CH01 : Séries numériques et sommabilité

Dans tout le chapitre, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.
La notation $|z|$ désignera la valeur absolue de z si z est un nombre réel, ou le module de z si z est un nombre complexe.

I Généralités sur les séries numériques

Nous allons rapidement rappeler les principales notions sur les séries numériques, déjà vues en MP2I.

1) Séries, sommes partielles

Notation
$\mathbb{K}^{\mathbb{N}}$ désigne l'ensemble des suites à valeurs dans $\mathbb{K}$ (c'est-à-dire les applications $u : \mathbb{N} \to \mathbb{K}$).
De telles suites u seront en général notées $(u_n)_{n\in\mathbb{N}}$ ou plus simplement (u_n).

Définition 1 (Série à valeurs réelles ou complexes)
Etant donnée une suite $(u_n) \in \mathbb{K}^{\mathbb{N}}$, on appelle **série de terme général u_n** *la suite $(S_n) \in \mathbb{K}^{\mathbb{N}}$ définie par*
$$\forall n \in \mathbb{N}, \qquad S_n = u_0 + u_1 + \cdots + u_n = \sum_{k=0}^{n} u_k.$$
Pour chaque entier n, la quantité S_n est appelée **somme partielle de rang n**.

Vocabulaire
On parle de **série numérique** car les termes u_n sont des nombres réels ou complexes. On généralisera ultérieurement pour des suites à valeurs dans un espace vectoriel de dimension finie E (par exemple $\mathbb{K}^n$ ou $\mathcal{M}_n(\mathbb{K})$).

2) Convergence, divergence

Définition 2 (Convergence/divergence d'une série)
On dit que la série de terme général u_n est **convergente** *lorsque la suite des sommes partielles (S_n) est convergente, c'est-à-dire lorsqu'il existe $S \in \mathbb{K}$ tel que $\sum_{k=0}^{n} u_k \underset{n\to+\infty}{\longrightarrow} S$.*
Le nombre $S \in \mathbb{K}$ est alors appelé **somme de la série** *et on note $S = \sum_{k=0}^{+\infty} u_k$.*
Dans le cas contraire (si (S_n) diverge), on dit que **la série est divergente**.

Notation
Souvent, on désignera par $\sum \boldsymbol{u_n}$ ou par $\sum_{\boldsymbol{n\geq n_0}} \boldsymbol{u_n}$ la série de terme général (u_n). La notation sans l'indice de départ n_0 illustre bien le fait que **la convergence d'une série ne dépend pas de ses premiers termes**.

Définition 3 (Reste d'une série convergente)
Si la série $\sum u_n$ converge, alors pour tout $n \in \mathbb{N}$, on pose
$$R_n = \sum_{k=n+1}^{+\infty} u_k = u_{n+1} + u_{n+2} + \dots.$$
Cette quantité s'appelle le **reste d'ordre n**.

3) Séries géométriques

Le premier exemple de référence est le cas des "séries géométriques", c'est-à-dire les séries de la forme $\sum q^n$ avec $q \in \mathbb{C}$. Rappelons d'abord les résultats connus sur les **suites** géométriques :

Propriété 4 (Convergence des suites géométriques)
Soit $q \in \mathbb{C}$.

(i) $\boxed{\text{Si } |q| > 1}$, *alors* (q^n) *diverge, et* $\lim\limits_{n\to+\infty} |q^n| = +\infty$.

(ii) $\boxed{\text{Si } |q| < 1}$, *alors* (q^n) *converge, et* $\lim\limits_{n\to+\infty} q^n = 0$.

(iii) $\boxed{\text{Si } |q| = 1}$, *alors* $\begin{cases} \text{si } q = 1, (q^n) \text{ converge (elle est constante) ;} \\ \text{si } q \neq 1, (q^n) \text{ diverge (en restant bornée).} \end{cases}$

Etablissons maintenant le résultat qui nous intéresse (pour les **séries**) :

Théorème 5 (Convergence des séries géométriques)
Soit $q \in \mathbb{C}$. La série géométrique $\sum q^n$ converge si et seulement si $|q| < 1$.
Dans ce cas, on a $\displaystyle\sum_{n=0}^{+\infty} q^n = \frac{1}{1-q}$.

Corollaire 6 (Reste d'une série géométrique convergente)
Soit $q \in \mathbb{C}$ tel que $|q| < 1$. Alors pour tout $n_0 \in \mathbb{N}$,

$$\sum_{k=n_0}^{+\infty} q^k = \frac{q^{n_0}}{1-q}.$$

4) Séries de Riemann

Voici maintenant le second exemple de référence :

Théorème 7 (Séries de Riemann)
Soit $\alpha \in \mathbb{R}$. La série $\displaystyle\sum_{n\geq 1} \frac{1}{n^\alpha}$ *est appelée* **série de Riemann** *d'exposant α.*
Cette série converge si et seulement si $\alpha > 1$.

Comme nous l'avons vu dans les exemples fondamentaux précédents, le principal problème des séries est qu'en général, **on ne sait pas expliciter les sommes partielles** S_n (voir les séries de Riemann), hormis certains cas simples. Donc, il est nécessaire de développer des outils pour l'étude de la convergence des séries, ce que nous allons faire dans les sections suivantes.

5) Condition nécessaire de convergence

Propriété 8 (Condition nécessaire de convergence d'une série)
Si *la série $\sum u_n$ converge,* **alors** $u_n \underset{n\to+\infty}{\longrightarrow} 0$.

Définition 9 (Divergence grossière)
On dit que la **série** $\sum u_n$ *est* **grossièrement divergente** *si son terme général u_n ne tend pas vers 0 lorsque $n \to +\infty$.*

Méthode
Pour étudier la convergence d'une série, on peut donc faire le **test** *rapide suivant :* **le terme général u_n tend-il vers 0 lorsque $n \to +\infty$?**
Si non, la série est trivialement divergente (d'où l'appellation "divergence grossière"). Mais dans la plupart des cas, on aura $u_n \underset{n\to+\infty}{\longrightarrow} 0$, ce qui ne dit rien sur la convergence de la série ...

6) Opérations algébriques

Comme pour les suites, on dispose d'opérations algébriques sur les séries :

Propriété 10 (Opérations algébriques)
Soient (u_n) et (v_n) deux suites de $\mathbb{K}^{\mathbb{N}}$ et $\lambda \in \mathbb{K}$.

(i) **Si** *les séries $\sum u_n$ et $\sum v_n$ convergent,* **alors** *la série $\sum(u_n + v_n)$ converge, et on a, pour tout entier n_0 :*

$$\sum_{k=n_0}^{\infty}(u_k + v_k) = \sum_{k=n_0}^{\infty} u_k + \sum_{k=n_0}^{\infty} v_k.$$

(ii) **Si** *$\sum u_n$ converge,* **alors** *la série $\sum(\lambda u_n)$ converge, et on a, pour tout entier n_0 :*

$$\sum_{k=n_0}^{\infty}(\lambda u_k) = \lambda \sum_{k=n_0}^{\infty} u_k.$$

(iii) **Si** *$\sum u_n$ converge et $\sum v_n$ diverge,* **alors** *$\sum(u_n + v_n)$ diverge.*

7) Téléscopage et lien suite-série

Le "téléscopage" est un **procédé de simplification de proche en proche** de certaines sommes.

Lemme 11 (Téléscopage)
Soient deux entiers naturels $n_0 \leq n$, et $(u_k) \in \mathbb{K}^{\mathbb{N}}$. On a :

$$\sum_{k=n_0}^{n}(u_{k+1} - u_k) = u_{n+1} - u_{n_0}.$$

Théorème 12 (Lien suite-série)
Soit $(u_n)_{n\geq n_0}$ une suite à valeurs dans $\mathbb{K}$. Alors, on a l'équivalence :

$$\text{la suite } (u_n) \text{ converge} \iff \text{la série } \sum(u_{n+1} - u_n) \text{ converge.}$$

II Séries réelles à termes positifs

Dans cette section on considère des séries réelles $\sum u_n$, dont les termes u_n sont positifs à partir d'un certain rang.

1) Croissance des sommes partielles

Pour étudier la convergence des séries **à termes positifs**, on dispose de critères spécifiques, basés sur l'idée suivante :

Propriété 13 (Croissance des sommes partielles)
Si *la suite réelle* (u_n) *est* **positive** *à partir d'un certain rang* $n_0 \in \mathbb{N}$, **alors** *la suite des sommes partielles* (S_n) *est croissante à partir du rang* n_0.

Corollaire 14 (Caractérisation des séries positives convergentes)
Si *la suite réelle* (u_n) *est* **positive** *à partir d'un certain rang* $n_0 \in \mathbb{N}$, **alors** *:*

$$\sum u_n \text{ converge} \iff \text{la suite } (S_n) \text{ est } \textbf{majorée}$$

("une série à termes positifs converge ssi ses sommes partielles sont majorées").

2) Comparaison de séries à termes positifs

On abrègera "série à termes positifs" en "SATP".

Théorème 15 (Critère de majoration des SATP)
Soient (u_n) *et* (v_n) *deux suites réelles qui vérifient* $\mathbf{0 \leq u_n \leq v_n}$ *à partir d'un certain rang* $n_0 \in \mathbb{N}$.

(i) **Si** $\sum v_n$ *converge,* **alors** $\sum u_n$ *converge, et on a*

$$0 \leq \sum_{n=n_0}^{+\infty} u_n \leq \sum_{n=n_0}^{+\infty} v_n.$$

(ii) **Si** $\sum u_n$ *diverge,* **alors** $\sum v_n$ *diverge.*

Corollaire 16 (Comparaison en O, o)
Soit (u_n), (v_n) *deux suites réelles positives à partir d'un certain rang* $n_0 \in \mathbb{N}$.

(i) Si $u_n = O(v_n)$ *et si* $\sum v_n$ *converge, alors* $\sum u_n$ *converge.*

(ii) Si $u_n = o(v_n)$ *et si* $\sum v_n$ *converge, alors* $\sum u_n$ *converge.*

Théorème 17 (Critère des équivalents pour les SATP)
Soient (u_n) *et* (v_n) *deux suites réelles* **positives** *à partir d'un certain rang et telles que* $\mathbf{u_n \underset{n\to+\infty}{\sim} v_n}$.
Alors, les séries $\sum u_n$ *et* $\sum v_n$ *sont* **de même nature**, *c'est-à-dire que*

$$\sum u_n \text{ converge} \iff \sum v_n \text{ converge.}$$

3) Règle de d'Alembert

Théorème 18 (Règle de d'Alembert)
Soit (u_n) *une suite* **strictement positive** *à partir d'un certain rang* $n_0 \in \mathbb{N}$.
On suppose que $\dfrac{\boldsymbol{u_{n+1}}}{\boldsymbol{u_n}} \underset{\boldsymbol{n\to+\infty}}{\longrightarrow} \boldsymbol{\ell \in \mathbb{R}_+ \cup \{+\infty\}}$.

(i) **Si** $0 \leq \ell < 1$, **alors** *la série* $\sum u_n$ *converge.*

(ii) **Si** $\ell > 1$, **alors** *la série* $\sum u_n$ *diverge grossièrement.*

(iii) **Si** $\ell = 1$, *alors on ne peut pas conclure quant à la nature de la série* $\sum u_n$.

4) Utilisation de la comparaison série-intégrale

Lorsque f est **monotone**, on peut déterminer par comparaison série-intégrale des **encadrements des sommes partielles et/ou des restes** de la série $\sum f(k)$ (comme dans la preuve du théorème de convergence des séries de Riemann).
Par monotonie de f, on peut se ramener au cas où la suite $(f(k))$ est positive à partir d'un certain rang (quitte à changer f en $-f$). En effet, si f est croissante, alors

- soit on a $f(k) \leq 0$ pour tout k et dans ce cas $-f$ est décroissante et positive ;
- soit on a $f(k) > 0$ à partir d'un certain rang et dans ce cas, f est croissante et positive APCR.

et de même si f est décroissante.

Méthode (Comparaison série-intégrale)
Pour tout entier k, on a si f est décroissante, on a

$$\int_k^{k+1} f(t)dt \leq f(k) \leq \int_{k-1}^{k} f(t)dt,$$

alors que si f est croissante, on a

$$\int_{k-1}^{k} f(t)dt \leq f(k) \leq \int_k^{k+1} f(t)dt.$$

Il n'y a plus qu'à sommer ces encadrements pour obtenir un encadrement de la somme partielle $S_n = \sum_{k=n_0}^{n} f(k)$ ou du reste $R_n = \sum_{k=n+1}^{+\infty} f(k)$ (dans le cas d'une série convergente).
Si les encadrements de S_n ou R_n obtenus sont assez fins (cela dépend de la rapidité de la décroissance/croissance de f), alors on peut même obtenir **un équivalent** *de S_n (si $\sum f(k)$ diverge) ou de R_n (si $\sum f(k)$ converge).*

III Séries numériques quelconques

Cette fois, on considère des séries $\sum u_n$ dont le terme général u_n est à valeurs dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

1) Convergence absolue

Définition 19 (Série absolument convergente)
Si (u_n) est une suite réelle ou complexe, on dit que la **série** $\sum u_n$ *est* **absolument convergente** *(ou "converge absolument") lorsque la série (positive) $\sum |u_n|$ est convergente.*

Théorème 20 (La convergence absolue entraîne la convergence)
Soit $(u_n) \in \mathbb{K}^{\mathbb{N}}$. **Si** $\sum u_n$ *converge absolument,* **alors** $\sum u_n$ *converge. En d'autres termes,*

$$\sum |u_n| \text{ converge } \implies \sum u_n \text{ converge.}$$

Méthode
Pour étudier la convergence d'une série à termes de signe non constant ou complexes, on peut **d'abord étudier la convergence absolue**.

- *Avantage : cela revient à travailler avec une* **série positive** $\sum |u_n|$*, sur laquelle on peut tester tous les critères de la partie précédente.*
- *Inconvénient : si la série ne converge pas absolument, alors ça ne montre rien quant à sa convergence.*

Définition 21 (Semi-convergence)
On dit qu'une **série** *numérique $\sum u_n$ est* **semi-convergente** *lorsqu'elle est* **convergente mais pas absolument convergente**, *c'est-à-dire lorsque $\sum u_n$ converge et $\sum |u_n|$ diverge.*

Propriété 22 (Inégalité triangulaire infinie)
Soit $(u_n) \in \mathbb{K}^{\mathbb{N}}$. **Si $\sum u_n$ converge absolument, alors** *on a l'inégalité suivante :*

$$\left| \sum_{k=0}^{+\infty} u_k \right| \leq \sum_{k=0}^{+\infty} |u_k|.$$

Propriété 23 (Comparaison en O, o)
Soit (u_n) une suite à valeurs dans $\mathbb{K}$ et (v_n) une suite réelle positive à partir d'un certain rang $n_0 \in \mathbb{N}$.

(i) Si $u_n = O(v_n)$ et si $\sum v_n$ converge, alors $\sum u_n$ converge absolument (donc converge).

(ii) Si $u_n = o(v_n)$ et si $\sum v_n$ converge, alors $\sum u_n$ converge absolument (donc converge).

2) Séries alternées

Un autre cas de référence est celui des **séries alternées**, c'est-à-dire dont le terme général u_n est réel et vérifie $u_n \times u_{n+1} \leq 0$ au moins à partir d'un certain rang, c'est-à-dire que chaque terme de la suite a un signe contraire au terme précédent).
De telles séries sont de la forme :

$$\pm \sum (-1)^n a_n, \qquad \text{avec } a_n \geq 0 \text{ à partir d'un certain rang.}$$

On dispose d'un résultat important sur ce type de série :

Théorème 24 (Critère spécial des séries alternées)
On considère la série $\sum(-1)^n a_n$.
Si la suite (a_n) *est décroissante à partir d'un certain rang* $n_0 \in \mathbb{N}$ *et si* $a_n \underset{n\to+\infty}{\longrightarrow} 0$ *(ce qui implique la positivité de* a_n *à partir de* n_0*), alors :*

(*i*) *La série* $\sum(-1)^n a_n$ *converge.*

(*ii*) *Pour tout* $n \geq n_0 - 1$, *le reste* $R_n = \sum_{k=n+1}^{+\infty} (-1)^k a_k$ *est du signe de son premier terme (donc* $(-1)^{n+1} a_{n+1}$*) et on a la majoration* $|R_n| \leq a_{n+1}$.

IV Sommation des relations de comparaison

Dans cette section, on présente des nouveaux résultats sur les séries numériques convergentes, mais aussi divergentes. Les "relations de comparaison" désignent ici o, O et $\sim$ (sous-entendu lorsque $n \to +\infty$ bien entendu).

1) Cas convergent

Théorème 25 (Sommation des relations de comparaison, cas convergent)
Soit $(u_n) \in \mathbb{K}^{\mathbb{N}}$, et $(v_n) \in \mathbb{R}^{\mathbb{N}}$.
On suppose que (v_n) est positive à partir d'un certain rang $n_0 \in \mathbb{N}$ et que $\sum v_n$ converge.

(i) Si $u_n = O(v_n)$, alors $\sum u_n$ converge et

$$\sum_{k=n+1}^{+\infty} u_k = O\left(\sum_{k=n+1}^{+\infty} v_k\right).$$

(ii) Si $u_n = o(v_n)$, alors $\sum u_n$ converge et

$$\sum_{k=n+1}^{+\infty} u_k = o\left(\sum_{k=n+1}^{+\infty} v_k\right).$$

(iii) Si $u_n \sim v_n$, alors $\sum u_n$ converge et

$$\sum_{k=n+1}^{+\infty} u_k \underset{n\to+\infty}{\sim} \sum_{k=n+1}^{+\infty} v_k.$$

2) Cas divergent

Théorème 26 (Sommation des relations de comparaison, cas divergent)
Soit $(u_n) \in \mathbb{K}^{\mathbb{N}}$, et $(v_n) \in \mathbb{R}^{\mathbb{N}}$.
On suppose que (v_n) est positive à partir d'un certain rang $n_0 \in \mathbb{N}$ et que $\sum v_n$ diverge.

(i) Si $u_n = O(v_n)$, alors

$$\sum_{k=0}^{n} u_k = O\left(\sum_{k=0}^{n} v_k\right).$$

(ii) Si $u_n = o(v_n)$, alors

$$\sum_{k=0}^{n} u_k = o\left(\sum_{k=0}^{n} v_k\right).$$

(iii) Si $u_n \sim v_n$, alors $\sum u_n$ diverge et

$$\sum_{k=0}^{n} u_k \underset{n\to+\infty}{\sim} \sum_{k=0}^{n} v_k.$$

3) Applications classiques

a) Lemme de Cesàro

Lemme 27 (Lemme de Cesàro)
Soit $(u_n) \in \mathbb{K}^{\mathbb{N}}$. Si $u_n \to \ell \in \mathbb{K}$, alors en posant $M_n = \dfrac{1}{n+1}\displaystyle\sum_{k=0}^{n} u_k$ pour tout $n \in \mathbb{N}$ (on dit que (M_n) est la suite des moyennes de Cesàro), on a aussi $M_n \to \ell$.

b) Développement asymptotique à 3 termes de la série harmonique

En utilisant la sommation des relations de comparaison, on va montrer que

$$\boxed{H_n = \sum_{k=1}^{n} \frac{1}{k} = \ln(n) + \gamma + \frac{1}{2n} + o\left(\frac{1}{n}\right)},$$

où γ est une constante réelle.

