $[\![0,n]\!]$; en effet :

$$\sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} = (p+1-p)^n = 1 .$$

Exemple XXIV.11. On considère une urne contenant N balles, dont r rouges ($r \leq N$). Pour tout $n \in \mathbb{N}^*$, la variable aléatoire X correspondant au nombre de balles rouges tirées après n tirages **avec remise** suit la loi $\mathscr{B}\left(n, \dfrac{r}{N}\right)$.

Remarque XXIV.17. La loi $\mathscr{B}(n,p)$ modélise le nombre de succès lors de la répétition de n expériences indépendantes suivant une loi de Bernoulli $\mathscr{B}(p)$. D'ailleurs, $\mathscr{B}(1,p) = \mathscr{B}(p)$, ce qui n'est pas anodin. Nous y reviendrons un peu plus tard (*cf.* proposition XXIV.13).

c) Couples de variables aléatoires

Dans tout ce paragraphe, on fixe deux ensembles E et F et deux variables aléatoires $X : \Omega \to E$ et $Y : \Omega \to F$. On appelle **couple associé à X et Y** la variable aléatoire suivante :

$$\begin{aligned}(X,Y) : \Omega &\longrightarrow E \times F \\ \omega &\mapsto (X(\omega), Y(\omega)) .\end{aligned}$$

Définition XXIV.13. La loi $\mathbb{P}_{(X,Y)}$ du couple (X,Y) est appelée **loi conjointe** de ce dernier. Les lois $\mathbb{P}_X$ et $\mathbb{P}_Y$ sont quant à elles appelées **lois marginales** du couple (X,Y).

Exemple XXIV.12. Le tableau *infra* décrit la loi conjointe d'un couple (X,Y) de variables aléatoires à valeurs dans $\{0,1,2\}^2$.

$\mathbb{P}$	$X=0$	$X=1$	$X=2$
$Y=0$	0.1	0.3	0
$Y=1$	0	0.2	0.2
$Y=2$	0.1	0	0.1

On y lit par exemple que $\mathbb{P}((X,Y)=(0,2))=0.1$. On peut déduire de ces données les lois marginales en sommant les probabilités rencontrées sur les lignes et colonnes comme suit.

$\mathbb{P}$	$X=0$	$X=1$	$X=2$	$\mathbb{P}_Y$
$Y=0$	0.1	0.3	0	0.4
$Y=1$	0	0.2	0.2	0.4
$Y=2$	0.1	0	0.1	0.2
$\mathbb{P}_X$	0.2	0.5	0.3	$\times$

Remarque XXIV.18. De façon générale, il est toujours possible de déterminer les lois marginales à partir de la loi conjointe : si $a\in X(\Omega)$ on a

$$\{X=a\}=\bigsqcup_{b\in Y(\Omega)}(X=a,Y=b)$$

et donc :

$$\mathbb{P}(X=a)=\sum_{b\in Y(\Omega)}\mathbb{P}((X,Y)=(a,b))\,.$$

Symétriquement, pour tout $b\in Y(\Omega)$ on a :

$$\mathbb{P}(Y=B)=\sum_{a\in X(\Omega)}\mathbb{P}((X,Y)=(a,b))\,.$$

✖ **Attention :** il n'est par contre pas en général possible de reconstituer la loi conjointe à partir de la seule donnée des lois marginales. Se référer à l'exemple XXIV.12 pour un contre–exemple.

Proposition/définition XXIV.14. Soit A un événement tel que $\mathbb{P}(A)>0$ et soit X une variable aléatoire ; on appelle **loi conditionnelle de X sachant A** la probabilité

$$\mathbb{P}_{X|A}:\mathscr{P}(X(\Omega))\longrightarrow[0,1]$$
$$B\mapsto\mathbb{P}(B\,|\,A)\,.$$

Remarque XXIV.19. Soit $y\in Y(\Omega)$. Alors

$$(Y=y)=\bigsqcup_{x\in X(\omega)}((X,Y)=(x,y))$$

et donc

$$\begin{aligned}\mathbb{P}(Y=y) &= \sum_{x\in X(\Omega)} \mathbb{P}((X,Y)=(x,y)) \\ &= \sum_{x\in X(\Omega)} \mathbb{P}((X=x)\cap(Y=y)) \\ &= \sum_{x\in X(\Omega)} \mathbb{P}(Y=y\,|\,X=x)\mathbb{P}(X=x)\,.\end{aligned}$$

Ceci signifie que la donnée de $\mathbb{P}_X$ et des lois conditionnelles de Y par rapport à X permet de reconstituer $\mathbb{P}_Y$ (et symétriquement) ainsi que la loi conjointe $\mathbb{P}_{(X,Y)}$.

◇ **Généralisation aux n–uplets de variables aléatoires**

Tout ce que nous venons d'exposer concernant les couples de variables aléatoires se généralise aux n–uplets de telles objets. On conserve la notion de loi conjointe, et on dispose désormais de n lois marginales. Les lois conditionnelles peuvent également être définies de façon analogue à ce qui a été fait *supra*. Les calculs auront une fâcheuse tendance à impliquer des doubles, triples, quadruples sommes et autres joyeusetés.

5.– Indépendance

a) Événements indépendants

Définition XXIV.15. Deux événements A et B sont dits indépendants si $\mathbb{P}(A\cap B)=\mathbb{P}(A)\mathbb{P}(B)$.

Notation. $A \perp\!\!\!\perp B$

✌ **Remarque XXIV.20.** **Si** $\mathbb{P}(B)>0$, alors

$$A \perp\!\!\!\perp B \iff \mathbb{P}_B(A)=\mathbb{P}(A)\,.$$

➠ **Exemple XXIV.13.**
- Les résultats donnés par deux lancers de dés successifs sont indépendants ;
- il en va de même pour les résultats de tirages **avec remise** dans une urne.
- Nous invitons le lecteur à repenser au statisticien évoqué dans un paragraphe précédent et à ses bombes.

Proposition XXIV.10. Soient A, B deux événements indépendants. Alors A et $\overline{B}$ sont indépendants.

Démonstration. Il suffit de remarquer que :

$$\begin{aligned}\mathbb{P}(A) &= \mathbb{P}(A \cap (B \sqcup \overline{B})) \\ &= \mathbb{P}((A \cap B) \sqcup (A \cap \overline{B}) \\ &= \mathbb{P}(A \cap B) + \mathbb{P}(A \cap \overline{B}) \\ &= \mathbb{P}(A)\mathbb{P}(B) + \mathbb{P}(A \cap \overline{B})\end{aligned}$$

et donc :

$$\mathbb{P}(A \cap \overline{B}) = \mathbb{P}(A)(1 - \mathbb{P}(B)) = \mathbb{P}(A)\mathbb{P}(\overline{B})\,.$$

□

Définition XXIV.16. On dit que des événements $A_1, \ldots, A_n$ sont **mutuellement indépendants** lorsque :

$$\forall J \subset [\![1, n]\!], \quad \mathbb{P}\left(\bigcap_{i \in J} A_i\right) = \prod_{i \in J} \mathbb{P}(A_i)\,.$$

✌ **Remarque XXIV.21.**
— Il est clair que l'indépendance mutuelle d'une famille implique l'indépendance deux à deux de ses éléments (prendre J de cardinal 2).
— La proposition XXIV.10 se généralise au cas de n événement smutuellement indépendants.

✖ **Attention :** la réciproque est cependant **fausse**. En effet, sur l'univers $\Omega = [\![1, 4]\!]$ muni de sa probabilité uniforme, les événements $A = \{1, 2\}$, $B = \{1, 3\}$ et $C = \{1, 4\}$ sont deux à deux indépendants tandis que :

$$\mathbb{P}(A \cap B \cap C) \neq \mathbb{P}(A)\mathbb{P}(B)\mathbb{P}(C)\,.$$

b) Variables aléatoires indépendantes

Définition XXIV.17. Soient X et Y deux variables aléatoires ; on dit que X et Y sont **indépendantes** si :

$$\forall (x, y) \in X(\Omega) \times Y(\Omega), \quad \mathbb{P}(X = x, Y = y) = \mathbb{P}(X = x)\mathbb{P}(Y = y)\,.$$

Notation. $X \perp\!\!\!\perp Y$

✌ **Remarque XXIV.22.** Dans ce cas on a, pour tout $y \in Y(\Omega)$, $PP_{X\,|\,Y=y} = \mathbb{P}_X$.

➠ **Exemple XXIV.14.** Si on lance deux fois un dé, la variable aléatoire correspondant au premier résultat obtenu est indépendante de celle correspondant au second.

Proposition XXIV.11. Soient X, Y deux variables aléatoires **indépendantes**. Alors, pour tout $A \subset X(\Omega)$ et tout $B \subset Y(\Omega)$ on a :

$$\mathbb{P}((X, Y) \in A \times B) = \mathbb{P}(X \in A)\mathbb{P}(Y \in B)\,.$$

✌ **Remarque XXIV.23.** Ceci se reformule par :

$$\mathbb{P}_{(X,Y)}(A \times B) = \mathbb{P}_X(A)\mathbb{P}_Y(B)\,.$$

Démonstration. On a :

$$\begin{aligned}
\mathbb{P}((X, Y) \in A \times B) &= \sum_{a \in A} \sum_{b \in B} \mathbb{P}((X, Y) = (a, b)) \\
&= \sum_{a \in A} \sum_{b \in B} \mathbb{P}(X = a, Y = b) \\
&= \sum_{a \in A} \sum_{b \in B} \mathbb{P}(X = a)\mathbb{P}(Y = b) \\
&= \left(\sum_{a \in A} \mathbb{P}(X = a)\right)\left(\sum_{b \in B} \mathbb{P}(Y = b)\right) \\
&= \mathbb{P}(X \in A)\mathbb{P}(Y \in B)
\end{aligned}$$

d'où le résultat. □

Corollaire XXIV.11.a. Soient X, Y deux variables aléatoires **indépendantes**. Alors pour tout $A \subset X(\Omega)$ et tout $B \subset Y(\Omega)$ les événements $(X \in A)$ et $(Y \in B)$ sont indépendants.

Corollaire XXIV.11.b. Soient X et Y deux variables aléatoires indépendantes et soient $f : X(\Omega) \to E$ et $g : Y \to F$ deux applications. Alors (X) et $g(Y)$ sont indépendantes.

c) Généralisation

Définition XXIV.18. Des variables aléatoires $X_1, \dots, X_n$ sont dites **mutuellement indépendantes** (ou simplement **indépendantes**) si pour toute famille d'entiers deux à deux distincts $i_1, \dots, i_k \in [\![1, n]\!]$, tous $(x_{i_1}, \dots, x_{i_k}) \in X_{i_1}(\Omega) \times \ldots \times X_{i_k}(\Omega)$ on a :

$$\mathbb{P}(X_{i_1} = x_{i_1}, \dots, X_{i_k} = x_{i_k}) = \prod_{j=1}^{k} \mathbb{P}(X_{i_j} = x_{i_j})\,.$$

✌ **Remarque XXIV.24.** Une telle famille de variables peut modéliser une suite d'expériences aléatoires indépendantes. Ceci étant souvent modélisé par des arbres en Terminale...

Proposition XXIV.12. Soient $X_1, \dots, X_n$ des variables aléatoires mutuellement indépendantes. Alors pour toute famille $(A_1, \dots, A_n) \in \mathscr{P}(X_1(\Omega)) \times \ldots \times \mathscr{P}(X_n(\Omega))$, les événements $(X_i \in A_i)$ sont mutuellement indépendants.

Démonstration. Trivial. □

Proposition XXIV.13. Soit $p \in [0,1]$ et soient $X_1, \dots, X_n$ des variables aléatoires **mutuellement indépendantes** de loi $\mathscr{B}(p)$. Alors :

$$X_1 + \ldots + X_n \sim \mathscr{B}(n,p)\,.$$

Démonstration. On le fait par récurrence sur n. Le cas $n = 1$ a déjà été traité et si on suppose tout ceci vrai au rang n alors pour toute famille $X_1, \dots, X_{n+1}$ de variables aléatoires mutuellement indépendantes de loi $\mathscr{B}(p)$, en remarquant que la variable X_{n+1} est à valeurs dans $\{0,1\}$ on a, par incompatibilité, indépendance puis hypothèse de récurrence, pour tout $k \in [\![1, n+1]\!]$:

$$\begin{aligned}
\mathbb{P}(X_1 + \ldots + X_{n+1} = k) &= \mathbb{P}(X_{n+1} = 0,\, X_1 + \ldots + X_n = k) \\
&\quad + \mathbb{P}(X_{n+1} = 1,\, X_1 + \ldots + X_n = k-1) \\
&= \mathbb{P}(X_{n+1} = 0)\mathbb{P}(X_1 + \ldots + X_n = k) \\
&\quad + \mathbb{P}(X_{n+1} = 1)\mathbb{P}(X_1 + \ldots + X_n = k-1) \\
&= (1-p)\binom{n}{k} p^k (1-p)^{n-k} + p\binom{n}{k-1} p^{k-1}(1-p)^{n-k+1} \\
&= \left(\binom{n}{k} + \binom{n}{k-1}\right) p^k (1-p)^{n+1-k} \\
&= \binom{n+1}{k} p^k (1-p)^{n+1-k}\,.
\end{aligned}$$

Si $k = 0$, on vérifie par un calcul rapide que tout fonctionne, ce qui permet de conclure. □

Proposition XXIV.14 (Lemme des coalitions)**.** Soient $X_1, \dots, X_n : \Omega \to E$ des variables aléatoires **mutuellement indépendantes**, soit $m \in [\![1, n]\!]$ et soient $f : E^m \to F$ et $g : E^{n-m} \to G$ deux applications. Alors :

$$f(X_1, \dots, X_m) \perp\!\!\!\perp g(X_{m+1}, \dots, X_n)\,.$$

✌ **Remarque XXIV.25.** Ce résultat, dont la preuve est pénible, se généralise au cas de plus de deux "coalitions" ($i.e$ applications).

Chapitre XXV

Espaces préhilbertiens réels

1.⁻ Produits scalaires

a) C'est quoi ?

Définition XXV.1. Soit E un $\mathbb{R}$–e.v ; on appelle **produit scalaire** sur E tout application $\phi : E \times E \to \mathbb{R}$ telle que :

(A) ϕ est une **forme bilinéaire**, *i.e* :

$$\forall x, y, z \in E, \forall \lambda \in \mathbb{R}, \quad \phi(x + \lambda y, z) = \phi(x, z) + \lambda\phi(y, z)$$

et

$$\forall x, y, z \in E, \forall \lambda \in \mathbb{R}, \quad \phi(z, x + \lambda y) = \phi(z, x) + \lambda\phi(z, y) \, ;$$

(B) ϕ est **symétrique**, *i.e* :

$$\forall x, y \in E, \quad \phi(x, y) = \phi(y, x) \, ;$$

(C) ϕ est **définie**, *i.e* :

$$\forall x \in E, \quad (\phi(x, x) = 0) \Rightarrow (x = 0) \, ;$$

(D) ϕ est **positive**, *i.e* :

$$\forall x \in E, \quad \phi(x, x) \geq 0 \, .$$

Notation. Le produit scalaire sur un $\mathbb{R}$–e.v E de deux vecteurs $x, y \in E$ sera souvent noté $\langle x \, , \, y\rangle$, $(x \,|\, y)$ ou $x \cdot y$.

➠ **Exemple XXV.1.**

— Sur $E = \mathbb{R}^n$ avec $n \in \mathbb{N}^*$, on définit le **produit scalaire canonique** de deux vecteurs $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ comme :

$$\langle x \, , \, y\rangle = \sum_{k=1}^{n} x_k y_k \, .$$

Cette formule définit bien un produit scalaire sur $\mathbb{R}^n$ dont la définition coïncide avec celle vue en sciences appliquées pour les dimensions 2 et 3. Notons également que si l'on identifie $\mathbb{R}^n$ à $\mathscr{M}_{n,1}(\mathbb{R})$ on a la formule :

$$\forall x, y \in \mathbb{R}^n, \quad \langle x\,,\,y\rangle = x^\top y\,.$$

— Sur $E = \mathscr{C}^0([a,b])$, on a le produit scalaire suivant :

$$\phi : (f,g) \mapsto \int_a^b f(t)g(t)\,\mathrm{d}t\,.$$

✌ **Remarque XXV.1.** Si $x \in E$ et $\langle \cdot\,,\,\cdot\rangle$ est un produit scalaire sur E, on a :

$$\begin{aligned}\langle x\,,\,0\rangle &= \langle x\,,\,2\cdot 0\rangle\\ &= 2\,\langle x\,,\,0\rangle\end{aligned}$$

et donc $\langle x\,,\,0\rangle = 0 = \langle 0\,,\,x\rangle$.

✍ **Exercice XXV.1.** Démontrer que l'application suivante est un produit scalaire sur $\mathscr{M}_{n,p}(\mathbb{R})$:

$$\begin{aligned}\langle \cdot\,,\,\cdot\rangle : \mathscr{M}_{n,p}(\mathbb{R})^2 &\longrightarrow \mathbb{R}\\ (A,B) &\mapsto \mathrm{Tr}(A^\top B)\,.\end{aligned}$$

Définition XXV.2. On appelle **espace préhilbertien réel** la donnée d'un couple $(E, \langle \cdot\,,\,\cdot\rangle)$, où :
— E est un $\mathbb{R}$–e.v ;
— $\langle \cdot\,,\,\cdot\rangle$ est un produit scalaire sur E.
Si de plus E est de dimension finie, on parle d'**espace euclidien**.

➠ **Exemple XXV.2.** L'exemple précédent met en exergue une structure d'espace préhilbertien réel sur $\mathscr{C}^0([a,b])$ une structure d'espace euclidien sur $\mathbb{R}^n$.

✌ **Remarque XXV.2.** Lorsque la donnée du produit scalaire sera sous–entendue/"évident", nous l'omettrons.

✍ **Exercice XXV.2.** Démontrer que l'application suivante induit sur $\mathbb{R}_n[X]$ une structure d'espace euclidien :

$$\langle \cdot\,,\,\cdot\rangle : (P,Q) \mapsto \int_0^1 P(t)Q(t)\,\mathrm{d}t\,.$$

b) Inégalité de Cauchy–Schwarz

L'inégalité qui suit est nommée en l'honneur du mathématicien français Augustin Louis Cauchy (1789—1857) et de son confrère allemand Hermann Amandus Schwarz (1843—1921), qu'il serait de bon ton de ne pas confondre avec Laurent Schwartz (mathématicien français, 1915—2002).

Proposition XXV.1 (Cauchy–Schwarz)**.** Soit E un espace préhilbertien réel ; alors pour tous $x, y \in E$ on a :

$$\langle x\,,\,y\rangle^2 \leq \langle x\,,\,x\rangle\,\langle y\,,\,y\rangle$$

avec égalité si et seulement si x et y sont colinéaires.

Démonstration. Commençons par remarquer que si $y = 0$, la proposition est relativement aisée à démontrer (même en cas d'électroencéphalogramme plat). Dans le cas contraire, remarquons que si $\lambda \in \mathbb{R}$ on a :

$$0 \leq \langle x + \lambda y \, , \, x + \lambda y \rangle = \langle x \, , \, x \rangle + 2\lambda \langle x \, , \, y \rangle + \lambda^2 \langle y \, , \, y \rangle \; .$$

Nous avons donc la un trinôme du second degré en λ de signe constant (positif) : son discriminant est donc négatif ou nul, *i.e*

$$4 \langle x \, , \, y \rangle^2 - 4 \langle x \, , \, x \rangle \langle y \, , \, y \rangle \leq 0$$

ce qui nous livre l'inégalité désirée.

Concernant le cas d'égalité, ce dernier se produit si et seulement si le discriminant *supra* est nul, et donc si et seulement si notre trinôme admet une racine double, *i.e* un réel α tel que :

$$\langle x + \alpha y \, , \, x + \alpha y \rangle = 0 \, .$$

Par caractère défini du produit scalaire, on a donc que $x + \alpha y = 0$, d'où le résultat. □

➠ **Exemple XXV.3.** Nous pouvons appliquer ce résultat aux produits scalaires vus dans le paragraphe précédent, obtenant les inégalités suivantes :

— $\forall x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{R}^n$,

$$\left(\sum_{k=1}^{n} x_k y_k \right)^2 \leq \left(\sum_{k=1}^{n} x_k^2 \right) \left(\sum_{k=1}^{n} y_k^2 \right) \; ;$$

— $\forall f, g \in \mathscr{C}^0([a, b])$,

$$\left(\int_a^b f(t) g(t) \, \mathrm{d}t \right)^2 \leq \left(\int_a^b f(t)^2 \, \mathrm{d}t \right) \left(\int_a^b g(t)^2 \, \mathrm{d}t \right) \; ;$$

— $\forall A, B \in \mathscr{M}_n(\mathbb{R})$,

$$\mathrm{Tr}(A^\top B)^2 \leq \mathrm{Tr}(A^\top A) \mathrm{Tr}(B^\top B) \, .$$

✍ **Exercice XXV.3.** On note $\ell^2(\mathbb{N})$ l'ensemble des séries $\sum u_n$ de nombres réels telles que $\sum u_n^2$ converge.

1. Démontrer que $\ell^2(\mathbb{N})$ est une $\mathbb{R}$–algèbre commutative.
2. Établir que l'application suivante définit un produit scalaire sur $\ell^2(\mathbb{N})$:

$$(u, v) \mapsto \sum_{n=0}^{\infty} u_n v_n \, .$$

c) Norme euclidienne

Définition XXV.3. Soit $(E, \langle \cdot \, , \, \cdot \rangle)$ un espace préhilbertien réel ; on appelle **norme euclidienne** associée au produit scalaire $\langle \cdot \, , \, \cdot \rangle$ sur E la fonction :

$$\begin{aligned} \| \cdot \| : E &\longrightarrow \mathbb{R}_+ \\ x &\mapsto \sqrt{\langle x \, , \, x \rangle} \, . \end{aligned}$$

Exemple XXV.4.
- Soit $x = (x_1, \dots, x_n) \in \mathbb{R}^n$; alors la norme de x associée au produit scalaire canonique est :
$$\|x\| = \sqrt{\sum_{k=1}^{n} x_k^2}\,;$$
- de même, si $f \in \mathscr{C}^0([a,b])$, on pose :
$$\|f\|_2 = \sqrt{\int_a^b f(t)^2\,\mathrm{d}t}\,.$$
Il s'agit de la norme associée au produit scalaire vu précédemment sur cet espace.

