0 Logique

1 Négation, conjonction, disjonction.

1.1 Non, Ou, Et : tables de vérité.

Définition 1.

Une **assertion** est une phrase pouvant prendre l'une des deux valeurs : Vrai (V) ou Faux (F).

Il n'y a pas d'autre possibilité que Vrai ou Faux en logique classique : c'est le principe du *tiers exclu*.

- « $1+1=2$ » est une assertion vraie et « $1+1=3$ » est une assertion fausse.
- « Comment allez-vous ? » n'est pas une assertion.
- « Il a plu le jour de la rentrée sur le lycée Paul Valéry. » est une assertion.
  Elle sera évaluée parfois vraie, parfois fausse... cela dépendra des années !

Définition 2.

On appelle **négation** d'une assertion P, et on note (non P), ou encore $\neg P$, l'assertion définie par

P	$\neg P$
V	F
F	V

Définition 3.

Soient deux assertions P et Q. Les assertions (P et Q), (P ou Q) et (P ou bien Q) sont appelées respectivement **conjonction**, **disjonction**, et disjonction exclusive de P et Q, et sont définies par

P	Q	P et Q	P ou Q	P ou bien Q
V	V	V	V	F
V	F	F	V	V
F	V	F	V	V
F	F	F	F	F

Exemple 4.

Évaluer les assertions ci-dessous.

- « Ali est un garçon et Elsa est une fille » :
- « Ali est un garçon ou Elsa est une fille » :
- « Ali est un garçon ou bien Elsa est une fille » :
- « Ali est un garçon et Elsa est en MP2I » :
- « Ali est un garçon ou Elsa est en MP2I » :

1.2 Calculer avec des assertions.

Soient P, Q, R trois assertions. On note p, q, r leurs valeurs de vérité respectives, de sorte que le triplet (p, q, r) appartient à $\{V, F\}^3$ et peut prendre $2^3 = 8$ valeurs différentes.

Considérons maintenant deux assertions $\mathcal{A}(P, Q, R)$ et $\mathcal{B}(P, Q, R)$ bien construites avec les lettres P, Q, R et avec des connecteurs logiques. Les valeurs de vérité de $\mathcal{A}(P, Q, R)$ et $\mathcal{B}(P, Q, R)$ dépendent de (p, q, r).

Notation.

Si dans les huit cas possibles, les assertions $\mathcal{A}(P, Q, R)$ et $\mathcal{B}(P, Q, R)$ ont la même valeur de vérité, on dira alors que les expressions $\mathcal{A}$ et $\mathcal{B}$ sont **synonymes**, ce que l'on notera dans la suite

$$\mathcal{A}(P, Q, R) \equiv \mathcal{B}(P, Q, R).$$

Proposition 5.

a) $(P \text{ et } P) \equiv P, \quad (P \text{ ou } P) \equiv P.$

b) $(P \text{ et } Q) \equiv (Q \text{ et } P), \quad (P \text{ ou } Q) \equiv (Q \text{ ou } P).$

c) $((P \text{ et } Q) \text{ et } R) \equiv (P \text{ et } (Q \text{ et } R)), \quad ((P \text{ ou } Q) \text{ ou } R) \equiv (P \text{ ou } (Q \text{ ou } R)).$

d) $P \text{ et } (Q \text{ ou } R) \equiv (P \text{ et } Q) \text{ ou } (P \text{ et } R) \quad P \text{ ou } (Q \text{ et } R) \equiv (P \text{ ou } Q) \text{ et } (P \text{ ou } R).$

Preuve : Voici la table de vérité qui démontre P et (Q ou R) $\equiv$ (P et Q) ou (P et R)

P	Q	R	Q ou R	P et (Q ou R)	P et Q	P et R	(P et Q) ou (P et R)
V	V	V					
V	V	F					
V	F	V					
V	F	F					
F	V	V					
F	V	F					
F	F	V					
F	F	F					

$\square$

Proposition 6.

a) $\neg(\neg P) \equiv P$. (négation de la négation).

b) $\neg(P$ et $Q) \equiv (\neg P)$ ou $(\neg Q)$, $\neg(P$ ou $Q) \equiv (\neg P)$ et $(\neg Q)$ (formules de Morgan).

Preuve :

P	$\neg P$	$\neg(\neg P)$
V	F	V
F	V	F

P	Q	$\neg P$	$\neg Q$	P et Q	$\neg(P$ et $Q)$	$(\neg P)$ ou $(\neg Q)$
V	V					
V	F					
F	V					
F	F					

$\square$

1.3 Un ou deux quantificateurs.

On appelle **prédicat** $\mathcal{P}(X)$ sur un ensemble E une phrase contenant la lettre X telle que lorsqu'on substitue à X un élément x de E, on obtient une assertion $\mathcal{P}(x)$. Par exemple, la phrase

« X est pair »

est un prédicat sur $\mathbb{Z}$. Il permet d'obtenir (entre autres) les assertions "4 est pair" et "3 est pair".

Définition 7.

Soit un prédicat $\mathcal{P}(X)$ sur un ensemble E.

- L'assertion « pour tout x dans E, $\mathcal{P}(x)$ est vraie » s'écrit

$$\forall x \in E \quad \mathcal{P}(x).$$

- L'assertion « il existe (au moins un) x dans E tel que $\mathcal{P}(x)$ est vraie » s'écrit

$$\exists x \in E \quad \mathcal{P}(x).$$

- L'assertion « il existe un unique x dans E tel que $\mathcal{P}(x)$ est vraie » s'écrit

$$\exists! x \in E \quad \mathcal{P}(x).$$

Un prédicat peut dépendre de plusieurs variables et on peut être amené à utiliser plusieurs quantificateurs.

Proposition 8 (Deux quantificateurs égaux *commutent*)**.**

Soient E, F deux ensembles et $\mathcal{P}(X, Y)$ un prédicat où X prend ses valeurs dans E et Y dans F. On a les synonymies :

$$\begin{array}{lcl} \forall x \in E \quad (\forall y \in F \quad \mathcal{P}(x,y)) & \equiv & \forall y \in F \quad (\forall x \in E \quad \mathcal{P}(x,y)) \\ \exists x \in E \quad (\exists y \in F \quad \mathcal{P}(x,y)) & \equiv & \exists y \in F \quad (\exists x \in E \quad \mathcal{P}(x,y)) \end{array}$$

⚠ En revanche, les assertions suivantes ne sont pas synonymes !

$$(A) \quad \forall x \in E \quad \exists y \in F \quad \mathcal{P}(x,y) \qquad\qquad (B) \quad \exists y \in F \quad \forall x \in E \quad \mathcal{P}(x,y).$$

• Dans la phrase (A) l'existence de y est affirmée après qu'on a parlé d'un élément x : l'élément y peut donc dépendre de x. On peut insister sur cette dépendance en écrivant (A) ainsi : $\forall x \in E \quad \exists y_x \in F \quad \mathcal{P}(x, y_x)$.

• Dans la phrase (B), y est introduit en premier.
Le reste de la phrase $(\forall x \in E\ \mathcal{P}(x,y))$ se comprend pour ce y fixé.

Exemple 9 (Une assertion de type A)**.**

Une théorie affirme que chacun sur Terre a une âme sœur (c'est sans doute vrai, je l'ai lu sur Internet). Formaliser en introduisant quelques notations.
Échanger l'ordre d'écriture des quantificateurs : quel sens a l'assertion obtenue ?

Exemple 10 (Une assertion de type B)**.**

Soit f une fonction définie sur $\mathbb{R}$. Écrire à l'aide de quantificateurs "la fonction f est majorée". Échanger l'ordre d'écriture des quantificateurs : quel sens a l'assertion obtenue ?

- « Tous les chats sont gris ».

  Négation : «

- « Il existe un MP2I qui n'aime pas ce petit cours de logique ».

  Négation : «

Théorème 11 (Négation d'une proposition contenant des quantificateurs)**.**

Soit $\mathcal{P}(X)$ un prédicat sur un ensemble E.

$$\begin{array}{lcl} \neg\,(\forall x \in E \quad \mathcal{P}(x)) & \equiv & \exists x \in E \quad \neg\mathcal{P}(x) \\ \neg\,(\exists x \in E \quad \mathcal{P}(x)) & \equiv & \forall x \in E \quad \neg\mathcal{P}(x) \end{array}$$

Exemple 12.

Soit (u_n) une suite réelle.
La phrase P ci-dessous sera notre définition de « (u_n) est majorée ». Écrire sa négation.

$$P: \quad \exists M \in \mathbb{R} \quad \forall n \in \mathbb{N} \quad u_n \leq M.$$

Exemple 13 (Quand on écrit deux « il existe »).

Soit $f : \mathbb{R} \to \mathbb{R}$.
Écrire puis nier l'assertion P : « la fonction f est constante égale à 1 ou constante égale à -1 ».

2 Implication, équivalence.

2.1 Implique, Équivaut : tables de vérité.

Définition 14.

Soient P et Q deux assertions.
Les assertions $P \Longrightarrow Q$ (« P **implique** Q ») et $P \Longleftrightarrow Q$ (« P est **équivalent** à Q ») sont définies par les tables ci-dessous :

P	Q	$P \Longrightarrow Q$	$P \Longleftrightarrow Q$
V	V	V	V
V	F	F	F
F	V		F
F	F		V

L'implication $Q \Longrightarrow P$ est appelée **implication réciproque** de l'implication $P \Longrightarrow Q$.

On veut que $\boxed{P \Longrightarrow Q \text{ signifie « Si } P \text{ est vraie, alors } Q \text{ est vraie »}}$.

Que décider pour la valeur de $P \Longrightarrow Q$ lorsque P est fausse ? Ce n'est pas très clair alors on a laissé deux cases vides.
Examinons les quatre tables correspondant aux quatre choix possibles pour ces deux cases :

A

P	Q	$P \Longrightarrow Q$	$Q \Longrightarrow P$	$*$	$P \Longleftrightarrow Q$
V	V	V	V	V	V
V	F	F	V	F	F
F	V	V	F	F	F
F	F	V	V	V	V

B

P	Q	$P \Longrightarrow Q$	$Q \Longrightarrow P$	$*$	$P \Longleftrightarrow Q$
V	V	V	V	V	V
V	F	F	V	F	F
F	V	V	F	F	F
F	F	F	F	F	V

C

P	Q	$P \Longrightarrow Q$	$Q \Longrightarrow P$	$*$	$P \Longleftrightarrow Q$
V	V	V	V	V	V
V	F	F	F	F	F
F	V	F	F	F	F
F	F	V	V	V	V

D

P	Q	$P \Longrightarrow Q$	$Q \Longrightarrow P$	$*$	$P \Longleftrightarrow Q$
V	V	V	V	V	V
V	F	F	F	F	F
F	V	F	F	F	F
F	F	F	F	F	V

La colonne * donne la valeur de la conjonction « $(P \Longrightarrow Q)$ et $(Q \Longrightarrow P)$ ».

Pour choisir parmi les quatre possibilités, procédons par élimination.

On veut que la synonymie

$$« (P \Longrightarrow Q) \text{ et } (Q \Longrightarrow P) » \equiv « P \Longleftrightarrow Q »$$

soit vraie, ce qui élimine les tables B et D.

Dans la table C, les implications $P \Longrightarrow Q$ et $Q \Longrightarrow P$ sont synonymes, ce que l'on veut éviter !

La table A est donc choisie pour définir $P \Longrightarrow Q$.

Exemple 15.

Maintenant que la table de $P \Longrightarrow Q$ est complète, évaluer les assertions suivantes :

- "6 est pair"$\Longrightarrow$ "7 est impair" :
- "5 est pair"$\Longrightarrow$ "7 est impair" :
- "5 est impair"$\Longrightarrow$ "7 est pair" :
- "5 est pair"$\Longrightarrow$ "je suis ton père" :

2.2 L'implication et les autres connecteurs logiques.

Théorème 16 (Lien entre $\Longrightarrow$ et ou)**.**

$$P \Longrightarrow Q \;\equiv\; (\neg P) \text{ ou } Q.$$

Proposition 17 (Négation d'une implication)**.**

$$\neg (P \Longrightarrow Q) \;\equiv\; P \text{ et } (\neg Q).$$

⚠ On remarquera notamment que la négation d'une implication n'est **pas** une implication.

Exemple 18.

Soit une fonction $f : X \to \mathbb{R}$ une fonction définie sur une partie X de $\mathbb{R}$.
Nier la phrase « f est croissante sur X ».

Proposition 19 (L'équivalence comme double-implication)**.**

Soient P et Q deux assertions. On a la synonymie

$$P \Longleftrightarrow Q \quad \equiv \quad (P \Longrightarrow Q) \text{ et } (Q \Longrightarrow P).$$

Lorsque $P \Longleftrightarrow Q$ est vraie, on dit que Q est une **condition nécessaire et suffisante** (CNS) pour que P soit vraie.

Preuve : Il suffit de lire la table A de la page 5. □

2.3 L'implication, dans la pratique.

Comment *prouver* une implication $P \Longrightarrow Q$?
Par définition, si P est fausse, $P \Longrightarrow Q$ est vraie... alors concentrons-nous sur le cas où P est vraie !

Méthode (Preuve directe d'une implication)**.**

Pour démontrer une implication $P \Longrightarrow Q$,

1. On suppose P (et on l'écrit),
2. puis on démontre Q.

Un peu de vocabulaire en commençant par une question concrète : pour faire un gâteau au chocolat, est-il nécessaire d'avoir du chocolat ? suffisant d'avoir du chocolat ?

Définition 20.