- Tout d'abord, $\frac{1}{k} \sim \ln(1+1/k) = \ln(k+1) - \ln(k)$, et la série téléscopique $\sum(\ln(k+1) - \ln(k))$ diverge (puisque la suite $(\ln(k))$ diverge), donc d'après le théorème de sommation des relations de comparaison (cas divergent), on a

$$H_n = \sum_{k=1}^{n} \frac{1}{k} \underset{n\to+\infty}{\sim} \sum_{k=1}^{n} (\ln(k+1) - \ln(k)) = \ln(n+1) = \ln(n) + \ln(1+1/n) \underset{n\to+\infty}{\sim} \ln(n).$$

- Posons $u_n = H_n - \ln(n)$ pour tout $n \geq 1$. Pour déterminer un équivalent de u_n, on utilise la série téléscopique $\sum(u_{n+1} - u_n)$. On a :

$$u_{n+1} - u_n = \frac{1}{n+1} - \ln(1+1/n) = \frac{1}{n}(1 - 1/n + o(1/n)) - (1/n - 1/(2n^2) + o(1/n)) \sim -1/(2n^2),$$

  donc la série téléscopique $\sum(u_{n+1} - u_n)$ converge, et donc la suite (u_n) converge vers un réel γ, ce qui donne $H_n = \ln(n) + \gamma + o(1)$.
- Enfin, posons $v_n = H_n - \ln(n) - \gamma = u_n - \gamma$ et déterminons un équivalent de (v_n) en utilisant (encore !) une série téléscopique :

$$v_{n+1} - v_n = u_{n+1} - u_n \sim -\frac{1}{2n^2},$$

  donc par sommation des relations de comparaison (cas convergent), on a, puisque $\lim_{k\to+\infty} v_k = 0$:

$$v_n = \sum_{k=n}^{+\infty} (v_k - v_{k+1}) \sim \sum_{k=n}^{+\infty} \frac{1}{2k^2},$$

  et on montre facilement par comparaison série-intégrale que $\sum_{k=n}^{+\infty} \frac{1}{k^2} \sim \frac{1}{n}$, donc finalement $v_n \sim \frac{1}{2n}$, ce qui donne $H_n = \ln(n) + \gamma + \frac{1}{2n} + o\left(\frac{1}{n}\right)$.

On pourrait poursuivre pour calculer le terme suivant de ce développement asymptotique...

c) Formule de Stirling, développement asymptotique de $n!$

Montrons qu'il existe une constante $K > 0$ telle que

$$\boxed{n! = Kn^n e^{-n}\sqrt{n}\left(1 + \frac{1}{12n} + o\left(\frac{1}{n}\right)\right)},$$

et donc en particulier $\boxed{n! \sim Kn^n e^{-n}\sqrt{n}}$ (*formule de Stirling*).
Cela se fait en étudiant la suite $(u_n)_{n\geq 1}$ définie par

$$u_n = \frac{n!}{n^n e^{-n}\sqrt{n}}.$$

- Cette fois, $u_{n+1} - u_n$ ne se simplifie pas par téléscopage, donc on travaille plutôt avec des logarithmes :

$$v_n = \ln(u_{n+1}) - \ln(u_n) = \cdots = 1 - \left(n + \frac{1}{2}\right)\ln\left(1 + \frac{1}{n}\right) \sim -\frac{1}{12n^2},$$

  donc la série $\sum(\ln(u_{n+1}) - \ln(u_n))$ converge. On en déduit que la suite $(\ln(u_n))$ converge vers un réel ℓ, et donc que la suite (u_n) converge vers $K = e^{\ell} > 0$.

- Par sommation des équivalents dans le cas des séries convergentes, on obtient l'équivalence des restes :
$$\ln(u_n) - \ell = \sum_{k=n}^{+\infty} (\ln(u_k) - \ln(u_{k+1})) \sim \sum_{k=n}^{+\infty} \frac{1}{12k^2} \sim \frac{1}{12n},$$
donc finalement :
$$\ln(u_n) = \ell + \frac{1}{12n} + o(1/n),$$
donc
$$u_n = e^{\ell + \frac{1}{12n} + o(1/n)} = K e^{\frac{1}{12n} + o(1/n)} = K\left(1 + \frac{1}{12n} + o(1/n)\right),$$
ce qui est le résultat voulu.

Si on veut la valeur de K, il faut utiliser les *intégrales de Wallis* ($I_n = \int_0^{\pi/2} \cos^n(x)dx$), et on obtient $K = \sqrt{2\pi}$ (voir les exercices).

V Dénombrabilité

Notation
Le cardinal d'un ensemble fini E sera noté $\#E$ ou $Card(E)$ ou encore $|E|$. C'est un entier naturel.

Définition 28 (Ensemble dénombrable)
Un ensemble E est dit **dénombrable** *s'il existe une bijection $\varphi : \mathbb{N} \to E$.*

Théorème 29 (Parties de $\mathbb{N}$)
Toute partie $X \subset \mathbb{N}$ est finie ou dénombrable.

Définition 30 (Ensemble au plus dénombrable)
Un ensemble E est dit **au plus dénombrable** *s'il existe une injection $i : E \to \mathbb{N}$.*

Propriété 31 (Caractérisation des ensembles au plus dénombrables)
Un ensemble E est au plus dénombrable si et seulement si il est fini ou dénombrable.

Corollaire 32 (Parties d'un ensemble dénombrable)
Soit E un ensemble dénombrable, et $A \subset E$. Alors A est fini ou dénombrable.

Théorème 33 (Produit cartésien fini d'ensembles dénombrables)

(*i*) *Tout produit cartésien fini d'ensembles finis ou dénombrables est un ensemble fini ou dénombrable.*

(*ii*) *Tout produit cartésien fini d'ensembles dénombrables est un ensemble dénombrable.*

Corollaire 34 (Quelques ensembles dénombrables classiques)
Les ensembles $\mathbb{N}^2$, $\mathbb{Z}^2$, $\mathbb{Q}$ sont dénombrables.

Lemme 35 (Une autre caractérisation des ensembles au plus dénombrables)
Un ensemble non vide E est au plus dénombrable si et seulement si il existe une surjection $s : \mathbb{N} \to E$.

Théorème 36 (Réunion finie ou dénombrable d'ensembles finis ou dénombrables)
Une réunion finie ou dénombrable d'ensembles finis ou dénombrables est un ensemble fini ou dénombrable.

Théorème 37 (Non dénombrabilité de $\mathbb{R}$)
$\mathbb{R}$ n'est pas dénombrable.

VI Familles sommables

Dans cette section, I désigne un ensemble quelconque, le plus souvent **fini ou dénombrable**.
Le but est de donner un sens à $\sum_{i\in I} u_i$, où $(u_i)_{i\in I}$ est une famille de nombres réels ou complexes.
Lorsque $I=\emptyset$, on adoptera la convention classique $\sum_{i\in\emptyset} u_i = 0$.

1) Cas des familles de réels positifs

Convention (Calculs dans $[0,+\infty]$)
On travaillera dans l'ensemble $[0,+\infty] = \mathbb{R}^+ \cup \{+\infty\}$.
L'opération + connue sur $\mathbb{R}^+$ se prolonge à $[0,+\infty]$ de la manière suivante :

$$\forall x \in \mathbb{R}^+, \qquad x + (+\infty) = (+\infty) + x = +\infty;$$

$$(+\infty) + (+\infty) = +\infty.$$

La relation d'ordre classique $\leq$ se prolonge également à $[0,+\infty]$ en convenant que :

$$\forall x \in \mathbb{R}^+, \qquad 0 \leq x < +\infty.$$

On obtient donc encore une relation d'ordre total sur $[0,+\infty]$, c'est-à-dire

$$\forall (x,y) \in [0,+\infty]^2, \qquad (x \leq y) \text{ ou } (y \leq x).$$

Enfin, cette relation d'ordre est compatible avec la somme :

$$\forall (x,y,z,t) \in [0,+\infty]^4, \qquad \big((x \leq y) \text{ et } (z \leq t)\big) \implies x+z \leq y+t.$$

Convention (Borne supérieure infinie)
Si $A \subset \mathbb{R}^+$ est une partie non vide et non majorée de $\mathbb{R}$, alors on conviendra que $\sup(A) = +\infty$.
Ainsi, toute partie non vide de $[0,+\infty]$ possède une borne supérieure dans $[0,+\infty]$, et on a

$$\sup(A) < +\infty \iff A \text{ est majorée.}$$

Définition 38 (Somme d'une famille d'éléments de $[0,+\infty]$)
Soit $(u_i)_{i\in I}$ une famille d'éléments de $[0,+\infty]$. On appelle **somme de la famille $(u_i)_{i\in I}$** *l'élément :*

$$\sum_{i\in I} u_i = \sup_{\substack{J\subset I \\ J \text{fini}}} \sum_{i\in J} u_i.$$

C'est un élément de $[0,+\infty]$.

Définition 39 (Famille sommable de réels positifs)
Soit $(u_i)_{i\in I}$ une famille de réels positifs. On dit que $(u_i)_{i\in I}$ est **sommable** *lorsque $\sum_{i\in I} u_i < +\infty$, c'est-à-dire lorsqu'il existe un réel $M \geq 0$ tel que pour toute partie finie $J \subset I$, on a $\sum_{i\in J} u_i \leq M$.*

Propriété 40 (Invariance par permutation)
Soit $(u_i)_{i\in I}$ une famille d'éléments de $[0,+\infty]$, et soit $\varphi : I \to I$ une bijection ("permutation" de I). Alors :

(i) *On a l'égalité $\sum_{i\in I} u_i = \sum_{i\in I} u_{\varphi(i)}$ dans $[0,+\infty]$.*

(ii) *En particulier, si les u_i sont dans $\mathbb{R}^+$, alors $(u_i)_{i\in I}$ est sommable si et seulement si $(u_{\varphi(i)})_{i\in I}$ est sommable.*

Propriété 41 (La sommabilité implique la dénombrabilité du support)
Si $(u_i)_{i\in I}$ est une famille sommable de réels positifs, alors l'ensemble $X = \{i \in I,\ u_i \neq 0\}$ (appelé support de la famille $(u_i)_{i\in I}$) est au plus dénombrable.

Propriété 42 (Sous-famille d'une famille sommable)
Soit $(u_i)_{i\in I}$ une famille de réels positifs.
Si $(u_i)_{i\in I}$ est sommable, alors pour toute partie $J \subset I$ (non nécessairement finie), la sous-famille $(u_i)_{i\in J}$ est sommable, et on a $\sum_{i\in J} u_i \leq \sum_{i\in I} u_i$.

Propriété 43 (Comparaison de familles sommables à termes positifs)
Soit $(u_i)_{i\in I}$ et $(v_i)_{i\in I}$ deux familles de réels positifs. Si on a $u_i \leq v_i$ pour tout $i \in I$ et si $(v_i)_{i\in I}$ est sommable, alors $(u_i)_{i\in I}$ est sommable et $\sum_{i\in I} u_i \leq \sum_{i\in I} v_i$.

Théorème 44 (Lien avec les séries)
On suppose que $I = \mathbb{N}$. Si $(u_i)_{i\in\mathbb{N}}$ est une famille (suite) de réels positifs, alors :

$$(u_i)_{i\in\mathbb{N}} \text{ est sommable} \iff \sum_{i\geq 0} u_i \text{ converge}$$

et dans ce cas, on a $\sum_{i\in\mathbb{N}} u_i = \sum_{i=0}^{+\infty} u_i$.

Théorème 45 (Sommation par paquets pour les familles positives)
Soit $(u_i)_{i\in I}$ une famille de réels positifs.
On suppose que $I = \bigcup_{n\in\mathbb{N}} I_n$ avec les I_n deux à deux disjoints ($m \neq n \implies I_n \cap I_m = \emptyset$).
Alors, on a dans $[0, +\infty]$:

$$\sum_{i\in I} u_i = \sum_{n=0}^{+\infty} \left(\sum_{i\in I_n} u_i \right).$$

Méthode
Grâce aux conventions de calculs avec $+\infty$, ce théorème est très simple d'utilisation : à condition de travailler avec des réels positifs, tous les calculs peuvent être menés en pratique **dans $[0, +\infty]$ sans aucune justification préalable de sommabilité** *et on peut regrouper les termes comme on l'entend. Obtenir à la fin des calculs une somme finie justifiera a posteriori la sommabilité de la famille.*

Vocabulaire
Lorsque $I = \bigcup_{n\in\mathbb{N}} I_n$ avec les I_n deux à deux disjoints, on dit que les $(I_n)_{n\in\mathbb{N}}$ forment une **pseudo-partition** de I.
Si de plus les I_n sont non vides, on parle alors de **partition**.

Corollaire 46 (Sommabilité et réindexation)
Soit $(u_i)_{i\in I}$ une famille dénombrable de réels positifs.
Si $\varphi : \mathbb{N} \to I$ est une bijection, alors on a $\sum_{i\in I} u_i = \sum_{n=0}^{+\infty} u_{\varphi(n)}$ dans $[0, +\infty]$.

2) Cas des familles de nombres complexes

On considère maintenant des familles $(u_i)_{i\in I}$ de nombres réels ou complexes indexées par un ensemble fini ou dénombrable I.

Notation
On notera $\mathbb{K}^I$ l'ensemble des familles $(u_i)_{i\in I}$ à valeurs dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Définition 47 (Famille sommable de nombres complexes)
Soit $(u_i)_{i\in I} \in \mathbb{K}^I$. On dit que $(u_i)_{i\in I}$ est **sommable** *lorsque $\sum_{i\in I} |u_i| < +\infty$.*

Propriété 48 (Comparaison en module)
Soit $(u_i)_{i\in I} \in \mathbb{K}^I$ et soit $(v_i)_{i\in I} \in (\mathbb{R}^+)^I$ telle que $\forall i \in I,\ |u_i| \leq v_i$.
Si $(v_i)_{i\in I}$ est sommable, alors $(u_i)_{i\in I}$ est sommable.

Définissons maintenant la somme d'une famille sommable de nombres réels (resp. complexes).

Lemme 49 (Parties positive et négative d'une famille de réels)
Soit $(u_i) \in \mathbb{R}^I$. Pour tout $i \in I$, on note

$$u_i^+ = \max(u_i, 0), \qquad u_i^- = \max(-u_i, 0).$$

(i) Pour tout $i \in I$, on a $u_i^+ \geq 0, u_i^- \geq 0$, ainsi que les relations :

$$\forall i \in I, \quad u_i^+ + u_i^- = |u_i|, \quad u_i^+ - u_i^- = u_i.$$

(ii) La famille $(u_i)_{i\in I}$ est sommable si et seulement si les familles de réels positifs $(u_i^+)_{i\in I}$ et $(u_i^-)_{i\in I}$ sont sommables.

Définition 50 (Somme d'une famille sommable de nombres réels)
Soit $(u_i)_{i\in I} \in \mathbb{R}^I$ une famille sommable.
On appelle **somme de la famille $(u_i)_{i\in I}$** *le nombre réel :*

$$\sum_{i\in I} u_i = \sum_{i\in I} u_i^+ - \sum_{i\in I} u_i^-.$$

Lemme 51 (Parties réelle et imaginaire d'une famille de complexes)
Soit $(u_i)_{i\in I} \in \mathbb{C}^I$. Si $(u_i)_{i\in I}$ est sommable, alors $(Re(u_i))_{i\in I}$ et $(Im(u_i))_{i\in I}$ sont sommables.

Définition 52 (Somme d'une famille sommable de nombres complexes)
Soit $(u_k)_{k\in I} \in \mathbb{C}^I$ une famille sommable.
On appelle **somme de la famille $(u_k)_{k\in I}$** *le nombre complexe :*

$$\sum_{k\in I} u_k = \sum_{k\in I} Re(u_k) + i \sum_{k\in I} Im(u_k).$$

Propriété 53 (Lien avec la convergence absolue des séries)
On suppose ici que $I = \mathbb{N}$. Si $(u_i)_{i\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$, alors

$$(u_i)_{i\in\mathbb{N}} \text{ est sommable } \iff \sum_{i\geq 0} u_i \text{ converge } \textbf{absolument},$$

et dans ce cas, on a $\displaystyle\sum_{i\in\mathbb{N}} u_i = \sum_{i=0}^{+\infty} u_i$.

Théorème 54 (Sommation par paquets pour les familles complexes)
On suppose que $I = \bigcup_{n\in\mathbb{N}} I_n$ avec les I_n deux à deux disjoints ($m \neq n \implies I_n \cap I_m = \emptyset$).
Si $(u_i)_{i\in I} \in \mathbb{K}^I$ est sommable, alors :

$$\sum_{i\in I} u_i = \sum_{n=0}^{+\infty} \left(\sum_{i\in I_n} u_i \right)$$

(avec convergence de la série).

Corollaire 55 (Sommation par paquets avec une réunion finie)
On suppose $I = I_1 \cup I_2 \cup \cdots I_N$ avec les $(I_n)_{1\leq n\leq N}$ deux à deux disjoints.
Si $(u_i)_{i\in I} \in \mathbb{K}^I$ est sommable, alors :

$$\sum_{i\in I} u_i = \sum_{n=1}^{N} \left(\sum_{i\in I_n} u_i \right).$$

Corollaire 56 (Réindexation des termes d'une famille sommable)
Soit $(u_i)_{i\in I} \in \mathbb{K}^I$ (avec I dénombrable) et soit $\varphi : \mathbb{N} \to I$ une bijection. Si la famille $(u_i)_{i\in I}$ est sommable, alors la série $\sum_n u_{\varphi(n)}$ converge absolument et

$$\sum_{i\in I} u_i = \sum_{n=0}^{+\infty} u_{\varphi(n)}.$$

Méthode
Pour appliquer ces théorèmes (sommation par paquets ou réindexation dans le cas non positif), il faut au préalable **justifier la sommabilité** *de la famille $(|u_i|)_{i\in I}$.*
En pratique :

- *On montre que $(u_i)_{i\in I}$ est sommable en* **trouvant un procédé de sommation** *(c'est-à-dire une pseudo-partition (I_n) de I) tel que*

$$\sum_{n\in\mathbb{N}} \left(\sum_{i\in I_n} |u_i| \right) < +\infty.$$

  En effet, cela montre que $\sum_{i\in I} |u_i| < +\infty$, puisqu'on a $\sum_{i\in I} |u_i| = \sum_{n\in\mathbb{N}} \left(\sum_{i\in I_n} |u_i| \right)$ dans $[0, +\infty]$.

- *Une fois la sommabilité de (u_i) acquise, on peut "enlever les modules" et calculer la somme $\sum_{i\in I} u_i$ en sommant* **suivant n'importe quel procédé** *(pas forcément le même que celui utilisé pour justifier la sommabilité). On a alors, pour toute pseudo-partition (L_n) de I :*

$$\sum_{i\in I} u_i = \sum_{n\in\mathbb{N}} \left(\sum_{i\in L_n} u_i \right)$$

Il faut bien distinguer ces deux étapes lors de la rédaction !

3) Propriétés algébriques des familles sommables

I désigne un ensemble fini ou dénombrable.

Propriété 57 (Linéarité)
Soit $(u_i)_{i\in I}$ et $(v_i)_{i\in I}$ deux familles d'éléments de $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$, et soit $(\lambda,\mu)\in\mathbb{K}^2$.
Si $(u_i)_{i\in I}$ et $(v_i)_{i\in I}$ sont sommables, alors $(\lambda u_i+\mu v_i)_{i\in I}$ est sommable et

$$\sum_{i\in I}(\lambda u_i+\mu v_i)=\lambda\sum_{i\in I}u_i+\mu\sum_{i\in I}v_i.$$

Corollaire 58 (Structure d'espace vectoriel des familles sommables)
L'ensemble des familles sommables est un sous-espace vectoriel de $\mathbb{K}^I$, et l'application $(u_i)_{i\in I}\mapsto\sum_{i\in I}u_i$ est une forme linéaire sur cet espace vectoriel.

Notation
On notera $\ell^1(I,\mathbb{K})$ (ou plus simplement $\ell^1(I)$) le $\mathbb{K}$-espace vectoriel des familles sommables de $\mathbb{K}^I$.

Propriété 59 (Positivité et croissance)
(i) Si $(u_i)_{i\in I}$ est une famille sommable de réels positifs, alors $\sum_{i\in I}u_i\geq 0$.
(ii) Si $(u_i)_{i\in I}$ et $(v_i)_{i\in I}$ sont deux familles sommables de nombres réels, alors

$$(\forall i\in I,\ u_i\leq v_i)\implies\sum_{i\in I}u_i\leq\sum_{i\in I}v_i.$$

Propriété 60 (Somme nulle de termes positifs)
Soit $(u_i)_{i\in I}$ une famille de réels positifs.
Si $(u_i)_{i\in I}$ est sommable et si $\sum_{i\in I}u_i=0$, alors $u_i=0$ pour tout $i\in I$.