Remarque XXV.3. Notons (avec soulagement) que la norme associée à un produit scalaire est bien définie par positivité de ce dernier.

Exercice XXV.4. Exprimer à l'aide des coefficients de $A \in \mathscr{M}_n(\mathbb{R})$ sa norme associée au produit scalaire $(A, B) \mapsto \mathrm{Tr}(A^\top B)$.

Proposition XXV.2. Soit E un espace préhilbertien réel et soit $x, y \in E$. Alors :
- (i) $\|x\| \geq 0$;
- (ii) $(\|x\| = 0) \Leftrightarrow (x = 0)$;
- (iii) $\forall \lambda \in \mathbb{R}$, $\|\lambda x\| = |\lambda|\,\|x\|$ **[homogénéité]** ;
- (iv) $\|x + y\| \leq \|x\| + \|y\|$ **[inégalité triangulaire]**.

Démonstration. Tout est trivial sauf l'inégalité triangulaire, qui découle de l'inégalité de Cauchy–Schwarz (proposition XXV.1) comme suit :
$$\begin{aligned}
\|x+y\|^2 &= \langle x+y\,,\,x+y\rangle \\
&= \langle x\,,\,x\rangle + 2\langle x\,,\,y\rangle + \langle y\,,\,y\rangle \\
&= \|x\|^2 + 2\langle x\,,\,y\rangle + \|y\|^2 \\
&\leq \|x\|^2 + 2\sqrt{\langle x\,,\,x\rangle\langle y\,,\,y\rangle} + \|y\|^2 \\
&= \|x\|^2 + 2\|x\|\|y\| + \|y\|^2 \\
&= (\|x\| + \|y\|)^2\,.
\end{aligned}$$
□

Exercice XXV.5. En s'inspirant des résultats analogues vus dans les chapitres III et VI, démontrer que si x, y sont deux points d'un espace préhilbertien réel on a :
$$\|x - y\| \geq \big|\,\|x\| - \|y\|\,\big|\,.$$

Remarque XXV.4.
- Le cas d'égalité dans l'inégalité triangulaire se produit lorsque il y a égalité dans l'inégalité de Cauchy–Schwarz, *i.e* si et seulement si x et y sont colinéaires.

— Muni de la norme associée à un espace préhilbertien réel E, il nous est possible de reformuler l'inégalité de Cauchy–Schwarz (proposition XXV.1) de la façon suivante :

$$\forall x, y \in E, \quad |\langle x\,,\,y\rangle| \leq \|x\|\|y\|\,.$$

On en déduit que, si $x, y \neq 0$:

$$\frac{\langle x\,,\,y\rangle}{\|x\|\|y\|} \in [-1, 1]\,,$$

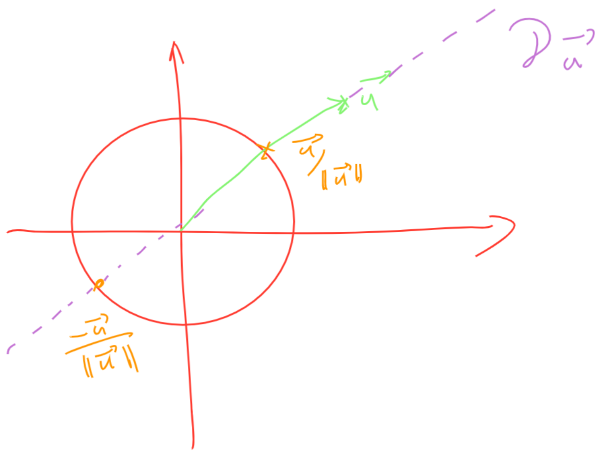
ce qui indique que la quantité suivante, appelée **écart angulaire** entre x et y, est dans $[0, \pi]$:

$$\theta_{x,y} = \arccos\left(\frac{\langle x\,,\,y\rangle}{\|x\|\|y\|}\right) \in [0, \pi]\,.$$

En dimension 2 ou 3, ceci coïncide avec la notion éponyme vue en sciences appliquées.

Définition XXV.4. Un vecteur de norme 1 est dit **unitaire**.

✌ **Remarque XXV.5.** Un vecteur non nul u d'un espace préhilbertien réel est colinéaire à exactement deux vecteurs unitaires : $\frac{u}{\|u\|}$ et $-\frac{u}{\|u\|}$. Notons que ce résultat n'est vrai que parce que nous travaillons sur des $\mathbb{R}$–e.v.



De plus, **en dimension** 2, si l'on pose $(x, y) = \frac{u}{\|u\|}$ on a naturellement $x^2 + y^2 = 1$, ce qui entraîne qu'il existe $\theta \in \mathbb{R}$ tel que $x = \cos(\theta)$ et $y = \sin(\theta)$. On en déduit que l'on peut écrire $x = r\cos(\theta)$ et $y = r\sin(\theta)$, avec $r = \|u\|$. Le couple (r, θ) détermine le vecteur u ; on parle de **coordonnées polaires** de ce dernier.

d) Distance euclidienne

Définition XXV.5. Soit E un espace préhilbertien réel ; on appelle **distance euclidienne** sur E l'application

$$\begin{aligned} d : E \times E &\to \mathbb{R}_+ \\ (x, y) &\mapsto \|y - x\|\,. \end{aligned}$$

Exemple XXV.5. On retrouve sur $\mathbb{R}^2$ et $\mathbb{R}^3$ la notion de distance vues en sciences physiques et de l'ingénieur.

Proposition XXV.3. Soit E un espace préhilbertien réel et soient $x, y, z \in E$. Alors :

(i) $d(x, y) \geq 0$;

(ii) $(d(x, y) = 0) \Leftrightarrow (x = y)$;

(iii) $d(x, y) = d(y, x)$;

(iv) $d(x, z) \leq d(x, y) + d(y, z)$.

Démonstration. Tout ceci découle trivialement des propriétés de la norme euclidienne. □

Exercice XXV.6. Soit $f : x \mapsto x$ et $g : x \mapsto x^2$. Déterminer $d(f, g)$ dans $\mathscr{C}^0([0, 1])$.

e) Formulaire

Nous concluons ce paragraphe par une compilation de formules usuelles, dont la démonstration est laissée à la discrétion du lecteur, qui se révéleront sans nul doute fort utiles en pratique. Pour tout espace préhilbertien réel E et tous $x, y \in E$, on a :

(i)
$$\|x + y\|^2 = \|x\|^2 + 2\langle x\,,\, y\rangle + \|y\|^2\ ;$$

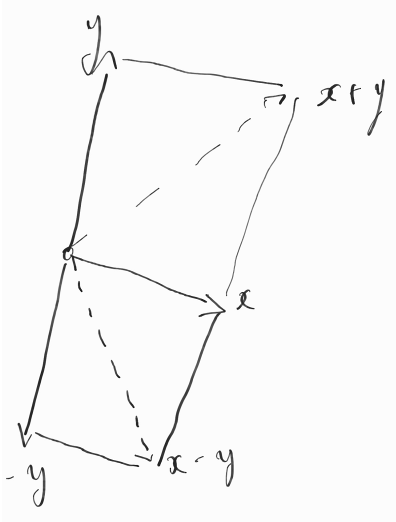
(ii)
$$\|x - y\|^2 = \|x\|^2 - 2\langle x\,,\, y\rangle + \|y\|^2\ ;$$

(iii)
$$\langle x\,,\, y\rangle = \frac{1}{2}(\|x + y\|^2 - \|x\|^2 - \|y\|^2)\ ;$$

(iv)
$$\langle x\,,\, y\rangle = \frac{1}{4}(\|x + y\|^2 - \|x - y\|^2)\ ;$$

(v)
$$\|x + y\|^2 + \|x - y\|^2 = 2(\|x\|^2 + \|y\|^2)\,.$$

Les égalités (iii) et (iv) sont appelées **formules de polarisation** et établissent le fait que la donnée d'un produit scalaire est équivalente à celle de sa norme euclidienne associée. Le point (v) est connu sous le nom **d'identité du parallélogramme** et peut être visualisée géométriquement en dimension 2 (*cf. infra*).



2.⁻ Orthogonalité

On fixe dans ce paragraphe un espace préhilbertien réel E.

a) Vecteurs orthogonaux

Définition XXV.6. Deux vecteurs $x, y \in E$ sont dits **orthogonaux** si $\langle x\,,\,y\rangle = 0$.

Notation. Si x et y sont orthogonaux, on notera $x \perp y$.

Exemple XXV.6.
- Les vecteurs $(1,0)$ et $(0,1)$ sont orthogonaux dans $\mathbb{R}^2$;
- les fonctions $x \mapsto x^2$ et $x \mapsto x$ sont orthogonales dans $\mathscr{C}^0([-1,1])$ (mais pas dans $\mathscr{C}^0([0,1])$).

Remarque XXV.6.
- Le vecteur nul est orthogonal à tout vecteur de E. Réciproquement, si $x \in E$ est orthogonal à tout vecteur de E, alors $\langle x\,,\,x\rangle = 0$ et donc $x = 0$.
- Comme le produit scalaire est une forme bilinéaire symétrique on a, pour tous $x, y \in E$, $(x \perp y) \Leftrightarrow (y \perp x)$.
- Si $x, y \neq 0$ sont orthogonaux, $\theta_{x,y} = \dfrac{\pi}{2}$.

Exercice XXV.7. Soit E un espace euclidien.

1. Pour $a \in E$, montrer que l'application
$$\begin{aligned}\varphi_a : E &\to \mathbb{R}\\ x &\mapsto \langle a\,,\,x\rangle\end{aligned}$$
est une forme linéaire.
2. Démontrer que $a \mapsto \varphi_a$ réalise un isomorphisme (canonique) de E vers son dual E^*.

➥ **Correction :**

1. *Trivial*
2. *On vérifie que* $\mathrm{Ker}(\varphi) = \{0\}$ *car* 0 *est le seul vecteur orthogonal à tout élément de* E*. L'application* φ *est donc injective, ergo bijective car dim*$(E) = \dim(E^*)$.

Définition XXV.7. Une famille $(x_i)_{i\in I}$ de vecteurs de E est dite **orthogonale** si :

$$\forall (i,j) \in I^2,\ (i \neq j) \Rightarrow (x_i \perp x_j)\,.$$

Si de plus les x_i sont tous unitaires, on parle de **famille orthonormée** (ou orthonormale).

✌ **Remarque XXV.7.** Une famille $(x_i)_{i\in I} \in E^I$ est donc orthonormée si et seulement si :

$$\forall (i,j) \in I^2,\ \langle x_i\,,\, x_j\rangle = \delta_{i,j}\,.$$

➠ **Exemple XXV.7.**

— La base canonique de $\mathbb{R}^n$ est orthonormée pour le produit scalaire canonique.

— La famille $(x \mapsto x^3, x \mapsto 1, x \mapsto x^7)$ n'est pas orthogonale dans $\mathscr{C}^0([-1,1])$.

Proposition XXV.4. Toute famille orthogonale de vecteurs **non nuls** est libre.

Démonstration. Soit $(x_i)_{i\in I} \in E^I$ une famille orthogonale telle que $\forall i \in I,\ x_i \neq 0$. Alors, si il existe $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ et $i_1, \dots, i_n \in I$ tels que $\sum_{k=1}^{n} \lambda_k x_{i_k} = 0$ on a, pour tout $j \in [\![1, n]\!]$:

$$\begin{aligned} 0 &= \left\langle \sum_{k=1}^{n} \lambda_k x_{i_k}\,,\, x_{i_j} \right\rangle \\ &= \sum_{k=1}^{n} \lambda_k \underbrace{\left\langle x_{i_k}\,,\, x_{i_j}\right\rangle}_{=0 \text{ si } k\neq j} \\ &= \lambda_j \|x_{i_j}\|^2 \end{aligned}$$

et donc $\lambda_j = 0$, ce qui livre le résultat voulu. □

Le théorème suivant est nommé en l'honneur du philosophe grec Pythagore de Samos (VI^e siècle avant J.–C.), auquel on attribue le cas particulier du triangle en dimension 2. On trouve cependant des traces d'un résultat similaire à ce dernier plus de mille ans auparavant en Mésopotamie. Concernant la démonstration, la plus ancienne qui nous soit connue est due à Euclide (300 av. J.–C.).

Théorème XXV.5 (Pythagore)**.**
Soit $(x_1, \dots, x_n)$ une famille **orthogonale** de vecteurs de E. Alors :

$$\left\| \sum_{k=1}^{n} x_k \right\|^2 = \sum_{k=1}^{n} \|x_k\|^2\,.$$

✌ **Remarque XXV.8.** Si $n = 2$, la réciproque est vraie : en effet, pour toute famille $(x, y) \in E^2$ telle que $\|x + y\|^2 = \|x\|^2 + \|y\|^2$, on a :

$$\begin{aligned}\langle x\,,\, y\rangle &= \frac{1}{2}(\|x+y\|^2 - \|x\|^2 - \|y\|^2) \\ &= \frac{1}{2}(\|x\|^2 + \|y\|^2 - \|x\|^2 - \|y\|^2) \\ &= 0\end{aligned}$$

et donc (x, y) est orthogonale. Ceci devrait rappeler au lecteur quelques souvenirs collégiens.

Démonstration. Calculons :

$$\begin{aligned}\left\|\sum_{k=1}^{n} x_k\right\|^2 &= \left\langle \sum_{k=1}^{n} x_k\,,\, \sum_{j=1}^{n} x_j \right\rangle \\ &= \sum_{k=1}^{n}\sum_{j=1}^{n} \underbrace{\langle x_k\,,\, x_j\rangle}_{=0 \text{ si } j\neq k} \\ &= \sum_{k=1}^{n} \langle x_k\,,\, x_k\rangle \\ &= \sum_{k=1}^{n} \|x_k\|^2 .\end{aligned}$$

□

b) Orthogonal d'une partie

Définition XXV.8. Soit $A \subset E$ une **partie** de E. On appelle **orthogonal** de A l'ensemble

$$A^{\perp} = \{y \in E \,|\, \forall x \in A,\ \langle x\,,\, y\rangle = 0\}.$$

✌ **Remarque XXV.9.** L'orthogonal de A est donc l'ensemble des vecteurs de E orthogonaux à tous ceux de A.

➠ **Exemple XXV.8.** Posons $A = \{(1, 1, -1)\} \subset \mathbb{R}^3$. Alors, pour tout $(a, b, c) \in \mathbb{R}^3$, on a :

$$\begin{aligned}(a, b, c) \in A^{\perp} &\Leftrightarrow \langle (1, 1, -1)\,,\, (a, b, c)\rangle = 0 \\ &\Leftrightarrow a + b - c = 0\end{aligned}$$

et donc $A^{\perp}$ est l'hyperplan de $\mathbb{R}^3$ d'équation $x+y-z = 0$. Une base de cet hyperplan est $((1, 0, 1), (1, 1, -2))$.

✍ **Exercice XXV.8.** Déterminer l'orthogonal du plan d'équation $x + 2y - z = 0$ dans $\mathbb{R}^3$.

Proposition XXV.6. Soient $A, B \in \mathscr{P}(E)$. Alors :

(i) $E^{\perp} = \{0\}$ et $\{0\}^{\perp} = E$;

(ii) $A^{\perp}$ est un s–e.v de E ;

(iii) $(A \subset B) \Rightarrow (B^{\perp} \subset A^{\perp})$;

(iv) $A^{\perp} = \text{Vect}(A)^{\perp}$;

(v) $A \subset (A^{\perp})^{\perp}$.

Démonstration.

(i) Immédiat.

(ii) $A^{\perp}$ est bien une partie de A contenant 0. De plus, pour tous $x, y \in A^{\perp}$ et $\lambda \in \mathbb{R}$ on a :

$$\forall a \in A,\ \langle x + \lambda y\,,\, a\rangle = \langle x\,,\, a\rangle + \lambda \langle y\,,\, a\rangle \\ = 0$$

et donc $x + \lambda y \in A^{\perp}$, d'où le résultat.

(iii) Supposons $A \subset B$ et fixons $x \in B^{\perp}$. Alors, pour tout $y \in B$, $\langle x\,,\, y\rangle = 0$ et donc, comme $A \subset B$, ceci reste vrai pour tout $y \in A$. *In fine*, $B^{\perp} \subset A^{\perp}$.

(iv) Comme $A \subset \text{Vect}(A)$, on par le point précédent que $\text{Vect}(A)^{\perp} \subset A^{\perp}$. Réciproquement, tout vecteur orthogonal à A sera (par bilinéarité du produit scalaire) orthogonal à toute combinaison linéaires d'éléments de cet ensemble, d'où l'inclusion réciproque.

(v) Soit $x \in A$ et $y \in A^{\perp}$. Alors $\langle x\,,\, y\rangle = 0$ et donc $x \perp y$, ce qui entraîne que $x \in (A^{\perp})^{\perp}$.

□

c) Algorithme de Gram–Schmidt

Le procédé exposé ici a été publié en 1883 par le mathématicien danois Jørgen Pedersen Gram (1850—1916) avant d'être reformulé par Erhard Schmidt (allemand, 1876—1959). On trouve un procédé analogue dans les écrits de Pierre–Simon de Laplace (mathématicien, astronome et physicien français, 1749—1827). Il permet, étant donné une base d'un espace euclidien, de la transformer en une base orthogonale ou orthonormée de ce même espace (on parle parfois de **procédé d'orthonormalisation**).

Théorème XXV.7 (Gram–Schmidt)**.**
Soit E un espace préhilbertien réel et soit $\mathscr{B} = (e_1, \dots, e_n)$ une famille libre E. Alors il existe une famille **orthogonale** $\mathscr{B}' = (u_1, \dots, u_n)$ de E telle que :

$$\forall k \in [\![1, n]\!], \quad \text{Vect}(e_1, \dots e_k) = \text{Vect}(u_1, \dots, u_k)\,.$$

Démonstration. Posons $u_1 = e_1$, puis pour tout $k \in [\![1, n-1]\!]$:

$$u_{k+1} = e_{k+1} - \sum_{i=1}^{k} \frac{\langle e_{k+1}\,,\, u_i\rangle}{\|u_i\|^2} u_i\,.$$

Nous démontrons ensuite par récurrence sur $k \in [\![1, n]\!]$ que :

(i) $\mathrm{Vect}(e_1, \dots e_k) = \mathrm{Vect}(u_1, \dots, u_k)$;

(ii) $u_k \in \{u_1, \dots, u_{k-1}\}^\perp$ pour $k \geq 2$.

— $k = 1$: trivial.

— Supposons la propriété vraie au rang k ; le premier point est alors vérifié au rang $k+1$ par construction de u_{k+1}, il ne nous reste donc plus qu'à vérifier la condition d'orthogonalité. Pour ce faire, fixons $j \in [\![1, k]\!]$ et notons que :

$$\begin{aligned}
\langle u_{k+1}\,,\, u_j\rangle &= \left\langle e_{k+1} - \sum_{i=1}^{k} \frac{\langle e_{k+1}\,,\, u_i\rangle}{\|u_i\|^2} u_i\,,\, u_j \right\rangle \\
&= \langle e_{k+1}\,,\, u_j\rangle - \sum_{i=1}^{k} \frac{\langle e_{k+1}\,,\, u_i\rangle}{\|u_i\|^2} \underbrace{\langle u_i\,,\, u_j\rangle}_{=0 \text{ si } i\neq j} \\
&= \langle e_{k+1}\,,\, u_j\rangle - \frac{\langle e_{k+1}\,,\, u_j\rangle}{\|u_j\|^2} \|u_j\|^2 \\
&= 0
\end{aligned}$$

d'où le résultat. Notons que la famille $(u_1, \dots, u_n)$ est bien une base car orthogonale (donc libre) et génératrice car $\mathrm{Vect}(e_1, \dots e_n) = \mathrm{Vect}(u_1, \dots, u_n)$. □

Remarque XXV.10. L'expression des vecteurs u_k peut être obtenue par analyse–synthèse, en cherchant u_{k+1} sous la forme $e_{k+1} + \omega$, avec $\omega \in \mathrm{Vect}(u_1, \dots, u_k)$.

Exemple XXV.9. Il est possible d'orthogonaliser la base $((1,0),(1,1))$ de $\mathbb{R}^2$ pour le produit scalaire canonique grace à ce procédé : on obtient $u_1 = (1,0)$ et

$$\begin{aligned}
u_2 &= (1,1) - \frac{\langle (1,1)\,,\,(1,0)\rangle}{\|(1,0)\|^2} \cdot (1,0) \\
&= (1,1) - (1,0) \\
&= (0,1)\,.
\end{aligned}$$

Corollaire XXV.7.a. Tout espace euclidien admet une base orthonormée.

Démonstration. Nous savons par le théorème de la base incomplète (XIX.2) qu'un tel espace admet une base. Via l'algorithme de Gram–Schmidt (théorème XXV.7), nous obtenons une base orthogonale de E, notée $(u_1, \dots, u_n)$. Une base orthonormée de E est alors donnée par la famille $\left(\frac{u_1}{\|u_1\|}, \dots, \frac{u_n}{\|u_n\|}\right)$. □

Exercice XXV.9. Déterminer une base orthonormée de $\mathbb{R}_2[X]$.