Dans l'écriture $P \Longrightarrow Q$ d'une implication,

— l'assertion Q est dite condition **nécessaire**, *[Il faut que Q soit vraie pour que P le soit].*
— l'assertion P est dite condition **suffisante**, *[Il suffit que P soit vraie pour que Q le soit].*

En mathématiques, nos théorèmes s'écrivent généralement comme des implications :

Si certaines hypothèses sont satisfaites **alors** un certain résultat est obtenu.

Comment *utiliser* une telle implication ?

Proposition 21 (Modus ponens)**.**

Soient P et Q deux assertions.

$$\text{Si} \quad (P \Longrightarrow Q) \text{ et } P \text{ sont vraies,} \quad \text{alors } Q \text{ est vraie.}$$

Exemple 22 (Application : un syllogisme célèbre)**.**

« Tous les hommes sont mortels ». Ce "théorème" affirme que l'implication « Si cet être est un homme, alors il est mortel » est vraie, quel que soit l'être que l'on considère.
C'est donc le Modus Ponens que l'on utilise dans le raisonnement célèbre suivant :

« Tous les hommes sont mortels et Socrate est un homme, donc Socrate est mortel. »

⚠ Lorsqu'on écrit que $P \Longrightarrow Q$ est vraie, on n'écrit pas que P est vraie, ni que Q est vraie.

Méthode (Ne pas écrire $\Longrightarrow$ à la place de « donc »)**.**

Écrire « $P \Longrightarrow Q$ » n'est **pas la même chose** qu'écrire « P est vraie, donc Q est vraie. »
Ainsi, nous utilisons volontiers le symbole $\Longrightarrow$ pour *énoncer* des résultats mais nous ne l'écrivons pas dans les *démonstrations* de ces résultats : on ne raisonne pas au conditionnel !

La *transitivité* de l'implication (et de l'équivalence) sont des propriétés naturelles et importantes.

Proposition 23 (Transitivité de l'implication et de l'équivalence)**.**

Les connecteurs $\Longrightarrow$ et $\Longleftrightarrow$ sont transitifs. En effet, si P, Q, R sont des assertions.

$$\text{Si} \quad (P \Longrightarrow Q) \text{ et } (Q \Longrightarrow R) \text{ sont vraies,} \quad \text{alors } (P \Longrightarrow R) \text{ est vraie.}$$

$$\text{Si} \quad (P \Longleftrightarrow Q) \text{ et } (Q \Longleftrightarrow R) \text{ sont vraies,} \quad \text{alors } (P \Longleftrightarrow R) \text{ est vraie.}$$

Exemple 24.

Proposer une façon de démontrer que 3 assertions données sont équivalentes deux à deux.

2.4 Contraposée d'une implication.

Définition 25.

Soient P et Q deux assertions. On appelle **contraposée** de l'implication $P \Longrightarrow Q$, l'implication

$$(\neg Q) \Longrightarrow (\neg P).$$

Théorème 26.

Soient P et Q deux assertions. On a la synonymie

$$P \Longrightarrow Q \quad \equiv \quad (\neg Q) \Longrightarrow (\neg P)$$

Autrement dit, une implication est vraie si et seulement si sa contraposée l'est.

Méthode (Preuve par contraposée d'une implication $P \Longrightarrow Q$)**.**

Au lieu d'utiliser la manière classique (*supposer* P*, montrer* Q) on pourra choisir, si cela paraît plus simple, de prouver la contraposée (*supposer (non* Q*), montrer (non* P*)*).

Exemple 27.

Soit n un entier naturel. Démontrer l'équivalence

$$n \text{ est pair} \iff n^2 \text{ est pair.}$$

3 Raisonnements usuels.

3.1 Raisonner par récurrence.

Soit une assertion dont le sens dépend d'un entier n, et que l'on note $\mathcal{P}(n)$. Soit un entier naturel n_0.
Le raisonnement par récurrence permet de démontrer l'assertion

$$\text{« Pour tout entier } n \text{ supérieur ou égal à } n_0,\ \mathcal{P}(n) \text{ est vraie. »} \qquad \text{ou} \qquad \text{« } \forall n \geq n_0 \quad \mathcal{P}(n). \text{ »}.$$

Raisonner par récurrence à partir de n_0, c'est démontrer les deux propriétés suivantes :

- L'initialisation : $\mathcal{P}(n_0)$ est vraie.
- L'hérédité : Pour tout n supérieur à n_0, si $\mathcal{P}(n)$ est vraie, alors $\mathcal{P}(n+1)$ l'est.

Le principe de récurrence (ou axiome de récurrence, puisqu'il est admis) garantit alors que pour tout entier n supérieur à n_0, $\mathcal{P}(n)$ est vraie.

L'idée : si la chute d'un domino quelconque entraîne celle du domino suivant (hérédité) et si le premier domino tombe (initialisation) alors tous les dominos tomberont.

Conformément au paragraphe 2.3, une bonne rédaction pour la preuve de l'hérédité sera

$$\boxed{\text{"Soit } n \geq n_0\text{. Supposons } \mathcal{P}(n)\text{. Montrons } \mathcal{P}(n+1)\text{..."}}$$

Un peu de logique formelle : on peut énoncer l'axiome de récurrence ainsi :

$$[\mathcal{P}(0) \ \text{ et } \ (\forall n \in \mathbb{N} \quad \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1))] \quad \Longrightarrow \quad (\forall n \in \mathbb{N} \ \ \mathcal{P}(n)).$$

Les récurrences dites « fortes ». Considérons un raisonnement par récurrence sur une propriété $\mathcal{P}(n)$. Lorsque l'on veut prouver $\mathcal{P}(n+1)$, on peut avoir besoin, en plus de $\mathcal{P}(n)$ d'utiliser les propriétés $\mathcal{P}(n-1)$, $\mathcal{P}(n-2)$ etc... On pourra donc, dans la preuve de l'hérédité, supposer que $\mathcal{P}(k)$ est vraie **pour tout** k inférieur à n. Cela revient à faire un raisonnement par récurrence, non pas sur $\mathcal{P}(n)$ mais sur

$$\mathcal{Q}(n) : \text{« pour tout } k \text{ inférieur à } n,\ \mathcal{P}(k) \text{ est vraie. »}$$

De la même façon, on peut qualifier de récurrence *double* un raisonnement où on suppose la propriété vraie pour deux rangs consécutifs avant de prouver qu'elle l'est au rang suivant.

Il n'y a donc pas vraiment de récurrence forte mais plutôt des propriétés de récurrence bien choisies !

Exemples 28.

Ils ne manqueront pas ! Voir TD.

3.2 Raisonner par l'absurde.

En mathématiques, une assertion qui n'est pas fausse est vraie, c'est ainsi que ce cours a débuté.
Cela conduit à la stratégie suivante, dite *preuve par l'absurde*. Pour prouver qu'une assertion P est vraie, on suppose que P est fausse et on raisonne jusqu'à trouver une contradiction manifeste, une « absurdité ».
Si cette absurdité est apparue (et que l'on a pas fait d'erreur dans notre raisonnement !), c'est que l'hypothèse faite au départ (« P est fausse ») est fausse. L'assertion P est donc... vraie.

Le raisonnement par l'absurde est souvent efficace pour prouver que quelque chose n'est pas vrai, démontrer qu'un objet n'existe pas, ou qu'un ensemble est vide car en supposant le contraire, on introduit une information positive et exploitable dans la suite du raisonnement.

Exemple 29.

On souhaite démontrer par l'absurde qu'une certaine porte est fermée.
Quelle est la première phrase de notre raisonnement ?

Exemple 30 (Une célébrité)**.**

Démontrer que $\sqrt{2}$ est irrationnel, c'est-à-dire qu'il n'est pas le quotient de deux entiers.

Un autre raisonnement par l'absurde célèbre : la preuve du théorème d'Euclide, qui affirme qu'il existe une infinité de nombres premiers.

3.3 Prouver une unicité.

Pour un problème donné, on dit qu'il y a unicité de la solution si le problème possède 0 ou 1 solution. Autrement dit, il y a unicité si, lorsqu'il existe une solution au problème, elle est la seule.

Méthode.

Pour démontrer une unicité,
- on considère deux solutions du problème X_1 et X_2, (« *Soient X_1 et X_2 deux solutions* »)
- on montre que $X_1 = X_2$.

Exemple 31.

Soit A un ensemble de réel. On dit qu'un réel M est *un* **maximum** de A si

$$M \in A \qquad \text{et} \qquad \forall x \in A \;\; x \leq M.$$

1. Prouver l'unicité du maximum pour une partie A de $\mathbb{R}$.
2. Démontrer que $[0, 1[$ ne possède pas de maximum.
   On voit ainsi que la question de l'unicité est décorrelée de celle de l'existence.

On souligne que ce genre de preuve n'est pas un raisonnement par l'absurde : dans la méthode ci-dessus, on ne suppose pas que $X_1 \neq X_2$.

3.4 Raisonner par analyse-synthèse.

Ce raisonnement sert à démontrer une équivalence entre deux propositions P et Q sans savoir à l'avance ce qu'est la proposition Q. C'est ce que réclament des énoncés de la forme

$\boxed{\text{Énoncé 1}}$: « Trouver une condition nécessaire et suffisante pour que la proposition P soit satisfaite. »

ou encore

$\boxed{\text{Énoncé 2}}$: « Trouver tous les objets possédant la propriété $\mathcal{P}$. »

En particulier, un raisonnement par analyse-synthèse pourra être proposé pour résoudre une équation (voir paragraphe suivant).

Méthode (Les deux étapes du raisonnement pour traiter l'énoncé 1)**.**

Analyse : Il s'agit de trouver une proposition Q qui découle de P ($P \Longrightarrow Q$ et la condition Q est nécessaire). Pour cela, on suppose P (et on l'écrit !) On cherche alors une proposition Q... qui permettra de réaliser l'étape suivante.

Synthèse : On montre que la proposition Q découverte dans la partie Analyse est suffisante. Pour cela, on suppose Q et on montre P. (preuve standard de $Q \Longrightarrow P$.)

Conclusion : La propriété P est vraie si et seulement si Q est vraie.

Toute la difficulté de ce raisonnement est qu'il nous appartient de trouver/choisir la proposition Q par analyse. Il faut donc savoir "quand s'arrêter" : le faire trop tôt conduira au choix d'une condition nécessaire Q qui ne sera pas suffisante pour P.

Exemple 32 (Une équation fonctionnelle)**.**

Déterminer les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que

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

<u>Analyse</u> : Supposons qu'il existe une fonction f qui satisfait la contrainte. Alors, en particulier, pour tout réel x, $f(x) = x + f(0)$. On voit donc que f est une fonction affine de pente 1.

<u>Synthèse</u> : Soit f une fonction affine de pente 1, c'est-à-dire une fonction $f : x \mapsto x + c$, avec $c \in \mathbb{R}$. Montrons que f satisfait la contrainte. Soient x et y deux réels ;

$$f(x+y) = (x+y) + c = x + (y+c) = x + f(y).$$

<u>Conclusion</u> : Les fonctions solutions du problème (de l'*équation fonctionnelle*) sont exactement les fonctions affines de pente 1, c'est-à-dire les fonctions du type $x \mapsto x + c$, où c est une constante réelle.

Vous trouverez parmi les exercices de la feuille de TD quelques exemples d'équations fonctionnelles.

Un cas particulier courant : preuve d'une existence+unicité.

Le raisonnement par analyse-synthèse est utile en particulier lorsqu'on veut démontrer l'existence et l'unicité d'une solution pour un certain problème $\mathscr{P}$:

Analyse : Supposons que le problème $\mathscr{P}$ possède une solution que l'on note x. Investigations, calculs... on obtient que nécessairement, x prend une certaine valeur x_0.
À ce stade, l'unicité est prouvée : si une solution existe, c'est forcément x_0.

Synthèse : Reste à montrer que x_0, notre unique candidat au poste de solution, en est bien une.
On vient de démontrer l'existence d'une solution, existence qui avait été supposée dans la partie analyse !

Conclusion : Il existe une unique solution au problème $\mathscr{P}$: x_0.

Exemple 33 (Parties paire et impaire d'une fonction)**.**

Démontrer le résultat (qu'on retiendra) ci-dessous.

Toute fonction définie sur $\mathbb{R}$ s'écrit de manière unique comme somme d'une fonction paire et d'une fonction impaire.

Preuve. Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction.

Analyse. Supposons qu'il existe deux fonctions g et h, avec g paire et h impaire, telles que $f = g+h$, . Pour un réel x, on peut écrire

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

En faisant la somme et la différence des deux lignes, on obtient

$$g(x) = \frac{1}{2}\left(f(x)+f(-x)\right) \quad \text{et} \quad h(x) = \frac{1}{2}\left(f(x)-f(-x)\right).$$

Cela met en évidence un unique couple (g,h) candidat, pour la décomposition.

Synthèse. Posons

$$g : x \mapsto \frac{1}{2}\left(f(x)+f(-x)\right) \quad \text{et} \quad h : x \mapsto \frac{1}{2}\left(f(x)-f(-x)\right).$$

Vérifions que le couple (g,f) convient pour la décomposition, c'est à dire $\begin{cases} f = g+h, \\ g \text{ est paire,} \\ h \text{ est impaire,} \end{cases}$

Pour cela on prend un réel x et on vérifie facilement que $g(x)+h(x) = f(x)$, que $g(-x) = g(x)$ et que $h(-x) = -h(x)$.