Propriété 61 (Conjugaison)
Si $(u_i)_{i\in I}\in\mathbb{C}^{\mathbb{N}}$ est sommable, alors $(\overline{u_i})_{i\in I}$ est sommable et $\displaystyle\sum_{i\in I}\overline{u_i}=\overline{\sum_{i\in I}u_i}$.

Propriété 62 (Inégalité triangulaire)
Si $(u_i)_{i\in I}\in\mathbb{K}^I$ est sommable, alors $\displaystyle\left|\sum_{i\in I}u_i\right|\leq\sum_{i\in I}|u_i|$.

VII Applications de la sommabilité aux séries

1) Permutation des termes d'une série absolument convergente

Propriété 63 (Permutation des termes d'une série absolument convergente)
Soit $(u_n) \in \mathbb{K}^{\mathbb{N}}$. Si $\sum u_n$ est absolument convergente, alors pour toute bijection $\sigma : \mathbb{N} \to \mathbb{N}$, la série permutée $\sum u_{\sigma(n)}$ est absolument convergente et on a

$$\sum_{n=0}^{+\infty} u_{\sigma(n)} = \sum_{n=0}^{+\infty} u_n.$$

2) Séries doubles

Théorème 64 (Théorème de Fubini pour les familles positives)
Soit $(u_{m,n})_{(m,n)\in\mathbb{N}^2}$ une famille de réels positifs. Alors on a dans $[0,+\infty]$:

$$\sum_{(m,n)\in\mathbb{N}^2} u_{m,n} = \sum_{n=0}^{+\infty}\left(\sum_{m=0}^{+\infty} u_{m,n}\right) = \sum_{m=0}^{+\infty}\left(\sum_{n=0}^{+\infty} u_{m,n}\right).$$

Théorème 65 (Théorème de Fubini pour les familles complexes)
Soit $(u_{m,n})_{(m,n)\in\mathbb{N}^2}$ une famille de nombres réels ou complexes.
Si $(u_{m,n})_{(m,n)\in\mathbb{N}^2}$ est sommable, alors on a

$$\sum_{(m,n)\in\mathbb{N}^2} u_{m,n} = \sum_{n=0}^{+\infty}\left(\sum_{m=0}^{+\infty} u_{m,n}\right) = \sum_{m=0}^{+\infty}\left(\sum_{n=0}^{+\infty} u_{m,n}\right)$$

(avec convergence absolue des séries qui interviennent dans cette expression).

Méthode
Pour intervertir deux sommes infinies dans un calcul :

- *si $u_{m,n} \geq 0$ pour tout $(m,n) \in \mathbb{N}^2$, alors tous les coups sont permis (on peut permuter les sommes avec égalité des résultats dans $[0,+\infty]$) !*
- *sinon, on peut permuter les sommes* **sous réserve de sommabilité** *de $(u_{m,n})_{(m,n)\in\mathbb{N}^2}$.*
  Et cette sommabilité doit se vérifier en montrant par exemple que

$$\sum_{m}\left(\sum_{n}|u_{m,n}|\right) < +\infty$$

  (ou dans l'autre sens).

3) Produit de Cauchy de deux séries

Définition 66 (Produit de Cauchy)
Soit $(u_n),(v_n) \in \mathbb{K}^{\mathbb{N}}$. On appelle **produit de Cauchy** *des séries $\sum u_n$ et $\sum v_n$ la série $\sum w_n$, où :*

$$\forall n \in \mathbb{N}, \quad w_n = \sum_{k=0}^{n} u_k v_{n-k} = \sum_{k=0}^{n} u_{n-k} v_k = \sum_{(k,l)\in\mathbb{N}^2,\ k+l=n} u_k v_l.$$

Lemme 67 (Famille produit)
Si $\sum u_n$ et $\sum v_n$ sont deux séries absolument convergentes, alors la famille $(u_k v_l)_{(k,l)\in\mathbb{N}^2}$ est sommable et

$$\sum_{(k,l)\in\mathbb{N}^2} u_k v_l = \left(\sum_{k=0}^{+\infty} u_k\right)\left(\sum_{l=0}^{+\infty} v_l\right).$$

Théorème 68 (Produit de Cauchy de deux séries absolument convergentes)
Si $\sum u_n$ et $\sum v_n$ sont deux séries absolument convergentes, alors le produit de Cauchy $\sum w_n$ converge absolument et on a :

$$\sum_{n=0}^{+\infty} w_n = \left(\sum_{k=0}^{+\infty} u_k\right)\left(\sum_{l=0}^{+\infty} v_l\right).$$

CH02 : Intégration sur un intervalle quelconque

On va étendre ici l'intégrale au cas de fonctions continues par morceaux sur des intervalles **qui ne sont pas des segments**, c'est-à-dire des intervalles non bornés et/ou non fermés.
Dans tout le chapitre, la lettre $\mathbb{K}$ désigne le corps $\mathbb{R}$ ou $\mathbb{C}$ et I désigne un intervalle de $\mathbb{R}$.

Définition 1 (Fonction continue par morceaux)

(*i*) *Soit deux réels $a < b$. Une fonction $f : [a,b] \to \mathbb{K}$ est dite* **continue par morceaux** *lorsqu'il existe une subdivision $(x_0, \cdots, x_n)$ de $[a,b]$ telle que pour tout $k \in \{0, \cdots, n-1\}$, la restriction $f_{]x_k, x_{k+1}[}$ possède un prolongement continu sur $[x_k, x_{k+1}]$.*

(*ii*) *Etant donné un intervalle I de $\mathbb{R}$ (pas nécessairement un segment), on dit qu'une fonction $f : I \to \mathbb{K}$ est continue par morceaux lorsque sa restriction à tout segment $[a,b] \subset I$ est continue par morceaux.*

Notation
Etant donné un intervalle I de $\mathbb{R}$, on notera :
$\mathcal{F}(I, \mathbb{K})$ ou $\mathbb{K}^I$ l'ensemble des fonctions définies sur I et à valeurs dans $\mathbb{K}$,
$\mathcal{C}^0(I, \mathbb{K})$ l'ensemble des fonctions continues sur I et à valeurs dans $\mathbb{K}$,
$\mathcal{C}^0_{pm}(I, \mathbb{K})$ l'ensemble des fonctions continues par morceaux sur I et à valeurs dans $\mathbb{K}$.

On obtient facilement les résultats suivants (que l'on admettra ici).

Théorème 2 (Structure algébrique des ensembles de fonctions)
Pour tout intervalle I, l'ensemble $\mathcal{F}(I, \mathbb{K})$ est un $\mathbb{K}$-espace vectoriel, et les ensembles $\mathcal{C}^0(I, \mathbb{K})$ et $\mathcal{C}^0_{pm}(I, \mathbb{K})$ sont des sous-espaces vectoriels de $\mathcal{F}(I, \mathbb{K})$, donc des $\mathbb{K}$-espaces vectoriels.
De plus, on a $\mathcal{C}^0(I, \mathbb{K}) \subset \mathcal{C}^0_{pm}(I, \mathbb{K})$.

I Intégrales impropres (ou généralisées)

1) Sur un intervalle semi-ouvert borné

On considère deux réels a, b tels que $a < b$.

Définition 3 (Convergence d'une intégrale impropre en b)
Soit $f \in \mathcal{C}^0_{pm}([a;b[, \mathbb{K})$.

(*i*) *On dit que* **l'intégrale impropre $\int_a^b f(t)\mathrm{d}t$ converge si** $\int_a^x f(t)\mathrm{d}t$ *possède une limite finie lorsque $x \to b^-$. Dans ce cas, on pose $\int_a^b f(t)\mathrm{d}t = \lim\limits_{x \to b^-} \int_a^x f(t)\mathrm{d}t$.*

(*ii*) *Sinon (si $\int_a^x f(t)\mathrm{d}t$ admet une lim. infinie ou pas de lim. quand $x \to b^-$), on dit que* **l'intégrale impropre $\int_a^b f(t)\mathrm{d}t$ diverge**.

Vocabulaire
On emploie indifféremment les expressions "intégrale impropre" ou "intégrale généralisée" dès que l'on veut intégrer une fonction sur un intervalle qui n'est pas un segment.

Notation
On peut également employer les notations abrégées ("sans la variable d'intégration") :

$$\int_a^b f = \lim_{x \to b^-} \int_a^x f.$$

Vocabulaire
Etudier **la nature** d'une intégrale impropre, c'est préciser si elle est convergente ou divergente.

Propriété 4 (Intégrale faussement impropre en b)
Si $f \in \mathcal{C}^0([a;b[,\mathbb{K})$ et si f possède une limite finie en b^-, alors l'intégrale impropre $\int_a^b f(t)\mathrm{d}t$ converge, et on a $\int_a^b f(t)\mathrm{d}t = \int_a^b \tilde{f}(t)\mathrm{d}t$, où $\tilde{f} \in \mathcal{C}^0([a;b],\mathbb{K})$ est le prolongement continu de f à $[a;b]$.
Dans ce cas, on dit que l'intégrale $\int_a^b f(t)\mathrm{d}t$ est **faussement impropre**.

2) Sur un intervalle fermé non borné

Définition 5 (Convergence d'une intégrale impropre en $+\infty$)
Soit $f \in \mathcal{C}^0_{pm}([a;+\infty[,\mathbb{K})$, avec $a \in \mathbb{R}$.

(i) On dit que **l'intégrale impropre $\boldsymbol{\int_a^{+\infty} f(t)\mathrm{d}t}$ converge si** $\int_a^x f(t)\mathrm{d}t$ *possède une limite finie lorsque $x \to +\infty$. Dans ce cas, on pose $\int_a^{+\infty} f(t)\mathrm{d}t = \lim\limits_{x\to+\infty} \int_a^x f(t)\mathrm{d}t$.*

(ii) Sinon (si $\int_a^x f(t)\mathrm{d}t$ admet une limite infinie ou pas de limite lorsque $x \to +\infty$), on dit que **l'intégrale impropre $\boldsymbol{\int_a^{+\infty} f(t)\mathrm{d}t}$ diverge**.

3) Sur un intervalle ouvert

Définition 6 (Convergence d'une intégrale doublement impropre)
Soit $f \in \mathcal{C}^0_{pm}(]a;b[,\mathbb{K})$ (avec $a \in \mathbb{R}\cup\{-\infty\}$ et $b \in \mathbb{R}\cup\{+\infty\}$). On fixe $c \in]a;b[$.

(i) On dit que **l'intégrale doublement impropre $\boldsymbol{\int_a^b f(t)\mathrm{d}t}$ converge** *si* **les deux intégrales impropres $\boldsymbol{\int_a^c f(t)\mathrm{d}t}$ et $\boldsymbol{\int_c^b f(t)\mathrm{d}t}$ convergent**.
Dans ce cas, on pose $\int_a^b f(t)\mathrm{d}t = \int_a^c f(t)\mathrm{d}t + \int_c^b f(t)\mathrm{d}t$.

(ii) Dans le cas contraire (dès que l'une des deux intégrales précédentes diverge), on dit que **l'intégrale doublement impropre $\boldsymbol{\int_a^b f(t)\mathrm{d}t}$** *diverge.*

4) Propriétés de base

Les propriétés établies ici sont vraies pour des intégrales $\int_a^b f$ impropres en a et/ou b, les bornes a et b étant des réels ou $\pm\infty$.

Propriété 7 (Linéarité, positivité et croissance de l'intégrale impropre)
Soient $f, g \in \mathcal{C}^0_{pm}(I, \mathbb{K})$, où I est un intervalle d'extrémités $a \in \mathbb{R} \cup \{-\infty\}$ et $b \in \mathbb{R} \cup \{+\infty\}$.

(i) Si les deux intégrales impropres $\int_a^b f$ et $\int_a^b g$ sont convergentes, alors pour tout $\lambda \in \mathbb{K}$, l'intégrale $\int_a^b (\lambda f + g)$ est convergente, et on a $\int_a^b (\lambda f + g) = \lambda \int_a^b f + \int_a^b g$.
En d'autres termes, l'ensemble des fonctions $f \in \mathcal{C}^0_{pm}(I, \mathbb{K})$ dont l'intégrale converge est un $\mathbb{K}$-espace vectoriel, et $f \mapsto \int_a^b f$ est une forme linéaire sur cet espace vectoriel.

(ii) La forme linéaire $f \mapsto \int_a^b f$ est positive, c'est-à-dire :

$$\left(f \geq 0 \text{ et } \int_a^b f \text{ converge} \right) \implies \int_a^b f \geq 0.$$

(iii) La forme linéaire $f \mapsto \int_a^b f$ est croissante, c'est-dire :

$$\left(f \leq g, \quad \int_a^b f \text{ converge et} \int_a^b g \text{ converge} \right) \implies \int_a^b f \leq \int_a^b g.$$

Propriété 8 (Convergence de l'intégrale impropre d'une fct. complexe)
Soit I un intervalle de $\mathbb{R}$ d'extrémités $a \in \mathbb{R} \cup \{-\infty\}$ et $b \in \mathbb{R} \cup \{+\infty\}$ et soit $f \in \mathcal{C}^0_{pm}(I, \mathbb{C})$.
Alors, l'intégrale impropre $\int_a^b f$ converge si et seulement si les deux intégrales impropres $\int_a^b \mathrm{Re}(f)$ et $\int_a^b \mathrm{Im}(f)$ convergent. Dans ce cas, on a $\int_a^b f = \int_a^b \mathrm{Re}(f) + i \int_a^b \mathrm{Im}(f)$.

Propriété 9 (Fonction continue positive d'intégrale impropre nulle)
Soit I un intervalle de $\mathbb{R}$ d'extrémités $a \in \mathbb{R} \cup \{-\infty\}$ et $b \in \mathbb{R} \cup \{+\infty\}$ Soit $f \in \mathcal{C}^0(I, \mathbb{R})$, telle que $\boldsymbol{f \geq 0}$ et $\int_a^b f(t)\mathrm{d}t$ converge. Alors,

$$\int_a^b f = 0 \implies \forall t \in [a; b[, \ f(t) = 0.$$

Propriété 10 (Relation de Chasles pour les intégrales impropres)
Soit I un intervalle de $\mathbb{R}$ d'extrémités $a \in \mathbb{R} \cup \{-\infty\}$ et $b \in \mathbb{R} \cup \{+\infty\}$ et $f \in \mathcal{C}^0_{pm}(I, \mathbb{K})$.
Si $\int_a^b f$ converge, alors pour tout $c \in I$, on a

$$\int_a^b f = \int_a^c f + \int_c^b f$$

(avec convergence des deux intégrales du membre de droite).

Propriété 11 (Dérivation par rapport à la borne inférieure)
Si $f \in \mathcal{C}^0([a, +\infty[, \mathbb{K})$ et si l'intégrale $\int_a^{+\infty} f(t)dt$ converge, alors la fonction $G : x \mapsto \int_x^{+\infty} f(t)dt$ est de classe $\mathcal{C}^1$ sur $[a, +\infty[$, et $G' = -f$.

II Comparaison de fonctions positives

Comme pour les séries, on va donner des méthodes pour **étudier la convergence** d'une intégrale impropre, **sans passer par les primitives de f**, qui hélas ne sont pas toujours calculables.

1) Exemples de référence

On dispose d'une liste d'exemples de référence, **qu'il faut connaître par coeur**. On utilisera ensuite cas de référence pour étudier les autres intégrales impropres.

a) En 0

Propriété 12 (Logarithme en 0^+)
L'intégrale $\displaystyle\int_0^1 \ln(t)\mathrm{d}t$ *converge et* $\displaystyle\int_0^1 \ln(t)\mathrm{d}t = -1$.

Propriété 13 (Intégrales de Riemann en 0^+)
Soit $\alpha \in \mathbb{R}$. *Alors, l'intégrale* $\displaystyle\int_0^1 \frac{1}{t^\alpha}\mathrm{d}t$ *(impropre en 0) converge si et seulement si* $\alpha < 1$. *Dans ce cas, on a* $\displaystyle\int_0^1 \frac{1}{t^\alpha}\mathrm{d}t = \frac{1}{1-\alpha}$.

b) En $+\infty$

Propriété 14 (Exponentielle en $+\infty$)
Soit $\alpha \in \mathbb{R}$. *L'intégrale* $\displaystyle\int_0^{+\infty} \mathrm{e}^{-\alpha t}\mathrm{d}t$ *converge si et seulement si* $\alpha > 0$.
Dans ce cas, on a $\displaystyle\int_0^{+\infty} \mathrm{e}^{-\alpha t}\mathrm{d}t = \frac{1}{\alpha}$.

Propriété 15 (Intégrales de Riemann en $+\infty$)
Soit $\alpha \in \mathbb{R}$. *Alors, l'intégrale* $\displaystyle\int_1^{+\infty} \frac{1}{t^\alpha}\mathrm{d}t$ *(impropre en* $+\infty$*) converge si et seulement si* $\alpha > 1$.
Dans ce cas, on a $\displaystyle\int_1^{+\infty} \frac{1}{t^\alpha}\mathrm{d}t = \frac{1}{\alpha-1}$.

2) Comparaison et équivalents

On dispose de résultats **spécifiques aux fonctions positives** pour étudier la convergence d'une intégrale impropre.
Pour éviter les répétitions, les résultats seront énoncés uniquement pour des fonctions continues par morceaux sur un intervalle $\boldsymbol{I = [a; b[}$ (avec $b \in \mathbb{R} \cup \{+\infty\}$), mais **ils s'adaptent à tout type d'intervalle**.

a) Critère de majoration

Propriété 16 (CNS de convergence de l'intégrale d'une fonction positive)
Soit $f \in \mathcal{C}^0_{pm}([a; b[, \mathbb{R})$ *positive. L'intégrale* $\displaystyle\int_a^b f$ *converge si et seulement si la fonction* $F : x \mapsto \displaystyle\int_a^x f$ *est majorée sur* $[a, b[$.

Notation
Lorsque $f \in \mathcal{C}^0_{pm}([a; b[, \mathbb{R})$ est **positive**, on pourra noter $\displaystyle\int_a^b f < +\infty$ lorsque cette intégrale converge, et noter $\displaystyle\int_a^b f = +\infty$ dans le cas divergent (puisque dans ce cas, $\displaystyle\int_a^x f \underset{x\to b^-}{\longrightarrow} +\infty$).
On dispose donc de notations analogues à celles des familles sommables.

Théorème 17 (Critère de majoration pour les fonctions positives)
Soient $f, g \in \mathcal{C}^0_{pm}([a;b[,\mathbb{R})$ telles que $0 \leq f \leq g$. Alors,

(i) $\int_a^b g$ *converge* $\implies \int_a^b f$ *converge, et dans ce cas,*

$$0 \leq \int_a^b f \leq \int_a^b g.$$

(ii) $\int_a^b f$ *diverge* $\implies \int_a^b g$ *diverge.*

b) Critère des équivalents

Théorème 18 (Critère des équivalents pour les fonctions positives)
Soient $f, g \in \mathcal{C}^0_{pm}([a;b[,\mathbb{R})$.

Si $f(t) \underset{t\to b^-}{\sim} g(t)$ et si $f \geq 0$ au voisinage de b^-, alors g aussi et les intégrales impropres $\int_a^b f$ et $\int_a^b g$ sont de même nature.

Pour résumer :

Méthode
Pour étudier la convergence de l'intégrale impropre d'une fonction f **positive**, *on peut* **comparer f à une fonction de référence** *(c'est-à-dire dont on connaît la convergence de l'intégrale), en utilisant soit une inégalité, soit un équivalent.*
Si f est équivalente à une fonction g qui garde un signe constant au voisinage de b, alors on peut utiliser le critère des équivalents.