✌ **Remarque XXV.11.** Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base **orthonormée** d'un espace euclidien E et soit $x, y \in E$; il existe de fait une unique famille $x_1, \dots, x_n, y_1, \dots y_n$ de réels telle que $x = \sum_{i=1}^n x_i e_i$ et $y = \sum_{i=1}^n y_i e_i$. Avec ces notations, il est aisé de vérifier les formules (utiles) suivantes :

(i)
$$\forall i \in [\![1, n]\!], \quad x_i = \langle x , e_i \rangle \ ;$$

(ii)
$$\langle x , y \rangle = \sum_{i=1}^n x_i y_i \ ;$$

(iii)
$$\|x\| = \sqrt{\sum_{i=1}^n x_i^2} \, .$$

✌ **Remarque XXV.12.** Pour $i \in [\![1, n]\!]$, l'application : $x \mapsto \langle x , e_i \rangle$ est en fait la forme coordonnée e_i^*.

3.⁻ Projecteurs orthogonaux

On fixe dans ce paragraphe un espace préhilbertien réel E.

a) Supplémentaire orthogonal d'un s–e.v

Proposition XXV.8. Soit F un s–e.v de E **de dimension finie**. Alors :

$$F \oplus F^\perp = E \, .$$

Démonstration. On vérifie que $F \cap F^\perp = \{0\}$. De plus, si $x \in E$ et que $(e_1, \dots, e_n)$ est une base orthonormée de F alors

$$y = \sum_{i=1}^n \langle x , e_i \rangle \, e_i \in F$$

et pour tout $j [\![1, n]\!]$ on a :

$$\begin{aligned}
\langle x - y , e_j \rangle &= \langle x , e_j \rangle - \sum_{i=1}^n \langle x , e_i \rangle \underbrace{\langle e_i , e_j \rangle}_{=\delta_{i,j}} \\
&= \langle x , e_j \rangle - \langle x , e_j \rangle \\
&= 0 \, .
\end{aligned}$$

In fine, on a :

$$x = \underbrace{x - y}_{\in F^\perp} + \underbrace{y}_{\in F}$$

d'où le résultat. □

Vocabulaire. $F^\perp$ est appelé **supplémentaire orthogonal** de F.

✌ **Remarque XXV.13.** Il y a unicité du supplémentaire orthogonal.

Proposition XXV.9. Soit E un espace **euclidien** et soit F un s–e.v de E. Alors ;
(i) $\dim(F^\perp) = \dim(E) - \dim(F)$;
(ii) $(F^\perp)^\perp = F$.

Démonstration.
(i) Découle immédiatement de la proposition XXV.8.
(ii) Nous avons vu (proposition XXV.6) que $F \subset (F^\perp)^\perp$. De plus, on déduit du point précédent que $\dim((F^\perp)^\perp) = \dim(F)$, ce qui permet de conclure.

□

➠ **Exemple XXV.10.** Dans $\mathbb{R}^3$, le supplémentaire orthogonal d'un plan est l'unique droite vectorielle perpendiculaire (au sens vu dans le secondaire) à ce dernier.

Vocabulaire. Tout vecteur unitaire engendrant le supplémentaire orthogonal à un hyperplan est appelé **vecteur normal** à ce dernier.

✌ **Remarque XXV.14.** Soit H un hyperplan et soit a un vecteur normal à H. Alors si $\mathscr{B} = (e_1, \ldots, e_n)$ est une base orthonormée de E dans laquelle les coordonnées de a sont $a_1, \ldots, a_n \in \mathbb{R}$ on a :

$$\forall\, x = \sum_{i=1}^{n} x_i e_i \in E, \quad x \in H \iff \langle x\,,\, a\rangle = 0$$
$$\iff \sum_{i=1}^{n} a_i x_i = 0\,.$$

On obtient ainsi une équation de l'hyperplan à l'aide des coordonnées de son vecteur normale dans une base orthonormée.

Définition XXV.9. Soit F un s–e.v de E **de dimension finie** ; alors on appelle **projecteur orthogonal** sur F le projecteur sur F parallèlement à $F^\perp$.

✌ **Remarque XXV.15.**
— Pour tout $x, y \in E$ on a équivalence entre les deux propriétés suivantes :
  (i) $y = p(x)$;
  (ii) $(y \in F) \wedge (x - y \in F^\perp)$.
— Soit $\mathscr{F} = (u_1, \ldots, u_k)$ une base orthogonale de F. On a alors (*cf.* démonstration de la proposition XXV.6), pour $x \in E$ et si p est le projecteur orthogonal sur F :

$$p(x) = \sum_{i=1}^{k} \frac{\langle x\,,\, u_i\rangle}{\|u_i\|^2} u_i\,.$$

Toute similarité avec les formules apparaissant dans l'algorithme de de Gram–Schmidt (théorème XXV.7) est violemment non fortuite. Similairement, si $F = \mathscr{D}_e$ est une droite, on a :

$$\forall x \in E, \quad p(x) = \frac{\langle x\,,\, e\rangle}{\|e\|^2} e\,,$$

formule qui devrait titiller les souvenirs du lecteur relatifs aux sciences appliquées. Pour finir, on peut obtenir le projecteur p' sur l'hyperplan $H = \mathscr{D}_e^{\perp}$ via :

$$\forall x \in E, \quad p'(x) = x - \frac{\langle x\,,\, e\rangle}{\|e\|^2} e\,.$$

b) Distance à un s–e.v

Définition XXV.10. Soit F un s–e.v de E et soit $x \in E$. On appelle **distance de x à F** la quantité

$$d(x, F) = \inf\{d(x, y) \mid y \in F\}\,.$$

✌ **Remarque XXV.16.** Cette borne inférieure existe bien. Pourquoi ?

➠ **Exemple XXV.11.** On se place dans l'espace $E = \mathscr{C}^0([0,1])$ muni du produit scalaire $(f, g) \mapsto \int_0^1 f(t)g(t)\,\mathrm{d}t$ et on pose :

$$F = \left\{ x \mapsto \sum_{n=0}^{N} \frac{x^n}{n!} \;\middle|\; N \in \mathbb{N} \right\}.$$

On peut alors vérifier par inégalité de Taylor–Lagrange (proposition XX.20) que $d(\exp, F) = 0$ et pourtant $\exp \notin F$.

Proposition XXV.10. Soit F un s–e.v de E **de dimension finie**, soit $x \in E$ et soit p le projecteur orthogonal sur F. Alors on a :

$$\forall y \in F, \quad d(x, y) \geq d(x, p(x))$$

avec égalité si et seulement si $y = p(x)$.

✌ **Remarque XXV.17.** Cela signifie que le point $p(x)$ est l'unique vecteur de F minimisant la distance à x et que :

$$d(x, F) = d(x, p(x))\,.$$

Démonstration. Soit $y \in F$; alors :

$$\begin{aligned} d(x, y)^2 &= \|y - x\|^2 \\ &= \|(y - p(x)) + (p(x) - x)\|^2 \\ &= \|y - p(x)\|^2 + \|p(x) - x\|^2 \end{aligned}$$

d'après le théorème de Pythagore (XXV.5). Ceci se reformule :

$$d(x,y)^2 = d(y,p(x))^2 + d(x,p(x))^2$$

d'où le résultat. □

✖ **Attention :** Le projeté orthogonal sur F est bien défini car F est de dimension finie.

Exemple XXV.12.

— Si H est un hyperplan d'un espace **euclidien** E et que $e \in E$ est tel que $H^\perp = \mathscr{D}_e$ (on dit que e est **normal** à H), on a :

$$\forall x \in E, \quad d(x,H) = \frac{|\langle x\,,\,e\rangle|}{\|e\|}.$$

— Si $e \in E$ alors (calcul en exercice) :

$$\begin{aligned}\forall x \in E, \quad d(x,\mathscr{D}_e) &= \left\| x - \frac{\langle x\,,\,e\rangle}{\|e\|^2} e \right\| \\ &= \frac{\sqrt{\|x\|^2\|e\|^2 - \langle x\,,\,e\rangle^2}}{\|e\|}.\end{aligned}$$

✍ **Exercice XXV.10.** Calculer les quantité suivante :

(a) $\displaystyle\inf_{a,b\in\mathbb{R}} \int_0^{2\pi} (x - a\cos(x) - b\sin(x))^2 \,\mathrm{d}x$; (b) $\displaystyle\inf_{a,b\in\mathbb{R}} \int_0^1 (t^2 - at - b)^2 \,\mathrm{d}t$.

Chapitre XXVI

Espérance, variance

On fixe dans ce chapitre un espace probabilisé $(\Omega, \mathbb{P})$ **fini**.

1.⁻ Espérance

a) Notion d'espérance

Définition XXVI.1. Soit X une variable aléatoire réelle ou complexe ; on appelle **espérance** de X la quantité

$$\mathbb{E}(X) = \sum_{x \in X(\Omega)} x \, \mathbb{P}(X = x) \, .$$

➠ **Exemple XXVI.1.** Si $X \sim \mathscr{U}(n)$, on a :

$$\mathbb{E}(X) = \sum_{k=1}^{n} \frac{k}{n} = \frac{n+1}{2} \, .$$

✌ **Remarque XXVI.1.**

— De façon générale, l'espérance de X est la moyenne de ses valeurs pondérée par leur fréquence (cette dernière étant donnée par la loi de X).

— L'espérance de X ne dépend que de sa loi.

Vocabulaire. Si $\mathbb{E}(X) = 0$, on dit que la variable aléatoire X est **centrée**.

Proposition XXVI.1. Soit X une variable aléatoire réelle ou complexe ; alors :

$$\mathbb{E}(X) = \sum_{\omega \in \Omega} \mathbb{P}(\{\omega\}) X(\omega) \, .$$

Démonstration. On a :

$$\begin{aligned}\sum_{\omega\in\Omega}\mathbb{P}(\{\omega\})X(\omega) &= \sum_{x\in X(\Omega)}\ \sum_{\omega\in X^{-1}(\{x\})} X(\omega)\mathbb{P}(\{\omega\})\\ &= \sum_{x\in X(\Omega)}\ \sum_{\omega\in X^{-1}(\{x\})} x\,\mathbb{P}(\{\omega\})\\ &= \sum_{x\in X(\Omega)} x \sum_{\omega\in X^{-1}(\{x\})} \mathbb{P}(\{\omega\})\\ &= \sum_{x\in X(\Omega)} x\,\mathbb{P}(X^{-1}(\{x\})\\ &= \sum_{x\in X(\Omega)} x\,\mathbb{P}(X=x)\end{aligned}$$

d'où le résultat. □

✍ **Exercice XXVI.1.** Soit $A\subset\Omega$. Démontrer que $\mathbb{E}(\mathbb{1}_A)=\mathbb{P}(A)$.

b) Zoologie

◇ Variable (presque) constante

Définition XXVI.2. Une variable aléatoire est dite **constante presque sûrement** si il existe $m\in\mathbb{C}$ tel que $\mathbb{P}(X=m)=1$.

✌ **Remarque XXVI.2.** Il est aisé de démontrer que si X est constante presque sûrement égale à $m\in\mathbb{C}$ alors $\mathbb{E}(X)=m$. On en déduit que pour toute variable aléatoire réelle ou complexe Y on a :

$$\mathbb{E}(\mathbb{E}(Y))=\mathbb{E}(Y)\,.$$

◇ Loi uniforme

Proposition XXVI.2. Soient $x_1,\dots,x_n\in\mathbb{C}$ et soit $X\sim\mathscr{U}(x_1,\dots,x_n)$. Alors :

$$\mathbb{E}(X)=\frac{1}{n}\sum_{k=1}^{n}x_k\,.$$

✌ **Remarque XXVI.3.** Il s'agit de la moyenne arithmétique des valeurs de X.

◇ Loi de Bernoulli

Proposition XXVI.3. Soit $p\in[0,1]$ et soit $X\sim\mathscr{B}(p)$. Alors :

$$\mathbb{E}(X)=p\,.$$

Démonstration. Il suffit de remarquer que :

$$\mathbb{E}(X) = 0 \times \mathbb{P}(X = 0) + 1 \times \mathbb{P}(X = 1) = p\,.$$

□

◇ **Loi binomiale**

Proposition XXVI.4. Soit $p \in [0,1]$ et $n \in \mathbb{N}^*$. Alors, si $X \sim \mathscr{B}(n,p)$ on a :

$$\mathbb{E}(X) = np\,.$$

Démonstration. On a :

$$\begin{aligned}
\mathbb{E}(X) &= \sum_{k=0}^{n} k \binom{n}{k} p^k (1-p)^{n-k} \\
&= \sum_{k=1}^{n} k \frac{n!}{k!(n-k)!} p^k (1-p)^{n-k} \\
&= \sum_{k=1}^{n} n \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} p^k (1-p)^{n-k} \\
&= np \sum_{k=1}^{n} \binom{n-1}{k-1} p^{k-1} (1-p)^{n-1-(k-1)} \\
&= np(p+1-p)^{n-1} \\
&= np
\end{aligned}$$

d'où le résultat. □

2.⁻ Propriétés de l'espérance

a) Propriétés élémentaires

Définition XXVI.3. Un événement $A \subset \Omega$ sera dit **presque sûr** si $\mathbb{P}(A) = 1$.

➠ **Exemple XXVI.2.** La variable aléatoire comptant le nombre de fois où une pièce équilibrée tombe sur la tranche parmi 42 lancers est nulle presque sûrement dans le modèle précédemment établi pour cette expérience aléatoire.

✌ **Remarque XXVI.4.** Avec cette terminologie, on peut dire que connaître la loi d'une variable aléatoire revient à connaître cette dernière presque sûrement.

Proposition XXVI.5 (Linéarité de l'espérance)**.** Soient X, Y deux variables aléatoires réelles ou complexes et soit $\lambda \in \mathbb{C}$. Alors :

$$\mathbb{E}(X + \lambda Y) = \mathbb{E}(X) + \lambda \mathbb{E}(Y)\,.$$

Démonstration. On a :

$$\mathbb{E}(X+\lambda Y)=\sum_{\omega\in\Omega}\mathbb{P}(\{\omega\})(X(\omega)+\lambda Y(\omega))$$

d'où le résultat. □

Proposition XXVI.6. Soit X une variable aléatoire réelle telle que $X \geq 0$ presque sûrement ($i.e$ $\mathbb{P}(X \geq 0)=1$) ; alors :

(i) $\mathbb{E}(X) \geq 0$;

(ii) $\mathbb{E}(X)=0 \Leftrightarrow X$ est nulle presque sûrement ($i.e$ $\mathbb{P}(X=0)=1$).

Démonstration. Posons $X(\Omega)=\{x_1,\dots,x_n\}$. Alors la quantité

$$\mathbb{E}(X)=\sum_{k=1}^{n}x_k\,\mathbb{P}(X=x_k)$$

est une somme de termes positifs, d'où le résultat. □

Corollaire XXVI.6.a (Croissance de l'espérance)**.** Soient X, Y deux variables aléatoires réelles telles que $X \leq Y$ presque sûrement ; alors $\mathbb{E}(X) \leq \mathbb{E}(Y)$.

✌ **Remarque XXVI.5.** On retrouve ainsi l'espérance d'une variable aléatoire de loi binomiale à l'aide de la proposition XXIV.13.

➠ **Exemple XXVI.3.** Soient $X, Y \sim \mathscr{U}(6)$; alors $\mathbb{E}(X+Y)=7$. Nous venons de déterminer la somme moyenne des résultats de deux dés à 6 faces.

b) Lemme de transfert

Proposition XXVI.7 (Lemme de transfert)**.** Soit $X : \Omega \to E$ une variable aléatoire **quelconque** et soit $\varphi : E \to \mathbb{R}$ une application. Alors :

$$\mathbb{E}(\varphi(X))=\sum_{x\in E}\varphi(x)\mathbb{P}(X=x)\,.$$

✌ **Remarque XXVI.6.** La somme *supra* est bien une somme finie, car si $x \notin X(\Omega)$, $\mathbb{P}(X=x)=0$.

Démonstration. Posons $X(\Omega)=\{x_1,\dots,x_n\}$. Alors, si l'on pose pour $k \in [\![1,n]\!]$ $A_k=\{X=x_k\}$ on a :

$$X=\sum_{k=1}^{n}x_k\mathbb{1}_{A_k}$$

et donc :

$$\varphi(X) = \sum_{k=1}^{n} \varphi(x_k)\mathbb{1}_{A_k}.$$

Ainsi :

$$\begin{aligned}\mathbb{E}(\varphi(X)) &= \mathbb{E}\left(\sum_{k=1}^{n} \varphi(x_k)\mathbb{1}_{A_k}\right) \\ &= \sum_{k=1}^{n} \varphi(x_k)\mathbb{E}(\mathbb{1}_{A_k}) \\ &= \sum_{k=1}^{n} \varphi(x_k)\mathbb{P}(A_k)\end{aligned}$$

d'après le résultat de l'exercice XXVI.1. On en déduit le résultat. □

Remarque XXVI.7.
- Une conséquence importante du lemme de transfert est que l'espérance de $\varphi(X)$ est totalement déterminée par la loi de X et la fonction φ.
- Noter que le lemme de transfert s'applique au cas où X est un couple ou un n–uplet (se placer sur un espace produit à l'arrivée).

Exemple XXVI.4.
- Soit $X \sim \mathscr{U}(n)$. Alors :

$$\begin{aligned}\mathbb{E}(X^2) &= \sum_{k=1}^{n} \frac{k^2}{n} \\ &= \frac{(n+1)(2n+1)}{6}.\end{aligned}$$

- Soit X une variable aléatoire réelle ou complexe. Alors :

$$\begin{aligned}\mathbb{E}(|X|) &= \sum_{x \in X(\Omega)} |x|\mathbb{P}(X=x) \\ &\geq \left|\sum_{x \in X(\Omega)} x\mathbb{P}(X=x)\right|\end{aligned}$$

et donc on obtient une "inégalité triangulaire" :

$$|\mathbb{E}(X)| \leq \mathbb{E}(|X|).$$

Exercice XXVI.2. Soient $X, Y \sim \mathscr{U}(n)$ deux variables aléatoires indépendantes ; déterminer $\mathbb{E}(XY^2)$.

c) Inégalité de Markov

La proposition *infra* est ainsi nommée en l'honneur du mathématicien russe Andreï Andreïevitch Markov (1856—1922), connu comme l'un des pionniers de la théorie moderne des probabilités (on lui doit notamment la notion de processus stochastique).

Théorème XXVI.8 (Inégalité de Markov)**.**
Soit X une variable aléatoire réelle telle que $X \geq 0$ presque sûrement et soit $t \in \mathbb{R}_+^*$. Alors :

$$\mathbb{P}(X \geq t) \leq \frac{\mathbb{E}(X)}{t}.$$

Démonstration. Posons $A = \{x \in X(\Omega) \,|\, x \geq t\}$. Alors :

$$\begin{aligned} t\,\mathbb{P}(X \geq t) &= t \sum_{x \in A} \mathbb{P}(X = x) \\ &= \sum_{x \in A} t\mathbb{P}(X = x) \\ &\leq \sum_{x \in A} x\mathbb{P}(X = x) \\ &\leq \mathbb{E}(X) \end{aligned}$$

d'où le résultat. □

✌ **Remarque XXVI.8.** Soit X une variable aléatoire réelle. Alors on a, par exemple, que :

$$\mathbb{P}(X \geq 100\mathbb{E}(X)) \leq \frac{1}{100}.$$

Ceci nous permet d'estimer la répartition des valeurs de notre variable aléatoire X et de visualiser la façon dont la probabilité d'un écart à la moyenne donné évolue.

d) Lien à l'indépendance

Proposition XXVI.9. Soient X et Y deux variables aléatoires réelles ou complexes **indépendantes**. Alors $\mathbb{E}(XY) = \mathbb{E}(X)\mathbb{E}(Y)$.

✖ **ATTENTION :** l'indépendance est ici essentielle. Si $X \sim \mathscr{B}(p)$, on a $\mathbb{E}(X^2) = \mathbb{E}(X) = p$ car $X^2 = X$ presque sûrement. Pour peu que p ne soit pas égal à 0 ou 1, on a donc $\mathbb{E}(X^2) \neq \mathbb{E}(X)^2$.

Démonstration. Posons $X(\Omega) = \{x_1, \dots, x_n\}$ et $Y(\Omega) = \{y_1, \dots, y_m\}$. Alors, en appliquant le lemme de transfert au couple (X, Y) on obtient :

$$\begin{aligned} \mathbb{E}(XY) &= \sum_{k=1}^{n} \sum_{\ell=1}^{m} x_k y_\ell \mathbb{P}(X = x_k, Y = y_\ell) \\ &= \sum_{k=1}^{n} \sum_{\ell=1}^{m} x_k y_\ell \mathbb{P}(X = x_k)\mathbb{P}(Y = y_\ell) \end{aligned}$$

par indépendance. *In fine*, on a donc :

$$\begin{aligned} \mathbb{E}(XY) &= \left(\sum_{k=1}^{n} x_k \mathbb{P}(X = x_k) \right) \left(\sum_{\ell=1}^{m} y_\ell \mathbb{P}(Y = y_\ell) \right) \\ &= \mathbb{E}(X)\mathbb{E}(Y). \end{aligned}$$

□

✖ **Attention :** la réciproque est **fausse** : si $X = m$ presque sûrement pour un certain $m \in \mathbb{R}$ on a $\mathbb{E}(X^2) = m^2 = \mathbb{E}(X)^2$ et pourtant X n'est pas indépendante d'elle même (avouez que ce serait sympathique, mais le monde est injuste).

✌ **Remarque XXVI.9.** Ce résultat se généralise au cas de n variables aléatoires mutuellement indépendantes.

3.⁻ Variance

a) C'est quoi ?

Connaître l'espérance d'une variable aléatoire réelle X nous permet d'avoir une idée de l'endroit moyen où se situent ses valeurs : c'est ce que l'on appelle un **paramètre de position**. Une telle donnée, bien qu'utile, n'est en général pas suffisante pour étudier finement le comportement de notre variable aléatoire malgré l'existence d'outils tels que l'inégalité de Markov (théorème XXVI.8). La question qui nous préoccupe dans ce paragraphe est la suivante : comment diable sont réparties les valeurs de X ? Sont–elles resserrées autour de la moyenne ? Fortement dispersées ? Les quantités nous renseignant à ce sujet sont traditionnellement appelés **paramètres de dispersion**.