Conclusion. La fonction f s'écrit bien de manière unique comme somme d'une fonction paire et d'une fonction impaire. C'est donc le cas pour toute fonction $f : \mathbb{R} \to \mathbb{R}$.

Un résultat similaire : toute matrice carrée s'écrit de manière unique comme la somme d'une matrice symétrique, et d'une matrice antisymétrique. Le cours d'algèbre linéaire viendra rapprocher ces deux résultats.

3.5 Résoudre une équation.

Qu'est-ce qu'une équation ?

C'est une égalité entre deux membres qui dépendent de *variables*. Des exemples :

$$\begin{array}{lrcl}(E_1) & 2x & = & x+1 \\ (E_2) & x & = & x+1\end{array} \qquad \begin{array}{lrcl}(E_3) & x^2+y^2 & = & 1 \\ (E_4) & y''+4y & = & 0\end{array}$$

Résoudre une équation, c'est trouver les valeurs (prises par les variables) pour lesquelles l'égalité est vraie. Une équation est donc une question, et les variables des lettres utilisées pour écrire cette question.

Équation (E_1).
C'est une équation sur $\mathbb{R}$: il s'agit de déterminer tous les réels qui satisfont l'égalité. Il est facile de montrer (voir paragraphe suivant) que (E_1) possède une unique solution : le nombre 1.

Équation (E_2).
À nouveau une équation sur $\mathbb{R}$. Celle-ci n'a pas de solution ! (voir paragraphe suivant) On comprend ici que le statut de la lettre x n'est pas celui d'un nombre, puisqu'il n'existe pas de nombre qui satisfait la contrainte. La lettre x est une variable dite *muette*, un outil pour poser la question : "quels sont les nombres réels dont la valeur reste inchangée en ajoutant 1 ?"

Équation (E_3).
Deux variables, x et y : il s'agit d'une équation sur $\mathbb{R}^2$. On cherche tous les couples (x, y) tels que $x^2+y^2 = 1$. Il y a une infinité de solutions, parmi lesquelles $(1, 0)$, $(0, 1)$ et $(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})$; lorsqu'on les représente dans un repère orthonormé, les solutions correspondent aux points du cercle trigonométrique.

Équation (E_4).
Cette fois il s'agit d'une équation sur $\mathcal{D}^2(\mathbb{R}, \mathbb{R})$, l'ensemble des fonctions deux fois dérivables sur $\mathbb{R}$.
Il s'agit de trouver toutes les fonctions y de ce type telles que pour tout t réel, $y''(t) + 4y(t) = 0$.
On parlera ici d'équation différentielle. Celle-ci modélise en physique un oscillateur harmonique de pulsation $\sqrt{4} = 2$. Elle possède une infinité de solutions qui seront déterminées dans un cours dédié.

Exemples de résolutions par équivalences.

Exemple (Équation $2x = x+1$).

Soit x un nombre réel.

$$\begin{aligned} x \text{ est solution } &\iff 2x = x+1 \\ &\iff x = 1 \end{aligned}$$

L'équation a donc une unique solution : le nombre 1.

Ici, c'est très simple mais normalement, chaque équivalence doit être justifiée (voir paragraphe 2.3).

On a établi l'équivalence [x est solution $\iff x = 1$], c'est-à-dire
- [x est solution $\implies x = 1$] : *si x est une solution, alors il vaut* 1 ;
- [$x = 1 \implies x$ est solution] : 1 *est solution.*

Exemple (Équation $x = x + 1$).

Soit x un nombre réel.

$$\begin{aligned} x \text{ est solution} &\iff x = x + 1 \\ &\iff 0 = 1 \end{aligned}$$

L'équation ne possède donc aucune solution.

Ici, seules les implications directes servent, finalement : si x est solution, alors $0 = 1$, ce qui est absurde... C'est donc que x n'est pas solution !

Méthode (Résolution d'une équation par équivalence).

On commence par déclarer la variable (disons x ici), puis on crée une chaîne d'équivalences en "partant" de l'assertion « x est solution ».

Attention : en écrivant le symbole $\iff$: il faut être capable de justifier les deux implications !

Pour plus de lisibilité, on alignera les symboles $\iff$, comme on aligne les $=$ dans un calcul sur plusieurs lignes.

Exemples de résolution par analyse-synthèse.

Parfois, (et c'est le cas dans les deux exemples ci-dessous), il est difficile de progresser en conservant des assertions équivalentes entre elles (on est gêné par une disjonction de cas...) Le raisonnement par analyse-synthèse est alors une bonne alternative.

Exemple (Équation $x = \sqrt{1 - x^2}$).

Soit x un nombre réel.

• Supposons que x est solution.
On a alors $x = \sqrt{1 - x^2}$. Passons au carré : $x^2 = 1 - x^2$. On a donc $x^2 = \frac{1}{2}$, d'où $x = \pm\frac{\sqrt{2}}{2}$.
  À ce stade, on sait que <u>*si*</u> *x est solution,* <u>*alors*</u> *x vaut* $\pm\frac{\sqrt{2}}{2}$.

• Examinons les candidats obtenus.
Il est facile de vérifier que $\frac{\sqrt{2}}{2}$ est une solution, et que $-\frac{\sqrt{2}}{2}$ n'en est pas une.

• Conclusion : l'équation possède une unique solution : $\frac{\sqrt{2}}{2}$.

Remarquons que le nombre $-\frac{\sqrt{2}}{2}$ aurait pu être écarté dans l'analyse : l'égalité $x = \sqrt{1 - x^2}$ impliquant que x, qu'on a supposé être une solution, est nécessairement positif.

Exemple (Équation $x-1=\sqrt{1+x^2}$).

Soit x un nombre réel.

• Supposons que x est solution.
On a alors $x-1=\sqrt{1+x^2}$.
En passant au carré, $x^2-2x+1=1+x^2$, ce qui laisse $-2x=0$ puis $x=0$.

• Or, il est facile de vérifier que 0 n'est pas solution.

• Conclusion : l'équation ne possède pas de solution.

Exercices

Assertions.

$\boxed{\textbf{0.1}}$ **[♦◇◇]** Que répond un mathématicien à la question « Vous êtes gaucher ou droitier ? ».

$\boxed{\textbf{0.2}}$ **[♦◇◇]** C'est l'histoire de cinq mathématiciens qui vont au restaurant. Ils ont pris un menu avec thé ou café compris. À la fin du repas, le serveur demande : tout le monde prendra du café ? Le premier mathématicien répond « Je ne sais pas ». Idem pour le second, le troisième, et le quatrième. Le cinquième répond « Quatre cafés et un thé SVP ». Expliquer.

$\boxed{\textbf{0.3}}$ **[♦◇◇]** Soit $(u_n)_{n\in\mathbb{N}}$ une suite de réels.
Plus tard dans l'année, nous définirons la phrase « $u_n \underset{n\to+\infty}{\longrightarrow} +\infty$ » par l'assertion

$$\forall M\in\mathbb{R}\quad \exists p\in\mathbb{N}\quad \forall n\in\mathbb{N}\quad n\geq p \Longrightarrow u_n\geq M.$$

(*pas besoin de comprendre pourquoi à ce stade !*) Écrire la négation de cette assertion.

$\boxed{\textbf{0.4}}$ **[♦◇◇]**

1. Nier l'assertion
$$\exists x\in\mathbb{R}\quad \forall y\in\mathbb{R}\quad x+y\geq 0.$$
2. Prouver que l'assertion ci-dessus est fausse.

$\boxed{\textbf{0.5}}$ **[♦◇◇]** « S'il fait beau, je ne prends pas mon parapluie. »
Écrire la contraposée de la réciproque.

$\boxed{\textbf{0.6}}$ **[♦♦◇]** Soit (u_n) une suite réelle. Démontrer l'équivalence des deux assertions

1. $\forall n\in\mathbb{N}\quad u_{n+1}\geq u_n$.
2. $\forall (n,p)\in\mathbb{N}^2\quad p\geq n \Longrightarrow u_p\geq u_n$.

Récurrence.

$\boxed{\textbf{0.7}}$ **[♦♦◇]** [Récurrence standard]
Déterminer les entiers naturels n tels que $2^n \geq n^2$.

$\boxed{\textbf{0.8}}$ **[♦♦◇]** [Récurrence double]
Soit un réel x non nul.

1. Pour n un entier naturel, calculer $\left(x^n + \frac{1}{x^n}\right) \cdot \left(x + \frac{1}{x}\right)$.
2. Supposons que $x + \dfrac{1}{x} \in \mathbb{Z}$. Démontrer que $\forall n \in \mathbb{N}\ x^n + \dfrac{1}{x^n} \in \mathbb{Z}$.

$\boxed{\textbf{0.9}}$ **[♦◇◇]** [Récurrence forte]

Soit (u_n), définie par récurrence par $\begin{cases} u_1 = 3 \\ \forall n \geq 1 \quad u_{n+1} = \frac{2}{n} \sum\limits_{k=1}^{n} u_k. \end{cases}$.

Démontrer par récurrence forte que $\forall n \geq 1\ u_n = 3n$.

$\boxed{\textbf{0.10}}$ **[♦♦◇]** Comme on l'a fait plus haut pour le principe de récurrence, écrire un « principe de récurrence forte » à l'aide d'une suite de quantificateurs.

Analyse-synthèse.

$\boxed{\textbf{0.11}}$ **[♦♦◇]** Déterminer les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que

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

$\boxed{\textbf{0.12}}$ **[♦♦◇]** Déterminer les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \quad f(x - f(y)) = 1 - x - y.$$

$\boxed{\textbf{0.13}}$ **[♦◇◇]** Déterminer les fonctions $f : \mathbb{R}_+^* \to \mathbb{R}_+^*$ telles que

$$\forall x, y \in \mathbb{R}_+^* \quad xf(xy) = f(y).$$

$\boxed{\textbf{0.14}}$ **[♦♦♦]** Déterminer les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que

$$\forall x, y \in \mathbb{R} \quad f\left(f(x) + y\right) = f\left(x^2 - y\right) + 4x^2 y.$$

$\boxed{\textbf{0.15}}$ **[♦♦◇]** Résoudre l'équation

$$x^2 + x\sqrt{1 - x^2} - 1 = 0.$$

$\boxed{\textbf{0.16}}$ **[♦♦♦]** Soit E l'ensemble des fonctions dérivables sur $\mathbb{R}$.
On considère F l'ensemble des fonctions affines, et G l'ensemble des fonctions g dérivables sur $\mathbb{R}$ telles que $g(0) = g'(0) = 0$.
Démontrer que toute fonction de E s'écrit de manière unique comme la somme d'une fonction de F et d'une fonction de G.

---

1 Ensembles

1 Notations.

Définition 1 (Naïve).

- Un **ensemble** non vide E est une collection d'objets x appelés **éléments**.
- On dit d'un élément x de E qu'il **appartient** à E, ce qui se note $x \in E$.
  Si l'objet x n'est pas un élément de l'ensemble E, on peut noter $x \notin E$.
- On pose qu'il existe un ensemble n'ayant pas d'éléments et que cet ensemble est unique.
  On l'appelle **ensemble vide** et on note $\emptyset$. Pour tout objet x, l'assertion "$x \in \emptyset$" est fausse.
- Signe « $=$ ». Si x et y deux éléments d'un ensemble E, on notera $x = y$ si on veut exprimer que x et y sont un seul et même élément de E.

Notation.

Le signe $=$ entre deux ensembles E et F peut être utilisé : en écrivant $E = F$, on veut signifier que les éléments de E sont exactement les éléments de F.

Remarque. *Ne la lisez surtout pas !*

La définition précédente est naïve car la description d'une collection peut conduire à des paradoxes, des non-sens. Dans un exercice de la feuille de TD, consacré au paradoxe de Russell, on comprend que parler d'*ensemble de tous les ensembles* n'a pas de sens.
Donnons une version pédagogique de ce paradoxe (mais est-ce bien pédagogique de commencer par là ?...)
Dans un village, on demande à un barbier de raser tous les villageois qui ne se rasent pas eux-même. Pourquoi est-il impossible à ce barbier d'accomplir sa mission ?

Exemple 2 (Ensembles de nombres).

1. $\mathbb{N}$ l'ensemble des entiers naturels : $\mathbb{N} = \{0, 1, 2, 3, 4, \cdots\}$; $\mathbb{Z}$ l'ensemble des entiers relatifs.
2. $\mathbb{Q}$ l'ensemble des nombres rationnels $\mathbb{Q} = \left\{\dfrac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}^*\right\}$.
3. $\mathbb{R}$ est l'ensemble des nombres réels. $\mathbb{R}_+^*$ celui des réels strictement positifs. On a $\mathbb{R}_+^* =]0, +\infty[$.
4. Soit $n \in \mathbb{N}^*$. L'ensemble des entiers compris entre 1 et n s'écrit
$$\{1, 2, \cdots, n\},$$
ou bien $\{k \in \mathbb{N} \mid 1 \leq k \leq n\}$. Cet intervalle d'entiers pourra aussi être noté $[\![1, n]\!]$.

$\boxed{\text{Comment décrire un ensemble non vide ?}}$
On utilise des accolades, ainsi qu'une description de ses éléments, qui peut prendre deux formes.