III Convergence absolue, intégrabilité

1) Convergence absolue

Dans le cas où l'on a affaire à des fonctions qui ne sont pas positives (réelles de signe non constant ou à valeurs complexes), on dispose d'un outil supplémentaire pour étudier la convergence d'une intégrale impropre.

Là encore, tout est énoncé sur un intervalle du type $\boldsymbol{I = [a, b[}$ avec $\boldsymbol{b \in \mathbb{R} \cup \{+\infty\}}$, mais tout s'adapte à tout type d'intervalle.

Définition 19 (Intégrale impropre absolument convergente)
Soit $f \in \mathcal{C}^0_{pm}([a;b[,\mathbb{K})$. On dit que l'intégrale impropre $\displaystyle\int_a^b f$ est **absolument convergente** *lorsque $\displaystyle\int_a^b |f|$ est convergente.*

Théorème 20 («CVA $\implies$ CV»)
Soit $f \in \mathcal{C}^0_{pm}([a;b[,\mathbb{K})$. **Si** *$\displaystyle\int_a^b f$ est absolument convergente,* **alors** *elle est convergente.*
On a donc $\left(\displaystyle\int_a^b |f| \text{ converge } \implies \int_a^b f \text{ converge }\right)$.

Méthode
Pour étudier la convergence de l'intégrale impropre d'une fonction de signe non constant ou à valeurs complexes, on peut **d'abord étudier sa convergence absolue**.

- *Avantage : cela revient à travailler avec une fonction positive, sur laquelle on peut tester les critères de la partie précédente.*
- *Inconvénient : si l'intégrale ne converge pas absolument, alors ça ne montre rien quant à sa convergence.*

Définition 21 (Intégrale impropre semi-convergente)
Soit $f \in \mathcal{C}^0_{pm}([a;b[,\mathbb{K})$. On dit que l'intégrale impropre $\displaystyle\int_a^b f$ est **semi-convergente** *lorsque $\displaystyle\int_a^b f$ est convergente mais pas absolument convergente, c'est-à-dire lorsque $\displaystyle\int_a^b f$ converge et $\displaystyle\int_a^b |f|$ diverge.*

Propriété 22 (Inégalité intégrale/module)
Soit $f \in \mathcal{C}^0_{pm}([a;b[,\mathbb{K})$. On suppose que l'intégrale impropre $\displaystyle\int_a^b f$ est absolument convergente.
Alors, on a $\left|\displaystyle\int_a^b f\right| \leq \int_a^b |f|$.

2) Fonctions intégrables

Ici, I désigne un intervalle de $\mathbb{R}$ quelconque (ouvert, semi-ouvert, borné ou non, fermé, etc.), d'extrémités $a \in \mathbb{R} \cup \{-\infty\}$ et $b \in \mathbb{R} \cup \{+\infty\}$.

Définition 23 (Fonction intégrable sur un intervalle quelconque)
Soit $f : I \to \mathbb{K}$. On dit que $\boldsymbol{f}$ **est intégrable sur** $\boldsymbol{I}$ *si elle est continue par morceaux et si l'intégrale $\displaystyle\int_a^b |f|$ converge.*

Notation
Lorsque f est intégrable sur I, on pourra noter $\displaystyle\int_I f = \int_a^b f$ son intégrale.
On évitera cette notation pour les intégrales semi-convergentes.

Propriété 24 (Propriétés immédiates des fonctions intégrables)
Soit $f, g \in \mathcal{C}^0_{pm}(I, \mathbb{K})$.

(i) Si f est intégrable sur I, alors f est intégrable sur tout intervalle $J \subset I$.

(ii) Si $|f| \leq g$ avec g intégrable sur I, alors f est intégrable sur I.

(iii) Si $I = [a, b[$ et $f(x) \underset{x \to b^-}{\sim} g(x)$, alors f est intégrable sur I ssi g est intégrable sur I.

(iv) Si f est intégrable sur I, alors $|f|$ aussi, et $\left| \int_I f \right| \leq \int_I |f|$.

(v) Si f est intégrable, **continue** *et positive sur I, alors*

$$\int_I f = 0 \implies f = 0.$$

Propriété 25 (Règle de comparaison en O, o)
Soient $f, g \in \mathcal{C}^0_{pm}([a, b[, \mathbb{K})$, avec $b \in \mathbb{R} \cup \{+\infty\}$.

(i) Si $f(x) = \underset{x \to b^-}{O}(g(x))$ et si g est intégrable sur $[a, b[$, alors f est intégrable sur $[a, b[$.

(ii) Si $f(x) = \underset{x \to b^-}{o}(g(x))$ et si g est intégrable sur $[a, b[$, alors f est intégrable sur $[a, b[$.

Théorème 26 (Structure d'espace vectoriel)
L'ensemble des fonctions intégrables $I \to \mathbb{K}$ est un $\mathbb{K}$ espace-vectoriel (en fait un sous-espace vectoriel de $\mathcal{C}^0_{pm}(I, \mathbb{K})$). De plus, $f \mapsto \int_I f$ est une forme linéaire sur cet espace vectoriel.

Notation
L'espace vectoriel des fonctions intégrables sur I et à valeurs dans $\mathbb{K}$ se note en général $L^1(I, \mathbb{K})$.

3) Des exemples

Méthode
Pour étudier la convergence absolue d'une intégrale impropre, on peut :

- *chercher à* **majorer $|f(t)|$** *par une fonction intégrable connue.*
- *chercher à déterminer* **un équivalent simple de $|f(t)|$** *lorsque $t \to b^-$.*
- *examiner* **la limite de $t^\alpha f(t)$** *lorsque $t \to 0^+$ ou $t \to +\infty$, pour* **comparer f à une fonction de Riemann $t \mapsto \dfrac{1}{t^\alpha}$** *au voisinage de 0 ou de $+\infty$.*

IV IPP et changement de variables généralisés

On ne traitera par commodité que le cas des intervalles du type $[\boldsymbol{a};\boldsymbol{b}[$ (avec $b \in \mathbb{R} \cup \{+\infty\}$), mais les résultats présentés ici restent vrais pour tout type d'intervalle.

1) Intégration par parties généralisée

Théorème 27 (IPP généralisée)
Soient $u, v \in \mathcal{C}^1([a,b[,\mathbb{K})$. Si $\lim\limits_{b^-} uv$ existe dans $\mathbb{K}$, alors les intégrales $\int_a^b u'v$ et $\int_a^b uv'$ sont de même nature, et si elles convergent, on a

$$\int_a^b u'v = [uv]_a^b - \int_a^b uv',$$

où $[uv]_a^b = \lim\limits_{x\to b^-} u(x)v(x) - u(a)v(a)$.

2) Changement de variable généralisé

Théorème 28 (Changement de variables généralisé)
Soit $f \in \mathcal{C}^0([a;b[,\mathbb{K})$, et soit $\varphi : [\alpha;\beta[\to [a;b[$ une **bijection** *strictement croissante de classe $\mathcal{C}^1$. Alors les intégrales impropres $\displaystyle\int_\alpha^\beta f(\varphi(u))\varphi'(u)\mathrm{d}u$ et $\displaystyle\int_a^b f(t)\mathrm{d}t$ sont de même nature et égales en cas de convergence.*

V Intégration des relations de comparaison

1) Cas convergent

Théorème 29 (Intégration des relations de comparaison, cas convergent)
Soit $f \in \mathcal{C}^0_{pm}([a,b[,\mathbb{K})$ et $g \in \mathcal{C}^0_{pm}([a,b[,\mathbb{R})$ (avec $b \in \mathbb{R} \cup \{+\infty\}$). On suppose que $g \geq 0$ et $\int_a^b g$ converge.

(i) Si $f(x) = \underset{x\to b^-}{O}(g(x))$, alors f est intégrable sur $[a,b[$ et $\int_x^b f = \underset{x\to b^-}{O}(\int_x^b g)$.

(ii) Si $f(x) = \underset{x\to b^-}{o}(g(x))$, alors f est intégrable sur $[a,b[$ et $\int_x^b f = \underset{x\to b^-}{o}(\int_x^b g)$.

(iii) Si $f(x) \underset{x\to b^-}{\sim} g(x)$, alors f est intégrable sur $[a,b[$ et $\int_x^b f \underset{x\to b^-}{\sim} \int_x^b g$.

2) Cas divergent

Théorème 30 (Intégration des relations de comparaison, cas divergent)
Soit $f \in \mathcal{C}^0_{pm}([a,b[,\mathbb{K})$ et $g \in \mathcal{C}^0_{pm}([a,b[,\mathbb{R})$ (avec $b \in \mathbb{R} \cup \{+\infty\}$). On suppose que $g \geq 0$ et $\int_a^b g$ diverge.

(i) Si $f(x) = \underset{x\to b^-}{O}(g(x))$, alors $\int_a^x f = \underset{x\to b^-}{O}(\int_a^x g)$.

(ii) Si $f(x) = \underset{x\to b^-}{o}(g(x))$, alors $\int_a^x f = \underset{x\to b^-}{o}(\int_a^x g)$.

(iii) Si $f(x) \underset{x\to b^-}{\sim} g(x)$, alors f est non intégrable sur $[a,b[$ et $\int_a^x f \underset{x\to b^-}{\sim} \int_a^x g$.

CH03 : Structures algébriques usuelles

I Groupes

1) Groupes et sous-groupes

Définition 1 (Groupe)
Un **groupe** *est un ensemble G muni d'une loi de composition interne $* : G \times G \to G$ qui vérifie les propriétés suivantes :*

(i) associativité : $\forall (x,y,z) \in G^3,\ x*(y*z) = (x*y)*z$;

(ii) existence d'un élément neutre : $\exists e \in G,\ \forall x \in G,\ x*e = e*x = x$;

(iii) existence d'un symétrique pour tout élément : $\forall x \in G,\ \exists y \in G,\ x*y = y*x = e$.

Notation
Un groupe sera noté $(G,*)$, où G est l'ensemble et $*$ la loi de composition interne.

Définition 2 (Groupe commutatif)
On dit qu'un groupe $(G,*)$ est **commutatif** *lorsque la loi $*$ est (en plus du reste) commutative, c'est-à-dire $\forall (x,y) \in G^2,\ x*y = y*x$.*

Vocabulaire
Un groupe commutatif est aussi appelé **groupe abélien** (en référence au mathématicien norvégien Abel).

Propriété 3 (Propriétés immédiates d'une loi de groupe)
Soit $(G,*)$ un groupe.

(i) L'élément neutre e est unique.

(ii) Tout élément $x \in G$ possède un unique symétrique.

(iii) Tout élément est simplifiable à gauche : $\forall (x,y,z) \in G^3,\ x*y = x*z \implies y = z$.

(iv) Tout élément est simplifiable à droite : $\forall (x,y,z) \in G^3,\ y*x = z*x \implies y = z$.

Notation

- Lorsque la loi du groupe G est notée $*$, $\times$ ou $\cdot$ ("notations multiplicatives"), le neutre sera noté e (ou e_G ou 1 ou 1_G) et le symétrique d'un élément $x \in G$ sera appelé "inverse" et noté x^{-1}. On notera également pour tout $n \in \mathbb{N}$:

$$x^n = x*x*\cdots*x \quad (n\ fois),$$

$$x^{-n} = (x*x*\cdots*x)^{-1} = x^{-1}*\cdots*x^{-1} \quad (n\ fois),$$

  avec la convention $x^0 = e$.
- Lorsque la loi du groupe G est notée $+$ ("notation additive"), le neutre sera noté 0 (ou 0_G) et le symétrique d'un élément $x \in G$ sera appelé "opposé" et noté $-x$. On notera également pour tout $n \in \mathbb{N}$:

$$nx = x + x + \cdots + x \quad (n\ fois),$$

$$(-n)x = -(x + x + \cdots + x) = (-x) + (-x) + \cdots + (-x) \quad (n\ fois),$$

  avec la convention $0x = 0_G$.
  Attention, la notation additive n'est employée que pour des groupes commutatifs.
- Les résultats généraux sur les groupes seront énoncés en notation multiplicative, mais se transposent bien évidemment en notation additive.

Propriété 4 (Produit fini de groupes)
Soit $n \in \mathbb{N}^*$ et $(G_1, *_1), \cdots, (G_n, *_n)$ des groupes. Alors, l'ensemble $G_1 \times \cdots \times G_n$ muni de la loi de composition interne :

$$(x_1, \cdots, x_n) * (y_1, \cdots, y_n) = (x_1 *_1 y_1, \cdots, x_n *_n y_n)$$

est un groupe. L'élément neutre est $(e_1, \cdots, e_n)$ (où e_i est le neutre de G_i pour tout i), et pour tout $(x_1, \cdots, x_n) \in G_1 \times \cdots \times G_n$, on a

$$(x_1, \cdots, x_n)^{-1} = (x_1^{-1}, \cdots, x_n^{-1}),$$

où x_i^{-1} désigne le symétrique de x_i dans G_i pour tout i).
Ce groupe $(G_1 \times \cdots \times G_n, *)$ est appelé **groupe produit** *des groupes $(G_1, *_1), \cdots, (G_n, *_n)$.*

Preuve laissée en exercice
Vérifications immédiates (bien qu'un peu fastidieuses).

Définition 5 (Sous-groupe)
Soit $(G, *)$ un groupe de neutre e. On dit qu'une partie $H \subset G$ est un **sous-groupe** *de G lorsque :*
(i) $e \in H$;
(ii) H est stable par $*$: $\forall (x, y) \in H^2,\ x * y \in H$;
(iii) H est stable par passage au symétrique : $\forall x \in H,\ x^{-1} \in H$.

Propriété 6 (Caractérisation d'un sous-groupe)
Soit $(G, *)$ un groupe et $H \subset G$. Alors, H est un sous-groupe de G si et seulement si :
(a) $H \neq \emptyset$;
(b) $\forall (x, y) \in H^2,\ x^{-1} * y \in H$.

Propriété 7 (Intersection de sous-groupes)
Soit I un ensemble d'indices quelconque et $(H_i)_{i \in I}$ une famille de sous-groupes d'un même groupe $(G, *)$. Alors, $\bigcap_{i \in I} H_i$ est un sous-groupe de G.

Définition 8 (Sous-groupe engendré par une partie)
Soit $(G, *)$ un groupe et $A \subset G$ une partie (quelconque). On appelle **sous-groupe engendré par** *A l'intersection de tous les sous-groupes de G contenant A.*

Notation
On notera $\langle A \rangle$ le sous-groupe engendré par A :

$$\langle A \rangle = \bigcap_{\substack{H \text{ sg de } G \\ A \subset H}} H.$$

Propriété 9 (Caractère minimal du sous-groupe engendré)
Soit $(G, *)$ un groupe et $A \subset G$ une partie (quelconque). Alors $\langle A \rangle$ est le plus petit sous-groupe de G (au sens de l'inclusion) contenant A.

Notation
Si $a_1, \cdots, a_n$ sont des éléments de G, alors on notera

$$\langle a_1, \cdots, a_n \rangle = \langle \{a_1, \cdots, a_n\} \rangle.$$

Ainsi, pour tout $a \in G$ et $b \in G$:
$\langle a \rangle$ désigne le plus petit sous-groupe de G contenant a,
$\langle a, b \rangle$ désigne le plus petit sous-groupe de G contenant a et b, etc.

Propriété 10 (Description du sous-groupe engendré par un élément)
Soit $(G,*)$ un groupe et $a \in G$. Alors

$$\langle a \rangle = \{a^k,\ k \in \mathbb{Z}\}.$$

Théorème 11 (Sous-groupes de $(\mathbb{Z},+)$)
Les sous-groupes de $(\mathbb{Z},+)$ sont exactement les $n\mathbb{Z} = \{nk,\ k \in \mathbb{Z}\}$, avec $n \in \mathbb{N}$.

2) Morphismes de groupes

Définition 12 (Morphisme de groupes)
Soit $(G,*)$ et $(G',\top)$ deux groupes. Un **morphisme de groupes** *de G dans G' est une application $\varphi : G \to G'$ telle que $\forall (x,y) \in G^2,\ \varphi(x*y) = \varphi(x)\top\varphi(y)$.*

Propriété 13 (Propriétés immédiates des morphismes de groupes)
Soit $\varphi : (G,*) \to (G',\top)$ un morphisme de groupes. Alors

(i) $\varphi(e_G) = e_{G'}$;

(ii) $\forall x \in G,\ \varphi(x^{-1}) = \varphi(x)^{-1}$.

Propriété 14 (Composée de deux morphismes de groupes)
La composée de deux morphismes de groupes en est un.

Propriété 15 (Image directe/réciproque d'un sous-groupe par un morphisme)
Soit $\varphi : (G,*) \to (G',\top)$ un morphisme de groupes. Alors

(i) Pour tout sous-groupe H de G, l'image directe $\varphi(H) = \{\varphi(x),\ x \in H\}$ est un sous-groupe de G'.

(ii) Pour tout sous-groupe H' de G', l'image réciproque $\varphi^{-1}(H') = \{x \in G,\ \varphi(x) \in H'\}$ est un sous-groupe de G.

Définition 16 (Image et noyau d'un morphisme de groupes)
Soit $\varphi : (G,*) \to (G',\top)$ un morphisme de groupes.

(i) On appelle **image** *de φ l'ensemble $Im(\varphi) = \varphi(G)$. C'est un sous-groupe de G'.*

(ii) On appelle **noyau** *de φ l'ensemble $Ker(\varphi) = \varphi^{-1}(\{e_{G'}\})$. C'est un sous-groupe de G.*

Propriété 17 (Caractérisation de l'injectivité/la surjectivité d'un morphisme de groupes)
Soit $\varphi : (G,*) \to (G',\top)$ un morphisme de groupes.

(i) φ est surjectif ssi $Im(\varphi) = G'$;

(ii) φ est injectif ssi $Ker(\varphi) = \{e_G\}$.

Définition 18 (Isomorphisme de groupes)
Un **isomorphisme** *de groupes de $(G,*)$ dans $(G',\top)$ est un morphisme de groupes bijectif de $(G,*)$ dans $(G',\top)$.*

Propriété 19 (Réciproque d'un isomorphisme de groupes)
Si $\varphi : (G,*) \to (G',\top)$ est un isomorphisme de groupes, alors l'application réciproque $\varphi^{-1} : (G',\top) \to (G,*)$ est aussi un isomorphisme de groupes.

3) Le groupe $(\mathbb{Z}/n\mathbb{Z},+)$

Propriété 20 (Relation de congruence modulo n)
Soit $n \in \mathbb{N}^*$. La relation définie par

$$\forall (x,y) \in \mathbb{Z}^2 : \quad x \equiv y\ [n] \iff n | y-x$$

est une relation d'équivalence sur $\mathbb{Z}$, appelée la **relation de congruence modulo n**.

Notation
Soit $n \in \mathbb{N}^*$ fixé. Pour tout $x \in \mathbb{Z}$, on notera $\overline{x}$ la classe d'équivalence de x pour la relation de congruence modulo n :

$$\overline{x} = \{y \in \mathbb{Z},\ x \equiv y\ [n]\} = \{x + kn,\ k \in \mathbb{Z}\} = x + n\mathbb{Z}.$$

Propriété 21 (Nombres de classes d'équivalence modulo n)
Soit $n \in \mathbb{N}^*$. Il y a exactement n classes d'équivalence distinctes pour la relation de congruence modulo n :

$$\overline{0}, \overline{1}, \cdots, \overline{n-1}.$$

Définition 22 (Ensemble $\mathbb{Z}/n\mathbb{Z}$)
Soit $n \in \mathbb{N}^*$. On appelle $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences modulo n :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}.$$

Théorème 23 (Structure de groupe additif de $\mathbb{Z}/n\mathbb{Z}$)
Soit $n \in \mathbb{N}^*$. La loi de composition interne $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ donnée par

$$\forall (x, y) \in \mathbb{Z}^2, \qquad \overline{x} + \overline{y} = \overline{x + y}$$

est bien définie, et $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif.