Une première idée pourrait être de déterminer l'espérance de la variable aléatoire réelle ou complexe $|X - \mathbb{E}(X)|$; celle se révèle hélas en général d'une étude assez pénible. C'est pourquoi nous introduisons les quantités *infra*, dont nous dédierons cet ultime paragraphe de l'année à l'étude.

Définition XXVI.4. Soit X une variable aléatoire réelle ; alors on appelle **variance** de X la quantité
$$V(X) = \mathbb{E}((X - \mathbb{E}(X))^2)$$
et **écart–type** de X la quantité :
$$\sigma(X) = \sqrt{V(X)}\,.$$

Vocabulaire. Une variable aléatoire réelle de variance égale à 1 est dite **réduite**.

✌ **Remarque XXVI.10.** Si nous souhaitions parler comme les physiciens, nous pourrions dire que $\sigma(X)$ est de même unité/dimension que X. Cette quantité représente l'écart moyen entre deux valeurs prises par la variable aléatoire X.

Le résultat *infra* est nommé en l'honneur du mathématicien (et élève de Jean Bernoulli, premier du nom) allemand Johann Samuel König (1712—1757), connu entre autres pour avoir traduit les éléments d'Euclide et du mathématicien, astronome et physicien néerlandais Christiaan Huygens (1629—1695), inventeur de la première horloge à pendule.

Théorème XXVI.10 (König–Huygens)**.**
Soit X une variable aléatoire réelle ; alors :
$$V(X) = \mathbb{E}(X^2) - \mathbb{E}(X)^2\,.$$

Démonstration. On a :

$$\begin{aligned} V(X) &= \mathbb{E}((X-\mathbb{E}(X))^2) \\ &= E(X^2 - 2X\mathbb{E}(X) + \mathbb{E}(X)^2) \\ &= \mathbb{E}(X^2) - 2\mathbb{E}(X)^2 + \mathbb{E}(X)^2 \\ &= \mathbb{E}(X^2) - \mathbb{E}(X)^2 . \end{aligned}$$

□

➠ **Exemple XXVI.5.** Si X correspond à la somme des résultats de deux dés à 6 faces indépendants, on a $V(X) = \frac{35}{6}$ et $\sigma(X) \simeq 2.4$.

Proposition XXVI.11. Soit X une variable aléatoire réelle et soient $a, b \in \mathbb{R}$. Alors :

(i) $V(aX+b) = a^2 V(X)$;

(ii) $\sigma(aX+b) = |a|\sigma(X)$.

Démonstration. Il s'agit d'un calcul direct. □

Corollaire XXVI.11.a. Soit X une variable aléatoire réelle telle que $\sigma(X) > 0$; alors la variable aléatoire $\dfrac{X-\mathbb{E}(X)}{\sigma(X)}$ est centrée réduite.

b) Zoologie

⋄ Variable presque constante

Soit X une variable aléatoire réelle telle que $X = m$ presque sûrement pour un certain $m \in \mathbb{R}$. Alors, il découle de la formule de König–Huygens (théorème XXVI.10) que $V(X) = \sigma(X) = 0$. La réciproque est, pour une fois, vraie.

Proposition XXVI.12. Soit X une variable aléatoire réelle telle que $V(X) = 0$. Alors X est constante presque sûrement.

Démonstration. Posons $Y = (X - \mathbb{E}(X))^2$; alors $\mathbb{E}(Y) = V(X) = 0$ et donc $Y = 0$ presque sûrement d'après la proposition XXVI.6, d'où le résultat. □

⋄ Loi de Bernoulli

Proposition XXVI.13. Soit $p \in [0,1]$ et soit $X \sim \mathscr{B}(p)$. Alors $V(X) = p(1-p)$.

Démonstration. Il suffit de faire le calcul en remarquant que $X^2 = X$ presque sûrement. □

◇ Loi binomiale

Proposition XXVI.14. Soit $p \in [0,1]$ et soit $n \in \mathbb{N}^*$. Alors, si $X \sim \mathscr{B}(n,p)$ on a $V(X) = np(1-p)$.

Démonstration. On a, par lemme de transfert (proposition XXVI.7) :

$$\begin{aligned}
\mathbb{E}(X^2) &= \sum_{k=0}^{n} k^2 \binom{n}{k} p^k (1-p)^{n-k} \\
&= \sum_{k=0}^{n} k(k-1+1) \binom{n}{k} p^k (1-p)^{n-k} \\
&= \sum_{k=0}^{n} k(k-1) \binom{n}{k} p^k (1-p)^{n-k} + \sum_{k=0}^{n} k \binom{n}{k} p^k (1-p)^{n-k} \\
&= \sum_{k=2}^{n} n(n-1) \binom{n-2}{k-2} p^k (1-p)^{n-k} + np \\
&= n(n-1)p^2 + np\,.
\end{aligned}$$

De fait, on a :

$$V(X) = \mathbb{E}(X^2) - (\mathbb{E}(X))^2 = n(n-1)p^2 + np - (np)^2 = np(1-p)\,.$$

□

✌ **Remarque XXVI.11.** Si $X \sim \mathscr{B}(n,p)$ on a $\sigma(X) = \sqrt{p(1-p)}\sqrt{n} = o(n)$ lorsque $n \to \infty$. Cela signifie que les écarts entre les valeurs prises par X et l'espérance $\mathbb{E}(X)$ sont faibles devant sa moyenne. À titre d'exemple, pour $n = 10\,000$ et $p = \dfrac{1}{2}$ on a $\mathbb{E}(X) = 5000$ et $\sigma(X) = 50$ ...

c) Inégalité de Bienaymé–Tchebychev

Le résultat présenté dans ce paragraphe est nommé en l'honneur du mathématicien français Irénée-Jules Bienaymé (1796—1878), connu pour ses contributions à la théorie des probabilité et à la statistique, et de son homologue russe Pafnouti Lvovitch Tchebychev (1821—1894), dont les travaux ont porté sur les probabilités, la statistique et la théorie des nombres.

Théorème XXVI.15 (Bienaymé–Tchebychev)**.**
Soit X une variable aléatoire réelle ; on pose $m = \mathbb{E}(X)$ et $\sigma = \sigma(X)$. Alors, pour tout $\lambda \in \mathbb{R}_+^*$ on a :

$$\mathbb{P}(|X-m| \geq \lambda) \leq \frac{\sigma^2}{\lambda^2}\,.$$

Démonstration. En appliquant l'inégalité de Markov (théorème XXVI.8) à la variable aléatoire réelle $(X-m)^2$ avec $t=\lambda^2$, on obtient :

$$\mathbb{P}((X-m)^2 \geq \lambda^2) \leq \frac{\mathbb{E}((X-m)^2)}{\lambda^2}$$

soit

$$\mathbb{P}((X-m)^2 \geq \lambda^2) \leq \frac{V(X)}{\lambda^2}.$$

Il suffit alors pour conclure de remarquer que $V(X)=\sigma^2$ et que, par positivité de λ :

$$\mathbb{P}((X-m)^2 \geq \lambda^2) = \mathbb{P}(|X-m| \geq \lambda).$$

□

✌ **Remarque XXVI.12.** Il peut être intéressant de formuler cette inégalité en remplaçant λ par le produit $\lambda\sigma$. On obtient alors :

$$\mathbb{P}(|X-m| \geq \lambda\sigma) \leq \frac{1}{\lambda^2}$$

ce qui nous permet d'estimer l'écart de la variable aléatoire X à sa moyenne par incréments proportionnels à son écart–type.

➠ **Exemple XXVI.6.** Lançons $n \geq 1$ dés à 6 faces et quantifions le nombre de 6 obtenus par une variable aléatoire X. Il est alors clair que $X \sim \mathscr{B}\left(n, \frac{1}{6}\right)$ et donc, par inégalité de Bienaymé–Tchebychev (théorème XXVI.15), on obtient pour tout $\lambda > 0$ que :

$$\mathbb{P}\left(\left|X-\frac{n}{6}\right| \geq \lambda\right) \leq \frac{5n}{36\lambda^2}.$$

Pour $\lambda = \frac{n}{6}$, ceci devient

$$\mathbb{P}\left(\left|X-\frac{n}{6}\right| \geq \frac{n}{6}\right) \leq \frac{5}{n}.$$

On vérifie ensuite par un rapide calcul que $\left|X-\frac{n}{6}\right| \geq \frac{n}{6} \Leftrightarrow X \geq \frac{n}{3}$ et donc, *in fine* :

$$\mathbb{P}\left(X \geq \frac{n}{3}\right) \leq \frac{5}{n}$$

i.e

$$\mathbb{P}\left(X < \frac{n}{3}\right) \geq 1 - \frac{5}{n}.$$

Ceci signifie que lorsque $n=10$, la probabilité que les 6 représentent moins d'un tiers des résultats obtenus est supérieure à $\frac{1}{2}$. Pour $n=50$, elle dépasse $\frac{9}{10}$.

4.⁻ Covariance

a) Co–quoi ?

Définition XXVI.5. Soient X, Y deux variables aléatoires réelles ; on appelle **covariance** de X et Y la quantité

$$\mathrm{Cov}(X,Y) = \mathbb{E}((X-\mathbb{E}(X))(Y-\mathbb{E}(Y)))$$

Remarque XXVI.13. $\mathrm{Cov}(X,X) = V(X)$ pour toute variable aléatoire réelle X.

Proposition XXVI.16. Soient X, Y deux variables aléatoires réelles ; alors :

$$\mathrm{Cov}(X,Y) = \mathbb{E}(XY) - \mathbb{E}(X)\mathbb{E}(Y)\,.$$

Démonstration. Il s'agit d'un calcul immédiat et remarquablement indolore (affirmation non contractuelle). □

Corollaire XXVI.16.a. Soient X, Y deux variables aléatoires réelles **indépendantes** ; alors $\mathrm{Cov}(X,Y) = 0$.

✖ **Attention :** la réciproque est **fausse** (avouez, vous êtes surpris). Prenons $X \sim \mathscr{U}(-1,0,1)$ et posons $Y = X^2$: il est clair que X et Y ne sont pas indépendantes et pourtant $XY = X^3 = X$ presque sûrement donc

$$\mathbb{E}(XY) = \mathbb{E}(X) = 0 = \mathbb{E}(X)\mathbb{E}(Y)\,.$$

Vocabulaire. Deux deux variables aléatoires réelles X, Y telles que $\mathrm{Cov}(X,Y) = 0$ sont dites **décorrélées**.

Proposition XXVI.17. Soient X, Y et Z trois variables aléatoires réelles et soient $a, b, c, d \in \mathbb{R}$. Alors :

(i) $\mathrm{Cov}(X,Y) = \mathrm{Cov}(Y,X)$;

(ii) $\mathrm{Cov}(aX+b, cY+d) = ac\mathrm{Cov}(X,Y)$;

(iii) $\mathrm{Cov}(X+Y,Z) = \mathrm{Cov}(X,Z) + \mathrm{Cov}(Y,Z)$.

Démonstration. Il s'agit d'une succession de calculs aussi enrichissants que la formidable activité consistant à regarder de la peinture sécher. □

b) Sommes de variables aléatoire

Proposition XXVI.18. Soient X, Y deux variables aléatoires réelles. Alors :

(i) $V(X+Y) = V(X) + V(Y) + 2\mathrm{Cov}(X,Y)$;

(ii) $V(X-Y) = V(X) + V(Y) - 2\mathrm{Cov}(X,Y)$.

Démonstration. Il suffit de remarquer que $V(X \pm Y) = \mathrm{Cov}(X \pm Y, X \pm Y)$ et de développer à l'aide des propriétés énoncées dans la proposition XXVI.17. □

Démonstration. On lance deux dés à 6 faces, notant X le résultant du premier et Y celui du second. Alors la variance de la somme est :

$$V(X+Y) = V(X) + V(Y) + 2\mathrm{Cov}(X,Y) = \frac{35}{12} + \frac{35}{12} + 2\times 0 = \frac{35}{6}\,.$$

□

✌ **Remarque XXVI.14.** On peut démontrer par récurrence (youpi) que pour toute famille $X_1,\dots,X_n$ de variables aléatoires réelles, on a :

$$V\left(\sum_{k=1}^{n} X_k\right) = \sum_{k=1}^{n} V(X_k) + 2\sum_{j=1}^{n}\sum_{i=1}^{j-1} \mathrm{Cov}(X_i,X_j)\,.$$

Corollaire XXVI.18.a. Soient $X_1,\dots,X_n$ des variables aléatoires réelles **mutuellement indépendantes**. Alors :

$$V\left(\sum_{k=1}^{n} X_k\right) = \sum_{k=1}^{n} V(X_k)\,.$$

✌ **Remarque XXVI.15.** Ce résultat permet de retrouver aisément la variance d'une variable aléatoire réelle ou complexe $X \sim \mathscr{B}(n,p)$ via la proposition XXIV.13.

✍ **Exercice XXVI.3.** Soient $X_1,\dots,X_n \sim \mathscr{B}(p)$ mutuellement indépendantes, avec $p\in[0,1]$. On pose :

$$Y_n = \frac{1}{n}\sum_{k=1}^{n} X_k\,.$$

Déterminer, pour $t\in\mathbb{R}$, la quantité $\mathbb{E}(e^{tY_n})$.

➥ **Correction :** *On commence par remarquer que :*

$$\mathbb{E}(e^{tY_n}) = \mathbb{E}\left(\prod_{k=1}^{n} e^{tX_k/n}\right)\,.$$

Or, par lemme des coalitions, les variables $e^{tX_1/n},\dots,e^{tX_n/n}$ sont mutuellement indépendantes, ergo :

$$\begin{aligned}\mathbb{E}(e^{tY_n}) &= \prod_{k=1}^{n} \mathbb{E}\left(e^{tX_k/n}\right)\\ &= \left(1+p\left(e^{t/n}-1\right)\right)^n\end{aligned}$$

la dernière égalité étant obtenue par lemme de transfert (proposition XXVI.7).

✌ **Remarque XXVI.16.** Soit $(X_n)_{n\geq 1}$ une suite de variables aléatoires indépendantes de même loi. On note m (resp. σ^2) l'espérance (resp. la variance) commune à ces variables. On pose alors, pour tout $n\geq 1$:

$$\bar{X}_n = \frac{1}{n}\sum_{k=1}^{n} X_k\,.$$

On vérifie rapidement que cette nouvelle variable aléatoire est d'espérance m et que :

$$\forall n \geq 1, \quad V(\bar{X}_n) = \sum_{k=1}^{n} V\left(\frac{X_k}{n}\right) = \sum_{k=1}^{n} \frac{V(X_k)}{n^2} = \frac{\sigma^2}{n}\,.$$

On a alors, par inégalité de Bienaymé–Tchebychev, pour tout $\varepsilon > 0$:

$$\forall n \geq 1, \quad \mathbb{P}\left(|\bar{X}_n - m| \geq \varepsilon\right) \leq \frac{\sigma^2 \varepsilon^2}{n^2}$$

et donc :

$$\forall \varepsilon > 0, \quad \mathbb{P}\left(|\bar{X}_n - m| \geq \varepsilon\right) \to 0\,.$$

Ce résultat est connu sous le nom de **loi faible des grands nombres**. Il nous indique que la moyenne empirique (la variable $\bar{X}_n$) "converge" (on parlera de convergence en probabilité) vers la moyenne "théorique" (l'espérance).

Chapitre XXVII

Fonctions de deux variables

On munit dans ce chapitre l'espace euclidien $\mathbb{R}^2$ de son produit scalaire canonique et de la norme euclidienne associée.

1.– Topologie de $\mathbb{R}^2$

a) Ouverts du plan

Définition XXVII.1. Soit $x \in \mathbb{R}^2$ et $r \in \mathbb{R}_+^*$. On appelle :
- **disque ouvert** de centre x et rayon r l'ensemble :

$$D(x,r) = \{y \in \mathbb{R}^2 \,|\, \|x-y\| < r\};$$

- **disque fermé** de centre x et rayon r l'ensemble :

$$\overline{D}(x,r) = \{y \in \mathbb{R}^2 \,|\, \|x-y\| \leq r\}.$$

✌ **Remarque XXVII.1.** Le lecteur motivé pourra démontrer que tout disque de $\mathbb{R}^2$ est convexe, au sens de la caractérisation vue au corollaire III.12.a. Il existe cependant des convexes qui ne sont pas des disques : par exemple, un "segment "

$$\{(1-\lambda)a + \lambda b \,|\, \lambda \in [0,1]\},$$

pour $a, b \in \mathbb{R}^2$, reste convexe dans $\mathbb{R}^2$ sans être un disque.

Définition XXVII.2. Une partie $A \subset \mathbb{R}^2$ est dite :
- **ouverte** si :

$$\forall x \in A,\ \exists r \in \mathbb{R}_+^*,\ \ D(x,r) \subset A;$$

- **fermée** si son complémentaire $\mathbb{R}^2 \setminus A$ est une partie ouverte de $\mathbb{R}^2$.

✌ **Remarque XXVII.2.** Un ouvert est donc un ensemble dont tous les points peuvent être "entourés" par un disque interne à l'ensemble : aucun de ses points n'est donc "au bord" de l'ensemble.

➠ **Exemple XXVII.1.**

— $\mathbb{R}^2$ et $\emptyset$ sont à la fois ouverts et fermés ;
— les singletons sont fermés ;
— les "segments épointés" $\{(1-\lambda)a + \lambda b \,|\, \lambda \in [0,1[\}$,, pour $a, b \in \mathbb{R}^2$, ne sont ni ouverts ni fermés.

Proposition XXVII.1. Tout disque ouvert (resp. fermé) est ouvert (resp. fermé).

Démonstration. Soit $x \in \mathbb{R}^2$ et soit $r \in \mathbb{R}_+^*$. Alors, si $y \in D(x,r)$, on a $\|x-y\| < r$ et donc si, on pose $\mu = r - \|x-y\|$ on a, pour tout $z \in D(y,\mu)$:

$$\begin{aligned} \|x-z\| &= \|x-y+y-z\| \\ &\leq \|x-y\| + \|y-z\| \\ &< \|x-y\| + r - \|x-y\| \\ &= r \end{aligned}$$

et donc on a bien $D(y,\mu) \subset D(x,r)$, *ergo* le disque ouvert $D(x,r)$ est...ouvert.

Concernant la fermeture du disque fermé, il nous faut démontrer que l'ensemble $A = \mathbb{R}^2 \setminus \overline{D}(x,r)$ est ouvert ; fixons donc $y \in A$ et remarquons qu'alors $\|x-y\| > r$. De fait, si l'on pose $\mu = \|x-y\| - r$ on a, pour tout $z \in D(y,\mu)$:

$$\begin{aligned} \|x-y\| &= \|x-z+z-y\| \\ &\leq \|x-z\| + \|z-y\| \\ &< \|x-z\| + \mu \end{aligned}$$

et donc :

$$\|x-z\| > \|x-y\| - \mu = r$$

d'où l'inclusion $D(y,\mu) \subset A$ et le résultat escompté. □

✌ **Remarque XXVII.3.** On peut démontrer que toute réunion d'ouverts est un ouvert (un dessin peut aider). De même, toute intersection **finie** d'ouverts reste ouverte ; une intersection infinie d'ouverts pouvant toutefois ne pas l'être. Par exemple :

$$\forall a \in \mathbb{R}^2, \quad \bigcap_{n \in \mathbb{N}^*} D\left(a, \frac{1}{n}\right) = \{a\}.$$

Proposition XXVII.2 (Séparation de $\mathbb{R}^2$)**.** Soient $u, v \in \mathbb{R}^2$ tels que $u \neq v$. Alors il existe $r > 0$ tel que :

$$D(u,r) \cap D(v,r) = \emptyset.$$

Démonstration. Poser $r = \dfrac{\|u-v\|}{3}$. □

b) Applications continues de $\mathbb{R}^2$ dans $\mathbb{R}$

Définition XXVII.3. Soit $\Omega \subset \mathbb{R}^2$ un **ouvert** et soit $f : \Omega \to \mathbb{R}$. On dit que f est **continue** en un point $a \in \Omega$ lorsque :

$$\forall \varepsilon > 0,\ \exists \delta > 0,\ \forall x \in \Omega, \quad (\|x - a\| \leq \delta) \Rightarrow (|f(x) - f(a)| \leq \varepsilon)\,.$$

Une fonction continue en tout point de l'ouvert Ω sera dite continue sur Ω.

Remarque XXVII.4. Cette définition peut être reformulée de la façon suivante : f est continue en $a \in \Omega$ si et seulement si :

$$\forall V \in \mathscr{V}(f(a)),\ \exists \delta > 0,\ f(\overline{D}(a, \delta) \cap \Omega) \subset V\,.$$

Exemple XXVII.2.

— La norme euclidienne est continue sur $\mathbb{R}^2$. En effet, si $a, x \in \mathbb{R}^2$, on a :

$$|\,\|x\| - \|a\|\,| \leq \|x - a\|$$

et donc, pour tout $\varepsilon > 0$, "$\delta = \varepsilon$" convient.

— Les fonctions $(x, y) \mapsto x$ et $(x, y) \mapsto y$ sont continues.

— Si $f : \Omega \to \mathbb{R}$ est telle qu'il existe $M > 0$ vérifiant la condition

$$\forall (x, y) \in \Omega, \quad |f(x) - f(y)| \leq M\|x - y\|$$

alors f est continue (on parle, sans surprise, de fonction *lipschitzienne*).

Exercice XXVII.1. Démontrer que l'application définie par $f((0, 0)) = 0$ et $f : (x, y) \mapsto \dfrac{xy}{x^2 + y^2}$ sur $\mathbb{R}^2 \setminus \{(0, 0)\}$ n'est pas continue en $(0, 0)$.