- En **extension** : les éléments sont présentés sous forme de liste, par exemple $\{1, 2, 3\}$. Signalons que l'ordre dans notre liste n'a pas d'importance : $\{1, 2, 3\} = \{3, 2, 1\}$. L'ensemble
$$\{2k, k \in \mathbb{N}\}$$
est l'ensemble des entiers naturels pairs, qu'il faut lire $\{0, 2, 4, 6, \ldots\}$ en comprenant le sens des points de suspension.
- En **compréhension** : on sélectionne dans un autre ensemble, des éléments possédant une certaine propriété. Par exemple, l'ensemble des entiers pairs se note, en compréhension
$$\{n \in \mathbb{N} \mid \exists p \in \mathbb{N} : n = 2p\}.$$
Dans la notation en compréhension
$$\{x \in E \mid \mathscr{P}(x) \text{ est vraie}\}$$
on écrit, dans l'ordre et entre accolades
x : l'élément typique, E : l'ensemble de sélection, $\mid$: tel que $\mathscr{P}(x)$: condition de sélection.

Exemple 3.

Écrire de deux façons l'ensemble des couples de réels opposés.

$\boxed{\text{Que dire de l'ensemble vide ?}}$ Si on imagine les ensembles comme des boîtes, il n'est pas difficile d'imaginer l'ensemble vide : c'est une boîte qui ne contient rien. On conviendra que l'assertion
$$\forall x \in \emptyset \quad \mathcal{P}(x)$$
est vraie, quelle que soit l'assertion $\mathcal{P}(x)$ énoncée à l'aide de x. Puisqu'il n'y a pas d'éléments dans l'ensemble vide, on peut dire que tous les éléments de l'ensemble vide sont verts. Ils sont aussi bleus à poils durs.

Méthode (Démontrer qu'un ensemble est vide).

Le raisonnement par l'absurde peut être utile : on suppose que l'ensemble n'est pas vide, on prend un élément de l'ensemble, et on cherche une contradiction.

2 Inclusion.

Définition 4.

Soit A et B deux ensembles. On dit que A est **inclus** dans B, ce que l'on note $A \subset B$, si tout élément de A est un élément de B :

$$\forall x \in A \quad x \in B.$$

On peut faire un lien entre inclusion et implication en écrivant que A est inclus dans B signifie :

$$\forall x \in E \quad x \in A \implies x \in B,$$

où E est un ensemble contenant les éléments de A et de B.

Méthode.

Pour prouver une inclusion $A \subset B$,

1. On considère un élément de A ("Soit $x \in A$")
2. puis on prouve qu'il est dans B (on devra conclure avec "donc $x \in B$").

Exemple 5.

Justifier que $\mathbb{Z} \subset \mathbb{Q}$ puis que $\mathbb{Q} \not\subset \mathbb{Z}$.

Proposition 6 (Transitivité de l'inclusion)**.**

Soient A, B, C trois ensembles.

$$(A \subset B \text{ et } B \subset C) \implies A \subset C.$$

Théorème 7 (Double-inclusion)**.**

Soient A et B deux ensembles. On a

$$A = B \iff A \subset B \text{ et } B \subset A.$$

Exemple 8 (Prouver une égalité par double-inclusion)**.**

Soient les ensembles

$$A = \mathbb{R}_- \qquad \text{et} \qquad B = \{x \in \mathbb{R} : \quad \forall y \in \mathbb{R}_+ \quad y \geq x\}$$

Montrer que $A = B$.

3 Parties d'un ensemble et opérations.

Définition 9.

On appelle **partie** d'un ensemble E tout ensemble A tel que $A \subset E$.
Alternativement, on pourra dire que A est un *sous-ensemble* de E.

Remarque. Pour tout ensemble E, les ensembles E et $\emptyset$ sont des parties de E.

Définition 10.

Soient A et B deux parties d'un ensemble E.
On définit l'**intersection** de A et B, notée $A \cap B$ et leur **réunion** $A \cup B$ par

$$A \cap B = \{x \in E \mid x \in A \text{ et } x \in B\} \qquad \text{et} \qquad A \cup B = \{x \in E \mid x \in A \text{ ou } x \in B\}.$$

On appelle **différence** de A et de B, (« A privé de B ») la partie

$$A \setminus B := \{x \in E \mid x \in A \text{ et } x \notin B\}.$$

On appelle **complémentaire** de A la partie $E \setminus A$. Cet ensemble pourra aussi être noté $\overline{A}$ ou A^c.

Dans le reste du paragraphe, on allège les énoncés en fixant une fois pour toutes un ensemble E et trois parties A, B, C de cet ensemble.

Proposition 11 (Évidences).

$$\begin{gathered} A \cup A = A \cap A = A \\ A \cup E = E \cup A = E \\ A \cap E = E \cap A = A \\ A \cup \emptyset = \emptyset \cup A = A \\ A \cap \emptyset = \emptyset \cap A = \emptyset \\ A \setminus A = \emptyset \\ A \setminus \emptyset = A \end{gathered}$$

$$\begin{gathered} \overline{\overline{A}} = A \\ A \cup B = B \cup A \\ A \cap B = B \cap A \\ A \cup (B \cup C) = (A \cup B) \cup C \\ A \cap (B \cap C) = (A \cap B) \cap C \\ A \cap B \subset A \subset A \cup B \end{gathered}$$

Proposition 12 (Distributivité).

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad \text{et} \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Proposition 13 (Lien entre différence et complémentaire).

$$A \setminus B = A \cap \overline{B}.$$

Proposition 14 (Formules de Morgan)**.**

$$\overline{A \cap B} = \overline{A} \cup \overline{B} \quad \text{et} \quad \overline{A \cup B} = \overline{A} \cap \overline{B}.$$

Exemple 15.

Soient A, B, C trois parties d'un ensemble E. Montrer que $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

Proposition 16 (*Décroissance* du passage au complémentaire)**.**

$$A \subset B \implies \overline{B} \subset \overline{A}.$$

Comprendre le mot *décroissance* nécessite ici d'apercevoir l'analogie entre $\leq$ et $\subset$. Nous formaliserons cette idée plus loin dans le paragraphe consacré aux *relations d'ordre*.

Définition 17 (Généralisation : Intersection et union d'une famille de parties.)**.**

Soit E un ensemble et $(A_i)_{i \in I}$ une famille de parties de E, indexée par un ensemble I.

- On appelle intersection des A_i, pour i parcourant I l'ensemble ci-dessous :

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

  C'est l'ensemble des éléments de E qui appartiennent à *tous* les A_i.
- On appelle réunion des A_i, pour i parcourant I l'ensemble ci-dessous :

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

  C'est l'ensemble des éléments de E qui appartiennent à (au moins) l'un des A_i.

Les propriétés vues pour l'intersection/réunion de deux ensembles se généralisent : pour un ensemble E, une partie A de E et une famille $(B_i)_{i \in I}$ de parties de E, on a les propriétés de distributivité ci-dessous :

$$A \cap \left(\bigcup_{i \in I} B_i \right) = \bigcup_{i \in I} (A \cap B_i) \qquad \text{et} \qquad A \cup \left(\bigcap_{i \in I} B_i \right) = \bigcap_{i \in I} (A \cup B_i).$$

Voici les formules de Morgan pour une famille $(A_i)_{i \in I}$ de parties de E :

$$\overline{\bigcap_{i \in I} A_i} = \bigcup_{i \in I} \overline{A_i} \qquad \text{et} \qquad \overline{\bigcup_{i \in I} A_i} = \bigcap_{i \in I} \overline{A_i}.$$

Exemple 18.

Pour $n \in \mathbb{N}^*$, on pose $A_n = [\frac{1}{n}, 1]$. Que valent $\bigcap_{n \in \mathbb{N}^*} A_n$ et $\bigcup_{n \in \mathbb{N}^*} A_n$?

4 Parties disjointes.

Définition 19.

Soient A et B deux parties d'un ensemble E. Lorsque $A \cap B = \emptyset$, c'est à dire qu'il n'existe pas d'élément commun à A et B, on dit que A et B sont **disjointes**.

Exemple 20.

Pour chacune des situations ci-dessous, donner l'exemple de deux ensembles A et B tels que

1. A et B sont distincts mais non disjoints.
2. A et B sont disjoints mais non distincts.
3. A et B sont disjoints et distincts.
4. A et B sont non disjoints et non distincts.

Définition 21.

Soit E un ensemble et $(A_i)_{i\in I}$ une famille de parties de E, indexée par un ensemble I. On dit que cette famille est constituée de parties **deux à deux disjointes** si

$$\forall (i,j) \in I^2 \quad i \neq j \implies A_i \cap A_j = \emptyset.$$

Exemple 22 (Il ne suffit pas à l'intersection d'être vide !)**.**

Considérons :

$$A = \{1,2\}, \quad B = \{2,3\}, \quad C = \{1,3\}.$$

Aucune partie n'est disjointe d'une autre, et pourtant $A \cap B \cap C = \emptyset$.
On notera que pour prouver que A, B et C ne sont *pas* deux à deux disjointes, il suffit de constater que A et B ne le sont pas (par exemple).

Définition 23.

Un **recouvrement disjoint** d'un ensemble E est une famille $(A_i)_{i\in I}$ de parties de E telle que

- $E = \bigcup_{i\in I} A_i$ (l'ensemble E est réunion des parties).
- $\forall i,j \in I \quad i \neq j \Longrightarrow A_i \cap A_j = \emptyset$ (les parties sont deux à deux disjointes).

Si de surcroît tous les A_i sont non vides, on dit que $(A_i)_{i\in I}$ est une **partition** de E.

Exemple 24.

Proposer une partition de $]0,+\infty[$ en trois parties puis en une infinité de parties.

5 Cardinal d'un ensemble fini.

On effleure seulement le sujet ici : un chapitre *Dénombrement* y sera consacré.

Définition 25 (point de vue naïf).

Soit E un ensemble non vide. Il est dit fini s'il a un nombre fini d'éléments.
Ce nombre est appelé **cardinal** de E et noté $|E|$, ou $\#E$, ou $\text{Card}(E)$. On pose que l'ensemble vide est fini et que son cardinal est 0.
Un ensemble constitué d'un unique élément est appelé **singleton**.
Un ensemble constitué d'exactement deux éléments est appelé une **paire**.

Par exemple, $\text{Card}\left(\{\bigstar, \blacktriangledown, \square\}\right) = 3$.

Soit $n \in \mathbb{N}^*$, $\text{Card}([\![1, n]\!]) = n$ et $\text{Card}([\![0, n]\!]) = n + 1$.

Si a et b sont deux entiers relatifs avec $a \leq b$, $\text{Card}([\![a, b]\!]) =$.

Proposition 26 (La partie et le tout).

Soit E un ensemble <u>fini</u> et A une partie de E.

- Tout partie A de E est un ensemble fini et $|A| \leq |E|$.
- Si A et B sont des parties de E, alors

$$A = B \iff \begin{cases} A \subset B \\ |A| = |B| \end{cases}$$

Ce résultat est admis, faute de définition suffisamment solide pour les ensembles finis et leurs cardinaux.
Le slogan derrière l'implication $\Longleftarrow$: *si la partie est aussi grande que le tout, alors elle est égale au tout.*

Proposition 27 (Réunion de parties disjointes).

Soit E un ensemble fini et A et B deux parties de E <u>disjointes</u> ($A \cap B = \emptyset$) ; alors la partie $A \cup B$ est finie et a pour cardinal

$$|A \cup B| = |A| + |B|.$$

Plus généralement, pour $n \in \mathbb{N}^*$, si $A_1, \dots A_n$ n parties d'un ensemble fini E, <u>deux à deux disjointes</u>, alors, leur réunion est un ensemble fini de cardinal

$$\left| \bigcup_{k=1}^{n} A_k \right| = \sum_{k=1}^{n} |A_k|.$$

6 Produit cartésien.

Définition 28.

Soient E et F deux ensembles. On appelle **produit cartésien** de E et F et on note $E \times F$ l'ensemble

$$\{(x, y) \mid \ x \in E, y \in F\}.$$

Les éléments de $E \times F$ sont appelés **couples**.

Notation.

On note $E^2 = E \times E$. Par exemple, $\mathbb{R}^2 = \{(x, y) \mid x \in \mathbb{R}, y \in \mathbb{R}\}$.

Exemple 29.

1. *Élémentaire.* Expliciter $E \times F$ lorsque $E = \{1, 2, 3\}$, et $F = \{\diamondsuit, \heartsuit\}$.
2. *Couple vs paire.* Écrire un couple de paires puis une paire de couples.

Définition 30.

Soient $E_1, E_2, \ldots E_n$, n ensembles. On appelle produit cartésien de $E_1, E_2, \ldots, E_n$ et on note $E_1 \times E_2 \times \ldots \times E_n$ l'ensemble

$$\{(x_1, x_2, \ldots, x_n) \ \mid \ x_1 \in E_1, \ x_2 \in E_2, \cdots, \ x_n \in E_n\}.$$

Les éléments de $E_1 \times E_2 \times \ldots \times E_n$ sont appelés **n-uplets**.

Proposition 31 (Égalité de deux n-uplets)**.**

Soient $(x_1, \ldots, x_n)$ et $(y_1, \ldots, y_n)$ deux n-uplets d'un produit cartésien $E_1 \times \cdots E_n$.

$$(x_1, \ldots, x_n) = (y_1 \ldots, y_n) \quad \Longleftrightarrow \quad [\forall i \in [\![1, n]\!] \quad x_i = y_i].$$

Le résultat suivant sera montré dans le cours de dénombrement (il est déjà facile de se convaincre qu'il est vrai). Il montre que le choix de la notation produit est naturelle pour ces ensembles de couples : pour des ensembles de n-uplets, le cardinal du produit, c'est le produit des cardinaux.

Proposition 32.