4) Groupes monogènes et cycliques

Définition 24 (Groupe monogène, groupe cyclique)
Un groupe $(G, *)$ est dit **monogène** *lorsqu'il est engendré par un élément, c'est-à-dire lorsqu'il existe $a \in G$ tel que $G = \langle a \rangle$. Un tel élément a est alors appelé* **générateur de G**.
Un groupe $(G, *)$ est dit **cyclique** *s'il est monogène et fini.*

Théorème 25 (Cyclicité et générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$)
Pour tout $n \in \mathbb{N}^*$, le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique et ses générateurs sont exactement les $\overline{k}$ où k est premier avec n.

Théorème 26 (Classification des groupes monogènes)
Soit $(G, *)$ un groupe monogène.

(i) Si G est infini, alors $(G, *)$ est isomorphe à $(\mathbb{Z}, +)$.

(ii) Si G est fini, alors $(G, *)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$, où $n = Card(G)$.

5) Ordre d'un élément dans un groupe

Définition 27 (Element d'ordre fini, ordre d'un élément)
Soit $(G, *)$ un groupe.

(i) On dit qu'un élément $x \in G$ est **d'ordre fini** *lorsqu'il existe $k \in \mathbb{N}^*$ tel que $x^k = e$.*

(ii) Si $x \in G$ est d'ordre fini, on appelle **ordre de x** *le plus petit entier $k \in \mathbb{N}^*$ tel que $x^k = e$. On le notera $ord(x)$.*

Propriété 28 (Propriétés de l'ordre d'un élément)
Soit $(G, *)$ un groupe et $x \in G$.

(i) x est d'ordre fini si et seulement si $\langle x \rangle$ est fini, et dans ce cas, on a $\langle x \rangle = \{e, x, \cdots, x^{ord(x)-1}\}$. En particulier, on a $ord(x) = Card(\langle x \rangle)$.

(ii) Si x est d'ordre fini, alors pour tout $k \in \mathbb{Z}$: $x^k = e \iff ord(x)$ divise k.

Corollaire 29 (Lien entre cyclicité et ordre des éléments)
Un groupe fini de cardinal n est cyclique si et seulement si il possède des éléments d'ordre n, et dans ce cas, les générateurs sont ces éléments d'ordre n.

Théorème 30 (Ordre des éléments d'un groupe fini)
Soit $(G, *)$ un groupe fini de cardinal $n \in \mathbb{N}^*$. Alors $\forall x \in G,\ x^n = e$.
En d'autres termes, tout $x \in G$ est d'ordre fini, et $ord(x)$ divise $Card(G)$.

II Anneaux, corps

1) Anneaux et sous-anneaux

Définition 31 (Anneau)
Un **anneau** *est un ensemble A muni de deux lois de composition interne $+ : A \times A \to A$ (appelée "somme") et $\times : A \times A \to A$ (appelée "produit") qui vérifient les propriétés suivantes :*

(i) $(A, +)$ *est un groupe commutatif (i.e. la loi $+$ est associative, commutative, possède un élément neutre et tout élément $x \in A$ possède un symétrique noté $-x$) ;*

(ii) la loi $\times$ est associative ;

(iii) la loi $\times$ possède un élément neutre ;

(iv) la loi $\times$ est distributive sur la loi $+$, i.e.

$$\forall (x, y, z) \in A^3, \quad x \times (y + z) = x \times y + x \times z, \qquad (y + z) \times x = y \times x + z \times x.$$

Notation
Un anneau sera noté $(A, +, \times)$, le neutre de la loi $+$ (qui est unique) sera noté 0_A (ou 0) et le neutre de la loi $\times$ (également unique) sera noté 1_A (ou 1).
Souvent le "produit" de deux éléments sera noté simplement xy plutôt que $x \times y$.

Définition 32 (Anneau commutatif)
Un anneau $(A, +, \times)$ est dit **commutatif** *lorsque la loi $\times$ est commutative.*

Définition 33 (Elément inversible)
Soit $(A, +, \times)$ un anneau. Un élement $x \in A$ est dit **inversible** *lorsqu'il existe $y \in A$ tel que $xy = yx = 1_A$.*

Propriété 34 (Calculs dans un anneau)
Soit $(A, +, \times)$ un anneau.

(i) Pour tout $x \in A$, $0_A \times x = x \times 0_A = 0_A$.

(ii) Pour tout $(x, y) \in A^2$, $(-x)y = -(xy) = x(-y)$.

(iii) Pour tout $n \in \mathbb{Z}$ et tout $(x, y) \in A^2$, $(nx)y = n(xy) = x(ny)$.

(iv) Si $x \in A$ est inversible, alors son inverse est unique. On le notera x^{-1}.

(v) Si $x \in A$ et $y \in A$ sont inversibles, alors xy est inversible et $(xy)^{-1} = y^{-1}x^{-1}$.

(vi) Si $(x, y) \in A^2$ sont tels que $\boldsymbol{xy = yx}$, alors pour tout $n \in \mathbb{N}$:

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \qquad \textit{(formule du binôme)}$$

(vii) Si $(x, y) \in A^2$ sont tels que $\boldsymbol{xy = yx}$, alors pour tout $n \in \mathbb{N}$:

$$x^n - y^n = (x - y) \left(\sum_{k=0}^{n-1} x^k y^{n-1-k} \right) \qquad \textit{(identité de Bernoulli).}$$

En particulier

$$1_A - x^n = (1_A - x)(1_A + x + x^2 + \cdots + x^{n-1}).$$

Propriété 35 (Groupe des inversibles d'un anneau)
Si $(A, +, \times)$ est un anneau, alors l'ensemble des éléments inversibles de A est un groupe pour la loi $\times$. On le notera $A^\times$ ou $U(A)$.

Propriété 36 (Produit fini d'anneaux)
Soit $n \in \mathbb{N}^*$ et $(A_1, +_1, \times_1), \cdots, (A_n, +_n, \times_n)$ des anneaux. Alors, l'ensemble $A_1 \times \cdots \times A_n$ muni des lois de composition interne :

$$(x_1, \cdots, x_n) + (y_1, \cdots, y_n) = (x_1 +_1 y_1, \cdots, x_n +_n y_n),$$

$$(x_1, \cdots, x_n) \times (y_1, \cdots, y_n) = (x_1 \times_1 y_1, \cdots, x_n \times_n y_n),$$

est un anneau.
L'élément neutre pour $+$ est $(0_{A_1}, \cdots, 0_{A_n})$, et l'élément neutre pour $\times$ est $(1_{A_1}, \cdots, 1_{A_n})$.
Pour tout $(x_1, \cdots, x_n) \in A_1 \times \cdots \times A_n$, on a

$$-(x_1, \cdots, x_n) = (-x_1, \cdots, -x_n).$$

Enfin, un élément $(x_1, \cdots, x_n)$ est inversible si et seulement si tous les x_i le sont, et on a

$$(x_1, \cdots, x_n)^{-1} = (x_1^{-1}, \cdots, x_n^{-1}).$$

Cet anneau $(A_1 \times \cdots \times A_n, +, \times)$ est appelé **anneau produit** *des anneaux $(A_1, +_1, \times_1), \cdots, (A_n, +_n, \times_n)$.*

Preuve laissée en exercice
Vérifications immédiates (mais fastidieuses).

Définition 37 (Sous-anneau)
Soit $(A, +, \times)$ un anneau. Un **sous-anneau** *de A est une partie $B \subset A$ telle que :*

(i) $1_A \in B$;

(ii) $(B, +)$ *est un sous-groupe de* $(A, +)$;

(iii) $\forall (x, y) \in B^2,\ xy \in B$ *(stabilité de B par produit).*

2) Morphismes d'anneaux

Définition 38 (Morphisme d'anneaux)
Soit $(A, +, \times)$ et $(B, +, \times)$ deux anneaux. Un **morphisme d'anneaux** *de A dans B est une application $\varphi : A \to B$ telle que :*

(i) $\varphi(1_A) = 1_B$;

(ii) φ *est un morphisme de groupes de* $(A, +)$ *dans* $(B, +)$
(i.e. $\forall (x, y) \in A^2,\ \varphi(x + y) = \varphi(x) + \varphi(y)$) ;

(iii) $\forall (x, y) \in A^2,\ \varphi(xy) = \varphi(x)\varphi(y)$.

Propriété 39 (Propriétés immédiates des morphismes d'anneaux)
Soit $\varphi : (A, +, \times) \to (B, +, \times)$ un morphisme d'anneaux. Alors :

(i) $\varphi(0_A) = 0_B$;

(ii) $\forall x \in A,\ \varphi(-x) = -\varphi(x)$;

(iii) Si $x \in A^\times$, alors $\varphi(x) \in B^\times$ et $(\varphi(x))^{-1} = \varphi(x^{-1})$.

Propriété 40 (Composée de deux morphismes d'anneaux)
La composée de deux morphismes d'anneaux en est un.

Définition 41 (Image et noyau d'un morphisme d'anneaux)
Soit $\varphi : (A, +, \times) \to (B, +, \times)$ un morphisme d'anneaux.

(i) On appelle **image de** φ *l'ensemble $Im(\varphi) = \varphi(A)$.*

(ii) On appelle **noyau de** φ *l'ensemble $Ker(\varphi) = \varphi^{-1}(\{0_B\})$.*

Propriété 42 (Structure algébrique de l'image d'un morphisme d'anneaux)
Soit $\varphi : (A, +, \times) \to (B, +, \times)$ un morphisme d'anneaux. Alors $Im(\varphi)$ est un sous-anneau de B.

Propriété 43 (Caractérisation de l'injectivité/la surjectivité d'un morphisme d'anneaux)
Soit $\varphi : (A, +, \times) \to (B, +, \times)$ un morphisme d'anneaux.
(i) φ est surjectif ssi $Im(\varphi) = B$;
(ii) φ est injectif ssi $Ker(\varphi) = \{0_A\}$.

Définition 44 (Isomorphisme d'anneaux)
Un **isomorphisme d'anneaux** *est un morphisme d'anneaux bijectif.*

Propriété 45 (Réciproque d'un isomorphisme d'anneaux)
Si $\varphi : A \to B$ est un isomorphisme d'anneaux, alors $\varphi^{-1} : B \to A$ est aussi un isomorphisme d'anneaux.

3) Anneaux intègres

Définition 46 (Anneau intègre)
Un anneau $(A, +, \times)$ est dit **intègre** *lorsqu'il est non réduit à $\{0_A\}$ et lorsque :*

$$\forall (x, y) \in A^2, \quad xy = 0_A \implies x = 0_A \text{ ou } y = 0_A.$$

Propriété 47 (Simplification dans un anneau intègre)
Si $(A, +, \times)$ est un anneau intègre, alors pour tous $(a, b, c) \in A^3$, on a :
(i) $(a \neq 0_A$ et $ab = ac) \implies b = c$;
(ii) $(a \neq 0_A$ et $ba = ca) \implies b = c$.

4) Corps

Définition 48 (Corps)
Un **corps** *est un anneau $(K, +, \times)$ commutatif, non réduit à $\{0_K\}$, dans lequel tout élément $x \neq 0_K$ est inversible.*

Propriété 49 (Intégrité d'un corps)
Tout corps K est un anneau intègre.

Définition 50 (Sous-corps)
Soit $(K, +, \times)$ un corps. Un **sous-corps** *de K est une partie $L \subset K$ telle que :*
(i) L est un sous-anneau de K ;
(ii) Pour tout $x \in L$, $x \neq 0_K \implies x^{-1} \in L$.

III Idéaux d'un anneau commutatif

1) Généralités

Définition 51 (Idéal)
Soit $(A,+,\times)$ un anneau commutatif. Un **idéal** *de A est une partie $I \subset A$ telle que :*

(i) $(I,+)$ est un sous-groupe de $(A,+)$;

(ii) $\forall x \in I,\ \forall a \in A,\ xa \in I$.

Vocabulaire
La propriété (ii) est appelée "propriété d'absorption".

Propriété 52 (Caractérisation d'un idéal)
Soit $(A,+,\times)$ un anneau commutatif et soit $I \subset A$. Alors, I est un idéal de A si et seulement si

(a) $0_A \in I$;

(b) $\forall (x,y) \in I^2,\ x+y \in I$;

(c) $\forall x \in I,\ \forall a \in A,\ xa \in I$.

Propriété 53 (Exemple fondamental : idéal engendré par un élément)
Soit $(A,+,\times)$ un anneau commutatif.
Pour tout $a \in A$, l'ensemble $aA = \{ax,\ x \in A\}$ est un idéal de A, et c'est le plus petit idéal de A contenant a. On dit que aA est **l'idéal engendré par a**.

Propriété 54 (Structure algébrique du noyau d'un morphisme d'anneaux)
Soit $\varphi : (A,+,\times) \to (B,+,\times)$ un morphisme d'anneaux, avec A commutatif.
Alors $Ker(\varphi)$ est un idéal de A.

Propriété 55 (Opérations algébriques sur les idéaux)
Soit $(A,+,\times)$ un anneau commutatif, et I et J deux idéaux de A. Alors :

(i) l'ensemble $I \cap J$ est un idéal de A ;

(ii) l'ensemble $I+J = \{x+y,\ x \in I,\ y \in J\}$ est un idéal de A, appelé **somme des idéaux I et J**. *C'est le plus petit idéal de A contenant I et J.*

Plus généralement, si $I_1, \cdots, I_n$ sont des idéaux de A, on peut définir les idéaux :

$$I_1 \cap \cdots \cap I_n = \{x \in A,\ \forall j \in [\![1,n]\!],\ x \in I_j\},$$

$$I_1 + \cdots + I_n = \{x_1 + \cdots + x_n,\ x_1 \in I_1, \cdots, x_n \in I_n\},$$

et ces opérations sur les idéaux sont associatives.

2) Idéaux et divisibilité

Définition 56 (Divisibilité dans un anneau commutatif)
Dans un anneau commutatif $(A,+,\times)$, étant donnés $(a,b) \in A^2$, on dit que **b divise a** *lorsqu'il existe $c \in A$ tel que $a = bc$. On note alors $b|a$.*

Propriété 57 (Eléments associés dans un anneau commutatif intègre)
Soit $(A,+,\times)$ un anneau commutatif et **intègre**. *Alors, pour tout $(a,b) \in A^2$, on a*

$$(b|a \text{ et } a|b) \iff \exists u \in A^\times,\ b = ua.$$

On dit dans ce cas que a et b sont **associés**.

Propriété 58 (Interprétation de la divisibilité en termes d'idéaux)
Soit $(A,+,\times)$ un anneau commutatif et **intègre**, *et soit $(a,b)\in A^2$.*
Alors :

(i) $b|a \iff aA\subset bA$.

(ii) a et b sont associés si et seulement si $aA=bA$.

3) Idéaux de $\mathbb{Z}$ et applications à l'arithmétique

Théorème 59 (Idéaux de $\mathbb{Z}$)
Les idéaux de l'anneau $(\mathbb{Z},+,\times)$ sont exactement les $n\mathbb{Z}$ avec $n\in\mathbb{N}$, et tous ces idéaux sont distincts.

Vocabulaire (HP)
On dit qu'un anneau commutatif A est **principal** s'il est intègre et si tous ses idéaux sont "monogènes", c'est-à-dire de la forme $I=aA$ avec $a\in A$. Ainsi, l'anneau $\mathbb{Z}$ possède cette propriété, et on verra plus loin que l'anneau de polynômes $\mathbb{K}[X]$ également.

Propriété 60 (Définition du PGCD d'entiers par les idéaux)
Soit $(a_1,\cdots,a_n)\in\mathbb{Z}^n$. Alors il existe un unique $d\in\mathbb{N}$ tel que $a_1\mathbb{Z}+\cdots+a_n\mathbb{Z}=d\mathbb{Z}$.
L'entier d est alors le **plus grand diviseur commun** *de $a_1,\cdots,a_n$, c'est-à-dire que :*

(i) $\forall i\in[\![1,n]\!],\ d|a_i$;

(ii) $\forall c\in\mathbb{Z},((\forall i\in[\![1,n]\!],\ c|a_i)\implies c|d)$.

On notera $d=pgcd(a_1,\cdots,a_n)$ ou $d=a_1\wedge\cdots\wedge a_n$.

Propriété 61 (Relation de Bézout)
Soit $(a_1,\cdots,a_n)\in\mathbb{Z}^n$ et $d=pgcd(a_1,\cdots,a_n)$.
Alors, il existe $(u_1,\cdots,u_n)\in\mathbb{Z}^n$ tel que $a_1u_1+\cdots+a_nu_n=d$.

Définition 62 (Entiers premiers entre eux)
Soit $(a_1,\cdots,a_n)\in\mathbb{Z}^n$ avec $n\geq 2$.
On dit que $a_1,\cdots,a_n$ sont **premiers entre eux dans leur ensemble** *lorsque $pgcd(a_1,\cdots,a_n)=1$.*
On dit que $a_1,\cdots,a_n$ sont **premiers entre eux deux à deux** *lorsque pour tout $(i,j)\in[\![1,n]\!]$, $i\neq j\implies pgcd(a_i,a_j)=1$.*

Propriété 63 (Théorème de Bézout)
Soit $(a_1,\cdots,a_n)\in\mathbb{Z}^n$. Alors :
$a_1,\cdots,a_n$ sont premiers entre eux dans leur ensemble ssi $\exists(u_1,\cdots,u_n)\in\mathbb{Z}^n,\ a_1u_1+\cdots+a_nu_n=1$.

Corollaire 64 (Lemme de Gauss)
Soit $(a,b,c)\in\mathbb{Z}^3$. Si $a|bc$ et si a et b sont premiers entre eux, alors $a|c$.

Corollaire 65 (Lemme d'Euclide)
Soit p un nombre premier et $(a,b)\in\mathbb{Z}^2$. Si p divise ab, alors p divise a ou b.

Propriété 66 (Définition du PPCM d'entiers par les idéaux)
Soit $(a_1,\cdots,a_n)\in\mathbb{Z}^n$. Alors il existe un unique $m\in\mathbb{N}$ tel que $a_1\mathbb{Z}\cap\cdots\cap a_n\mathbb{Z}=m\mathbb{Z}$.
L'entier m est alors le **plus petit multiple commun** *de $a_1,\cdots,a_n$, c'est-à-dire que :*

(i) $\forall i\in[\![1,n]\!],\ a_i|m$;

(ii) $\forall c\in\mathbb{Z},((\forall i\in[\![1,n]\!],\ a_i|c)\implies m|c)$.

On notera $m=ppcm(a_1,\cdots,a_n)$ ou $m=a_1\vee\cdots\vee a_n$.

IV Anneau $\mathbb{Z}/n\mathbb{Z}$ et applications à l'arithmétique

1) L'anneau $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$. On rappelle que l'ensemble $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \cdots, \overline{n-1}\}$ peut être muni d'une structure de groupe additif (cf. prop. 23). On peut également munir $\mathbb{Z}/n\mathbb{Z}$ d'une structure d'anneau.

Théorème 67 (Structure d'anneau commutatif de $\mathbb{Z}/n\mathbb{Z}$)
Soit $n \in \mathbb{N}^*$. Les lois de composition interne $+ : \mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ et $\times : \mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ données par

$$\forall (x,y) \in \mathbb{Z}^2, \qquad \overline{x} + \overline{y} = \overline{x+y},$$

$$\forall (x,y) \in \mathbb{Z}^2, \qquad \overline{x} \times \overline{y} = \overline{xy},$$

sont bien définies, et $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif, de neutres respectifs $\overline{0}$ et $\overline{1}$.

2) Théorème chinois

Théorème 68 (Théorème chinois)
Soient $(m,n) \in (\mathbb{N}^*)^2$ deux entiers **premiers entre eux**. *Alors l'application*

$$\psi : \left\{ \begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \overline{x} & \longmapsto & (\dot{x}, \hat{x}) \end{array} \right.$$

est un isomorphisme d'anneaux, où $\overline{x}$ (resp. $\dot{x}$, resp. $\hat{x}$) désigne la classe de l'entier x modulo mn (resp. modulo m, resp. modulo n). L'isomorphisme réciproque est :

$$\psi^{-1} : \left\{ \begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/mn\mathbb{Z} \\ (\dot{a}, \hat{b}) & \longmapsto & \overline{anv + bmu} \end{array} \right. ,$$

où $(u,v) \in \mathbb{Z}$ sont tels que $mu + nv = 1$.