Correction : *Soit $(x, y) \in \mathbb{R}^2 \setminus \{(0, 0)\}$. Alors, si l'on pose $r = \|(x, y)\|$, nous avons vu au chapitre XXV qu'il existe $\theta \in \mathbb{R}$ tel que $x = r\cos(\theta)$ et $y = r\sin(\theta)$. On a ensuite :*

$$f(x, y) = \frac{r^2 \cos(\theta)\sin(\theta)}{r^2} = \frac{1}{2}\sin(2\theta)$$

ce qui entraîne que :

$$|f(x, y) - f(0, 0)| = \frac{1}{2}|\sin(2\theta)|\,.$$

Fixons $\alpha > 0$; si l'on choisit $\theta \notin \pi\mathbb{Z}$ et $r \leq \alpha$, on a :

$$\|(x, y) - (0, 0)\| = r \leq \alpha$$

et pourtant

$$|f(x, y) - f(0, 0)| = \frac{1}{2}|\sin(2\theta)|$$

ce qui contredit la définition de limite avec tout $\varepsilon < \dfrac{1}{2}|\sin(2\theta)|$.

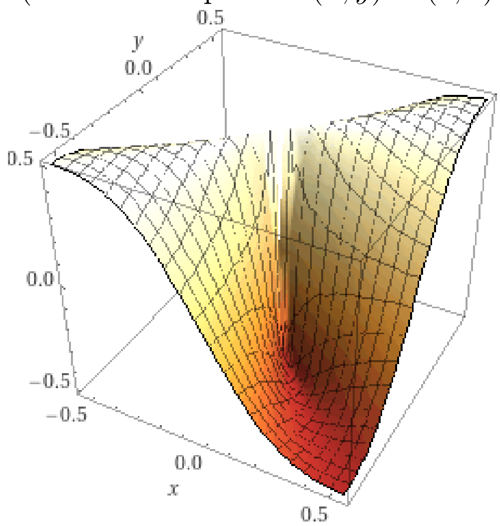
Remarque XXVII.5.

— Le passage en coordonnées polaire (r, θ) est très commode au voisinage de l'origine car il permet de contrôler la "convergence" du couple (x, y) "vers l'origine" en faisant tendre (de façon rigoureuse) r vers 0. Pour se convaincre de la nécessité de ce type de démarche, remarquer que

$$\lim_{x \to 0} \left(\lim_{y \to 0} \frac{y}{x^2 + y} \right) \neq \lim_{y \to 0} \left(\lim_{x \to 0} \frac{y}{x^2 + y} \right).$$

Oui je sais, c'est glauque. Mais c'est la vie.

— Une fonction $f : \Omega \to \mathbb{R}$ peut être représentée graphiquement par la surface d'équation $z = f(x, y)$ dans $\mathbb{R}^3$. Par exemple, la fonction *supra* correspond à la surface suivante (observer le "pic" en $(x, y) = (0, 0)$).



Les propositions qui suivent s'obtiennent de façon analogue au cas d'une variable réelle vu au chapitre IX. Leur démonstration ne constitue pas un attendu du programme de MPSI.

Proposition XXVII.3. Soient Ω un ouvert de $\mathbb{R}^2$, $a \in \Omega$, $f, g : \Omega \to \mathbb{R}$ deux applications continues en a et $\lambda \in \mathbb{R}$. Alors :

(i) $f + \lambda g$ est continue en a ;

(ii) $f \times g$ est continue en a ;

(iii) si $g(a) \neq 0$, il existe un $r > 0$ tel que g ne s'annule pas sur $D(a, r) \cap \Omega$ et $\frac{f}{g}$ est continue en a.

Exemple XXVII.3.

— Les fonctions polynomiales, *i.e* celles de la forme :

$$(x, y) \mapsto \sum_{i=0}^{p} \sum_{j=0}^{q} \lambda_{i,j} x^i y^j$$

avec les $\lambda_{i,j} \in \mathbb{R}$ sont continues.

— La fonction $(x, y) \mapsto \dfrac{xy}{x^2 + y^2}$ est continue sur $\mathbb{R}^2 \setminus \{(0, 0)\}$

Proposition XXVII.4. Soient Ω un ouvert de $\mathbb{R}^2$, I un intervalle de $\mathbb{R}$, $a \in \Omega$, $f : \Omega \to I$ continue en a et $g : I \to \mathbb{R}$ continue en $f(a)$. Alors $g \circ f$ est continue en a.

2.⁻ Dérivées partielles

On fixe dans ce paragraphe un ouvert Ω de $\mathbb{R}^2$.

a) C'est quoi ?

Définition XXVII.4. Soit $u \in \mathbb{R}^2$, $a \in \Omega$ et $f : \Omega \to \mathbb{R}$. On dit que f est **dérivable selon le vecteur** u si il existe $\ell \in \mathbb{R}$ tel que :

$$\frac{f(a+tu)-f(a)}{t} \xrightarrow[t\to 0]{} \ell\,.$$

Le nombre réel ℓ est alors appelé **nombre dérivé** de f en a selon u et noté $\mathrm{d}f(a)(u)$.

✌ **Remarque XXVII.6.**
- v Pour que cette définition ait un sens, il nous faut remarquer que, comme Ω est ouvert, il existe $r > 0$ tel que $D(a,r) \subset \Omega$. De fait, si $|t|\|u\| < r$, on a bien $a + tu \in \Omega$ et donc la quantité $f(a+tu)$ a un sens quel que soit u pour t au voisinage de 0.
- On obtient ainsi un "développement limité" à l'ordre 1 de la fonction f dans la direction du vecteur u. En effet, pour $|t|$ assez petit, on a :

$$f(a+tu) = f(a) + t\,\mathrm{d}f(a)(u) + t\varepsilon(t)$$

avec $\varepsilon(t) \xrightarrow[t\to 0]{} 0$.

➠ **Exemple XXVII.4.** Soit $f : (x,y) \mapsto x^2 + y$, définie sur $\mathbb{R}^2$. Alors, pour tous $a = (x,y), u = (\alpha,\beta) \in \mathbb{R}^2$ et $t \in \mathbb{R}^*$ on a :

$$\begin{aligned}\frac{f(a+tu)-f(a)}{t} &= \frac{(x+t\alpha)^2 + y + t\beta - x^2 - y}{t} \\ &= \frac{t(2x\alpha + t\alpha^2 + \beta)}{t} \\ &= 2x\alpha + t\alpha^2 + \beta \\ &\xrightarrow[t\to 0]{} 2x\alpha + \beta\,.\end{aligned}$$

On en déduit que l'application $\mathrm{d}f(a)$ est la forme linéaire

$$\begin{aligned}\mathrm{d}f(a) : \mathbb{R}^2 &\to \mathbb{R} \\ (\alpha,\beta) &\mapsto 2x\alpha + \beta\,.\end{aligned}$$

Ceci préfigure un résultat plus général qui sera démontré en deuxième année.

Définition XXVII.5. Posons $e_1 = (1,0)$ et $e_2 = (0,1)$ les deux vecteurs de la base canonique de $\mathbb{R}^2$. Si $f : \Omega \to \mathbb{R}$ est une application et que $a \in \Omega$, on appelle **dérivées partielles** de f en a les quantités $\mathrm{d}f(a)(e_1)$ et $\mathrm{d}f(a)(e_2)$, lorsqu'elles existent.

Notation. On pose dans ce cas $\dfrac{\partial f}{\partial x}(a) = \mathrm{d}f(a)(e_1)$ et $\dfrac{\partial f}{\partial y}(a) = \mathrm{d}f(a)(e_2)$. On trouve aussi dans la littérature les notations $\partial_x f(a)$ et $\partial_y f(a)$.

✌ **Remarque XXVII.7.** Si $a = (x,y)$ est un point en lequel f admet des dérivées partielles, on a :

$$\frac{\partial f}{\partial x} f(a) = \lim_{t\to 0} \frac{f(x+t,y) - f(x,y)}{t}$$

et

$$\frac{\partial f}{\partial y} f(a) = \lim_{t\to 0} \frac{f(x,y+t) - f(x,y)}{t} \,.$$

On reconnaît ici deux taux d'accroissements : le premier étant celui de $x \mapsto f(x,y)$ à y fixé, et le second celui de $y \mapsto f(x,y)$ à x fixé. On en déduit que les dérivées partielles peuvent être obtenues en dérivant "par rapport à la variable considérée" sans crainte de se planter violemment.

➠ **Exemple XXVII.5.** Les dérivées partielles de $f : (x,y) \mapsto x^2 - 3\cos(y) + xy$ sont :

$$\frac{\partial f}{\partial x} : (x,y) \mapsto 2x + y \quad \text{et} \quad \frac{\partial f}{\partial y} : (x,y) \mapsto 3\sin(y) + x \,,$$

ces deux fonctions étant définies sur $\mathbb{R}^2$.

✖ **ATTENTION :** l'existence des dérivées partielles n'implique **PAS** la continuité de la fonction au point considéré. En effet, si l'on reprend la fonction définie par $f((0,0)) = 0$ et $f : (x,y) \mapsto \dfrac{xy}{x^2+y^2}$ sur $\mathbb{R}^2 \setminus \{(0,0)\}$ (que nous savons discontinue en 0), nous avons, pour tout $t \in \mathbb{R}^*$:

$$\frac{f(t,0) - f(0,0)}{t} = 0 \quad \text{et} \quad \frac{f(0,t) - f(0,0)}{t} = 0$$

ce qui entraîne que les deux dérivées partielles $\dfrac{\partial f}{\partial x}(0,0)$ et $\dfrac{\partial f}{\partial y}(0,0)$ existent et sont nulles.

Proposition XXVII.5. Soient $f, g : \Omega \to \mathbb{R}$ deux applications admettant une dérivée partielle "selon x" ($i.e$ selon e_1) en un point $a \in \Omega$ et soit $\lambda \in \mathbb{R}$. Alors :

(i) $f + \lambda g$ admet une dérivée partielle "selon x" en a et

$$\frac{\partial}{\partial x}(f + \lambda g)(a) = \frac{\partial f}{\partial x}(a) + \lambda \frac{\partial g}{\partial x}(a)\ ;$$

(ii) $f \times g$ admet une dérivée partielle "selon x" en a et

$$\frac{\partial}{\partial x}(f \times g)(a) = \frac{\partial f}{\partial x}(a) \times g(a) + f(a) \times \frac{\partial g}{\partial x}(a)\ ;$$

(iii) si $g(a) \neq 0$, il existe un $r > 0$ tel que g ne s'annule pas sur $D(a, r) \cap \Omega$, les fonction $\frac{1}{g}$ et $\frac{f}{g}$ admettent une dérivée partielle "selon x" en a vérifant :

$$\frac{\partial}{\partial x}\left(\frac{1}{g}\right)(a) = -\frac{1}{g^2(a)}\frac{\partial g}{\partial x}(a) \text{ et } \frac{\partial}{\partial x}\left(\frac{f}{g}\right)(a) = \frac{\frac{\partial f}{\partial x}(a) \times g(a) - f(a) \times \frac{\partial g}{\partial x}(a)}{g^2(a)}.$$

Démonstration. Par le calcul, et dans la douleur. □

✌ **Remarque XXVII.8.** On peut (et on doit !) évidemment obtenir un résultat similaire pour les dérivées partielles "selon y" (et même sur les dérivées selon un vecteur quelconque).

b) Fonctions de classe $\mathscr{C}^1$

Définition XXVII.6. Une fonction $f : \Omega \to \mathbb{R}$ est dite **de classe** $\mathscr{C}^1$ si elle admet des dérivées partielles **continues** en tout point de Ω.

Notation. $f \in \mathscr{C}^1(\Omega)$

✌ **Remarque XXVII.9.** La proposition XXVII.5 nous permet d'affirmer que l'ensemble $(\mathscr{C}^1(\Omega), +, \times, \cdot)$ est une $\mathbb{R}$–algèbre commutative ($i.e$ un anneau commutatif et un $\mathbb{R}$–e.v).

➠ **Exemple XXVII.6.**

— Les fonctions polynomiales sont de classe $\mathscr{C}^1$ sur $\mathbb{R}^2$.
— La fonction $(x, y) \mapsto e^x + x\ln(y)$ est de classe $\mathscr{C}^1$ sur $\mathbb{R} \times \mathbb{R}_+^*$.

Proposition XXVII.6. Soit $f \in \mathscr{C}^1(\Omega)$ et soit $a \in \Omega$. Alors, pour tout $u = (h,k) \in \mathbb{R}^2$ tel que $a + u \in \Omega$ on a :

$$f(a+u) = f(a) + h\frac{\partial f}{\partial x}(a) + k\frac{\partial f}{\partial y}(a) + o_0(\|u\|)\,,$$

où $o_0(\|u\|)$ représente un produit de la forme $\varphi(u)\|u\|$, avec une fonction φ définie sur un disque ouvert centré en $(0,0)$ et vérifiant que :

$$\forall \varepsilon > 0,\ \exists \delta > 0,\ \forall u \in \mathbb{R}^2, \quad (\|u\| \leq \delta) \Rightarrow (|\varphi(u)| \leq \varepsilon)\,.$$

Démonstration. Admis. □

Remarque XXVII.10.

— Plus généralement, on peut démontrer que si $f \in \mathscr{C}^1(\Omega)$, alors elle admet une dérivée selon tout vecteur $u \in \mathbb{R}^2$ et qu'alors, pour tout $a \in \Omega$:

$$\mathrm{d}f(a)(u) = h\frac{\partial f}{\partial x}(a) + k\frac{\partial f}{\partial y}(a)$$

et donc :

$$f(a+u) = f(a) + \mathrm{d}f(a)(u) + o_0(\|u\|)\,.$$

Ceci est remarquable : l'existence et la continuité des dérivées partielle entraîne l'existence de dérivée selon tous les vecteurs du plan.

— La fonction f pouvant être représentée graphiquement par la surface d'équation $z = f(x,y)$ dans $\mathbb{R}^3$, il est raisonnable de se demander si le développement limité *supra* possède une interprétation géométrique. Si $a = (x_0, y_0)$ et $u = (h,k)$ on a, en posant $b = (x,y) = a + u$, $\lambda = \frac{\partial f}{\partial x}(a)$ et $\mu = \frac{\partial f}{\partial y}(a)$:

$$\begin{aligned} f(b) &= f(a) + \lambda h + \mu k + o_0(\|u\|) \\ &= f(a) + \lambda(x - x_0) + \mu(y - y_0) + o_0(\|u\|)\,. \end{aligned}$$

Nous savons (*cf.* chapitre XXI) que l'ensemble d'équation :

$$z = f(a) + \lambda(x - x_0) + \mu(y - y_0)$$

est un plan affine de $\mathbb{R}^3$. Celui–ci se retrouve "confondu" à la surface représentative de f "au voisinage" du point a ; on l'appelera **plan tangent** en a à cette dernière.

Corollaire XXVII.6.a. Toute fonction de classe $\mathscr{C}^1$ est continue.

Démonstration. Soit $f \in \mathscr{C}^1(\Omega)$ et soit $a \in \Omega$. Alors, pour tout $\varepsilon > 0$ et tout $x \in \Omega$

on a, en posant $(h,k) = x - a$ et en utilisant la proposition XXVII.6 :

$$\begin{aligned}
|f(x) - f(a)| &= \left| h\frac{\partial f}{\partial x}(a) + k\frac{\partial f}{\partial y}(a) + o_0(\|x-a\|) \right| \\
&\leq \left| h\frac{\partial f}{\partial x}(a) + k\frac{\partial f}{\partial y}(a) \right| + |o_0(\|x-a\|)| \\
&\leq 2\max\left(\left|\frac{\partial f}{\partial x}(a)\right|, \left|\frac{\partial f}{\partial y}(a)\right| \right) \|x-a\| + o_0(\|x-a\|)\,.
\end{aligned}$$

Ainsi, on a par définition de continuité et de o le résultat voulu. □

c) Gradient, extrema

Définition XXVII.7. Soit $f \in \mathscr{C}^1(\Omega)$ et soit $a \in \Omega$. On appelle **gradient** de f en a le vecteur

$$\nabla f(a) = \left(\frac{\partial f}{\partial x}(a), \frac{\partial f}{\partial y}(a) \right) \in \mathbb{R}^2\,.$$

➠ **Exemple XXVII.7.** Soit $f : (x,y) \mapsto x^3 + e^x y - 7$; alors :

$$\forall (x,y) \in \mathbb{R}^2, \quad \nabla f(x,y) = (3x^2 + e^x y, e^x)\,.$$

✌ **Remarque XXVII.11.** La proposition XXVII.6 se réécrit de la façon suivante : pour tout $a \in \Omega$ et tout $u \in \mathbb{R}^2$ tel que $a + u \in \Omega$:

$$f(a+u) = f(a) + \langle \nabla f(a)\,,\, u \rangle + o_0(\|u\|)\,,$$

en remarquant au passage que :

$$\mathrm{d}f(a)(u) = \langle \nabla f(a)\,,\, u \rangle\ .$$

Si l'on suppose que $\nabla f(a) \neq 0$ et que l'on prend $u \neq (0,0)$, alors on a :

$$f(a+u) - f(a) = \|\nabla f(a)\|\|u\| \cos(\theta) + o_0(\|u\|)\,,$$

où θ est l'écart angulaire (*cf.* XXV) entre $\nabla f(a)$ et u. À la louche, en fixant $\|u\|$, on obtient que la valeur absolue $|f(a+u) - f(a)|$ est maximale lorsque $\theta \equiv 0\,[2\pi]$ ou $\theta \equiv \pi\,[2\pi]$, *i.e* lorsque $\nabla f(a)$ et u sont colinéaires dans $\mathbb{R}^2$. On en déduit que **le gradient de f en a définit la direction dans laquelle f croît le plus vite** au voisinage de a.

Vocabulaire. Un point $a \in \Omega$ tel que $\nabla f(a) = (0,0)$ est appelé **point critique** de la fonction f.

Le lecteur perspicace se souviendra que lorsqu'il est question de points critiques, les extrema ne sont généralement pas loin. Ce lecteur a raison.

Définition XXVII.8. Soit $f \in \mathscr{C}^1(\Omega)$ et soit $a \in \Omega$. Alors :
- on dit que f admet un **maximum** (resp. minimum) **local** en a si :
$$\exists \varepsilon > 0,\ \forall x \in D(a,\varepsilon) \cap \Omega, \quad f(x) \leq f(a) \quad (\text{resp. } f(x) \geq f(a))\ ;$$
- on dit que f admet un **maximum** (resp. minimum) **global** en a si :
$$\forall x \in \Omega, \quad f(x) \leq f(a) \quad (\text{resp. } f(x) \geq f(a))\,.$$

L'étude des extrema locaux de fonctions de plusieurs variables est sensiblement plus subtile que son analogue dans le cas univarié. En effet, une surface possède une infinité de directions dans lesquelles elle peut "monter" ou "descendre" au voisinage d'un point. On note toutefois avec soulagement que l'on dispose d'une condition nécessaire analogue à celle vue au chapitre XI (proposition XI.9).

Proposition XXVII.7. Soit $f \in \mathscr{C}^1(\Omega)$ et soit $a \in \Omega$. **Si** f admet un extremum local en a, **alors** $\nabla f(a) = 0$.

Démonstration. Supposons, pour fixer les idées, que f admet un maximum local en a et soit $u \in \mathbb{R}^2$. Alors, pour tout $t \in \mathbb{R}_+^*$ assez proche de zéro, on a $a + tu \in \Omega$ et $f(a+tu) \leq f(a)$, ce qui entraîne que
$$\frac{f(a+tu) - f(a)}{t} \leq 0$$
et donc en passant à la limite quand $t \to 0$, on obtient que $\mathrm{d}f(a)(u) \leq 0$. Le même raisonnement mené avec $t < 0$ nous livre l'inégalité inverse et donc $\mathrm{d}f(a)(u) = 0$; en particulier on a bien $\nabla f(a) = 0$. □

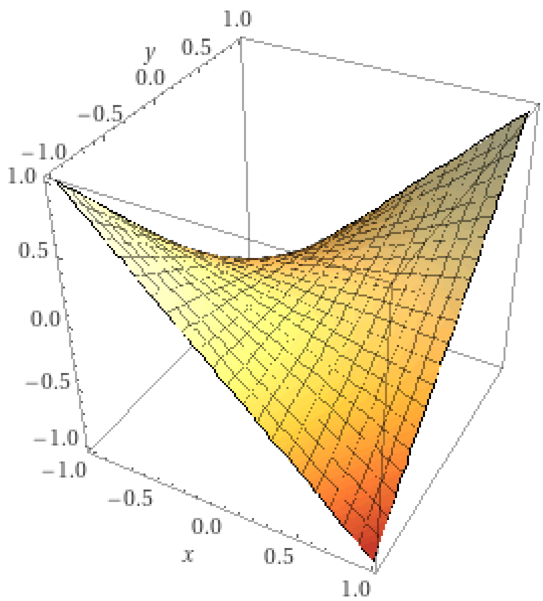
✌ **Remarque XXVII.12.** La démonstration *supra* nous indique qu'en plus du gradient, toutes les dérivées selon un vecteur donnée sont nulles en un extremum local. Le plan tangent est alors "horizontal", *i.e* de direction "$z = 0$".

➠ **Exemple XXVII.8.**
- Il est aisé de vérifier que $(x, y) \mapsto x^2 + y^2$ admet un minimum local et un point critique en $(0, 0)$.
- La fonction $f : (x, y) \mapsto x^2 - y^2$ admet un point critique en $(0, 0)$. Cependant, si $t \in \mathbb{R}_+^*$ on a :
$$f(t, 0) = t^2 > 0 \quad \text{et} \quad f(0, t) = -t^2 < 0$$
ce qui prouve que f n'admet ni un maximum local ni un minimum local en $(0, 0)$. La réciproque de la proposition XXVII.7 est donc, une fois n'est pas coutume, **fausse.**

✍ **Exercice XXVII.2.** Déterminer les éventuels extrema locaux de la fonction $f : (x, y) \mapsto xy^3$.