Soient n ensembles <u>finis</u> $E_1, E_2, \ldots, E_n$. Alors le produit cartésien $E_1 \times \cdots \times E_n$ est fini et

$$|E_1 \times \cdots \times E_n| = \prod_{i=1}^{n} |E_i|.$$

7 Ensemble des parties d'un ensemble.

Notation.

L'**ensemble des parties** d'un ensemble E est noté $\mathcal{P}(E)$.

Remarque. Si E est un ensemble, l'assertion « A est une partie de E » peut s'écrire au choix

$$\text{« } A \in \mathcal{P}(E) \text{ »} \qquad \text{ou} \qquad \text{« } A \subset E \text{ ».}$$

Exemple 33.

Expliciter $\qquad \mathcal{P}(\{1,2,3\}), \qquad \mathcal{P}(\{1\}), \qquad \mathcal{P}(\emptyset), \qquad \mathcal{P}\left(\mathcal{P}(\{1\})\right).$

Proposition 34 (admis pour le moment)**.**

Si E est un ensemble fini à n éléments, $\mathcal{P}(E)$ est fini et a 2^n éléments.
Autrement dit, il y a 2^n parties dans un ensemble à n éléments.
Si $p \in [\![0, n]\!]$, le nombre de ces parties ayant exactement p éléments est $\displaystyle\binom{n}{p} = \frac{n!}{p!(n-p)!}$.

Exercices

$\boxed{1.1}$ **[♦◇◇]** Soient A, B deux parties d'un ensemble E. Établir que

$$A \setminus (A \setminus B) = A \cap B \quad \text{et} \quad A \setminus (A \cap B) = A \setminus B = (A \cup B) \setminus B.$$

$\boxed{1.2}$ **[♦◇◇]** Soient A, B, C, D quatre parties d'un ensemble E, telles que

$$E = A \cup B \cup C, \qquad A \cap D \subset B, \qquad B \cap D \subset C, \qquad C \cap D \subset A.$$

Montrer que $D \subset A \cap B \cap C$.

$\boxed{1.3}$ **[♦◇◇]** Soient A, B, C trois parties d'un ensemble E. Montrer

$$A \cap B = A \cap C \iff A \cap \overline{B} = A \cap \overline{C}.$$

$\boxed{1.4}$ **[♦◇◇]** Soient A, B, C trois parties d'un ensemble E.
Démontrer que les trois assertions ci-dessous sont deux à deux équivalentes

$$1.\ A \setminus B \subset C. \qquad 2.\ A \setminus C \subset B. \qquad 3.\ A \subset B \cup C.$$

$\boxed{1.5}$ **[♦♦◇]** Soit E un ensemble et A, B deux parties de E. Démontrer que

$$B \subset A \quad \Longleftrightarrow \quad (\forall X \in \mathcal{P}(E) \quad (A \cap X) \cup B = A \cap (X \cup B)).$$

$\boxed{1.6}$ **[♦◇◇]** Démontrer que

$$\mathbb{R} = \left\{x \in \mathbb{R} \mid \exists a \in \mathbb{R}_+^* \ \exists b \in \mathbb{R}_-^* : x = a + b\right\}.$$

$\boxed{1.7}$ **[♦◇◇]** Prouver que les ensembles A et B définis ci-dessous : sont égaux :

$$A = \left\{(x, y) \in \mathbb{R}^2 \ \mid \ 3x - 2y = 1\right\} \qquad \text{et} \qquad B = \{(1 + 2\lambda, 1 + 3\lambda), \ \lambda \in \mathbb{R}\}.$$

$\boxed{1.8}$ **[♦◇◇]** Soient A et B deux ensembles. Prouver que

1. $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.
2. $\mathcal{P}(A \cup B) \supset \mathcal{P}(A) \cup \mathcal{P}(B)$.
   Donner l'exemple de deux ensembles A et B telles que l'inclusion réciproque est fausse.

$\boxed{1.9}$ **[♦◇◇]** Soit E un ensemble et $(A_i)_{i\in I}$ un recouvrement disjoint de E.
On considère une partie F de E et on pose, pour tout $i \in I$, $B_i := A_i \cap F$.
Vérifier que la famille $(B_i)_{i\in I}$ est un recouvrement disjoint de F.

$\boxed{1.10}$ **[♦♦♦]** Expliciter les ensembles $\displaystyle\bigcap_{n\in\mathbb{N}^*} [\tfrac{1}{n+1}, \tfrac{1}{n}]$ et $\displaystyle\bigcup_{n\in\mathbb{N}^*} [\tfrac{1}{n+1}, \tfrac{1}{n}]$.

$\boxed{1.11}$ **[♦♦♦]** (Différence symétrique)
Soit E un ensemble. Pour toutes parties A et B de E, on appelle différence symétrique de A et B et on note $A\Delta B$ l'ensemble

$$A\Delta B = (A \cup B) \setminus (A \cap B).$$

1. Représenter deux parties A et B de E ainsi que $A\Delta B$ sur un dessin.
   Compléter : « un élément x de E est dans $A\Delta B$ si et seulement si $x \in A$ ... $x \in B$. »
2. Montrer que pour tout couple de parties $(A, B) \in (\mathcal{P}(E))^2$,
   $$A\Delta B = (A \cap \overline{B}) \cup (\overline{A} \cap B).$$
3. Soient A, B et C trois parties de E.
   (a) Démontrer que
   $$(A\Delta B)\Delta C = (A \cap B \cap C) \cup (A \cap \overline{B} \cap \overline{C}) \cup (\overline{A} \cap B \cap \overline{C}) \cup (\overline{A} \cap \overline{B} \cap C).$$
   (b) En déduire une description (phrase en français) de l'ensemble $(A\Delta B)\Delta C$ qui mette en évidence que les rôles de A, B, C sont ici interchangeables.
   (c) En déduire sans aucun calcul supplémentaire que
   $$(A\Delta B)\Delta C = A\Delta(B\Delta C).$$

$\boxed{1.12}$ **[♦♦◇]** Paradoxe de Russell.
Supposons qu'il existe un *ensemble de tous les ensembles* et notons-le $\mathcal{E}$.
Considérons alors l'ensemble des ensembles n'appartenant pas à eux-mêmes :

$$y = \{x \in \mathcal{E} | x \notin x\}.$$

Démontrer que $y \in y \Longleftrightarrow y \notin y$.

---

2 Sommes et produits

Dans ce cours, on énonce toutes nos propositions pour des familles de nombres *complexes*. Si vous ne savez pas encore ce que c'est, ce n'est pas bien grave car les nombres réels sont des nombres complexes (et ceux-là, vous les connaissez). On dira parfois juste « nombres » de toute façon. L'ensemble des nombres complexes est noté $\mathbb{C}$. Pour le moment, vous pouvez le remplacer par $\mathbb{R}$ chaque fois que vous le voyez.

La notion de *famille* sera définie dans le cours sur les applications. Pour le moment, une définition vague suffit : une famille $(a_i)_{i\in I}$ de nombres complexes est une collection de nombres « étiquetée »(on dit indexée) par un ensemble d'indices I. Dans tout ce cours, et même si on s'abstient de le préciser, l'ensemble I sera **fini**. On donnera un jour un sens à certaines sommes ayant une infinité de termes mais... patience. Pour un indice (une « étiquette ») $i \in I$ donné, l'écriture a_i désigne un certain nombre complexe. Bien sûr, si on veut manipuler une collection de trois nombres, il est naturel de l'indexer par l'ensemble $\{1, 2, 3\}$ mais on verra dans l'année qu'il peut être utile d'indexer certaines familles par autre chose que des entiers.

1 Somme et produit d'une famille finie de nombres.

Notations 1.

Soit $(a_i)_{i\in I}$ une famille de nombres complexes indexée par un ensemble **fini non vide** I.

On note $\sum_{i\in I} a_i$ (resp. $\prod_{i\in I} a_i$) la somme (resp. le produit) des éléments de la famille $(a_i)_{i\in I}$.

Exemple. Notons $I = \{\Diamond, \heartsuit, \Delta\}$, puis posons $a_\Diamond := 2$, $a_\heartsuit := e$, $a_\Delta := \pi$.
Alors, $(a_i)_{i\in I}$ est une famille de trois nombres complexes.

$$\sum_{i\in I} a_i = a_\Diamond + a_\heartsuit + a_\Delta = 2 + e + \pi \quad \text{et} \quad \prod_{i\in I} a_i = a_\Diamond \times a_\heartsuit \times a_\Delta = 2e\pi.$$

Notation.

Pour $n \in \mathbb{N}^*$, si $I = [\![1, n]\!] = \{1, 2, \ldots, n\}$, on peut aussi noter

$$a_1 + \cdots + a_n = \sum_{i \in [\![1,n]\!]} a_i = \sum_{1 \leq i \leq n} a_i = \sum_{i=1}^{n} a_i$$

Plus généralement, si $m, n \in \mathbb{Z}$, $m \leq n$ et $I = [\![m, n]\!] = \{m, m+1, \ldots, n\}$ on peut noter

$$a_m + \cdots + a_n = \sum_{i \in [\![m,n]\!]} a_i = \sum_{m \leq i \leq n} a_i = \sum_{i=m}^{n} a_i.$$

Remarque. La lettre i est une variable *muette* elle a seulement un sens localement, dans l'écriture de la somme ou du produit :

$$\sum_{i=1}^{n} a_i = \sum_{j=1}^{n} a_j = \sum_{k=1}^{n} a_k.$$

Notation.

Si I est l'ensemble vide, on convient qu'une expression du type $\displaystyle\sum_{i \in I} a_i$ vaut 0 et que $\displaystyle\prod_{i \in I} a_i$ vaut 1.

Exemple 2.

Soit $n \in \mathbb{N}^*$. Détailler les sommes suivantes, éventuellement avec des points de suspension.

$$\sum_{k=2}^{5} k, \qquad \sum_{k=0}^{0} 2^k, \qquad \sum_{k=0}^{n} k^2, \qquad \sum_{k=0}^{n} (-1)^k k^2, \qquad \sum_{k=1}^{0} k, \qquad \sum_{k=0}^{n} 1.$$

Proposition 3.

Soient deux entiers m et n tels que $m \leq n$ et $a_m, a_{m+1}, \cdots, a_n$ des nombres.
L'ensemble $[\![m, n]\!]$ contient $n - m + 1$ entiers, de sorte que

$\sum_{i=m}^{n} a_i$ est une somme de $n - m + 1$ **termes**,

$\prod_{i=m}^{n} a_i$ est un produit de $n - m + 1$ **facteurs**.

Exemple 4 (Termes ou facteurs égaux)**.**

Soit $n \in \mathbb{N}^*$ et $a \in \mathbb{C}$. Que valent $\displaystyle\sum_{k=0}^{n} a$ et $\displaystyle\prod_{k=0}^{n} a$?

2 Règles de calcul.

Proposition 5 (Linéarité de la somme).

Soient deux familles de nombres $(a_i)_{i\in I}$ et $(b_i)_{i\in I}$, où I est un ensemble fini et $\lambda \in \mathbb{C}$.

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

Corollaire 6 (La somme de la combinaison linéaire, c'est la combinaison linéaire des sommes).

Soient deux familles de nombres $(a_i)_{i\in I}$ et $(b_i)_{i\in I}$, et $\lambda,\mu\in\mathbb{C}$.

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

Proposition 7 (Produits de produits).

Soient deux familles de nombres complexes $(a_i)_{i\in I}$ et $(b_i)_{i\in I}$. Soient $\lambda\in\mathbb{C}$ et $n\in\mathbb{N}^*$.

$$\prod_{i\in I}(a_i\cdot b_i)=\left(\prod_{i\in I}a_i\right)\cdot\left(\prod_{i\in I}b_i\right)$$

En particulier, $\displaystyle\prod_{i=1}^{n}(\lambda a_i)=\lambda^n\prod_{i=1}^{n}a_i$

Si de surcroît tous les b_i sont non nuls,

$$\prod_{i\in I}\frac{a_i}{b_i}=\frac{\prod_{i\in I}a_i}{\prod_{i\in I}b_i}.$$

Pour tout entier naturel p,

$$\left(\prod_{i\in I}a_i\right)^p=\prod_{i\in I}a_i^p.$$

Proposition 8 (Relations de Chasles).

Soient $n\in\mathbb{N}^*$ et m un entier tel que $1\le m\le n$. Soit $(a_i)_{i\in[\![1,n]\!]}$ une famille de nombres complexes.

$$\sum_{i=1}^{n}a_i=\sum_{i=1}^{m}a_i+\sum_{i=m+1}^{n}a_i \qquad \text{et} \qquad \prod_{i=1}^{n}a_i=\left(\prod_{i=1}^{m}a_i\right)\cdot\left(\prod_{i=m+1}^{n}a_i\right).$$

Proposition 9 (Exponentielle d'une somme, logarithme d'un produit).

Soient $(a_i)_{i\in I}$ et $(b_i)_{i\in I}$ deux familles finies de nombres réels, les b_i étant tous strictement positifs.

$$\exp\left(\sum_{i\in I}a_i\right)=\prod_{i\in I}\exp(a_i) \qquad \text{et} \qquad \ln\left(\prod_{i\in I}b_i\right)=\sum_{i\in I}\ln(b_i).$$

3 Télescopage.

Théorème 10 (Sommes télescopiques)**.**

Soient $a_m, a_{m+1}, \cdots, a_n, a_{n+1}$ des nombres complexes. Alors,

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

Proposition 11 (Produits télescopiques)**.**

Soient $a_m, a_{m+1}, \cdots, a_n, a_{n+1}$ des nombres complexes non nuls. Alors,

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

Exemple 12.