Théorème 69 (Théorème chinois généralisé)
Soit $k \geq 2$ et $m_1, \cdots, m_k$ des entiers **premiers entre eux deux à deux**. *Alors l'application :*

$$\psi : \left\{ \begin{array}{ccc} \mathbb{Z}/(m_1 \cdots m_k)\mathbb{Z} & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \\ \overline{x} & \longmapsto & (\dot{x}_{(1)}, \cdots, \dot{x}_{(k)}) \end{array} \right.$$

est un isomorphisme d'anneaux, où $\overline{x}$ désigne la classe de l'entier x modulo $m_1 \cdots m_k$ et pour tout $i \in [\![1,k]\!]$, $\dot{x}_{(i)}$ désigne la classe de x modulo m_i.

3) Elements inversibles, indicatrice d'Euler

Propriété 70 (Eléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$)
Soit $k \in \mathbb{Z}$. L'élément $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k est premier avec n.

Théorème 71 (Structure de corps de $(\mathbb{Z}/n\mathbb{Z})$)
L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est un nombre premier.

Notation
Pour tout nombre premier p, on notera $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

Définition 72 (Indicatrice d'Euler)
Pour tout $n \in \mathbb{N}^*$, on note $\varphi(n) = Card\{k \in [\![1, n]\!],\ pgcd(k, n) = 1\}$.
La fonction $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ est appelée **indicatrice d'Euler**.

Propriété 73 (Propriétés de l'indicatrice d'Euler)
L'indicatrice d'Euler $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ possède les propriétés suivantes :

(i) $\varphi(1) = 1$.

(ii) Pour tout nombre premier p et pour tout $\alpha \in \mathbb{N}^*$, on a $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

(iii) Pour tous entiers $m, n \geq 1$ premiers entre eux, on a $\varphi(mn) = \varphi(m)\varphi(n)$.

Corollaire 74 (Expression de $\varphi(n)$ à partir de la décomposition en facteurs premiers)
Soit $n \geq 2$. Si la décomposition en facteurs premiers de n est

$$n = p_1^{\alpha_1} \cdots p_N^{\alpha_N},$$

avec $p_1, \cdots, p_N$ des nombres premiers deux à deux distincts et $\alpha_1, \cdots, \alpha_N \in \mathbb{N}^*$, alors

$$\varphi(n) = n \prod_{i=1}^{N} \left(1 - \frac{1}{p_i}\right).$$

Théorème 75 (Théorème d'Euler)
Soit $n \in \mathbb{N}^*$ et soit $a \in \mathbb{Z}$ un entier premier avec n. Alors $a^{\varphi(n)} \equiv 1\ [n]$.

V Anneau $\mathbb{K}[X]$ et arithmétique des polynômes

$\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$.

1) Premières propriétés

Propriété 76 (Intégrité de $\mathbb{K}[\![X]\!]$)
L'anneau $(\mathbb{K}[X], +, \times)$ est intègre.

Propriété 77 (Polynômes inversibles)
Les éléments inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls.

2) Idéaux, PGCD, PPCM

Théorème 78 (Idéaux de $\mathbb{K}[\![X]\!]$)
Les idéaux de $\mathbb{K}[X]$ sont exactement les $A\mathbb{K}[X]$, avec $A \in \mathbb{K}[X]$.

Propriété 79 (Définition du PGCD de polynômes par les idéaux)
Soit $(A_1, \cdots, A_n) \in \mathbb{K}[X]^n$. Alors, il existe un unique polynôme **unitaire ou nul** *D tel que :*

$$A_1\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X] = D\mathbb{K}[X].$$

Le polynôme D est alors le **plus grand diviseur commun** *de $A_1, \cdots, A_n$, c'est-à-dire que :*
(i) $\forall i \in [\![1, n]\!],\ D|A_i$;
(ii) $\forall P \in \mathbb{K}[X],\ ((\forall i \in [\![1, n]\!],\ P|A_i) \implies P|D)$.
On notera $D = pgcd(A_1, \cdots, A_n)$ ou $D = A_1 \wedge \cdots \wedge A_n$.

Propriété 80 (Relation de Bézout pour les polynômes)
Soit $(A_1, \cdots, A_n) \in \mathbb{K}[X]^n$ et $D = pgcd(A_1, \cdots, A_n)$.
Alors, il existe $(U_1, \cdots, U_n) \in \mathbb{K}[X]^n$ tel que $A_1U_1 + \cdots + A_nU_n = D$.

Définition 81 (Polynômes premiers entre eux)
Soit $(A_1, \cdots, A_n) \in \mathbb{K}[X]^n$ avec $n \geq 2$.
On dit que $A_1, \cdots, A_n$ sont **premiers entre eux dans leur ensemble** *lorsque $pgcd(A_1, \cdots, A_n) = 1$.*
On dit que $A_1, \cdots, A_n$ sont **premiers entre eux deux à deux** *lorsque pour tout $(i, j) \in [\![1, n]\!]$, $i \neq j \implies pgcd(A_i, A_j) = 1$.*

Propriété 82 (Théorème de Bézout)
Soit $(A_1, \cdots, A_n) \in \mathbb{K}[X]^n$. Alors :
$A_1, \cdots, A_n$ sont premiers entre eux dans leur ensemble ssi
$\exists (U_1, \cdots, U_n) \in \mathbb{K}[X]^n,\ A_1U_1 + \cdots + A_nU_n = 1$.

Corollaire 83 (Lemme de Gauss)
Soit $(A, B, C) \in \mathbb{K}[X]^3$. Si $A|BC$ et si A et B sont premiers entre eux, alors $A|C$.

Propriété 84 (Définition du PPCM de polynômes par les idéaux)
Soit $(A_1, \cdots, A_n) \in \mathbb{K}[X]^n$. Alors il existe un unique polynômes **unitaire ou nul** *M tel que*

$$A_1\mathbb{K}[X] \cap \cdots \cap A_n\mathbb{K}[X] = M\mathbb{K}[X].$$

Le polynôme M est alors le **plus petit multiple commun** *de $A_1, \cdots, A_n$, c'est-à-dire que :*
(i) $\forall i \in [\![1, n]\!],\ A_i|M$;
(ii) $\forall P \in \mathbb{K}[X], ((\forall i \in [\![1, n]\!],\ A_i|P) \implies M|P)$.
On notera $M = ppcm(A_1, \cdots, A_n)$ ou $M = A_1 \vee \cdots \vee A_n$.

3) Polynômes irréductibles

Définition 85 (Polynôme irréductible)
Un polynôme $P \in \mathbb{K}[X]$ est dit irréductible lorsque :

(i) P est non constant

(ii) $\forall (P_1, P_2) \in \mathbb{K}[X]^2,\ P = P_1 P_2 \implies P_1$ ou P_2 constant.

Vocabulaire
Un polynôme non constant et non irréductible sera qualifié de "réductible".

Propriété 86 (Exemple fondamental : les polynômes de degré 1)
Tout polynôme de degré 1 est irréductible dans $\mathbb{K}[X]$.

Propriété 87 (Lien entre irréductibilité et racines)
Si P est irréductible dans $\mathbb{K}[X]$ et si $\deg(P) \geq 2$, alors P ne possède pas de racines dans $\mathbb{K}$.

Théorème 88 (Polynômes irréductibles dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$)

(*i*) *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*

(*ii*) *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif.*

Lemme 89
Soit $P \in \mathbb{K}[X]$ irréductible. Alors P est premier avec tout polynôme qu'il ne divise pas.

Propriété 90 (Lemme d'Euclide)
Soit P, P_1, P_2 dans $\mathbb{K}[X]$. Si P est irréductible et si P divise $P_1 P_2$, alors P divise P_1 ou P divise P_2.

Enfin, on dispose comme dans $\mathbb{Z}$ d'un théorème de décomposition en facteurs irréductibles :

Théorème 91 (Décomposition en facteurs irréductibles dans $\mathbb{K}[X]$)
Tout polynôme P non constant peut s'écrire à une constante non nulle près comme produit de polynômes **unitaires et irréductibles** *dans $\mathbb{K}[X]$ (pas nécessairement distincts).*
De plus, cette décomposition est unique à l'ordre des facteurs près.

CH04 : Compléments d'algèbre linéaire

En MP2I, les notions d'algèbre linéaire ont été étudiées dans le cadre des $\mathbb{K}$-espaces vectoriels avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$. En fait, elles restent vraies si $\mathbb{K}$ est un sous-corps quelconque de $\mathbb{C}$, comme $\mathbb{Q}$ (ou $\mathbb{Q}[\sqrt{2}]$, etc.), et la plupart des notions subsistent si $\mathbb{K}$ est un corps quelconque (comme $\mathbb{Z}/p\mathbb{Z}$ avec p premier par exemple).

Dans tout ce chapitre, $\mathbb{K}$ désignera un sous-corps de $\mathbb{C}$, conformément au programme.

I Somme de sous-espaces vectoriels

On fixe un entier $p \geq 2$, et $(E, +, .)$ un $\mathbb{K}$-espace vectoriel.

1) Somme

Définition 1 (Somme de sous-espaces vectoriels)
Si $F_1, \cdots, F_p$ sont des sous-espaces vectoriels de E, alors on appelle **somme de $\boldsymbol{F_1, \cdots, F_p}$** *l'ensemble*

$$\sum_{i=1}^{p} F_i = \{x \in E,\ \exists (x_1, \cdots, x_p) \in F_1 \times \cdots \times F_p,\ x = x_1 + \cdots + x_p\}.$$

C'est l'ensemble des éléments de E pouvant s'écrire comme somme d'éléments des F_i.

Propriété 2 (Propriétés de la somme)
Soit $F_1, \cdots, F_p$ des sous-espaces vectoriels de E. Alors :

(i) $\sum_{i=1}^{p} F_i$ *est un sous-espace vectoriel de E, et* $\sum_{i=1}^{p} F_i = Vect\left(\bigcup_{i=1}^{p} F_i\right)$.
C'est donc le plus petit sev de E contenant tous les F_i.

(ii) Si les F_i sont de dimensions finies, alors $\dim\left(\sum_{i=1}^{p} F_i\right) \leq \sum_{i=1}^{p} \dim(F_i)$.

2) Somme directe et supplémentarité

Définition 3 (Somme directe de sous-espaces vectoriels)
Soit $F_1, \cdots, F_p$ des sous-espaces vectoriels de E. On dit que $F_1, \cdots, F_p$ sont en **somme directe** *lorsque tout vecteur $x \in \sum_{i=1}^{p} F_i$ possède une unique décomposition $x = \sum_{i=1}^{p} x_i$ avec $x_i \in F_i$ pour tout i.*
On note alors $\sum_{i=1}^{p} F_i = \bigoplus_{i=1}^{p} F_i$.

Définition 4 (Sous-espaces vectoriels supplémentaires dans E)
Soit $F_1, \cdots, F_p$ des sous-espaces vectoriels de E. On dit que $F_1, \cdots, F_p$ sont **supplémentaires dans $\boldsymbol{E}$** *lorsqu'ils sont en somme directe et $\sum_{i=1}^{p} F_i = E$, c'est-à-dire $E = \bigoplus_{i=1}^{p} F_i$.*

Théorème 5 (Caractérisations d'une somme directe)
Soit $F_1, \cdots, F_p$ des sous-espaces vectoriels de E. Il y a équivalence entre :

(*i*) *La somme* $\sum_{i=1}^{p} F_i$ *est directe.*

(*ii*) *Pour tous vecteurs* $x_1 \in F_1, \cdots, x_p \in F_p$ *:*

$$(x_1 + \cdots + x_p = 0_E) \implies (x_1 = \cdots = x_p = 0_E).$$

(*iii*) *Pour tout* $j \in [\![1, p-1]\!]$ *:*

$$\left(\sum_{i=1}^{j} F_i\right) \cap F_{j+1} = \{0_E\}.$$

Théorème 6 (Cararactérisation d'une somme directe avec les dimensions)
Soit $F_1, \cdots, F_p$ des sous-espaces vectoriels de dimension finie de E, et $\mathcal{B}_i$ une base de F_i pour tout i. Il y a équivalence entre :

(*i*) *La somme* $\sum_{i=1}^{p} F_i$ *est directe.*

(*ii*) *La famille concaténée* $\mathcal{B} = (\mathcal{B}_1, \cdots, \mathcal{B}_p)$ *est libre.*

(*iii*) *La famille concaténée* $\mathcal{B} = (\mathcal{B}_1, \cdots, \mathcal{B}_p)$ *est une base de* $\sum_{i=1}^{p} F_i$.

(*iv*) $\dim\left(\sum_{i=1}^{p} F_i\right) = \sum_{i=1}^{p} \dim(F_i)$.

Vocabulaire
On dira dans ces conditions que $\mathcal{B} = (\mathcal{B}_1, \cdots, \mathcal{B}_p)$ est une **base adaptée à la somme directe** $\boldsymbol{\bigoplus_{i=1}^{p} F_i}$.

Corollaire 7 (Caractérisation de la supplémentarité en dimension finie)
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, soit $F_1, \cdots, F_p$ des sous-espaces vectoriels de E. et $\mathcal{B}_i$ une base de F_i pour tout i. Il y a équivalence entre :

(*i*) *$F_1, \cdots, F_p$ sont supplémentaires dans E.*

(*ii*) *La famille concaténée* $\mathcal{B} = (\mathcal{B}_1, \cdots, \mathcal{B}_p)$ *est une base de E.*

(*iii*) *La somme* $\sum_{i=1}^{p} F_i$ *est directe et* $\sum_{i=1}^{p} \dim(F_i) = \dim(E)$.

3) Applications linéaires et sommes directes

Définition 8 (Projecteurs associés à une décomposition de E en somme directe)
Soient $E_1, \cdots, E_r$ des sous-espaces vectoriels de E tels que $E = \bigoplus_{i=1}^{r} E_i$.
Pour tout i, on note p_i le projecteur sur E_i parallèment à $\bigoplus_{j \neq i} E_j$. *La famille $(p_1, \cdots, p_r)$ est alors appelée* **famille de projecteurs associés à la somme directe** $\boldsymbol{E = \bigoplus_{i=1}^{r} E_i}$.

Notation
Si $u : E \to F$ est une application linéaire et si E' est un sous-espace vectoriel de E, alors $u_{|E'} : E' \to F$ désigne la restriction de u à E'. On a $u_{|E'} \in \mathcal{L}(E', F)$.

Théorème 9 (Détermination d'une application linéaire sur une somme directe)
Soit E, F deux $\mathbb{K}$-espaces vectoriels et $E_1, \cdots, E_r$ des sous-espaces vectoriels de E tels que $E = \bigoplus_{i=1}^{r} E_i$. Soient des applications linéaires $u_1 \in \mathcal{L}(E_1, F), \cdots, u_r \in \mathcal{L}(E_r, F)$.
Alors il existe une unique application linéaire $u \in \mathcal{L}(E, F)$ telle que $u_{|E_i} = u_i$ pour tout $i \in [\![1, r]\!]$.

II Opérations matricielles par blocs

On considère ici des **matrices définies "par blocs"**, c'est-à-dire de la forme

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

avec $A \in \mathcal{M}_{n_1,n_2}(\mathbb{K})$, $B \in \mathcal{M}_{n_1,n_4}(\mathbb{K})$, $C \in \mathcal{M}_{n_3,n_2}(\mathbb{K})$ et $D \in \mathcal{M}_{n_3,n_4}(\mathbb{K})$, où $(n_1, n_2, n_3, n_4) \in (\mathbb{N}^*)^4$. Une telle matrice M est donc un élément de $\mathcal{M}_{n_1+n_3,n_2+n_4}(\mathbb{K})$.

Théorème 10 (Produit de matrices définies par blocs)
Soient $A, B, C, D, A', B', C', D'$ des matrices à coefficients dans $\mathbb{K}$ telles que :

- *le nombre de colonnes de A et C est égal au nombre de lignes de A' et B' ;*
- *le nombre de colonnes de B et D est égal au nombre de lignes de C' et D'.*

Alors, on a

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} = \begin{pmatrix} AA'+BC' & AB'+BD' \\ CA'+DC' & CB'+DD' \end{pmatrix}.$$

Définition 11 (Matrice triangulaire/diagonale par blocs)
Une matrice **triangulaire supérieure par blocs** *est une matrice de la forme :*

$$\begin{pmatrix} A_1 & * & \cdots & * \\ 0 & A_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & A_r \end{pmatrix},$$

où les A_i sont des matrices carrées (pas nécessairement de même taille).
On définit de même une matrice **triangulaire inférieure par blocs**.
Une matrice **diagonale par blocs** *est une matrice de la forme :*

$$\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & A_r \end{pmatrix},$$

où les A_i sont des matrices carrées (pas nécessairement de même taille).

Théorème 12 (Déterminant d'une matrice triangulaire par blocs)
Si A et D sont deux matrices carrées (pas nécessairement de même taille), alors :

$$\det\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = \det(A)\det(D).$$

Plus généralement : le déterminant d'une matrice triangulaire par blocs (et a fortiori diagonale par blocs) est le produit des déterminants des blocs diagonaux.

Définition 13 (Transvection par blocs)
On appelle **transvection par blocs** *une opération transformant une matrice $(A \;\; B)$ en une matrice $(A \;\; B+\lambda A)$, ou transformant une matrice $\begin{pmatrix} A \\ B \end{pmatrix}$ en une matrice $\begin{pmatrix} A \\ B+\lambda A \end{pmatrix}$*
(A et B désignent deux matrices de même format et $\lambda \in \mathbb{K}$).

Propriété 14 (Invariance du déterminant par transvection par blocs)
Le déterminant d'une matrice carrée est invariant par transvection par blocs.

III $\mathbb{K}$-algèbres

Définition 15 ($\mathbb{K}$-algèbre)
Une **$\mathbb{K}$-algèbre** *est un ensemble A muni de deux lois internes $+ : A \times A \to A$, $\times : A \times A \to A$ et d'une loi externe $. : \mathbb{K} \times A \to A$ qui vérifient :*

(i) $(A, +, \times)$ *est un anneau ;*

(ii) $(A, +, .)$ *est un $\mathbb{K}$-espace vectoriel ;*

(iii) $\forall \lambda \in \mathbb{K}$, $\forall (x, y) \in A^2$, $(\lambda.x)y = \lambda.(xy) = x(\lambda.y)$.

On dit que la $\mathbb{K}$-algèbre A est **commutative** *si l'anneau $(A, +, \times)$ est commutatif, c'est-à-dire si la loi $\times$ est commutative.*

Définition 16 (Sous-algèbre)
Soit $(A, +, \times, .)$ une $\mathbb{K}$-algèbre. Une **sous-algèbre de** *A est une partie $B \subset A$ telle que :*

(i) $(B, +, \times)$ *est un sous-anneau de $(A, +, \times)$;*

(ii) $(B, +, .)$ *est un sous-espace vectoriel de $(A, +, .)$.*

Propriété 17 (Caractérisation d'une sous-algèbre)
Soit $(A, +, \times, .)$ une $\mathbb{K}$-algèbre et soit $B \subset A$. Alors, B est une sous-algèbre de A si et seulement si :

(a) $1_A \in B$;

(b) $\forall (x, y) \in B^2$, $xy \in B$;

(c) $\forall (\lambda, x, y) \in \mathbb{K} \times B \times B$, $\lambda x + y \in B$.

Définition 18 (Morphisme d'algèbres)
Soit $(A, +, \times, .)$ et $(B, +, \times, .)$ deux $\mathbb{K}$-algèbres. Un **morphisme d'algèbres** *de A dans B est une application $\varphi : A \to B$ qui est à la fois un morphisme d'anneaux et une application linéaire.*

Propriété 19 (Caractérisation d'un morphisme d'algèbres)
Soit $(A, +, \times, .)$ et $(B, +, \times, .)$ deux $\mathbb{K}$-algèbres. Alors, $\varphi : A \to B$ est un morphisme d'algèbres si et seulement si :

(a) $\varphi(1_A) = 1_B$;

(b) $\forall (x, y) \in A^2$, $\varphi(xy) = \varphi(x)\varphi(y)$;

(c) $\forall (\lambda, x, y) \in \mathbb{K} \times A \times A$, $\varphi(\lambda x + y) = \lambda\varphi(x) + \varphi(y)$.