➥ **Correction :** *La fonction f est de classe $\mathscr{C}^1$ sur $\mathbb{R}^2$ car polynomiale. De plus, pour tout $(x, y) \in \mathbb{R}^2$:*
$$\nabla f(x, y) = (y^3, 3xy^2)$$

et donc les seuls points critiques de f sont les $(t, 0)$, pour $t \in \mathbb{R}$, et $f(t{\cdot}0) = 0$. Si x et y sont de même signe, on a $f(x, y) > 0$; à l'inverse, si ils sont de signes opposés, on a $f(x, y) < 0$. De fait, f n'admet aucun extremum local.



d) Composition

Proposition XXVII.8 (Règle de la chaîne)**.** Soit I un intervalle de $\mathbb{R}$, $f \in \mathscr{C}^1(\Omega)$, et $x, y \in \mathscr{C}^1(I)$ telles que :

$$\forall t \in I,\ (x(t), y(t)) \in \Omega\,.$$

Alors :

(i) la fonction $g : t \mapsto f(x(t), y(t))$ est de classe $\mathscr{C}^1(I)$;

(ii) pour tout $t \in I$, on a :

$$g'(t) = x'(t)\frac{\partial f}{\partial x}(x(t), y(t)) + y'(t)\frac{\partial f}{\partial y}(x(t), y(t))\,.$$

Démonstration. Soit $t \in I$ et $h \in \mathbb{R}^*$ tel que $t + h \in I$; si on pose $T = (x(t), y(t))$ et $U = (x(t+h), y(t+h))$ on a :

$$\begin{aligned} g(t+h) - g(t) &= f(U) - f(T) \\ &= \langle \nabla f(T)\,,\, U - T\rangle + o_0(\|U - T\|) \end{aligned}$$

d'après la proposition XXVII.6. De plus, comme $x, y \in \mathscr{C}^1(I)$ on a (*cf.* proposition XI.1) :

$$\begin{aligned} U - T &= (x(t+h) - x(t), y(t+h) - y(t)) \\ &= (hx'(t) + o_0(h), hy'(t) + o_0(h)) \end{aligned}$$

ce qui entraîne que $o_0(\|U-T\|) = o_0(h)$ et donc :

$$g(t+h) - g(t) = (hx'(t) + o_0(h))\frac{\partial f}{\partial x}((x(t), y(t)) + (hy'(t) + o_0(h))\frac{\partial f}{\partial y}(x(t), y(t)) + o_0(h)$$

ergo :

$$\begin{aligned}\frac{g(t+h)-g(t)}{h} &= (x'(t) + o_0(1))\frac{\partial f}{\partial x}((x(t), y(t)) + (y'(t) + o_0(1))\frac{\partial f}{\partial y}(x(t), y(t)) + o_0(1)\\ &\xrightarrow[h\to 0]{} x'(t)\frac{\partial f}{\partial x}(x(t), y(t)) + y'(t)\frac{\partial f}{\partial y}(x(t), y(t))\end{aligned}$$

d'où le résultat. □

Remarque XXVII.13.

— Cette formule peut se résumer, "à la physicienne", de la façon suivante :

$$\frac{\mathrm{d}g}{\mathrm{d}t} = \frac{\mathrm{d}x}{\mathrm{d}t}\frac{\partial f}{\partial x} + \frac{\mathrm{d}y}{\mathrm{d}t}\frac{\partial f}{\partial y}$$

pour peu que l'on sache en quels points ces dérivées sont calculées, ce qui se déduit aisément du contexte.

— Cinématiquement / géométriquement, la fonction g correspond à la "restriction" de f le long d'un arc paramétré par $\gamma : t \mapsto (x(t), y(t))$. La règle de la chaîne se réécrit alors :

$$\forall t \in I, \quad (f\circ\gamma)'(t) = \langle \nabla f(\gamma(t)) \,, \, \gamma'(t)\rangle \;.$$

Cette expression correspond à la dérivée de f le long de l'arc γ. Ce type de considération est très courant (par exemple) en mécanique. Par exemple, pour déterminer la distance maximale ou minimal d'un mobile $t \mapsto (x(t), y(t))$ à l'origine, on pourra étudier les extrema de $t \mapsto x(t)^2 + y^2(t)$.

Définition XXVII.9. Soit $f : \Omega \to \mathbb{R}$ et soit $c \in \mathbb{R}$. On appelle **ligne de niveau** c de f l'ensemble (éventuellement vide) :

$$\mathscr{L}_c(f) = \{(x,y) \in \Omega \,|\, f(x,y) = c\} \,.$$

Exemple XXVII.9. Sur une carte IGN, on peut lire les lignes de niveau de la fonction qui à un point (x, y) du plan associe l'altitude (relative au niveau de la mer) au sol en ce point.

Exercice XXVII.3. Déterminer les lignes de niveau des fonction $(x, y) \mapsto x^2+y^2$ et $g : (x, y) \mapsto x^2 - y$.

Proposition XXVII.9. Soit $f \in \mathscr{C}^1(\Omega)$ et soit $c \in \mathbb{R}$. Alors, pour tout arc paramétré de classe $\mathscr{C}^1$ (coordonnée par coordonnée) $\gamma : I \to \mathscr{L}_c(f)$ on a :

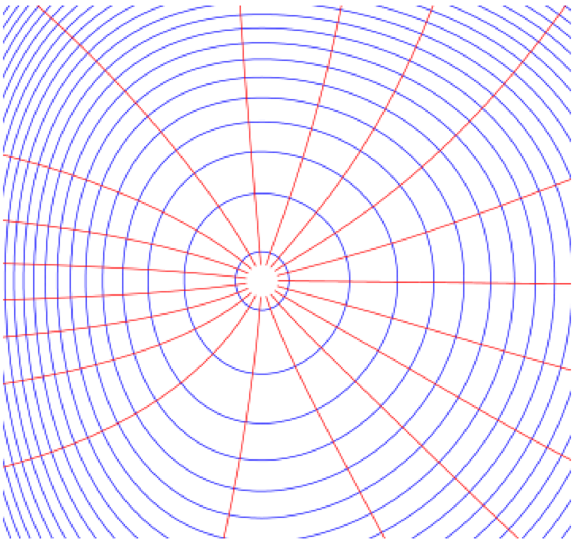
$$\forall t \in I, \quad \langle \nabla f(\gamma(t)), \gamma'(t) \rangle = 0$$

Démonstration. Si γ vérifie les conditions de l'énoncé, d'après la remarque XXVII.13 :

$$\forall t \in I, \quad (f \circ \gamma)'(t) = \langle \nabla f(\gamma(t)), \gamma'(t) \rangle \ .$$

Or, par définition de $\mathscr{L}_c(f)$, la fonction $f \circ \gamma$ est constante égale à c, d'où le résultat. □

Remarque XXVII.14. Cela signifie que le gradient est "orthogonal" en tout point à toute courbe de niveau passant par ce point, au sens où il est orthogonal à la tangente (dirigée par $\gamma'(t)$ en tout t) de celle–ci.



Proposition XXVII.10 (Règle de la chaîne généralisée)**.** Soit Λ un ouvert de $\mathbb{R}^2$, $f \in \mathscr{C}^1(\Omega)$ et $u, v : \Lambda \to \mathbb{R}$ deux fonctions de classes $\mathscr{C}^1$ telles que :

$$\forall x, y \in \Lambda,\ (u(x,y), v(x,y)) \in \Omega\,.$$

Alors :

(i) la fonction $g : (x,y) \mapsto f(u(x,y), v(x,y))$ est de classe $\mathscr{C}^1$ sur Λ ;

(ii) pour tout $(x,y) \in \Lambda$ on a :

$$\frac{\partial g}{\partial x}(x,y) = \frac{\partial u}{\partial x}(x,y)\frac{\partial f}{\partial x}(u(x,y), v(x,y)) + \frac{\partial v}{\partial x}(x,y)\frac{\partial f}{\partial y}(u(x,y), v(x,y))$$

et

$$\frac{\partial g}{\partial y}(x,y) = \frac{\partial u}{\partial y}(x,y)\frac{\partial f}{\partial x}(u(x,y), v(x,y)) + \frac{\partial v}{\partial y}(x,y)\frac{\partial f}{\partial y}(u(x,y), v(x,y))\,.$$

Démonstration. Beurk. □

✌ **Remarque XXVII.15.** Si on prend le partie de noter $\frac{\partial f}{\partial u}$ et $\frac{\partial f}{\partial v}$ les dérivées partielles de f, on peut "résumer" (comme pour la règle de la chaîne "basique") la proposition *supra* par les "formules" suivante :

$$\frac{\partial g}{\partial x} = \frac{\partial u}{\partial x}\frac{\partial f}{\partial u} + \frac{\partial v}{\partial x}\frac{\partial f}{\partial v}$$

et

$$\frac{\partial g}{\partial y} = \frac{\partial u}{\partial y}\frac{\partial f}{\partial u} + \frac{\partial v}{\partial y}\frac{\partial f}{\partial v}\,.$$

✍ **Exercice XXVII.4.** Déterminer toutes les fonctions $f \in \mathscr{C}^1(\mathbb{R}^2)$ vérifiant l'équation :

$$\frac{\partial f}{\partial x} + \frac{\partial f}{\partial y} = 0\,. \qquad \text{(**E** :XXVII.1)}$$

On pourra faire usage du changement de variable $u = x+y$, $v = x-y$.

➥ **Correction :** *Procédons par analyse–synthèse et supposons trouvée f solution de (**E** :XXVII.1). Alors, comme les fonctions $u : (x,y) \mapsto x+y$ et $v : (x,y) \mapsto x-y$ sont de classe $\mathscr{C}^1$, la fonction $\varphi : (x,y) \mapsto (x+y, x-y)$ est une bijection $\mathscr{C}^1$ de $\mathbb{R}^2$. En posant $g = f \circ \varphi^{-1}$ on, par proposition XXVII.10 et comme $f = g \circ \varphi$, pour tout $(x,y) \in \mathbb{R}^2$:*

$$\frac{\partial f}{\partial x}(x,y) = \frac{\partial g}{\partial u}(x+y, x-y) + \frac{\partial g}{\partial v}(x+y, x-y)$$

et

$$\frac{\partial f}{\partial y}(x,y) = \frac{\partial g}{\partial u}(x+y, x-y) - \frac{\partial g}{\partial v}(x+y, x-y)\,.$$

De fait, en réinjectant dans l'équation, on obtient :

$$\frac{\partial g}{\partial u}(x+y, x-y) = 0$$

ce qui signifie qu'il existe G de classe $\mathscr{C}^1$ sur $\mathbb{R}$ telle que :

$$\forall x, y \in \mathbb{R},\ g(x+y, x-y) = G(x-y)$$

i.e

$$\forall (x,y) \in \mathbb{R}^2,\ f(x,y) = G(x-y)\,.$$

*On vérifie ensuite rapidement que les fonctions de cette forme sont bien solution de (**E** :XXVII.1).*

Addendum : méthode des moindres carrés

Ce qui suit n'est pas *stricto sensu* au programme mais nous semble un approfondissement adapté aux sujets déjà étudiés.

Nous nous intéressons dans ce paragraphe à une méthode de **régression linéaire** : l'idée est que l'on dispose de n points (x_i, y_i) du plan d'abscisses deux à deux distinctes, que l'on cherche à "approcher" par une droite affine d'équation $y = ax + b$ "raisonnablement proche" (pour parler comme un chimiste) de ces derniers. Deux (ou trois) questions nous viennent alors (en tous cas je l'espère) à l'esprit :

— quel sens donner à "raisonnablement proche" ?

— Cela est–il toujours réalisable ? Et si oui, comment ?

Pour formaliser ceci, introduisons la fonction suivante :

$$\begin{aligned} J :\ \mathbb{R}^2 &\longrightarrow \mathbb{R} \\ (a,b) &\mapsto \sum_{i=1}^{n} (y_i - (ax_i + b))^2\,. \end{aligned}$$

Cette fonction calcule la somme la somme des carrés des distances des points (x_i, y_i) à une droite d'équation donnée. Minimiser J semble donc une bonne idée pour trouver des paramètres a et b définissant une droite "raisonnablement proche" de notre nuage de points.

Existence du minimum

Commençons par remarquer que J est une fonction de classe $\mathscr{C}^1$ de $\mathbb{R}^2$ dans $\mathbb{R}$ à valeurs positives. De fait, l'ensemble (non vide) $J(\mathbb{R}^2)$ admet une borne inférieure positive. Le problème devient donc de savoir si cette dernière est atteinte.

On se place dans $\mathbb{R}^n$ muni de son produit scalaire canonique. Alors, en posant $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$ et $e = (1, \dots, 1)$, on a :

$$\forall a, b \in \mathbb{R}, \quad J(a,b) = \|y - (ax + be)\|^2$$

et donc, si on pose $F = \mathrm{Vect}(x, e)$, on a :

$$\inf(J) = d(y, F)\,.$$

F est un s–e.v de $\mathbb{R}^n$ de dimension 2 (car les x_i sont deux à deux distincts), donc cette distance est atteinte en le projeté orthogonal de y sur F : $\min(J)$ existe donc.

Calcul explicite

Pour le calcul effectif du minimum, il serait possible de déterminer le projeté orthogonal mentionné *supra* par les méthodes vues au chapitre XXV. Cependant, il est bien plus rapide ici de s'intéresser aux point(s) critique(s) de J. En effet, on a pour tous $a, b \in \mathbb{R}$:

$$\frac{\partial J}{\partial a}(a,b) = -2\sum_{i=1}^{n} x_i(y_i - ax_i - b)$$

et

$$\frac{\partial J}{\partial b}(a,b) = -2\sum_{i=1}^{n} (y_i - ax_i - b)\,.$$

Posons :

$$\mu_x = \sum_{i=1}^{n} x_i^2,\ \ \lambda_x = \sum_{i=1}^{n} x_i,\ \ \lambda_y = \sum_{i=1}^{n} y_i \ \text{ et }\ \mu_{xy} = \sum_{i=1}^{n} x_i y_i\,;$$

on a alors que (a, b) est un point critique de J si et seulement si :

$$\left\{\begin{array}{rcl} \mu_x a + \lambda_x b & = & \mu_{xy} \\ \lambda_x a + nb & = & \lambda_y \end{array}\right.$$

Les x_i étant deux à deux distincts, on a $n\mu_x - \lambda_x^2 \neq 0$ (appliquer l'inégalité de Cauchy–Schwarz aux vecteurs x et e) et donc ce système admet une unique solution donnée par :

$$a = \frac{n\mu_{xy} - \lambda_x\lambda_y}{n\mu_x - \lambda_x^2} \quad \text{ et } b = \frac{\lambda_y\mu_x - \lambda_x\mu xy}{n\mu_x - \lambda_x^2}\,.$$

Comme J admet un minimum et un unique point critique, ces derniers sont confondus : nous venons de déterminer les paramètres optimaux de régression linéaire (au sens de notre fonction J), qui sont *in fine* donnés par la magnifique expression suivante[1] :

$$a = \frac{n\sum\limits_{i=1}^{n} x_i y_i - \left(\sum\limits_{i=1}^{n} x_i\right)\left(\sum\limits_{i=1}^{n} y_i\right)}{n\sum\limits_{i=1}^{n} x_i^2 - \left(\sum\limits_{i=1}^{n} x_i\right)^2} \quad \text{ et } b = \frac{\left(\sum\limits_{i=1}^{n} x_i\right)\left(\sum\limits_{i=1}^{n} x_i^2\right) - \left(\sum\limits_{i=1}^{n} x_i\right)\left(\sum\limits_{i=1}^{n} x_i y_i\right)}{n\sum\limits_{i=1}^{n} x_i^2 - \left(\sum\limits_{i=1}^{n} x_i\right)^2}\,.$$

Vision probabiliste

Nous donnons dans ce paragraphe une vision probabiliste[2] du résultat précédent. Pour ce faire, plaçons nous dans un espace probabilisé $(\Omega, \mathbb{P})$ et considérons que nos points (x_i, y_i) sont en réalité une série de n réalisations d'un couple de variables aléatoires réelles (X, Y). Plus précisément, supposons que :

$$\forall i \in [\![1, n]\!], \quad (x_i, y_i) \in X \times Y(\Omega)$$

et rajoutons l'hypothèse (raisonnable !) que $V(X) \neq 0$.

1. Lunettes de protection recommandées.
2. En vérité, cela relève plutôt d'une approche statistique mais préservons notre santé mentale, voulez–vous.

Remarquons que, par loi faible des grands nombres, on peut "raisonnablement" approximer l'espérance de X par sa moyenne empirique, *i.e*, à la statisticienne :

$$\mathbb{E}(X) \cong \frac{1}{n}\sum_{i=1}^{n} x_i$$

et, similairement :

$$V(X) = \mathbb{E}(X^2) - \mathbb{E}(X)^2 \cong \frac{1}{n}\sum_{i=1}^{n} x_i^2 - \frac{1}{n^2}\left(\sum_{i=1}^{n} x_i\right)^2 .$$

En persévérant dans cette approche, on arrive à l'approximation :

$$\mathrm{Cov}(X,Y) \cong \frac{1}{n}\left(\sum_{i=1}^{n} x_i y_i\right) - \frac{1}{n^2}\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{i=1}^{n} y_i\right) .$$

Ainsi, les coefficients optimaux déterminés dans la section précédente deviennent :

$$a = \frac{\mathrm{Cov}(X,Y)}{V(X)} \quad \text{et } b = \mathbb{E}(Y) - \frac{\mathrm{Cov}(X,Y)}{V(X)}\mathbb{E}(X) .$$

Cette approche nous permet de réaliser rapidement une régression linéaire de réalisations de variables aléatoires dont les lois sont connues ou supposées (pour des raisons physiques, par exemple).

Généralisations diverses

Il est possible de généraliser l'approche développée ici à l'approximation de nuages de points par des fonctions non affines. On sera amené à considérer des applications du type :

$$J : f \mapsto \sum_{i=1}^{n}(y_i - f(x_i))^2$$

définies sur un espace de fonctions raisonnable (idéalement décrit par un nombre fini de paramètres). Par exemple, on pourra s'intéresser aux fonctions polynomiales de degré borné ou à des familles d'exponentielles à paramètres.

Il est important de noter que ces espaces fonctionnels seront rarement des $\mathbb{R}$–e.v de dimension finie : l'existence du minimum de J ne sera donc pas toujours aisée à établir, et son calcul explicite peut être difficile.

Chapitre XXVIII

Familles sommables

Nous fixons dans ce chapitre un ensemble I quelconque.

1.⁻ Familles sommables de réels positifs

a) C'est quoi ?

Proposition XXVIII.1. Soit $(u_i)_{i\in I}$ de réels positifs. Alors l'ensemble

$$S(u) = \left\{ \sum_{i\in J} u_i \,\middle|\, J \subset I \text{ fini} \right\}$$

admet une borne supérieure dans $\overline{\mathbb{R}}$.

Démonstration. L'ensemble $S(u)$ est une partie de $\overline{\mathbb{R}}$ et donc admet une borne supérieure d'après la proposition III.9. Notons de plus que $S(u) \subset \mathbb{R}_+$, ce qui entraîne que $\sup(S(u)) \in \mathbb{R}_+ \cup \{+\infty\}$. □

Notation. La quantité $\sup(S(u))$ est appelée **somme** de la famille $(u_i)_{i\in I}$ et est notée $\sum_{i\in I} u_i$.

✌ **Remarque XXVIII.1.** Comme indiqué dans la démonstration *supra*, on a :

$$\sum_{i\in I} u_i \in \mathbb{R}_+ \cup \{+\infty\} .$$

Notons au passage que la somme d'une famille de réels positifs existe **toujours** (mais peut être égale à $+\infty$).

Définition XXVIII.1. Une famille $(u_i)_{i\in I}$ est dite **sommable** si

$$\sum_{i\in I} u_i < +\infty .$$

Remarque XXVIII.2. Cela est équivalent à dire que la somme de la famille appartient à $\mathbb{R}_+$. Notons que dans le cas présent, une famille est soit sommable, soit de somme infinie, ce qui est fort pratique car l'on peut toujours "calculer" sa somme.

Exemple XXVIII.1.

— La famille $u = \left(\frac{1}{n}\right)_{n\in\mathbb{N}^*}$ n'est pas sommable. En effet, l'ensemble $S(u)$ contient les sommes

$$H_N = \sum_{n=1}^{N} \frac{1}{N}$$

qui sont équivalentes à $\ln(N)$ lorsque $N \to \infty$ (*cf.* chapitre XXII) et donc ne sont pas bornées. De fait, $\sup(S(u)) = +\infty$.

— Fixons $x \in [0, 1[$ et étudions le caractère sommable de la famille $u = (x^{|n|})_{n\in\mathbb{Z}}$; pour ce faire, fixons $F \subset \mathbb{Z}$ un ensemble fini et remarquons que :

$$\sum_{n\in F} x^{|n|} = \underbrace{\sum_{n\in F\cap\mathbb{N}} x^n}_{S_1} + \underbrace{\sum_{n\in F\setminus\mathbb{N}} x^{-n}}_{S_2} .$$

Posons $M = \max\{|n| \mid n \in F\}$; alors on a :

$$S_1 \leq \sum_{n=0}^{M} x^n = \frac{1 - x^{M+1}}{1 - x} \leq \frac{1}{1 - x}$$

et :

$$S_2 \leq \sum_{n=-M}^{-1} x^{-n} = \sum_{n=1}^{M} x^n = x\frac{1 - x^M}{1 - x} \leq \frac{x}{1 - x} .$$

In fine, on en déduit que :

$$\sum_{n\in F} x^{|n|} = S_1 + S_2 \leq \frac{1 + x}{1 - x}$$

et donc, comme ce majorant ne dépend pas de l'ensemble F, il majore l'ensemble $S(u)$. On en déduit que la borne supérieure de cet ensemble existe dans $\mathbb{R}_+$ et donc que la famille u est sommable. Par ailleurs, remarquons que, pour tout $N \geq 1$:

$$\begin{aligned}
\sum_{n=-N}^{N} x^{|n|} &= \sum_{n=0}^{N} x^n + \sum_{n=-N}^{-1} x^{-n} \\
&= \sum_{n=0}^{N} x^n + \sum_{n=1}^{N} x^n \\
&= \frac{1 - x^{N+1}}{1 - x} + \frac{x - x^{N+1}}{1 - x} \\
&= \frac{1 + x - 2x^{N+1}}{1 - x} \\
&\xrightarrow[N\to\infty]{} \frac{1 + x}{1 - x}
\end{aligned}$$

et donc, par caractérisation séquentielle de la borne supérieure (proposition VII.22), on a :

$$\sum_{n\in\mathbb{Z}} x^{|n|} = \frac{1+x}{1-x}\,.$$

Proposition XXVIII.2. Soit $(u_i)_{i\in I}$ une famille sommable de réels positifs et soit $J \subset I$. Alors :

(i) la famille $(u_i)_{i\in J}$ est sommable ;

(ii)

$$\sum_{i\in J} u_i \leq \sum_{i\in I} u_i\,.$$

Démonstration. Alors, si on pose $u' = (u_i)_{i\in J}$, a clairement $S(u') \subset S(u)$ et donc, dans $\overline{\mathbb{R}}$, $\sup(S(u')) \leq \sup(S(u))$. La borne supérieure de $S(u)$ étant finie, on obtient le résultat voulu. □

Exemple XXVIII.2. La famille $(x^{2|n|+1})_{n\in\mathbb{Z}}$ est sommable pour $x \in]0,1[$ (considérer $J = \{k \in \mathbb{Z} \mid |k| \equiv 1\,[2]\}$.