Soit n un entier supérieur à 2. Simplifier

$$\sum_{k=0}^{n} \left((k+1)^6 - k^6\right), \qquad \sum_{k=1}^{n+1} \left(\sqrt{k+1} - \sqrt{k}\right), \qquad \sum_{k=1}^{n} \frac{1}{k(k+1)}, \qquad \prod_{k=2}^{n} \left(1 - \frac{1}{k}\right).$$

4 Sommes et produits de référence.

Proposition 13 ($\sum_{k=1}^{n} k^p$ avec $p \in \{1, 2, 3\}$)**.**

Soit $n \in \mathbb{N}^*$. On a

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}, \qquad \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}, \qquad \sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

Proposition 14 (Progression géométrique)**.**

Soit $n \in \mathbb{N}$ et q un nombre complexe.

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

Pour $x \in \mathbb{R}$ et $n \in \mathbb{N}^*$, ce qui précède permet d'écrire une factorisation de $x^n - 1$ par $x - 1$:

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

Exemple 15 (de sommes de progressions géométriques)**.**

Soit $m, n \in \mathbb{N}$ $(m \leq n)$ et $x \in \mathbb{R}$. Calculer : $\displaystyle\sum_{k=0}^{n} \frac{1}{2^k}$, $\displaystyle\sum_{k=1}^{n} 2^k$, $\displaystyle\sum_{k=0}^{n} (-1)^k x^{2k}$, $\displaystyle\sum_{k=m}^{n} x^k$.

Généralisons la factorisation de $x^n - 1$ obtenue plus haut :

Proposition 16 (Factorisation de $a^n - b^n$ par $a - b$)**.**

Soient a et b deux nombres complexes et $n \in \mathbb{N}^*$. On a

$$a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k = (a-b)\left(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + ab^{n-2} + b^{n-1}\right).$$

Exemple 17.

Factoriser : $a^2 - b^2$, $a^3 - b^3$, $a^4 - b^4$, $a^3 + b^3$.

Définition 18.

Soit $n \in \mathbb{N}$. On appelle **factorielle** de n et on note $n!$ le nombre

$$n! = \prod_{k=1}^{n} k$$

En particulier, on a $0! = 1$, $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, $5! = 120$.

Remarque. Vu en Terminale : $n!$ est le nombre de permutations d'un ensemble à n éléments. C'est aussi le nombre de façons différentes de numéroter n objets. Sera revu dans le cours de dénombrement.

Proposition 19 (Une relation simple et utile)**.**

$$\forall n \in \mathbb{N} \quad (n+1)! = (n+1) \cdot n!.$$

Exemple 20 (Produit des entiers pairs, des entiers impairs)**.**

Soit $n \in \mathbb{N}^*$. Montrer que

$$\prod_{k=1}^{n}(2k) = 2^n n! \qquad \text{et} \qquad \prod_{k=0}^{n-1}(2k+1) = \frac{(2n)!}{2^n n!}.$$

5 Changements d'indice.

Pas de définition formelle ici : il s'agit d'écrire une même somme de deux manières différentes, en changeant la forme de l'indice (en fait, l'ensemble des indices). Dans ce qui suit, $(u_k)_{k\in\mathbb{N}}$ est une suite de nombres complexes.

- Décalage $[j=k-1]$: $\displaystyle\sum_{k=1}^{n} u_k = \sum_{j=0}^{n-1} u_{j+1}$.

k	1	2	$\cdots$	n
j	0	1	$\cdots$	$n-1$

- Inversion de compteur $[j=n-k]$: $\displaystyle\sum_{k=1}^{n} u_k = \sum_{j=0}^{n-1} u_{n-j}$.

k	1	2	$\cdots$	n
j	$n-1$	$n-2$	$\cdots$	0

- Tri des termes d'indice pair et d'indice impair.

La famille $(u_k)_{0\le k\le 2n}$ est une famille de $2n+1$ nombres.
Les nombres $u_0, u_2, u_4, \dots, u_{2n}$ portent un indice pair : ce sont les nombres de la famille $(u_{2j})_{0\le j\le n}$:

$$u_0 + u_2 + u_4 + \dots u_{2n} = \sum_{j=0}^{n} u_{2j}$$

j	0	1	2	$\cdots$	n
$2j$	0	2	4	$\cdots$	$2n$

Les autres $(u_1, u_3 \dots, u_{2n-1})$ portent un indice impair

$$u_1 + u_3 + \dots u_{2n-1} = \sum_{j=0}^{n-1} u_{2j+1}$$

j	0	1	$\cdots$	$n-1$
$2j+1$	1	3	$\cdots$	$2n-1$

On a donc

$$\boxed{\sum_{k=0}^{2n} u_k = \sum_{j=0}^{n} u_{2j} + \sum_{j=0}^{n-1} u_{2j+1}}.$$

Lorsqu'on ne connaît pas la parité du nombre de termes dans la somme de départ, on peut écrire ceci :

$$\begin{aligned}\sum_{k=0}^{n} u_k &= \sum_{j\,:\,2j\le n} u_{2j} + \sum_{j\,:\,2j+1\le n} u_{2j+1} \\ &= \sum_{j\,:\,j\le \frac{n}{2}} u_{2j} + \sum_{j\,:\,j\le \frac{n-1}{2}} u_{2j+1}\end{aligned}$$

$$\boxed{\sum_{k=0}^{n} u_k = \sum_{j=0}^{\lfloor \frac{n}{2}\rfloor} u_{2j} + \sum_{j=0}^{\lfloor \frac{n-1}{2}\rfloor} u_{2j+1}}$$

Exemple 21.

Soit $n\in\mathbb{N}$. Calculer :

$$\sum_{k=0}^{n}\left(\sqrt{k+2}-\sqrt{k}\right) \qquad \text{et} \qquad \sum_{k=1}^{2n} k^2 + \sum_{k=1}^{2n} (-1)^k k^2.$$

On formalise (et on généralise) ce qui précède à l'aide de la proposition suivante. Elle est admise et peut être laissée pour une seconde lecture.

Proposition 22.

Soit $(u_i)_{i\in I}$ une famille de nombres complexes indexée par un ensemble fini I et σ une bijection de I vers I. Alors

$$\sum_{i\in I} u_{\sigma(i)} = \sum_{i\in I} u_i.$$

6 Coefficients binomiaux et formule du binôme.

Définition 23.

Pour deux entiers $n \in \mathbb{N}$ et $p \in \mathbb{Z}$, on appelle **coefficient binomial** « p parmi n » le nombre

$$\binom{n}{p} := \begin{cases} \dfrac{n!}{p!(n-p)!} & \text{si } p \in [\![0, n]\!], \\ 0 & \text{sinon.} \end{cases}$$

Proposition 24.

Soient n et p deux entiers naturels.

Le nombre $\binom{n}{p}$ est le nombre de parties à p éléments dans un ensemble à n éléments.

Pour $n \in \mathbb{N}$ et $p \in [\![0, n]\!]$, on a $\displaystyle\binom{n}{p} = \frac{n(n-1)(n-2)\cdots(n-p+1)}{p!}$.

Exemple 25.

$$\forall n \in \mathbb{N} \qquad \binom{n}{0} = 1, \qquad \binom{n}{1} = n, \qquad \binom{n}{2} = \frac{n(n-1)}{2}.$$

Proposition 26.

Soit $n \in \mathbb{N}$.

$$\forall p \in \mathbb{N}\ \binom{n}{p} = \binom{n}{n-p}, \qquad \forall p \in \mathbb{N}^*\ \binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1}, \qquad \forall p \in \mathbb{N}\ \binom{n+1}{p+1} = \binom{n}{p+1} + \binom{n}{p}.$$

(symétrie) (formule *sans nom*) (formule de Pascal)

Conséquence. Triangle de Pascal/algorithme de calcul.

$n\backslash p$	0	1	2	3	4	5	6	$\cdots$
0								$\cdots$
1								$\cdots$
2								$\cdots$
3								$\cdots$
4								$\cdots$
5								$\cdots$
6								$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Exemple 27.

Démontrer que les coefficients binomiaux sont des entiers.

On connaît l'identité $(a+b)^2 = a^2 + 2ab + b^2$. On va généraliser pour un exposant quelconque.

Théorème 28 (Formule du binôme)**.**

Soient $a, b \in \mathbb{C}$, et $n \in \mathbb{N}$. On a

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

Exemple 29.

$$\begin{aligned}
(a+b)^2 &= a^2 + 2ab + b^2 \\
(a+b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3 \\
(a+b)^4 &= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4 \\
(a+b)^5 &= a^5 + 5a^4b + 10a^2b^3 + 10a^3b^2 + 5ab^4 + b^5
\end{aligned}$$

Exemple 30 (Calculs classiques)**.**

Soit $n \in \mathbb{N}$. Calculer

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

7 Sommes doubles.

Pour n et p dans $\mathbb{N}^*$, on rappelle la définition du produit cartésien $[\![1,n]\!]\times[\![1,p]\!] = \{(i,j), i \in [\![1,n]\!], j \in [\![1,p]\!]\}$.

Il est courant de noter $a_{i,j}$ plutôt que $a_{(i,j)}$, même si ici, l'indice est un couple (i,j).

Théorème 31 (Sommes doubles : deux écritures)**.**

Soient n et p dans $\mathbb{N}^*$, $I = [\![1,n]\!] \times [\![1,p]\!]$ et $(a_{i,j})_{(i,j)\in I}$ une famille de nombres complexes.

$$\sum_{(i,j)\in I} a_{i,j} = \sum_{i=1}^{n}\sum_{j=1}^{p} a_{i,j} = \sum_{j=1}^{p}\sum_{i=1}^{n} a_{i,j}.$$

Proposition 32 (Produit de deux sommes)**.**

Soient n et p dans $\mathbb{N}^*$ et deux familles de nombres complexes $(a_i)_{i\in[\![1,n]\!]}$ et $(b_i)_{i\in[\![1,p]\!]}$. On a

$$\left(\sum_{i=1}^{n} a_i\right)\cdot\left(\sum_{j=1}^{p} b_j\right) = \sum_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]} a_i \cdot b_j.$$

En particulier,

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

Proposition 33 (Sommes triangulaires : deux écritures)**.**

Soient n et p dans $\mathbb{N}^*$, et $I = \{(i,j) \in [\![1,n]\!] \times [\![1,p]\!] : i \le j\}$.
Soit $(a_{i,j})_{(i,j)\in I}$ une famille de nombres complexes indexée par I. Leur somme peut s'écrire

$$\sum_{(i,j)\in I} a_{i,j} = \sum_{j=1}^{p}\sum_{i=1}^{j} a_{i,j} = \sum_{i=1}^{n}\sum_{j=i}^{p} a_{i,j}.$$

Remarque. On saura adapter. Par exemple, $\displaystyle\sum_{0\le i<j\le n} a_{i,j} =$.

Méthode.

Dans les doubles sommes, on peut ajouter des parenthèses superflues :

$$\sum_{(i,j)\in I} a_{i,j} = \sum_{j=1}^{p}\left(\sum_{i=1}^{j} a_{i,j}\right).$$

À l'intérieur des parenthèses, on calcule à j fixé, c'est à dire que *l'on traite j comme une constante.*

Exemple 34.

Soit $n \in \mathbb{N}^*$. Calculer $\displaystyle\sum_{1 \leq i \leq j \leq n} \frac{i}{j+1}$.

Exercices

2.1 [♦◇◇] Démontrer :

$$\forall n \in \mathbb{N}^* \quad \sum_{k=1}^{n} (-1)^k k = \frac{(-1)^n(2n+1)-1}{4}.$$

2.2 [♦◇◇] Soit $n \in \mathbb{N}$. Calculer

$$\sum_{k=1}^{n} k(k+1), \quad \sum_{k=n}^{2n} e^{-k}, \quad \sum_{k=0}^{2n} |k-n|.$$

2.3 [♦♦◇]

Soit $n \in \mathbb{N}^*$. Calculer

$$\sum_{k=-n}^{n} (k+2) \quad \text{et} \quad \sum_{k=1}^{2n} (-1)^k k^2.$$

2.4 [♦♦◇] Ci-dessous, n est un entier naturel. Calculer

$$\sum_{k=1}^{n} \ln\left(1+\frac{1}{k}\right); \qquad \sum_{k=2}^{n} \frac{1}{k(k-1)}; \qquad \sum_{k=0}^{n} k \cdot k!$$

2.5 [♦♦◇] Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle et $n \in \mathbb{N}$ un entier naturel. non nul. Simplifier.

$$\sum_{k=0}^{n-1} (u_{2k+2} - u_{2k}) \quad \text{et} \quad \sum_{k=1}^{n} (u_{2k+1} - u_{2k-1}).$$

2.6 [♦♦◇] Soit $q \in \mathbb{R}$ et $n \in \mathbb{N}$. On cherche à calculer la somme

$$S_n = \sum_{k=0}^{n} k q^{k-1}.$$

Que vaut-elle si $q = 1$? Désormais, on supposera $q \neq 1$.
Soit la fonction $f_n : x \mapsto \sum_{k=0}^{n} k x^{k-1}$. En la voyant comme la dérivée d'une autre que l'on calculera, calculer S_n.

2.7 [♦♦◇] Expliquer l'écriture

$$0,999... = 1.$$

$\boxed{\textbf{2.8}}$ **[♦♦♢]** Soit $n \in \mathbb{N}$ et $f_n : x \mapsto x^n$. On se donne un entier naturel p et un réel x.
Exprimer le nombre $f_n^{(p)}(x)$ à l'aide de factorielles.
Précision sur la notation : la fonction $f_n^{(p)}$ est la dérivée $p$ème de f_n.