CH05 : Espaces vectoriels normés - Généralités

Dans ce chapitre, E désigne un $\mathbb{K}$-espace vectoriel, avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$.

I Normes et espaces vectoriels normés

1) Normes

Définition 1 (Norme)
Une **norme** *sur E est une application $N : E \to \mathbb{R}^+$ vérifiant les propriétés suivantes :*

(i) $\forall x \in E,\ N(x) = 0 \implies x = 0_E$ *(séparation) ;*

(ii) $\forall (\lambda, x) \in \mathbb{K} \times E,\ N(\lambda x) = |\lambda| N(x)$ *(homogénéité) ;*

(iii) $\forall (x, y) \in E^2,\ N(x + y) \leq N(x) + N(y)$ *(inégalité triangulaire).*

Notation
En général, une norme se notera $\| \ . \ \|$ plutôt que N.

Propriété 2 (Inégalité triangulaire renversée)
Si $\| \ . \ \|$ est une norme sur E, alors :

$$\forall (x, y) \in E^2, \qquad |\, \|x\| - \|y\| \,| \leq \|x - y\|.$$

Définition 3 (Espace vectoriel normé)
Un **espace vectoriel normé** *est un $\mathbb{K}$-espace vectoriel E muni d'une norme $\| \ . \ \|$.*

Notation
Souvent, un espace vectoriel normé se note par un couple $(E, \| \ . \|)$, où $\| \ . \|$ est la norme choisie sur l'espace vectoriel E.

Dans la suite, on fixe un espace vectoriel normé $(E, \| \ . \|)$.

Définition 4 (Vecteur unitaire)
Un vecteur $x \in E$ est dit **unitaire** *lorsque $\|x\| = 1$.*

2) Distances, boules

Définition 5 (Distance associée à une norme)
On appelle **distance associée à la norme** $\| \ . \ \|$ *l'application $d : E \times E \to \mathbb{R}^+$ définie par*

$$\forall (x, y) \in E^2, \qquad d(x, y) = \|y - x\|.$$

Propriété 6 (Propriétés de la distance)
L'application distance $d : E \times E \to \mathbb{R}^+$ possède les propriétés suivantes :

(i) $\forall (x, y) \in E^2,\ d(x, y) = 0 \iff x = y$ *(séparation) ;*

(ii) $\forall (x, y) \in E^2,\ d(y, x) = d(x, y)$ *(symétrie) ;*

(iii) $\forall (x, y, z) \in E^3,\ d(x, y) \leq d(x, z) + d(z, y)$ *(inégalité triangulaire).*

Définition 7 (Distance d'un point à une partie)
Etant donné un point $x \in E$ et une partie non vide $A \subset E$, on appelle **distance de x à A** *le réel positif :*

$$d(x, A) = \inf_{a \in A} d(x, a) = \inf_{a \in A} \|x - a\|.$$

Définition 8 (Boule fermée, boule ouverte, sphère)
Soit $a \in E$ et soit un réel $r > 0$.
On appelle **boule ouverte de centre a et de rayon r** *l'ensemble*

$$B(a,r) = \{x \in E,\ d(a,x) < r\}.$$

On appelle **boule fermée de centre a et de rayon r** *l'ensemble*

$$B_f(a,r) = \{x \in E,\ d(a,x) \leq r\}.$$

On appelle **sphère de centre a et de rayon r** *l'ensemble*

$$S(a,r) = \{x \in E,\ d(a,x) = r\}.$$

Définition 9 (Partie bornée)
Une partie $A \subset E$ est dite **bornée** *s'il existe $a \in E$ et $r \in]0;+\infty[$ tel que $A \subset B_f(a,r)$.*

Lemme 10 (Caractérisation des parties bornées)
Une partie $A \subset E$ est bornée si et seulement si $\exists M > 0,\ \forall x \in A,\ \|x\| \leq M$.

3) Segments et convexité des boules

E désigne ici un $\mathbb{R}$-espace vectoriel normé.

Définition 11 (Segment)
Etant donnés deux points a et b de E, on appelle **segment $[a,b]$** *l'ensemble :*

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

Définition 12 (Partie convexe)
Une partie $A \subset E$ est dite **convexe** *si pour tout $(a,b) \in A^2$, $[a,b] \subset A$.*

Propriété 13 (Convexité des boules dans un evn)
Soit E un $\mathbb{R}$-espace vectoriel normé. Toute boule (ouverte ou fermée) est convexe.

4) Suites et fonctions bornées

Définition 14 (Suite vectorielle)
Une **suite de vecteurs de E** *est une application $u : \mathbb{N} \to E$.*

Notation
Une suite de vecteurs de E sera notée en général u ou $(u_n)_{n\in\mathbb{N}}$.
On notera $E^{\mathbb{N}}$ l'ensemble des suites de E indexées par $\mathbb{N}$.

Définition 15 (Suite vectorielle bornée)
Une suite vectorielle $u \in E^{\mathbb{N}}$ est dite **bornée** *si la partie $\{u_n,\ n \in \mathbb{N}\}$ est bornée, ce qui équivaut à $\exists M > 0,\ \forall n \in \mathbb{N},\ \|u_n\| \leq M$.*

Définition 16 (Fonction bornée)
Soit X un ensemble. Une fonction $f : X \to E$ est dite **bornée** *si son image $f(X)$ est une partie bornée de E, ce qui équivaut à $\exists M > 0,\ \forall x \in X,\ \|f(x)\| \leq M$.*

Propriété 17 (Structure d'espace vectoriel des fonctions bornées)
Pour tout ensemble X, l'ensemble $\mathcal{B}(X,E)$ des fonctions bornées de X dans E est un $\mathbb{K}$-espace vectoriel.

Corollaire 18 (Structure d'espace vectoriel des suites bornées)
L'ensemble $\ell^\infty(E)$ des suites bornées à valeurs dans E est un $\mathbb{K}$-espace vectoriel.

II Exemples importants de normes

1) Normes issues d'un produit scalaire

Théorème 19 (Norme associée à un produit scalaire)
Si $(E, (\ .|.\ ))$ est un espace préhilbertien réel, alors l'application $N : x \mapsto \sqrt{(x|x)}$ est une norme sur E.

2) Normes usuelles sur $\mathbb{K}^n$

Propriété 20 (Normes classiques sur $\mathbb{K}^n$)
Pour tout entier $n \geq 1$, les applications suivantes :

$$\|\ .\ \|_1 : (x_1, \cdots, x_n) \mapsto \sum_{i=1}^{n} |x_i|,$$

$$\|\ .\ \|_2 : (x_1, \cdots, x_n) \mapsto \sqrt{\sum_{i=1}^{n} |x_i|^2},$$

$$\|\ .\ \|_\infty : (x_1, \cdots, x_n) \mapsto \max_{1 \leq i \leq n} |x_i|$$

sont des normes sur $\mathbb{K}^n$ ($|\ .\ |$ désigne la valeur absolue ou le module, selon que $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$).

3) Normes sur des espaces de fonctions

Propriété 21 (Norme uniforme sur l'espace des fonctions bornées)
Soit X un ensemble non vide. Pour $f : X \to E$ bornée, on pose

$$\|f\|_\infty = \sup_{x \in X} \|f(x)\|.$$

L'application $\|\ .\ \|_\infty : f \mapsto \|f\|_\infty$ est alors une norme sur l'espace vectoriel $\mathcal{B}(X, E)$.

Corollaire 22 (Norme uniforme sur l'espace des suites bornées)
Pour toute suite bornée $u \in E^{\mathbb{N}}$, on pose

$$\|u\|_\infty = \sup_{n \in \mathbb{N}} \|u_n\|.$$

L'application $u \mapsto \|u\|_\infty$ est une norme sur l'espace vectoriel $\ell^\infty(E)$.

Propriété 23 (Normes 1 et 2 sur l'espace des fonctions continues)
Soit $[a, b]$ un segment de $\mathbb{R}$ avec $a < b$. Pour tout $f \in \mathcal{C}^0([a, b], \mathbb{K})$, on pose :

$$\|f\|_1 = \int_a^b |f(x)|dx, \qquad \|f\|_2 = \sqrt{\int_a^b |f(x)|^2 dx}.$$

Alors, les applications $\|\ .\ \|_1$ et $\|\ .\ \|_2$ sont des normes sur $\mathcal{C}^0([a, b], \mathbb{K})$.

4) Structure d'evn produit

Propriété 24 (Produit fini d'espaces vectoriels normés)
Soit $(E_1, N_1), \cdots, (E_n, N_n)$ des espaces vectoriels normés sur $\mathbb{K}$. Alors, l'application

$$N : E_1 \times \cdots \times E_n \to \mathbb{R}^+, \qquad x = (x_1, \cdots, x_n) \mapsto N(x) = \max(N_1(x_1), \cdots, N_n(x_n))$$

est une norme sur l'espace vectoriel produit $E_1 \times \cdots \times E_n$.

III Convergence des suites de vecteurs

On fixe un espace vectoriel normé $(E, \|\ .\ \|)$ sur le corps $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.
Lorsque $E = \mathbb{K}$, cet espace sera muni de la valeur absolue / du module.
On rappelle que $E^{\mathbb{N}}$ désigne l'espace vectoriel des suites $(u_n)_{n\in\mathbb{N}}$ à valeurs dans E.

1) Définition et premières propriétés

Définition 25 (Suite convergente)
On dit qu'une suite $(u_n) \in E^{\mathbb{N}}$ est **convergente** *(ou* **converge***) s'il existe un vecteur $\ell \in E$ tel que*

$$\forall \varepsilon \in \mathbb{R}_+^*,\ \exists n_0 \in \mathbb{N}, \qquad n \geq n_0 \implies \|u_n - \ell\| \leq \varepsilon.$$

Dans ce cas, on dit que (u_n) **converge vers ℓ** *(ou* **tend vers ℓ***), et on note $u_n \underset{n\to+\infty}{\longrightarrow} \ell$, ou encore $u_n \to \ell$.*
Dans le cas contraire, on dit que (u_n) est **divergente** *(ou* **diverge***).*

Propriété 26 (Unicité de la limite)
Si $u_n \underset{n\to+\infty}{\longrightarrow} \ell$ et $u_n \underset{n\to+\infty}{\longrightarrow} \ell'$, alors $\ell = \ell'$.
On dit alors que ℓ est **la limite** *de (u_n), et on note $\ell = \lim\limits_{n\to+\infty} u_n$.*

Propriété 27 (Majoration par une suite de limite nulle)
Soit $(u_n) \in E^{\mathbb{N}}$, soit $\ell \in E$ et soit (α_n) une suite réelle positive.
Si $\|u_n - \ell\| \leq \alpha_n$ à partir d'un certain rang n_0 et si $\alpha_n \underset{n\to+\infty}{\longrightarrow} 0$, alors $u_n \underset{n\to+\infty}{\longrightarrow} \ell$.

Propriété 28 (Toute suite convergente est bornée)
Soit $(u_n) \in E^{\mathbb{N}}$. Si (u_n) converge, alors (u_n) est bornée.

2) Opérations sur les limites

Propriété 29 (Opérations algébriques sur les suites convergentes)
Soit (u_n) et (v_n) deux suites de $E^{\mathbb{N}}$. On suppose que $u_n \underset{n\to+\infty}{\longrightarrow} \ell \in E$ et $v_n \underset{n\to+\infty}{\longrightarrow} \ell' \in E$.

(i) On a $u_n + v_n \underset{n\to+\infty}{\longrightarrow} \ell + \ell'$.

(ii) Pour tout $\lambda \in \mathbb{K}$, on a $\lambda u_n \underset{n\to+\infty}{\longrightarrow} \lambda\ell$.

Propriété 30 (Compatibilité des limites avec la norme / le produit externe)
Soit (λ_n) une suite de $\mathbb{K}^{\mathbb{N}}$ et (u_n) une suite de $E^{\mathbb{N}}$. On suppose que $\lambda_n \underset{n\to+\infty}{\longrightarrow} \lambda \in \mathbb{K}$ et $u_n \underset{n\to+\infty}{\longrightarrow} \ell \in E$. Alors :

(i) $\|u_n\| \underset{n\to+\infty}{\longrightarrow} \|\ell\|$;

(ii) $\lambda_n u_n \underset{n\to+\infty}{\longrightarrow} \lambda\ell$.

Propriété 31 (Limite d'un inverse scalaire)
Soit $(u_n) \in \mathbb{K}^{\mathbb{N}}$.
Si $u_n \underset{n\to+\infty}{\longrightarrow} \ell \in \mathbb{K} \setminus \{0\}$, alors u_n est non nul à partir d'un certain rang et $\frac{1}{u_n} \underset{n\to+\infty}{\longrightarrow} \frac{1}{\ell}$.

3) Convergence dans un espace produit

Propriété 32 (Convergence d'une suite à valeurs dans un espace produit)
Soit $(E_1, N_1), \cdots, (E_n, N_n)$ des espaces vectoriels normés sur $\mathbb{K}$.
On munit l'espace produit $E = E_1 \times \cdots \times E_n$ de la norme $N : E \to \mathbb{R}^+$ définie par :

$$N(x_1, \cdots, x_n) = \max(N_1(x_1), \cdots, N_n(x_n)).$$

Alors, pour toute suite $(u_k)_{k\in\mathbb{N}} = (u_k^{(1)}, \cdots, u_k^{(n)})_{k\in\mathbb{N}} \in E^{\mathbb{N}}$ et tout vecteur $\ell = (\ell_1, \cdots, \ell_n) \in E$, on a :

$$u_k \underset{k\to+\infty}{\longrightarrow} \ell \iff \forall i \in \{1, \cdots, n\},\ u_k^{(i)} \underset{k\to+\infty}{\longrightarrow} \ell_i.$$

4) Algèbres normées

Les $\mathbb{K}$-algèbres sont des cas particuliers de $\mathbb{K}$-espaces vectoriels (en plus de la somme et du produit externe, elles disposent d'un produit "interne"), sur lesquels on s'intéresse à un certain type de normes.

Définition 33 (Norme sous-multiplicative)
Soit A une $\mathbb{K}$-algèbre. Une norme sur A est dite **sous-multiplicative** *lorsque*

$$\forall (x, y) \in A^2, \quad \|xy\| \leq \|x\|\ \|y\|.$$

Propriété 34 (Convergence d'un produit dans une algèbre normée)
Soit A une $\mathbb{K}$-algèbre munie d'une norme sous-multiplicative, soit (u_n) et (v_n) deux suites de $A^{\mathbb{N}}$. On suppose que $u_n \underset{n\to+\infty}{\longrightarrow} \ell \in A$ et $v_n \underset{n\to+\infty}{\longrightarrow} \ell' \in A$. Alors $u_n v_n \underset{n\to+\infty}{\longrightarrow} \ell\ell'$.

5) Suites extraites, valeurs d'adhérence

Définition 35 (Suite extraite)
Si $(u_n) \in E^{\mathbb{N}}$, on appelle **suite extraite de (u_n)** *(ou* **sous-suite de (u_n)***) toute suite de la forme $(u_{\varphi(n)})$, où $\varphi : \mathbb{N} \to \mathbb{N}$ est une application strictement croissante.*

Lemme 36 (Minoration d'une extractrice)
Si $\varphi : \mathbb{N} \to \mathbb{N}$ est strictement croissante, alors $\varphi(n) \geq n$ pour tout $n \in \mathbb{N}$.

Propriété 37 (Suites extraites d'une suite convergente)
Si (u_n) converge vers $\ell \in E$, alors toute suite extraite de (u_n) converge vers ℓ.

Définition 38 (Valeur d'adhérence d'une suite)
Etant donné une suite $(u_n) \in E^{\mathbb{N}}$, on appelle **valeur d'adhérence de (u_n)** *tout vecteur $\ell \in E$ qui est la limite d'une suite extraite de (u_n).*

Propriété 39 (Valeurs d'adhérence et convergence)

(i) Une suite convergente possède une seule valeur d'adhérence : sa limite.

(ii) Une suite qui possède au moins deux valeurs d'adhérence diverge.

(iii) Une suite qui ne possède pas de valeurs d'adhérence diverge.

IV Comparaison des normes

E désigne toujours un $\mathbb{K}$-espace vectoriel, avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Définition 40 (Domination d'une norme par une autre)
*Soient N_1 et N_2 deux normes sur E. On dit que $\boldsymbol{N_2}$ **domine** $\boldsymbol{N_1}$ s'il existe une constante $C > 0$ telle que*

$$\forall x \in E, \qquad N_1(x) \leq C N_2(x).$$

Définition 41 (Normes équivalentes)
Soient N_1 et N_2 deux normes sur E. On dit que N_1 et N_2 sont **équivalentes** *lorsqu'elles se dominent mutuellement, c'est-à-dire lorsqu'il existe deux constantes $C_1, C_2 > 0$ telles que*

$$\forall x \in E, \qquad N_1(x) \leq C_1 N_2(x) \text{ et } N_2(x) \leq C_2 N_1(x).$$

Propriété 42 (Relation d'équivalence de normes)
La relation "être équivalente à" est une relation d'équivalence sur l'ensemble des normes sur E.

Propriété 43 (Invariance du caractère borné par des normes équivalentes)
Soit N_1 et N_2 deux normes équivalentes sur E. Alors :

(i) Une partie $A \subset E$ est bornée pour N_1 si et seulement si elle est bornée pour N_2.

(ii) Une suite $(u_n) \in E^{\mathbb{N}}$ est bornée pour N_1 si et seulement si elle est bornée pour N_2.

(iii) Si X est un ensemble, alors une fonction $f : X \to E$ est bornée pour N_1 si et seulement si elle est bornée pour N_2.

Propriété 44 (Invariance du caractère convergent par des normes équivalentes)
Soit N_1 et N_2 deux normes équivalentes sur E et soit $(u_n) \in E^{\mathbb{N}}$. Alors :
(u_n) converge dans (E, N_1) si et seulement si (u_n) converge dans (E, N_2).
Dans ce cas, les limites sont les mêmes.

Méthode (Pour montrer que deux normes ne sont pas équivalentes)
Pour montrer que deux normes N_1 et N_2 sur E **ne sont pas** *équivalentes, il suffit de trouver une suite $(u_n) \in E^{\mathbb{N}}$ qui soit bornée (ou convergente) pour une norme et pas pour l'autre.*

CH06 : Espaces préhilbertiens et groupe orthogonal

I Projections orthogonales

E désigne un espace préhilbertien réel (pas nécessairement de dimension finie). On note $(\cdot|\cdot)$ son produit scalaire, et $\|.\|$ la norme associée.

1) Supplémentaire orthogonal d'un sev de dimension finie

Théorème 1 (L'orthogonal d'un sev de dim finie est un supplémentaire)
Soit E un espace préhilbertien réel, et F un sous-espace vectoriel de dimension finie.
Alors le sev $F^\perp$ est un supplémentaire de F dans E (i.e. $E = F \oplus F^\perp$).

Vocabulaire
On parle alors de **supplémentaire orthogonal**.

Corollaire 2 (Dimension de l'orthogonal en dimension finie)
Soit E un espace **euclidien**. *Pour tout sous-espace vectoriel F de E, on a*

$$\dim(F^\perp) = \dim(E) - \dim(F).$$

Corollaire 3 (Double orthogonal d'un sev de dim finie)
Soit E un espace préhilbertien réel, et F un sous-espace vectoriel de dimension finie. Alors

$$(F^\perp)^\perp = F.$$

2) Projection orthogonale sur un sev de dimension finie

Dans la suite, on fixe un espace préhilbertien réel E.