Proposition XXVIII.3. Soient $(u_i)_{i\in I}$ et $(v_i)_{i\in I}$ deux familles de réels positifs telles que $\forall i \in I$, $u_i \leq v_i$. Alors :

$$\sum_{i\in I} u_i \leq \sum_{i\in I} v_i\,.$$

Démonstration. Si $F \subset I$ est un ensemble fini alors on a, par définition de borne supérieure :

$$\sum_{i\in F} u_i \leq \sum_{i\in F} v_i \leq \sum_{i\in I} v_i\,.$$

Ceci entraîne que $\sum\limits_{i\in I} v_i$ majore $S(u)$ et donc que :

$$\sup(S(u)) = \sum_{i\in J} u_i \leq \sum_{i\in I} u_i\,.$$

□

Remarque XXVIII.3. On en déduit que la sommabilité de $(v_i)_i$ (resp. la non sommabilité de $(u_i)_i$) entraîne celle de $(u_i)_i$ (resp. de $(v_i)_i$).

b) Exemples fondamentaux

Proposition XXVIII.4. Si $I = \{i_1, \dots, i_n\}$ est un ensemble fini, toute famille $(u_i)_{i\in I} \in (\mathbb{R}_+)^I$ est sommable et :

$$\sum_{i\in I} u_i = \sum_{k=1}^{n} u_{i_k} .$$

Démonstration. Par positivité on a, pour tout $F \subset I$ (automatiquement fini, donc) :

$$\sum_{i\in F} u_i \leq \sum_{k=1}^{n} u_{i_k} .$$

Ceci entraîne que $\sup(S(u))$ est fini et majoré par $\sum_{k=1}^{n} u_{i_k}$. Cette borne étant atteinte en $F = I$, on obtient le résultat désiré. □

✌ **Remarque XXVIII.4.** Ceci est plutôt rassurant, nous en convenons.

Proposition XXVIII.5. Soit $(u_n)_n$ une suite de réels positifs. Alors :

(i) la famille $(u_n)_n$ est sommable si et seulement si la série $\sum u_n$ converge ;

(ii) dans ce cas, on a :

$$\sum_{n\in\mathbb{N}} u_n = \sum_{n=0}^{\infty} u_n .$$

Démonstration. Soit $F \subset N$ un ensemble fini ; on peut alors poser $N = \max(F)$. Si la série $\sum u_n$ converge, on a par positivité :

$$\sum_{n\in F} u_n \leq \sum_{n=0}^{N} u_n \leq \sum_{n=0}^{\infty} u_n$$

et donc la famille $(u_n)_n$ est sommable, avec :

$$\sum_{n\in\mathbb{N} u_n} \leq \sum_{n=0}^{\infty} u_n .$$

Pour démontrer l'égalité, il ne nous reste qu'à remarquer que, pour $F = [\![0, N]\!]$:

$$\sum_{n\in F} u_n = \sum_{n=0}^{N} u_n \xrightarrow[N\to\infty]{} \sum_{n=0}^{\infty} u_n$$

et à appliquer la caractérisation séquentielle de la borne supérieure (proposition VII.22).

Inversement, si la série $\sum u_n$ est divergente, alors on a, par positivité, que :

$$\forall M \in \mathbb{R}_+,\ \exists N \in \mathbb{N}, \quad \sum_{n=0}^{N} u_n \geq M\,.$$

On en déduit que l'ensemble $S(u)$ n'est pas majoré et donc que sa borne supérieure dans $\overline{\mathbb{R}}$ est égale à $+\infty$. □

c) Opérations sur les sommes

Proposition XXVIII.6 (Invariance par permutation)**.** Soit $(u_i)_{i\in I}$ une famille de réels positifs et soit $\sigma \in \mathfrak{S}(I)$. Alors :

$$\sum_{i\in I} u_{\sigma(i)} = \sum_{i\in I} u_i\,.$$

En particulier, la famille $(u_{\sigma(i)})_{i\in I}$ est sommable si et seulement $(u_i)_{i\in I}$ l'est.

Démonstration. Si $F \subset I$ est un ensemble fini, alors $G = \sigma(F)$ est également une partie finie de I (de même cardinal que F) et l'on a :

$$\sum_{i\in F} u_{\sigma(i)} = \sum_{j\in G} u_j \leq \sum_{i\in I} u_i$$

et donc, par majoration :

$$\sum_{i\in I} u_{\sigma(i)} \leq \sum_{i\in I} u_i\,.$$

Réciproquement, en posant $H = \sigma^{-1}(F)$:

$$\sum_{i\in F} u_i = \sum_{i\in F} u_{\sigma(\sigma^{-1}(i))} = \sum_{j\in H} u_{\sigma(j)} \leq \sum_{i\in I} u_{\sigma(i)}$$

ergo, par majoration :

$$\sum_{i\in I} u_i \leq \sum_{i\in I} u_{\sigma(i)}\,,$$

d'où le résultat. □

✌ **Remarque XXVIII.5.** Un corollaire de ce résultat est que pour toute série $\sum u_n$ à termes positifs et toute bijection $\sigma \in \mathfrak{S}(\mathbb{N})$, la convergence de la série $\sum u_{\sigma(n)}$ équivaut à celle de $\sum u_n$ et on a, le cas échéant, l'égalité :

$$\sum_{n=0}^{\infty} u_{\sigma(n)} = \sum_{n=0}^{\infty} u_n\,.$$

✖ **Attention :** ce résultat est faux en général ; nous citons *infra* un résultat hors programme mais édifiant.

Théorème XXVIII.7 (Théorème de réarrangement de Riemann)**.**
Soit $\sum u_n$ une série réelle convergente mais non absolument convergente et soit $M \in \mathbb{R}$ un réel quelconque. Alors il existe une bijection $\sigma \in \mathfrak{S}(\mathbb{N})$ telle que la série $\sum u_{\sigma(n)}$ converge et que

$$\sum_{n=0}^{\infty} u_{\sigma(n)} = M\,.$$

Proposition XXVIII.8. Soient $(u_i)_{i\in I}$ et $(v_i)_{i\in I}$ deux familles de réels positifs et soit $\mu \in \mathbb{R}_+$. Alors :

$$\sum_{i\in I} u_i + \mu v_i = \sum_{i\in I} u_i + \mu \sum_{i\in I} v_i\,.$$

✖ **Attention : nous avons supposé μ positif.**

Démonstration. Soit $F \subset I$ un ensemble fini. Alors :

$$\sum_{i\in F} u_i + \mu v_i = \sum_{F\in I} u_i + \mu \sum_{F\in I} v_i \leq \sum_{i\in I} u_i + \mu \sum_{i\in I} v_i$$

et donc par majoration

$$\sum_{i\in I} u_i + \mu v_i \leq \sum_{i\in I} u_i + \mu \sum_{i\in I} v_i\,.$$

De plus, par caracterisation séquentielle de la borne supérieure (proposition VII.22), il existe des ensembles finis $F_n, G_n \subset I$ tels que :

$$\sum_{i\in F_n} u_i \xrightarrow[n\to\infty]{} \sum_{i\in I} u_i \quad \text{et} \quad \sum_{i\in G_n} v_i \xrightarrow[n\to\infty]{} \sum_{i\in I} v_i\,.$$

De plus, notons que comme $F_n \subset F_n \cup G_n$ on a, pour tout $n \geq 0$:

$$\sum_{i\in F_n} u_i \leq \sum_{i\in F_n\cup G_n} u_i \leq \sum_{i\in I} u_i$$

et donc, par encadrement (théorème VII.11) on a :

$$\sum_{i\in F_n\cup G_n} u_i \xrightarrow[n\to\infty]{} \sum_{i\in I} u_i\,.$$

Un raisonnement similaire pouvant être appliqué à G_n, on obtient *in fine* :

$$\sum_{i\in F_n\cup G_n} u_i + \mu v_i = \sum_{F\in F_n\cup G_n} u_i + \mu \sum_{F\in F_n\cup G_n} v_i \xrightarrow[n\to\infty]{} \sum_{i\in I} u_i + \mu \sum_{i\in I} v_i$$

d'où le résultat, une fois encore par caractérisation séquentielle. □

d) Sommation par paquets

Théorème XXVIII.9 (Sommation par paquets)**.**
On suppose ici qu'il existe une famille $(I_j)_{j\in J}$ d'ensembles deux à deux disjoints tels que :

$$I = \bigsqcup_{j\in J} I_j$$

et on fixe $(u_i)_{i\in I}$ une famille de réels positifs. Alors on a :

$$\sum_{i\in I} u_i = \sum_{j\in J} \left(\sum_{i\in I_j} u_i \right).$$

Démonstration. Admis. □

Remarque XXVIII.6. On en déduit que la famille $(u_i)_{i\in I}$ est sommable si et seulement si les deux conditions suivantes sont vérifiées :

(i) les familles $(u_i)_{i\in I_j}$ sont sommables ;

(ii) la famille $\left(\sum_{i\in I_j} u_i \right)_{j\in J}$ est sommable.

Exemple XXVIII.3.

— On peut retrouver la somme de la famille $(x^{|n|})_{n\in\mathbb{Z}}$ en observant que $\mathbb{Z} = \mathbb{N} \sqcup \{n\in\mathbb{Z} \mid n<0\}$ et en appliquant le théorème XXVIII.9.

— Une partition classique (dite *diagonale*) de $\mathbb{N}^2$ est la suivante :

$$\mathbb{N}^2 = \bigsqcup_{n=0}^{\infty} \{(p,q)\in\mathbb{N}^2 \mid p+q=n\} = \bigsqcup_{n=0}^{\infty} \{(k,n-k) \mid k\in[\![0,n]\!]\}.$$

On en déduit que :

$$\begin{aligned}
\sum_{(p,q)\in\mathbb{N}^2} \frac{1}{p!q!(p+q+1)} &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} \frac{1}{k!(n-k)!(n+1)} \right) \\
&= \sum_{n=0}^{\infty} \frac{1}{n+1} \left(\sum_{k=0}^{n} \frac{1}{k!(n-k)!} \right) \\
&= \sum_{n=0}^{\infty} \frac{1}{(n+1)!} \left(\sum_{k=0}^{n} \binom{n}{k} \right) \\
&= \sum_{n=0}^{\infty} \frac{2^n}{(n+1)!} \\
&= \frac{1}{2} \sum_{n=1}^{\infty} \frac{2^n}{n!} \\
&= \frac{e^2-1}{2}.
\end{aligned}$$

✍ **Exercice XXVIII.1.** Soit $x \in [0,1[$; démontrer que :

$$\frac{x}{1-x} = \sum_{p=0}^{\infty} \frac{x^{2^p}}{1-x^{2^{p+1}}}.$$

➥ **Correction :** *Commençons par remarquer que l'égalité*

$$\mathbb{N}^* = \bigsqcup_{p=0}^{\infty} \{(2q+1)2^p \mid q \in \mathbb{N}\}$$

décrit une partition de $\mathbb{N}^*$ *(penser à la valuation* 2*–adique). De fait :*

$$\begin{aligned}
\frac{x}{1-x} &= \sum_{n=1}^{\infty} x^n \\
&= \sum_{p=0}^{\infty}\sum_{q=0}^{\infty} x^{(2q+1)2^p} \\
&= \sum_{p=0}^{\infty} x^{2^p}\left(\sum_{q=0}^{\infty} x^{2^p 2q}\right) \\
&= \sum_{p=0}^{\infty} x^{2^p}\left(\sum_{q=0}^{\infty} \left(x^{2^{p+1}}\right)^q\right) \\
&= \sum_{p=0}^{\infty} \frac{x^{2^p}}{1-x^{2^{p+1}}}.
\end{aligned}$$

Un cas particulier absolument fondamental du théorème XXVIII.9 est celui où l'ensemble I est un produit cartésien $A \times B$. En effet, on a dans ce cas :

$$I = \bigsqcup_{a \in A} \{a\} \times B = \bigsqcup_{b \in B} A \times \{b\}.$$

Ceci nous permet de démontrer le résultat suivant, souvent attribué au mathématicien italien Guido Fubini (1879—1943), spécialiste du calcul intégral.

Corollaire XXVIII.9.a (Fubini)**.** Soit $(u_{a,b})_{(a,b)\in A\times B}$ une famille de réels positifs. Alors :

$$\sum_{(a,b)\in A\times B} u_{a,b} = \sum_{a\in A}\left(\sum_{b\in B} u_{a,b}\right) = \sum_{b\in B}\left(\sum_{a\in A} u_{a,b}\right).$$

➠ **Exemple XXVIII.4.** Soit $x \in [0,1[$; alors par théorème de Fubini (corollaire

XXVIII.9.a) on a :

$$\begin{aligned}
\sum_{(p,q)\in\mathbb{N}^2} x^{p+q} &= \sum_{p\in\mathbb{N}}\left(\sum_{q\in\mathbb{N}} x^p x^q\right)\\
&= \sum_{p\in\mathbb{N}} x^p\left(\sum_{q\in\mathbb{N}} x^q\right)\\
&= \sum_{p\in\mathbb{N}} x^p\left(\sum_{q=0}^{\infty} x^q\right)\\
&= \sum_{p\in\mathbb{N}} x^p \frac{1}{1-x}\\
&= \frac{1}{1-x}\sum_{p\in\mathbb{N}} x^p\\
&= \frac{1}{(1-x)^2}\,.
\end{aligned}$$

✍ **Exercice XXVIII.2.** Soit $x \in [0, e^{-1}[$; démontrer que :

$$\sum_{(p,q)\in\mathbb{N}^2} \frac{x^q q^p}{p!} = \frac{1}{1-xe}\,.$$

2.⁻ Familles sommables numériques

L'objectif de ce paragraphe est de généraliser les notions que nous venons d'aborder au cas général de familles de nombres complexes. Notons que ceci va nous demander bien plus de précautions et de vigilance quant aux hypothèses ; il serait dommageable au lecteur d'envisager cette partie du cours comme une simple extension des résultats précédemment démontrés.

a) Notion de sommabilité

Définition XXVIII.2. Une famille de nombres complexes $(u_i)_{i\in I}$ sera dite **sommable** si la famille **de réels positifs** $(|u_i|)_{i\in I}$ l'est, *i.e* si l'on, dans $\overline{\mathbb{R}}$:

$$\sum_{i\in I} |u_i| < \infty\,.$$

Notation. L'ensemble des familles sommables indexées par I sera noté $\ell^1(I)$.

✌ **Remarque XXVIII.7.**

— Les familles de réels positifs sommables sont également sommable au sens de la définition *supra*. Cela va sans dire, mais va mieux en le disant.

— Il découle de la proposition XXVIII.2 que toute sous–famille d'une famille sommable est sommable.

— L'ensemble $\ell^1(\mathbb{N})$ est, d'après la proposition XXVIII.5, égal à l'ensemble des séries **absolument** convergentes.

✖ **Attention :** la sommabilité d'une famille numérique indexée par $\mathbb{N}$ n'est donc pas équivalente à la convergence de la série associée : penser à $\sum \frac{(-1)^n}{n+1}\dots$

➠ **Exemple XXVIII.5.** Soit $\theta \in \mathbb{R}$; alors la famille $\left(\dfrac{e^{in\theta}}{n^2}\right)_{n\geq 1}$ est sommable.

Proposition XXVIII.10. Soit $(u_i)_{i\in I}$ une famille de nombres complexes et soit $(v_i)_{i\in I}$ une famille de nombres réels **positifs**. On suppose que :

1. la famille $(v_i)_{i\in I}$ est sommable ;
2. $\forall i \in I$, $|u_i| \leq v_i$.

Alors la famille $(u_i)_{i\in I}$ est sommable.

Démonstration. Découle trivialement de la proposition XXVIII.3. □

➠ **Exemple XXVIII.6.** Si $x \in \mathbb{C}^*$, on a pour tout $n \in \mathbb{Z}$, $|x^{|n|}| = |x|^{|n|}$. On en déduit que la famille $(x^{|n|})_{n\in\mathbb{Z}}$ est sommable lorsque $|x| < 1$ d'après un exemple précédemment traité.

b) Somme d'une famille sommable

Proposition/définition XXVIII.3. Une famille $(u_i)_{i\in I}$ de nombres **réels** est sommable si et seulement si les familles de réels **positifs** $(u_i^+)_{i\in I}$ et $(u_i^-)_{i\in I}$ le sont. Dans ce cas, on appelle **somme** de la famille $(u_i)_{i\in I}$ la quantité

$$\sum_{i\in I} u_i = \sum_{i\in I} u_i^+ - \sum_{i\in I} u_i^- \in \mathbb{R}\,.$$

✌ **Remarque XXVIII.8.** Rappelons que pour $x \in \mathbb{R}$, $x^\pm = \max(0, \pm x)$; on a alors $x = x^+ - x^-$ et $|x| = x^+ + x^-$.

Démonstration. Si les familles $(u_i^+)_{i\in I}$ et $(u_i^-)_{i\in I}$ sont sommables, alors par linéarité positive (proposition XXVIII.8), la famille $(|u_i|)_{i\in I}$ l'est et donc $(u_i)_{i\in I}$ est bien sommable. Réciproquement, si $(u_i)_{i\in I}$ est sommable alors les familles $(u_i^+)_{i\in I}$ et $(u_i^-)_{i\in I}$ le sont également car l'inégalité $\forall i \in I$, $u_i^\pm \leq |u_i|$ permet de leur appliquer la proposition XXVIII.10. □

➠ **Exemple XXVIII.7.** Soit $x \in]-1, 0[$; on a vu que la famille $(x^{|n|})_{n\in\mathbb{Z}}$ était sommable et l'on peut vérifier que :

$$(x^{|n|})^+ = \begin{cases} x^{|n|} & \text{si } n \text{ est pair} \\ 0 & \text{sinon} \end{cases} \quad \text{et} \quad (x^{|n|})^- = \begin{cases} -x^{|n|} & \text{si } n \text{ est impair} \\ 0 & \text{sinon} \end{cases}.$$

De fait, on a :

$$\sum_{n\in\mathbb{Z}} x^{|n|} = \sum_{n\in\mathbb{Z}} x^{2|n|} - \sum_{n\in\mathbb{Z}} -x^{|2n+1|}\,.$$

Proposition/définition XXVIII.4. Une famille $(u_j)_{j\in I}$ de nombres **complexes** est sommable si et seulement si les familles de **réels** $(\mathrm{Re}(u_j))_{j\in I}$ et $(\mathrm{Im}(u_j))_{j\in I}$ le sont. Dans ce cas, on appelle **somme** de la famille $(u_j)_{j\in I}$ la quantité

$$\sum_{j\in I} u_j = \sum_{j\in I} \mathrm{Re}(u_j) + i \sum_{j\in I} \mathrm{Im}(u_j) \in \mathbb{C}\,.$$

Démonstration. Soit $j \in I$; alors on sait que $|\mathrm{Re}(u_j)| \leq |u_j|$ et $|\mathrm{Im}(u_j)| \leq |u_j|$. Ceci entraîne le résultat par proposition XXVIII.10 (de façon directe dans un sens, en contraposant dans l'autre). □

✌ Remarque XXVIII.9.

— On déduit de ces deux définitions que la somme d'une famille numérique sommable est invariante par permutation.