$\boxed{\textbf{2.9}}$ **[♦♦♢]** Soit n un entier naturel non nul et p un entier naturel.

1. À l'aide d'un télescopage, démontrer l'identité
$$\sum_{k=p}^{n} \binom{k}{p} = \binom{n+1}{p+1}.$$
2. Grâce au cas $p = 1$, retrouver l'expression connue de $\sum_{k=1}^{n} k$.
3. Grâce au cas $p = 2$, retrouver l'expression connue de $\sum_{k=1}^{n} k^2$.

$\boxed{\textbf{2.10}}$ **[♦♦♢]** Soit $n \in \mathbb{N}$. Calculer $\displaystyle\sum_{0 \le i \le j \le n} 2^{-j} \binom{j}{i}$.

$\boxed{\textbf{2.11}}$ **[♦♦♢]** Soit $n \in \mathbb{N}$. $\displaystyle\sum_{1 \le i,j \le n} |i - j|$

$\boxed{\textbf{2.12}}$ **[♦♦♢]** Soit $n \in \mathbb{N}^*$. Calculer
$$\sum_{k=0}^{n} \sum_{i=k}^{n} \binom{n}{i} \binom{i}{k}.$$

$\boxed{\textbf{2.13}}$ **[♦♦♦]** Démontrer :
$$\forall n \in \mathbb{N}^* \quad \sum_{k=1}^{n} \binom{n}{k} \frac{(-1)^{k-1}}{k} = \sum_{k=1}^{n} \frac{1}{k}.$$

$\boxed{\textbf{2.14}}$ **[♦♦♦]** Pour $k \in \mathbb{N}^*$, on pose $H_k = \displaystyle\sum_{p=1}^{k} \frac{1}{p}$.

Pour $n \in \mathbb{N}^*$, exprimer $\displaystyle\sum_{k=1}^{n} H_k$ et $\displaystyle\sum_{k=1}^{n} k H_k$ en fonction de n et H_n.

Indications.

2.4 Ça télescope, mais il faut arriver à faire apparaître la forme $u_{k+1} - u_k$.

2.9 Une formule du cours vous aidera. Quel est l'indice qui "bouge" ? Quelle est alors la forme d'une somme "télescopable" ?

2.12 Quel type de somme avons-nous sous les yeux ? Quelle est la seule chose que nous ayons dite sur ces sommes ?

3 Exponentielle, logarithmes, puissances

1 Fonction exponentielle.

Définition 1.

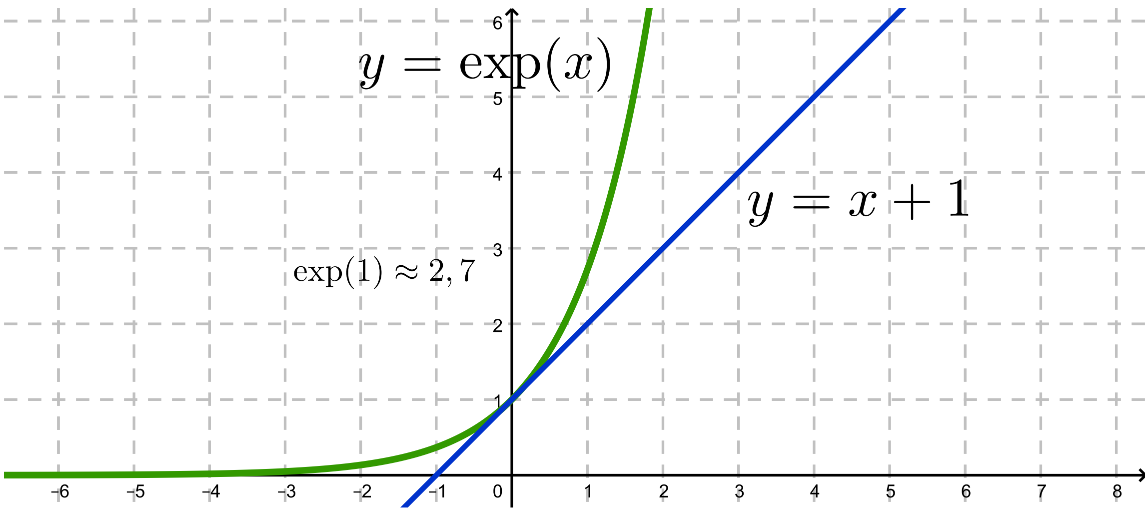
La fonction **exponentielle** est l'unique fonction $\exp : \mathbb{R} \to \mathbb{R}$ dérivable sur $\mathbb{R}$ et telle que

$$\exp(0) = 1 \quad \text{et} \quad \forall x \in \mathbb{R} \quad \exp'(x) = \exp(x).$$

Remarque. L'*unicité* de la fonction exponentielle comme solution du problème posé est un exercice de TD. Pour ce qui concerne l'*existence*, il faudra attendre. Le nombre $\exp(x)$ pour x réel sera défini un jour par

$$\exp(x) = \sum_{n=0}^{+\infty} \frac{x^n}{n!}.$$

Pour l'instant, cette somme infinie... c'est de la science-fiction !



Proposition 2 (Faits).

1. La fonction exp prend ses valeurs dans $]0, +\infty[$.
2. Elle est strictement croissante sur $\mathbb{R}$.
3. Le graphe de l'exponentielle a une tangente en 0 d'équation $y = x + 1$. De plus,

$$\forall x \in \mathbb{R} \quad \exp(x) \geq x + 1.$$

Théorème 3 (Propriété de morphisme de l'exponentielle).

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

Il découle de cette propriété que

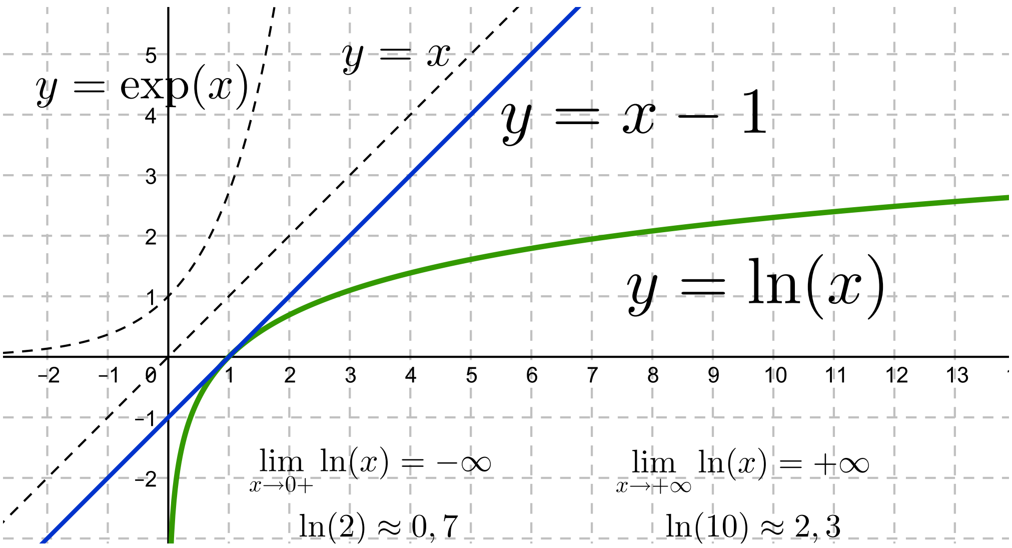
- $\forall x \in \mathbb{R} \quad \exp(-x) = \dfrac{1}{\exp(x)}$.
- $\forall x \in \mathbb{R}\ \forall y \in \mathbb{R} \quad \exp(x - y) = \dfrac{\exp(x)}{\exp(y)}$
- $\forall x \in \mathbb{R}\ \forall p \in \mathbb{Z} \quad \exp(px) = \exp(x)^p$.

2 Logarithme népérien.

La fonction exp est une bijection de $\mathbb{R}$ dans $]0, +\infty[$. Plus précisément, tout élément $y \in \mathbb{R}_+^*$ possède un unique antécédent par exp dans $\mathbb{R}$, que l'on va noter $\ln(y)$.

Définition 4.

On appelle **logarithme népérien** la fonction $\ln :]0, +\infty[\to \mathbb{R}$, réciproque de l'exponentielle.



La réciprocité de ln et de exp implique notamment

$$\boxed{\forall x \in \mathbb{R} \quad \ln(\exp(x)) = x} \quad \text{et} \quad \boxed{\forall y \in \mathbb{R}_+^* \quad \exp(\ln(y)) = y}.$$

Proposition 5.

La fonction ln est dérivable sur $]0, +\infty[$ de dérivée la fonction inverse : $\forall y \in]0, +\infty[\; \ln'(y) = \frac{1}{y}$. Le graphe de ln a une tangente en 1 d'équation $y = x - 1$. De plus,

$$\forall x \in]0, +\infty[\quad \ln(x) \leq x - 1.$$

Proposition 6 (Propriété de morphisme du logarithme)**.**

$$\forall x \in \mathbb{R}_+^* \; \forall y \in \mathbb{R}_+^* \quad \ln(xy) = \ln(x) + \ln(y).$$

Il découle de cette propriété que

- $\forall x \in \mathbb{R}_+^* \; \ln\left(\frac{1}{x}\right) = -\ln(x)$.
- $\forall p \in \mathbb{Z} \; \forall x \in \mathbb{R}_+^* \; \ln(x^p) = p\ln(x)$.

Exemple 7.

Le logarithme de dix milliards, c'est grand comment ?

Définition 8.

Soit $a \in \mathbb{R}_+^* \setminus \{1\}$. La fonction **logarithme en base** a, notée $\log_a$, est définie par

$$\log_a : \left\{ \begin{array}{ccc} \mathbb{R}_+^* & \to & \mathbb{R} \\ x & \mapsto & \log_a(x) := \dfrac{\ln(x)}{\ln(a)} \end{array} \right. .$$

Proposition 9 (sa raison d'être)**.**

$$\forall a \in \mathbb{R}_+^* \setminus \{1\} \quad \forall N \in \mathbb{N} \qquad \log_a\left(a^N\right) = N.$$

En informatique, on pourra apprécier le logarithme en base 2.

En physique et en SI, le logarithme en base 10.

3 Puissances.

3.1 Fonctions $x \mapsto x^p$, où p est entier.

• Exposants entiers positifs.

Soit n un entier naturel non nul et x un nombre réel. Le nombre x^n « x puissance n » est défini par

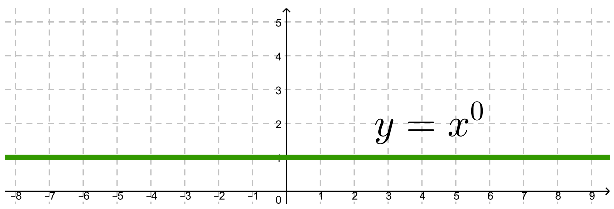
$$x^n := x \times x \times \ldots \times x. \qquad \text{(facteur } x \text{ présent } n \text{ fois).}$$

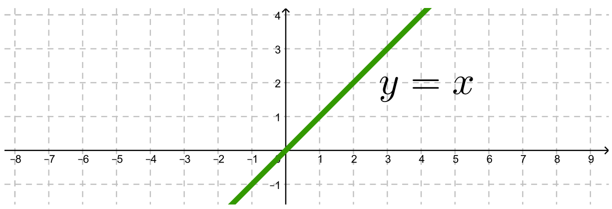
Il vient immédiatement $\boxed{\forall m, n \in \mathbb{N}^* \quad x^m \cdot x^n = x^{m+n}}$.
Quel sens donner alors à l'écriture x^0 ? Si on veut que la relation $x^0 \cdot x^n = x^{0+n}$ soit vraie pour tout entier naturel n, on posera

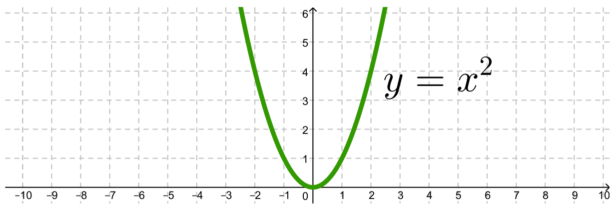
$$x^0 := 1.$$

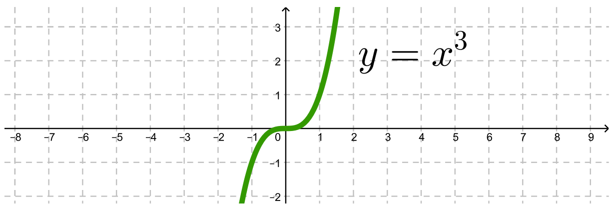
Définition 10.

Si n est un entier naturel, la fonction $x \mapsto x^n$, est définie sur $\mathbb{R}$.





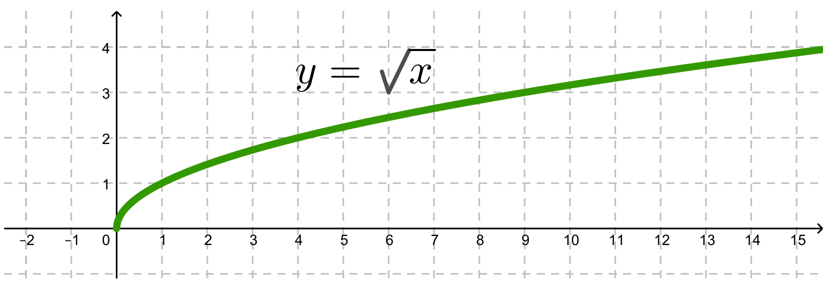




Définition 11.