Définition 4 (Projection orthogonale)
Soit F un sev de dimension finie de E. On appelle **projection orthogonale sur** *F le projecteur sur F parallèlement à $F^\perp$. On notera $p_F : E \to E$ cette application.*

Propriété 5 (Propriétés d'une projection orthogonale)
Soit F un sev de dimension finie de E , et p_F la projection orthogonale sur F.

(i) On a $p_F \in \mathcal{L}(E,E)$ et $p_F \circ p_F = p_F$.

(ii) On a la décomposition $E = Im(p_F) \oplus Ker(p_F)$, avec

$$Im(p_F) = Ker(p_F - Id_E) = F \quad et \quad Ker(p_F) = F^\perp = Im(p_F)^\perp.$$

(iii) $\forall x \in E$, $p_F(x)$ est l'unique vecteur de E tel que $\begin{cases} p_F(x) \in F \\ x - p_F(x) \in F^\perp \end{cases}$.

Propriété 6 (Expression d'une projection orthogonale en base orthonormée)
Soit F un sev de dimension finie de E, et $(e_1, \cdots, e_r)$ une base **orthonormée** *de F. Alors on a l'expression :*

$$\forall x \in E, \qquad p_F(x) = \sum_{i=1}^{r} (x|e_i)e_i.$$

3) Symétrie orthogonale, réflexion

Définition 7 (Symétrie orthogonale)
Soit F un sev de dimension finie de E. On appelle **symétrie orthogonale par rapport à F** *la symétrie par rapport à F et parallèlement à $F^\perp$. On notera $\sigma_F : E \to E$ cette application.*

Vocabulaire
Dans le cas particulier où E est de dimension finie et F est un hyperplan de E (i.e. $\dim(F) = \dim(E) - 1$), on parle de **réflexion par rapport à F**.

Propriété 8 (Propriétés d'une symétrie orthogonale)
Soit F un sev de dimension finie de E, et σ_F la symétrie orthogonale par rapport à F.

(i) On a $\sigma_F \in \mathcal{L}(E,E)$ et $\sigma_F \circ \sigma_F = Id_E$.

(ii) On a la décomposition $Ker(\sigma_F - Id_E) \oplus Ker(\sigma_F + Id_E) = E$, avec

$$F = Ker(\sigma_F - Id_E) \quad et \quad F^\perp = Ker(\sigma_F + Id_E).$$

(iii) Pour tout $x \in E$, on a $\sigma_F(x) = 2p_F(x) - x$. D'où $\sigma_F = 2p_F - Id_E$.

4) Distance d'un point à un sev de dimension finie

On rappelle que si $(E, \|.\|)$ est un espace vectoriel normé, la distance d'un point $x \in E$ à une partie non vide $A \subset E$ est le réel positif :

$$d(x,A) = \inf_{a \in A} \|x - a\|.$$

On étudie ici le problème de calcul de distance dans notre cadre préhilbertien.

Théorème 9 (Distance atteinte par la projection orthogonale)
Soit E un espace préhilbertien réel et F un sous-espace vectoriel de dimension finie.
Alors, pour tout $x \in E$, la distance **$d(x,F)$ est atteinte en un seul point** *: le projeté orthogonal $p_F(x)$.*
En d'autres termes :

$$\forall x \in E,\ \forall y \in F, \quad \|x - p_F(x)\| \leq \|x - y\|,$$

avec égalité si et seulement si $y = p_F(x)$.

Corollaire 10 (Autre formule de la distance)
Avec les notations précédentes, on a aussi

$$d(x,F)^2 = \|x\|^2 - \|p_F(x)\|^2.$$

5) Inégalité de Bessel

Propriété 11 (Inégalité de Bessel)
Soit $(e_1, \cdots, e_n)$ une famille orthonormée de E. Alors

$$\forall x \in E, \qquad \sum_{k=1}^{n} (x|e_k)^2 \leq \|x\|^2.$$

Corollaire 12 (Inégalité de Bessel pour une suite orthonormée)
Si $(e_k)_{k \in \mathbb{N}}$ est une suite orthonormée de E, alors pour tout $x \in E$, la série $\sum_{k \geq 0} (x|e_k)^2$ converge et

$$\sum_{k=0}^{+\infty} (x|e_k)^2 \leq \|x\|^2.$$

Dans la suite du chapitre, E désigne un espace euclidien (c'est-à-dire un espace préhilbertien réel de dimension finie), non réduit à $\{0_E\}$.

II Isométries vectorielles d'un espace euclidien

1) Définition et premières propriétés

Définition 13 (Isométrie vectorielle)
Une **isométrie vectorielle** *de E est un endomorphisme $u \in \mathcal{L}(E)$ qui conserve la norme, c'est-à-dire $\forall x \in E,\ \|u(x)\| = \|x\|$.*

Propriété 14 (Equivalence avec la conservation du produit scalaire)
Soit $u \in \mathcal{L}(E)$. On a l'équivalence :

$$u \text{ est une isométrie vectorielle} \iff \forall (x;y) \in E^2, \quad (u(x)|u(y)) = (x|y).$$

Vocabulaire
Les isométries vectorielles sont parfois appelées **endomorphismes orthogonaux**, car elles conservent l'orthogonalité :

$$x \perp y \iff (x|y) = 0 \iff (u(x)|u(y)) = 0 \iff u(x) \perp u(y).$$

On parle même **d'automorphismes orthogonaux**, puisque les isométries sont bijectives (voir prop. suivante).

Notation
On notera $\boldsymbol{\mathcal{O}(E)}$ l'ensemble des isométries vectorielles de E.

Propriété 15 (Structure de groupe de $\mathcal{O}(E)$)
L'ensemble $\mathcal{O}(E)$ est un sous-groupe de $(GL(E), \circ)$, donc un groupe.
On appelle $\mathcal{O}(E)$ le **groupe orthogonal** *de E.*

2) Conservation des bases orthonormées

Propriété 16 (Conservation des bases orthonormées)
Soit $u \in \mathcal{L}(E)$. Alors, les assertions suivantes sont **équivalentes** *:*

(i) $u \in \mathcal{O}(E)$;

(ii) Pour toute base **orthonormée** $(e_i)_{1\leq i\leq n}$ *de E, la famille image $(u(e_i))_{1\leq i\leq n}$ est une base orthonormée de E ;*

(iii) Il existe une base **orthonormée** $(e_i)_{1\leq i\leq n}$ *de E telle que la famille image $(u(e_i))_{1\leq i\leq n}$ est une base orthonormée de E.*

III Matrices orthogonales

Dans la suite, n désigne un entier naturel non nul.

1) Définition et propriétés

Propriété 17 (Représentation d'une isométrie vectorielle dans une b.o.n)
Soit $u \in \mathcal{O}(E)$ et $\mathcal{B} = (e_i)_{1\leq i\leq n}$ une base **orthonormée** *de E.*
On note $A = Mat_{\mathcal{B}}(u)$. Alors $A \in GL_n(\mathbb{R})$ et $A^{-1} = A^\top$.

Ceci amène la définition suivante :

Définition 18 (Matrice orthogonale)
Une matrice $A \in \mathcal{M}_n(\mathbb{R})$ est dite **orthogonale** *lorsque $A^\top \times A = I_n$.*

Notation
Pour $n \in \mathbb{N}^*$ fixé, on notera $\boldsymbol{\mathcal{O}_n(\mathbb{R})}$ (ou encore $\boldsymbol{\mathcal{O}(n)}$) l'ensemble des matrices orthogonales de $\mathcal{M}_n(\mathbb{R})$.

Propriété 19 (Structure de groupe de $\mathcal{O}_n(\mathbb{R})$)
L'ensemble $\mathcal{O}_n(\mathbb{R})$ est un sous-groupe de $(GL_n(\mathbb{R}), \times)$, donc un groupe.
On appelle $\mathcal{O}_n(\mathbb{R})$ le **groupe orthogonal matriciel d'ordre n.**

Propriété 20 (Correspondance $\mathcal{O}(E)/\mathcal{O}_n(\mathbb{R})$)
Soit $u \in \mathcal{L}(E)$ et soit $\mathcal{B}$ une base **orthonormée** *de E. Alors on a*

$$u \in \mathcal{O}(E) \iff Mat_{\mathcal{B}}(u) \in \mathcal{O}_n(\mathbb{R}).$$

On donne ici une caractérisation des matrices orthogonales à partir d'une propriété géométrique sur les colonnes.

Propriété 21 (Diverses caractérisations des matrices orthogonales)
Les assertions suivantes sont **équivalentes** *:*

(i) $A \in \mathcal{O}_n(\mathbb{R})$ *;*
(ii) les colonnes de A forment une base orthonormée de $\mathbb{R}^n$ (pour le produit scalaire canonique) ;
(iii) $A^\top \in \mathcal{O}_n(\mathbb{R})$ *;*
(iv) les lignes de A forment une base orthonormée de $\mathbb{R}^n$.

Propriété 22 (Changement de bases orthonormées)
Soit $\mathcal{B} = (e_1, \cdots, e_n)$ une base orthonormée de E et soit $\mathcal{B}' = (e'_1, \cdots, e'_n)$ une famille de vecteurs de E. Alors :

$$\mathcal{B}' \text{ est une base orthonormée de } E \iff P = Mat_{\mathcal{B}}(\mathcal{B}') \in \mathcal{O}_n(\mathbb{R}).$$

Dans ce cas, on a de plus $Mat_{\mathcal{B}'}(\mathcal{B}) = P^\top$.

Corollaire 23 (Changement de bases orthonormées pour les endomorphismes)
Soit $u \in \mathcal{L}(E)$ et $\mathcal{B}$ et $\mathcal{B}'$ deux bases orthonormées de E.
Alors, en notant $A = Mat_{\mathcal{B}}(u)$, $A' = Mat_{\mathcal{B}'}(u)$ et $P = Mat_{\mathcal{B}}(\mathcal{B}')$, on a $A' = P^\top AP$.

Vocabulaire
On dira que deux matrices $A, A' \in \mathcal{M}_n(\mathbb{R})$ sont **orthogonalement semblables** lorsqu'il existe $P \in \mathcal{O}_n(\mathbb{R})$ tel que $A' = P^{-1}AP = P^\top AP$, ce qui implique évidemment qu'elles sont semblables.

2) Caractérisation des symétries orthogonales

Propriété 24 (Les symétries orthogonales sont des isométries)
Soit F un sous-espace vectoriel de E. Alors, la symétrie orthogonale par rapport à F, notée σ_F, appartient à $\mathcal{O}(E)$.

Propriété 25 (Caractérisation des symétries orthogonales)
Soit E un espace euclidien, soit $u \in \mathcal{L}(E)$, et soit $\mathcal{B}$ une base **orthonormée** *de E.*
On note $A = Mat_{\mathcal{B}}(u)$. Alors :

$$u \text{ est une symétrie orthogonale} \iff A \text{ est orthogonale et symétrique.}$$

IV Signe d'une isométrie vectorielle

E désigne toujours un espace euclidien non nul et n un entier naturel non nul.

1) Isométries positives / négatives

Propriété 26 (Déterminant d'une isométrie vectorielle / d'une matrice orthogonale)
(i) Si $A \in \mathcal{O}_n(\mathbb{R})$, alors $\det(A) = \pm 1$.
(ii) Si $u \in \mathcal{O}(E)$, alors $\det(u) = \pm 1$.

Définition 27 (Isométries vectorielles positives/négatives)
Soit $u \in \mathcal{O}(E)$. On dit que
(i) u est une **isométrie positive** *(ou "directe") si* $\det(u) = 1$,
(ii) u est une **isométrie négative** *(ou "indirecte") si* $\det(u) = -1$.

Notation
On notera $\mathcal{SO}(E)$ (ou $\mathcal{O}^+(E)$) l'ensemble des isométries vectorielles positives de E, et $\mathcal{O}^-(E)$ l'ensemble des isométries vectorielles négatives de E.
Formellement :

$$\mathcal{SO}(E) = \{u \in \mathcal{O}(E),\ \det(u) = 1\}.$$

Propriété 28 (Structure de groupe de $\mathcal{SO}(E)$)
L'ensemble $\mathcal{SO}(E)$ est un sous-groupe de $(\mathcal{O}(E), \circ)$, donc un groupe.
On l'appelle **groupe spécial orthogonal** *de E.*

Définition 29 (Groupe spécial orthogonal matriciel)
On définit

$$\mathcal{SO}_n(\mathbb{R}) = \{A \in \mathcal{O}_n(\mathbb{R}),\ \det(A) = 1\} = \{A \in \mathcal{M}_n(\mathbb{R}),\ A^\top \times A = I_n,\ \det(A) = 1\}.$$

(on le note aussi $\mathcal{O}_n^+(\mathbb{R})$ ou $\mathcal{SO}(n)$). On définit également

$$\mathcal{O}_n^-(\mathbb{R}) = \{A \in \mathcal{O}_n(\mathbb{R}),\ \det(A) = -1\} = \{A \in \mathcal{M}_n(\mathbb{R}),\ A^\top \times A = I_n,\ \det(A) = -1\}.$$

Propriété 30 (Structure de groupe de $\mathcal{SO}_n(\mathbb{R})$)
L'ensemble $\mathcal{SO}_n(\mathbb{R})$ est un sous-groupe de $(\mathcal{O}_n(\mathbb{R}), \times)$, donc un groupe.

Propriété 31 (Correspondance $\mathcal{SO}(E)$ / $\mathcal{SO}_n(\mathbb{R})$)
Soit $\mathcal{B}$ une base **orthonormée** *de E et $u \in \mathcal{L}(E)$. Alors :*

$$u \in \mathcal{SO}(E) \iff Mat_{\mathcal{B}}(u) \in \mathcal{SO}_n(\mathbb{R}).$$

2) Action sur l'orientation des bases

On rappelle que dans un $\mathbb{R}$-espace vectoriel E de dimension $n \in \mathbb{N}^*$, on a, pour toute base $\mathcal{B} = (e_1, \cdots, e_n)$ et toute famille de vecteurs $\mathcal{F} = (x_1, \cdots, x_n)$:

$$\mathcal{F} \text{ est une base de } E \iff \det_{\mathcal{B}}(\mathcal{F}) \neq 0.$$

Définition 32 (Orientation d'un espace vectoriel réel)
Un $\mathbb{R}$-espace vectoriel E est dit **orienté** *lorsqu'on choisit une base $\mathcal{B}_0$ de référence.*
Dans ce cas, on appelle :

- *bases* **directes** *les bases $\mathcal{B}$ telles que* $\det_{\mathcal{B}_0}(\mathcal{B}) > 0$ *;*
- *bases* **indirectes** *les bases $\mathcal{B}$ telles que* $\det_{\mathcal{B}_0}(\mathcal{B}) < 0$.

On dit que deux bases $\mathcal{B}$ et $\mathcal{B}'$ ont **même orientation** *lorsque* $\det_{\mathcal{B}}(\mathcal{B}') > 0$.

Propriété 33 (Isométries positives et orientation)
Soit E un espace euclidien orienté et soit $u \in \mathcal{L}(E)$.

(*i*) *Si $u \in \mathcal{SO}(E)$, alors u préserve les bases orthonormées directes et indirectes de E (c'est-à-dire que pour toute base orthonormée $\mathcal{B}$ de E, $u(\mathcal{B})$ est une base orthonormée de E de même orientation que $\mathcal{B}$)*

(*ii*) *Réciproquement, s'il existe une base orthonormée $\mathcal{B}$ de E telle que $u(\mathcal{B})$ soit une base orthonormée de E de même orientation que $\mathcal{B}$, alors $u \in \mathcal{SO}(E)$.*

Corollaire 34 (Indépendance du déterminant vis-à-vis des b.o.n.d)
Soit E un espace euclidien orienté de dimension n.
Soit $(x_1, \cdots, x_n)$ une famille de vecteurs de E. Alors, le nombre $\det_{\mathcal{B}}(x_1, \cdots, x_n)$ ne dépend pas de la base orthonormée **directe** *de E choisie.*

V Groupe orthogonal en dimension 2

Etudions maintenant ce qui se passe **en dimension** 2, dans un **plan euclidien** E.

1) Description de $\mathcal{O}_2(\mathbb{R})$

La connaissance du groupe orthogonal matriciel $\mathcal{O}_2(\mathbb{R})$ suffit à connaître $\mathcal{O}(E)$.

Propriété 35 (Description de $\mathcal{O}_2(\mathbb{R})$)

(i) Les matrices de $\mathcal{SO}_2(\mathbb{R})$ sont exactement les matrices $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ *avec $\theta \in \mathbb{R}$.*

(ii) Les matrices de $\mathcal{O}_2^-(\mathbb{R})$ sont exactement les matrices $\begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix}$ *avec $\varphi \in \mathbb{R}$.*

Définition 36 (Matrices de rotation)

Pour $\theta \in \mathbb{R}$, on notera $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \in \mathcal{SO}_2(\mathbb{R})$.

On l'appelle **matrice de rotation d'angle** θ *(le réel θ est unique à 2π près).*

Propriété 37 (Le groupe $\mathcal{SO}_2(\mathbb{R})$ est commutatif)

Pour tous $(\theta, \theta') \in \mathbb{R}^2$, on a $R_\theta \times R_{\theta'} = R_{\theta+\theta'} = R_{\theta'} \times R_\theta$.

En particulier, le groupe $(\mathcal{SO}_2(\mathbb{R}), \times)$ est commutatif, et l'application

$$\varphi : \left\{ \begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathcal{SO}_2(\mathbb{R}), \times) \\ \theta & \longmapsto & R_\theta \end{array} \right.$$

est un morphisme de groupes surjectif, de noyau $2\pi\mathbb{Z}$.

2) Description de $\mathcal{SO}(E)$

Propriété 38 (Invariance de la matrice de $u \in \mathcal{SO}(E)$ dans une b.o.n.d)

Soit E un espace euclidien de dimension 2 **orienté**, *et soit $u \in \mathcal{SO}(E)$.*

Alors, il existe un unique réel $\theta \in]-\pi, \pi]$ tel que **pour toute base orthonormée directe** $\mathcal{B}$ *de E, $Mat_{\mathcal{B}}(u) = R_\theta$.*

La proposition précédente donne un sens à la définition suivante :

Définition 39 (Rotation plane d'angle θ)

Soit E un espace euclidien de dimension 2 **orienté**. *Pour $\theta \in \mathbb{R}$, la* **rotation vectorielle d'angle** *θ, notée r_θ, est l'unique endomorphisme de E dont la matrice dans* **toute** *base orthonormée* **directe** *est R_θ.*

Corollaire 40 (Nature des isométries positives en dimension 2)

Si E est un espace euclidien de dimension 2, alors les éléments de $\mathcal{SO}(E)$ sont exactement les rotations vectorielles.

3) Description de $\mathcal{O}^-(E)$

On va maintenant étudier les $u \in \mathcal{O}(E)$ tels que $\det(u) = -1$.

Propriété 41 (Nature des isométries négatives en dimension 2)

Si E est un espace euclidien de dimension 2, alors les éléments de $\mathcal{O}^-(E)$ sont exactement les symétries orthogonales **par rapport à une droite**. *Ce sont donc les réflexions du plan E.*

4) Classification des isométries en dimension 2

Théorème 42 (Classification des isométries en dimension 2)
Soit E un espace euclidien de dimension 2 et soit $u \in \mathcal{O}(E)$.
On dispose de la classification suivante :

$\det(u)$	*Forme réduite dans une b.o.n.d adaptée*	*Nature géométrique de u*
1	$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ *avec* $\theta \neq 0\ [\pi]$	*Rotation vectorielle d'angle* $\theta \neq 0\ [\pi]$
1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	Id_E
1	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$-Id_E$
-1	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	*Réflexion par rapport à la droite* $Ker(u - Id_E)$

On dispose aussi de la classification suivante, suivant la dimension des invariants :

$\dim(Ker(u - Id_E))$	*Nature géométrique de u*	$\det(u)$
0	*Rotation vectorielle différente de* Id_E	1
1	*Réflexion par rapport à la droite* $Ker(u - Id_E)$	-1
2	Id_E	1