— Si $(u_i)_i$ est une famille sommable numérique, on a :

$$\left|\sum_{i\in I} u_i\right| \leq \sum_{i\in I} |u_i|\,.$$

— On a par défintion que, si $(u_j)_{j\in I}$ est sommable :

$$\mathrm{Re}\left(\sum_{j\in I} u_j\right) = \sum_{j\in I} \mathrm{Re}(u_j) \quad \text{et} \quad \mathrm{Im}\left(\sum_{j\in I} u_j\right) = \sum_{j\in I} \mathrm{Im}(u_j)\,.$$

Proposition XXVIII.11. Soit $(u_i)_{i\in I} \in \ell^1(I)$ et soit $\varepsilon > 0$. Alors il existe un ensemble **fini** $F \subset I$ tel que :

$$\left|\sum_{i\in I} u_i - \sum_{i\in F} u_i\right| \leq \varepsilon\,.$$

Démonstration. Plaçons dans le cas où la famille $(u_i)_{i\in I}$ est réelle. Alors, par sommabilité, les familles de réels positifs $(u_i^+)_{i\in I}$ et $(u_i^-)_{i\in I}$ sont sommables, de sommes respectives $S^+, S^- \in \mathbb{R}_+$. Par définition de borne supérieure, il existe deux ensembles finis F_+ et F_- inclus dans I tels que :

$$\left|\sum_{i\in F_+} u_i^+ - S^+\right| \leq \frac{\varepsilon}{2} \quad \text{et} \quad \left|\sum_{i\in F_-} u_i^- - S^-\right| \leq \frac{\varepsilon}{2}\,.$$

Ces inégalités restant vérifiées sur $F = F_+ \cup F_-$ (se référer à la démonstration de la proposition XXVIII.8), on a :

$$\begin{aligned}\left|\sum_{i\in I}u_i-\sum_{i\in F}u_i\right| &= \left|(S^+-S^-)-\left(\sum_{i\in F}u_i^+-\sum_{i\in F}u_i^-\right)\right|\\ &\leq \left|\sum_{i\in F}u_i^+-S^+\right|+\left|\sum_{i\in F}u_i^--S^-\right|\\ &\leq \varepsilon\end{aligned}$$

d'où le résultat. Le cas d'une famille complexe se traite en appliquant le raisonnement *supra* à ses parties réelle et imaginaire. ☐

✌ **Remarque XXVIII.10.** La somme de la famille sommable $(u_i)_{i\in I}$ est l'unique nombre complexe vérifiant cette propriété. En effet, à supposer qu'il existe deux tels complexes z, z' on aurait pour tout $\varepsilon > 0$ l'existence d'un ensemble fini $F \subset I$ tel que :

$$|z-z'| = \left|z-\sum_{i\in F}u_i+\sum_{i\in F}u_i-z'\right| \leq \left|z-\sum_{i\in F}u_i\right|+\left|\sum_{i\in F}u_i-z'\right| \leq 2\varepsilon$$

ce qui entraîne que $z = z'$.

Proposition XXVIII.12. Soient $(u_i)_{i\in I}, (v_i)_{i\in I} \in \ell^1(I)$ et soit $\lambda \in \mathbb{C}$. Alors :

(i) la famille $(u_i+\lambda v_i)_{i\in I}$ est sommable ;

(ii)
$$\sum_{i\in I}u_i+\lambda v_i = \sum_{i\in I}u_i+\lambda\sum_{i\in I}v_i\,.$$

Démonstration. La sommabilité est une conséquence triviale de l'inégalité triangulaire et de la linéarité positive (proposition XXVIII.8). Fixons ensuite $\varepsilon > 0$; alors d'après la proposition XXVIII.11 et quitte à prendre la réunion de deux ensembles *ad–hoc*, il existe un ensemble fini $F \subset I$ tel que :

$$\left|\sum_{i\in F}u_i-\sum_{i\in I}u_i\right| \leq \frac{\varepsilon}{1+|\lambda|} \quad \text{et} \quad \left|\sum_{i\in F}v_i-\sum_{i\in I}v_i\right| \leq \frac{\varepsilon}{1+|\lambda|}\,.$$

On a donc :

$$\begin{aligned}\left|\sum_{i\in F}u_i+\lambda v_i-\left(\sum_{i\in I}u_i+\lambda\sum_{i\in I}v_i\right)\right| &\leq \left|\sum_{i\in F}u_i-\sum_{i\in I}u_i\right|+|\lambda|\left|\sum_{i\in F}v_i-\sum_{i\in I}v_i\right|\\ &\leq \varepsilon\end{aligned}$$

d'où le résultat par unicité de la somme (remarque XXVIII.10). ☐

Corollaire XXVIII.12.a. L'ensemble $\ell^1(I)$ est un $\mathbb{C}$–e.v.

Démonstration. Il s'agit d'un s–e.v de $\mathbb{C}^I$. ☐

c) Sommation par paquets, le retour

Théorème XXVIII.13 (Sommation par paquets, cas général)**.**
On suppose ici qu'il existe une famille $(I_j)_{j\in J}$ d'ensembles disjoints tels que :

$$I = \bigsqcup_{j\in J} I_j$$

et on fixe $(u_i)_{i\in I}$ une famille **sommable**. Alors :

(i) pour tout $j \in J$, la famille $(u_i)_{i\in I_j}$ est sommable ;

(ii) la famille $\left(\sum_{i\in I_j} u_i\right)_{j\in J}$ est sommable ;

(iii)
$$\sum_{i\in I} u_i = \sum_{j\in J}\left(\sum_{i\in I_j} u_i\right).$$

Démonstration. Admis. □

✖ **Attention :** contrairement au cas positif, il n'y a pas équivalence entre les propriétés (i) et (ii) et la sommabilité de $(u_i)_{i\in I}$. Pour un contre–exemple, posons $I = \mathbb{N}$ et, pour $j \in \mathbb{N}$, $I_j = \{2j, 2j+1\}$; si l'on pose $u_i = (-1)^i$ pour $i \in \mathbb{N}$, la famille $(u_i)_{i\in I_j}$ est sommable (de somme nulle) pour tout entier j et donc la famille $\left(\sum_{i\in I_j} u_i\right)_{j\in J}$ est sommable de somme nulle. Pourtant, la famille $(u_i)_{i\in\mathbb{N}}$ n'est pas sommable car la série $\sum(-1)^i$ diverge grossièrement.

Remarque XXVIII.11. Cependant, il découle du théorème de Fubini "positif" (corollaire XXVIII.9.a) que la famille $(u_i)_{i\in I}$ est sommable si et seulement si les deux conditions suivantes sont vérifiées :

(i) les familles $(u_i)_{i\in I_j}$ sont sommables ;

(ii) la famille $\left(\sum_{i\in I_j} |u_i|\right)_{j\in J}$ est sommable.

Exercice XXVIII.3. Soit $r \in [0, 1[$ et $\theta \in \mathbb{R}$. On pose, pour $n \in \mathbb{Z}$, $a_n = r^{|n|}e^{in\theta}$. Étudier la sommabilité et, le cas échéant, calculer la somme de la famille $(a_n)_{n\in\mathbb{Z}}$.

➥ **Correction :** *On a, pour $n \in \mathbb{Z}$, :*

$$|a_n| = \left|r^{|n|}e^{in\theta}\right| = r^{|n|}$$

donc la famille $(a_n)_{n\in\mathbb{Z}}$ par comparaison avec une famille déjà étudiée. Posons ensuite $A = \mathbb{N}$ et $B = \{n \in \mathbb{Z} \mid n < 0\}$; on a alors $\mathbb{Z} = A \sqcup B$. Alors, par théorème de *sommation par paquets (XXVIII.13) on a l'existence des sommes infra et l'égalité :*

$$\begin{aligned}\sum_{n\in\mathbb{Z}} a_n &= \sum_{n\in A} a_n + \sum_{n\in B} a_n \\ &= \sum_{n=0}^{\infty} r^n e^{in\theta} + \sum_{n=1}^{\infty} r^n e^{-in\theta} \\ &= \frac{1}{1-re^{i\theta}} + \frac{re^{-i\theta}}{1-re^{-i\theta}} \\ &= \frac{1-r^2}{1-2r\cos(\theta)+r^2}.\end{aligned}$$

Corollaire XXVIII.13.a (Fubini)**.** Soit $(u_{a,b})_{(a,b)\in A\times B}$ une famille sommable de nombres complexes. Alors :

(i) pour tout $a \in A$, les famille $(u_{a,b})_{b\in B}$ et $(u_{a,b})_{a\in A}$ sont sommables ;

(ii) les familles $\left(\sum_{b\in B} u_{a,b}\right)_{a\in A}$ et $\left(\sum_{a\in A} u_{a,b}\right)_{b\in B}$ sont sommables ;

(iii)

$$\sum_{(a,b)\in A\times B} u_{a,b} = \sum_{a\in A}\left(\sum_{b\in B} u_{a,b}\right) = \sum_{b\in B}\left(\sum_{a\in A} u_{a,b}\right).$$

✌ **Remarque XXVIII.12.** On peut étendre ce résultat à des familles à plus de deux indices, sans modification de l'hypothèse.

✍ **Exercice XXVIII.4.** On fixe $x \in \mathbb{C}$ tel que $|x| < 1$.

1. Démontrer que la famille $(x^{mn})_{m,n\in\mathbb{N}^*}$ est sommable.
2. Exprimer la somme de cette famille comme somme d'une série numérique.

➥ **Correction :**

1. D'après le théorème de Fubini "positif" (corollaire XXVIII.9.a), on a :

$$\sum_{m,n\in\mathbb{N}^*} |x^{mn}| = \sum_{m\in\mathbb{N}^*}\sum_{n\in\mathbb{N}^*} (|x|^m)^n = \sum_{m\in\mathbb{N}^*} \frac{|x|^m}{1-|x|^m}$$

Or, on a l'équivalent $\dfrac{|x|^m}{1-|x|^m} \sim |x|^m$ et donc, par théorème sur les séries à termes positifs (proposition XXII.9), comme la série $\sum_{(n\geq 1)} |x|^m$ converge, on a la converge de la série $\sum_{(n\geq 1)} \dfrac{|x|^m}{1-|x|^m}$ et donc la sommabilité de la famille $(x^{mn})_{m,n\in\mathbb{N}^*}$.

2. Comme la famille $(x^{mn})_{m,n\in\mathbb{N}^*}$ est sommable, on a, d'après le théorème de Fubini (corollaire XXVIII.13.a) :

$$\sum_{m,n\in\mathbb{N}^*} x^{mn} = \sum_{m\in\mathbb{N}^*}\sum_{n\in\mathbb{N}^*} (x^m)^n = \sum_{m\in\mathbb{N}^*} \frac{x^m}{1-x^m},$$

*qui est bien la somme d'une série numérique, dont la convergence **absolue** découle du point (ii) du théorème précité.*

d) Produit de Cauchy

L'objectif de ce paragraphe est de développer, à l'aide de la variante du théorème de Fubini *infra*, un outil de sommation sur les produits de séries absolument convergentes.

Proposition XXVIII.14. Soient A, B deux ensembles, $(u_a)_{a\in A} \in \ell^1(A)$ et $(v_b)_{b\in B} \in \ell^1(B)$. Alors :

(i) la famille $(u_a v_b)_{(a,b)\in A\times B}$ est sommable ;

(ii)
$$\sum_{(a,b)\in A\times B} u_a v_b = \left(\sum_{a\in A} u_a\right)\left(\sum_{b\in B} v_b\right).$$

Démonstration. Posons, pour $(a, b) \in A \times B$, $w_{a,b} = u_a v_b$.

(i) On sait que la famille $(w_{a,b})_{b\in B}$ est sommable pour tout $a \in A$ car la famille $(v_b)_{b\in B}$ l'est. De plus, pour tout $a \in A$ on a :
$$\sum_{b\in B} |w_{a,b}| = \sum_{b\in B} |u_a||v_b| = |u_a| \sum_{b\in B} |v_b|$$
qui est le terme général d'une famille sommable car $(u_a)_{a\in A}$ l'est. On a donc la sommabilité de la famille $(w_{a,b})_{a,b}$ par remarque XXVIII.11.

(ii) D'après le théorème de Fubini (corollaire XXVIII.13.a) appliqué à la famille $(w_{a,b})_{a,b}$, on a :
$$\begin{aligned}\sum_{(a,b)\in A\times B} u_a v_b &= \sum_{(a,b)\in A\times B} w_{a,b}\\ &= \sum_{a\in A}\left(\sum_{b\in B} u_a v_b\right)\\ &= \left(\sum_{a\in A} u_a\right)\left(\sum_{b\in B} v_b\right)\end{aligned}$$
ce qui conclut la démonstration.

□

➠ **Exemple XXVIII.8.** Ce résultat permet de retrouver très rapidement la somme de la famille $(x^{p+q})_{p,q\in\mathbb{N}}$ pour $x \in \mathbb{C}$ tel que $|x| < 1$. En effet, toutes sommabilités bues, on a :
$$\sum_{p,q\in\mathbb{N}} x^{p+q} = \sum_{p,q\in\mathbb{N}} x^p x^q = \left(\sum_{p\in\mathbb{N}} x^p\right)\left(\sum_{q\in\mathbb{N}} x^q\right) = \frac{1}{(1-x)^2}.$$

Définition XXVIII.5. Soient $\sum u_n$ et $\sum w_n$ deux séries numériques. On appelle **produit de Cauchy** de ces deux séries la série $\sum w_n$, où :

$$\forall n \in \mathbb{N}, \quad w_n = \sum_{k=0}^{n} u_k v_{n-k} \,.$$

✌ **Remarque XXVIII.13.** Toute ressemblance avec l'expression des coefficients du produit de polynômes est remarquablement non fortuite.

Proposition XXVIII.15. Soient $\sum u_n$ et $\sum v_n$ deux séries numériques **absolument convergentes**. Alors :

(i) le produit de Cauchy $\sum w_n$ de ces deux séries converge absolument ;

(ii)
$$\sum_{n=0}^{\infty} w_n = \left(\sum_{n=0}^{\infty} u_n\right)\left(\sum_{n=0}^{\infty} v_n\right) \,.$$

✌ **Remarque XXVIII.14.** Le point (ii) se traduit par la formule suivante :

$$\left(\sum_{n=0}^{\infty} u_n\right)\left(\sum_{n=0}^{\infty} v_n\right) = \sum_{n=0}^{\infty}\sum_{k=0}^{n} u_k v_{n-k} \,.$$

Démonstration. Pour $n, m \in \mathbb{N}$, posons $\mu_{m,n} = u_n v_m$; alors, d'après la proposition XXVIII.14, la famille $(\mu_{m,n})_{m,n\in\mathbb{N}}$ est sommable et :

$$\sum_{n,m\in\mathbb{N}} \mu_{m,n} = \left(\sum_{n=0}^{\infty} u_n\right)\left(\sum_{n=0}^{\infty} v_n\right) \,.$$

Posons ensuite, pour $n \in \mathbb{N}$:

$$I_n = \{(k,\ell) \in \mathbb{N}^2 \mid k + \ell = n\} \,.$$

Les I_n sont deux à deux disjoints de réunion égale à $\mathbb{N}^2$ (exercice) et donc, d'après le théorème de sommation par paquets (XXVIII.13) on a :

$$\begin{aligned}
\sum_{n,m\in\mathbb{N}} \mu_{m,n} &= \sum_{n\in\mathbb{N}} \sum_{(k,\ell)\in I_n} u_k v_\ell \\
&= \sum_{n\in\mathbb{N}} \sum_{k=0}^{n} u_k v_{n-k} \\
&= \sum_{n=0}^{\infty} \sum_{k=0}^{n} u_k v_{n-k} \,.
\end{aligned}$$

□

➠ **Exemple XXVIII.9.**

— Fixons $a, b \in \mathbb{C}$ tels que $a \neq b$ et $|a|, |b| < 1$; on sait alors que :

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

Ceci signifie que l'on a le produit de Cauchy suivant (les séries concernées étant absolument convergentes) :

$$\sum_{n=0}^{\infty} \frac{a^{n+1} - b^{n+1}}{a - b} = \left(\sum_{n=0}^{\infty} a_n\right)\left(\sum_{n=0}^{\infty} b_n\right) = \frac{1}{(1-a)(1-b)},$$

avec convergence absolue de la série $\sum \frac{a^{n+1}-b^{n+1}}{a-b}$.

— Nous avons (proposition XXII.5) que, pour tout $z \in \mathbb{C}$:

$$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!},$$

la série concernée convergeant absolument. Ainsi, si l'on fixe $z, z' \in \mathbb{C}$ on a, par produit de Cauchy :

$$\begin{aligned} e^z e^{z'} &= \left(\sum_{n=0}^{\infty} \frac{z^n}{n!}\right)\left(\sum_{n=0}^{\infty} \frac{(z')^n}{n!}\right) \\ &= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{z^k}{k!} \frac{(z')^{n-k}}{(n-k)!} \\ &= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{1}{n!} \binom{n}{k} z^n (z')^{n-k} \\ &= \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} z^n (z')^{n-k} \\ &= \sum_{n=0}^{\infty} \frac{(z+z')^n}{n!} \\ &= e^{z+z'}, \end{aligned}$$

formule qui (nous l'espérons !) sera familière au lecteur...

Addendum : ensembles dénombrables

Ce qui suit relève du programme de MP mais fournit un complément intéressant aux notions que nous venons de développer.

Dénombrabilité

Définition XXVIII.6. Un ensemble E est dit **dénombrable** si il existe une bijection $f : \mathbb{N} \to E$.

Remarque XXVIII.15. Un tel ensemble est nécessairement infini : en effet, si on suppose E fini de cardinal n alors il ne peut exister une injection de $[\![1, n+1]\!]$ dans E et *a fortiori* de $\mathbb{N}$ dans E.

Exemple XXVIII.10.
— $\mathbb{N}$ est dénombrable ;
— $\mathbb{N}^*$ est dénombrable (poser $fn \mapsto n+1$) ;
— $2\mathbb{N}$ est dénombrable (poser $fn \mapsto 2n$) ;
— $\mathbb{Z}$ est dénombrable : il suffit de poser $f : \mathbb{N} \to \mathbb{Z}$ qui a tout entier pair associe $\frac{n}{2}$ et à tout entier impair associe $\frac{1-n}{2}$ (quelle est sa réciproque ?) ;
— $\mathbb{N}^2$ est dénombrable : en effet tout entier $n \in \mathbb{N}$ peut s'écrire de façon unique sous la forme $n = 2^a(2b+1)$ (a est alors la valuation dyadique de n) et donc $n \mapsto (a, b)$ réalise une bijection de $\mathbb{N}$ dans $\mathbb{N}^2$.

Proposition XXVIII.16. Tout produit cartésien fini d'ensembles dénombrables est dénombrable.

Démonstration. Si E_1 et E_2 sont deux ensembles dénombrables et que $f_1 : \mathbb{N} \to E_1$ et $f_2 : \mathbb{N} \to E_2$ sont bijectives alors $f : (x, y) \mapsto (f_1(x), f_2(y))$ réalise une bijection de $\mathbb{N}^2$ dans $E_1 \times E_2$. Comme $\mathbb{N}^2$ est dénombrable, il existe une bijection $\sigma : \mathbb{N} \to \mathbb{N}^2$ et donc $f \circ \sigma : \mathbb{N} \to E_1 \times E_2$ est bijective par composition : $E_1 \times E_2$ est donc dénombrable. On termine par récurrence. □

Proposition XXVIII.17. toute réunion finie ou dénombrable d'ensembles finis ou dénombrables est finie ou dénombrable.

Démonstration. Dans le cas d'une réunion d'ensembles $(A_n)_n$ dénombrables, on peut poser :

$$f : \mathbb{N}^2 \longrightarrow \bigcup_{n \in \mathbb{N}} A_n$$
$$(i, k) \mapsto f_i(k)$$

où les f_i sont des bijections de $\mathbb{N}$ dans A_i. On vérifie rapidement que cette application est bijective, et on conclut par dénombrabilité de $\mathbb{N}^2$. Il est ensuite assez aisé d'adapter cette démonstration au cas d'une réunion finie et/ou d'ensembles finis. □

Exercice XXVIII.5. On fixe une bijection $\eta : \mathbb{N} \to \mathbb{Z} \times \mathbb{N}^*$. Pour tout $n \in \mathbb{N}$, on note $\eta(n) = (a_n, b_n)$ l'image de l'entier n par cette application. On procède ensuite selon l'algorithme suivant :
— on pose $q_0 = \frac{a_0}{b_0}$;
— pour tout $n \in \mathbb{N}$, on détermine $k_n = \min \left\{ k \in \mathbb{N} \;\middle|\; \forall i \in [\![0, n]\!],\ \frac{a_k}{b_k} \neq q_i \right\}$ et on pose

$$q_{n+1} = \frac{a_{k_n}}{b_{k_n}} .$$

1. Justifier que k_n est bien défini pour tout $n \in \mathbb{N}$ et que pour tout $n \in \mathbb{N}$, $k_n < k_{n+1}$.
2. Démontrer que pour tous $n, m \in \mathbb{N}$ on a l'implication $(q_n = q_m) \Rightarrow (n = m)$.
   Indication : on pourra commencer par démontrer que $(q_n = q_m) \Rightarrow (k_n = k_m)$.
3. Soit $x \in \mathbb{Q}$; on rappelle que l'on peut alors écrire $x = \dfrac{p}{q}$ avec $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$.
   (a) Justifier qu'il existe $n \in \mathbb{N}$ tel que $(p, q) = (a_n, b_n)$.
   (b) En déduire qu'il existe $n_0 \in \mathbb{N}$ tel que $x = q_{n_0}$.
4. En déduire que $\mathbb{Q}$ est dénombrable en utilisant l'application

$$\begin{aligned} \zeta : \mathbb{N} &\to \mathbb{Q} \\ n &\mapsto q_n \ . \end{aligned}$$

On pourrait à ce rythme être tenté de penser que tout ensemble est dénombrable. Ceci est faux, et la fête s'arrête rapidement [1] après l'ensemble des rationnels.

Théorème XXVIII.18.
$\mathbb{R}$ n'est pas dénombrable.

Démonstration. Admis. □

Lien à la sommabilité

L'objet de notre digression tient dans le résultat suivant, plutôt sympathique au demeurant.

Proposition XXVIII.19. Soit $(u_i)_{i\in I}$ une famille sommable. Alors l'ensemble

$$\{i \in I \,|\, u_i \neq 0\}$$

est fini ou dénombrable.

Démonstration. Soit $n \geq 1$; comme la famille $(u_i)_{i\in I}$ est sommable alors par proposition XXVIII.11 il existe un ensemble **fini** $F_n \subset I$ tel que :

$$\left| \sum_{i\in I} u_i - \sum_{i\in F_n} u_i \right| \leq \frac{1}{n} \, .$$

De fait, par différence, si on pose :

$$E_n = \left\{ i \in I \;\middle|\; |u_i| > \frac{1}{n} \right\}$$

on a $E_n \subset F_n$ et donc l'ensemble E_n est fini. Or, on a :

$$\{i \in I \,|\, u_i \neq 0\} = \bigcup_{n\geq 1} E_n$$

et donc l'ensemble de gauche est dénombrable comme réunion dénombrable d'ensembles finis. □

1. Tout est relatif