Soit a un réel positif. L'équation $x^2 = a$ possède deux solutions dans $\mathbb{R}$ qui sont de signes opposés.
La solution positive de cette équation est appelée **racine carrée** de a et notée $\sqrt{a}$.
Dans le cas de l'équation $x^2 = 0$, les deux solutions sont confondues et $\sqrt{0} = 0$.

La fonction $x \mapsto \sqrt{x}$ est définie sur $\mathbb{R}_+$.



On peut démontrer à partir de cette définition que si x et y sont deux réels positifs,

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

Proposition 12.

$$\forall a \in \mathbb{R} \quad \sqrt{a^2} = |a|\,.$$

• <u>Exposants entiers négatifs.</u>

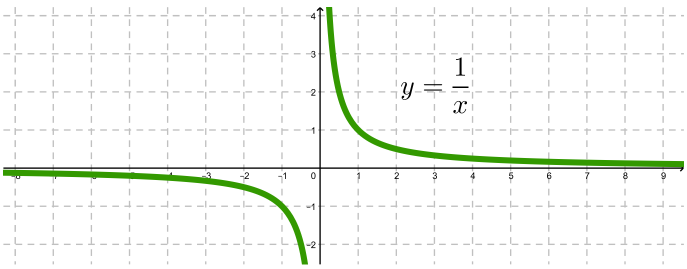
Soit x un nombre réel <u>non nul</u> et $n \in \mathbb{N}^*$, de sorte que $-n \in \mathbb{Z} \setminus \mathbb{N}$. Le nombre x^n, non nul, possède un inverse : on peut poser :

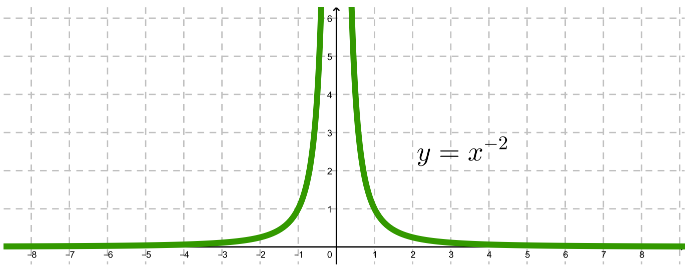
$$x^{-n} := \frac{1}{x^n}.$$

On peut alors prouver (laissé au lecteur) que $\boxed{\forall p, q \in \mathbb{Z} \quad x^p \cdot x^q = x^{p+q}}$.

Définition 13.

Si p est un entier strictement négatif ($p \in \mathbb{Z} \setminus \mathbb{N}$), la fonction $x \mapsto x^p$, est définie sur $\mathbb{R}^*$.





3.2 Puissances d'exposant réel.

On souhaite maintenant donner un sens à l'écriture x^a, avec a un réel quelconque, *non forcément entier*. Pour cela, remarquons que si p est un entier relatif, et si $x \in \mathbb{R}_+^*$, en utilisant la propriété de morphisme,

$$x^p = (\exp(\ln(x)))^p \underset{(*)}{=} \exp(p\ln(x))\,.$$

Définition 14.

Pour $\boxed{x > 0}$ et $a \in \mathbb{R}$, on définit le réel x^a (« x puissance a ») par

$$\boxed{x^a = \exp(a\ln(x)).}$$

Exemple. L'écriture π^3 a toujours eu un sens pour nous : $\pi \times \pi \times \pi$.
En revanche, l'écriture 3^π n'en avait pas. Désormais si ! il s'agit de $\exp(\pi\ln(3))$.

Remarque. Si $p \in \mathbb{Z}$ et $x \in \mathbb{R}_+^*$, $(*)$ montre que la "nouvelle" définition de x^p est cohérente avec l'ancienne. On peut donc dire que l'on a *étendu* la définition de x^a des puissances au cas d'un exposant a réel (au prix d'une contrainte de stricte positivité pour x).

Proposition 15 (Notation puissance pour exp)**.**

Notons e le nombre $\exp(1)$. Ce nombre vaut environ $2,71$ et il est tel que $\ln(e) = 1$. On a

$$\boxed{\forall x \in \mathbb{R} \quad \exp(x) = e^x.}$$

La propriété de morphisme se récrit

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

De plus,

$$\forall a \in \mathbb{R} \quad \forall x \in \mathbb{R} \quad \forall y \in \mathbb{R}_+^* \qquad (e^x)^a = e^{ax} \quad \text{et} \quad \ln(y^a) = a\ln(y).$$

Proposition 16.

Pour $a, b \in \mathbb{R}$ et $x, y \in \mathbb{R}_+^*$,

$$x^{a+b} = x^a x^b \qquad x^{-a} = \frac{1}{x^a} \qquad (xy)^a = x^a y^a.$$

$$\left(\frac{x}{y}\right)^a = \frac{x^a}{y^a} \qquad (x^a)^b = x^{ab}.$$

Corollaire 17.

$$\forall x \in \mathbb{R}_+^* \qquad \sqrt{x} = x^{1/2} \quad \text{et} \quad \frac{1}{\sqrt{x}} = x^{-1/2}.$$

Proposition 18 (Comparer deux puissances)**.**

Soient a, b deux réels. On a

$$\forall x \in]0,1[\qquad a \leq b \iff x^a \geq x^b$$

$$\forall x \in]1,+\infty[\qquad a \leq b \iff x^a \leq x^b$$

Remarque. Par exemple, l'inégalité $x^2 \leq x^3$ est fausse lorsque $0 < x < 1$!
On l'écrit en remarque car cette erreur grossière demeure assez fréquente. Voir le graphe de comparaison dans la proposition 24

Exemple 19.

Domaine de définition et simplification de $x \mapsto x^{\frac{\ln(\ln(x))}{\ln(x)}}$.

3.3 Fonctions $x \mapsto x^a$, où a est réel.

Définition 20.

Pour un réel a quelconque, la fonction $x \mapsto x^a$ est définie sur $\mathbb{R}_+^*$.

Comme on va le voir ci-dessous, lorsque $\underline{a > 0}$, cette fonction peut être prolongée en 0 en une fonction continue, en posant $0^a := 0$.

Soit $a \in \mathbb{R}$. Dans la suite, on notera f_a la fonction $f_a : \left\{ \begin{array}{ccc} \mathbb{R}_+^* & \to & \mathbb{R} \\ x & \mapsto & x^a \end{array} \right.$.

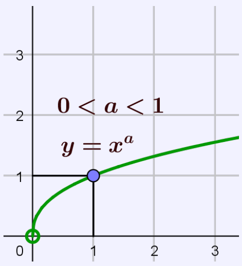
Proposition 21.

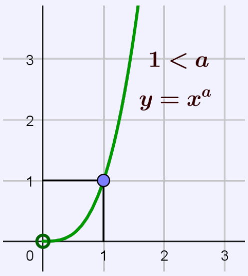
La fonction f_a est dérivable sur $\mathbb{R}_+^*$ et $\forall x \in \mathbb{R}_+^*\ f_a'(x) = ax^{a-1}$.

Proposition 22 (cas $a > 0$)**.**

Soit $a > 0$. Alors f_a est strictement croissante sur $\mathbb{R}_+^*$ et

$$\lim_{x \to 0} x^a = 0 \qquad \lim_{x \to +\infty} x^a = +\infty$$

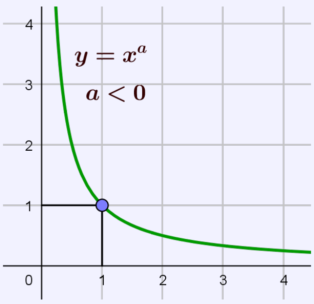




Proposition 23 (cas $a < 0$)**.**

Soit $a < 0$. Alors f_a est strictement décroissante sur $\mathbb{R}_+^*$ et

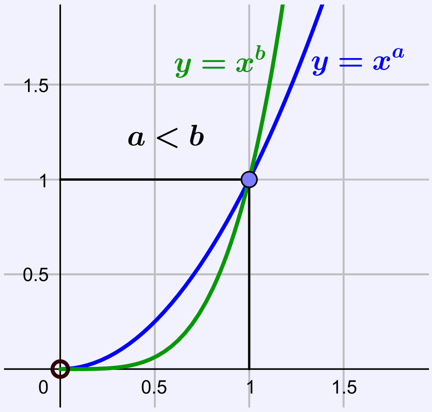
$$\lim_{x \to 0} x^a = +\infty \qquad \lim_{x \to +\infty} x^a = 0$$



Proposition 24 (comparaison)**.**

Si $a < b$, alors

$$\begin{aligned} \forall x \in]0,1] &\quad : \quad x^b \leq x^a \\ \forall x \in [1,+\infty[&\quad : \quad x^a \leq x^b. \end{aligned}$$



Proposition 25.

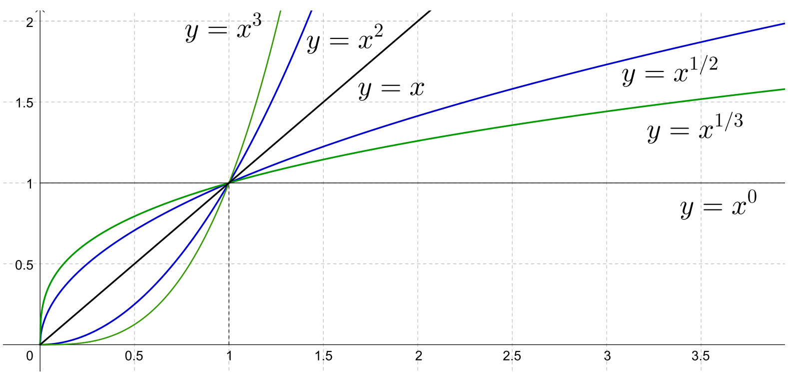
Soit a un réel non nul. Pour tout réel strictement positif y, le nombre $y^{\frac{1}{a}}$ est l'unique solution sur $\mathbb{R}_+^*$ de l'équation $x^a = y$.

La fonction $f_a : \left\{ \begin{array}{ccc} \mathbb{R}_+^* & \to & \mathbb{R}_+^* \\ x & \mapsto & x^a \end{array} \right.$ est donc bijective, et sa réciproque est la fonction $x \mapsto x^{1/a}$.

Notation.

Mentionnons que la puissance d'exposant $1/n$, peut être notée avec un symbole radical :

$$\forall x \in \mathbb{R}_+^* \quad \sqrt[n]{x} := x^{1/n}.$$



Fonctions puissances d'exposant positif.

3.4 Croissances comparées.

On compare les fonctions puissances avec les fonctions exponentielle et logarithme, et ce du point de vue *asymptotique* (celui des limites).

Lemme 26.

Soit $a \in \mathbb{R}_+^*$. Il existe une constante $C_a \in \mathbb{R}_+$ telle que $\forall x \in \mathbb{R}_+^* \quad \frac{x^a}{e^x} \leq C_a x^{-a}$.

Théorème 27 (Croissances comparées)**.**

Soit $a \in \mathbb{R}_+^*$. On a les limites suivantes.

$$\lim_{x \to +\infty} \frac{x^a}{e^x} = 0; \quad \lim_{x \to -\infty} |x|^a e^x = 0; \quad \lim_{x \to +\infty} \frac{\ln(x)}{x^a} = 0; \quad \lim_{x \to 0_+} x^a \ln(x) = 0.$$

Exemple 28.

Donner les limites suivantes (en précisant lorsque vous utilisez les croissances comparées)

$$\lim_{x \to +\infty} xe^{-x}, \qquad \lim_{x \to -\infty} xe^{-x}, \qquad \lim_{x \to +\infty} \frac{\ln(x)}{\sqrt{x}}, \qquad \lim_{x \to 0_+} \frac{\ln(x)}{\sqrt{x}}.$$

Pour se ramener à une limite connue, il faut parfois **factoriser par le terme prépondérant** dans une somme, comme dans l'exemple suivant.

Exemple 29.

Calculer

$$\lim_{x \to +\infty} \frac{x + \ln(x^2)}{\sqrt{x^2+1}} \quad \text{et} \quad \lim_{x \to -\infty} \frac{x + \ln(x^2)}{\sqrt{x^2+1}}$$

Exercices

$\boxed{\textbf{3.1}}$ **[♦◇◇]** Résoudre $2\ln\left(\frac{x+3}{2}\right) = \ln(x) + \ln(3)$, sur $\mathbb{R}_+^*$.

$\boxed{\textbf{3.2}}$ **[♦◇◇]** Résoudre sur $\mathbb{R}_+^*$ l'équation $x^{\sqrt{x}} = \sqrt{x}^x$.

$\boxed{\textbf{3.3}}$ **[♦♦◇]** Sans calculatrice, comparer π^e et e^π.

$\boxed{\textbf{3.4}}$ **[♦◇◇]** Donner le tableau de variations complet de

$$f : x \mapsto x^{\frac{1}{x}}.$$

Nécessite de se souvenir comment on dérive une composée.

$\boxed{\textbf{3.5}}$ **[♦♦◇]** Donner le tableau de variations complet de

$$f : x \mapsto x^{x\ln(x)}.$$

Nécessite de se souvenir comment on dérive une composée.

$\boxed{\textbf{3.6}}$ **[♦♦◇]** Calcul de $\displaystyle\lim_{x\to+\infty} \frac{\ln(x^2+1)}{\sqrt{x}}$ et de $\displaystyle\lim_{x\to+\infty} \frac{\ln(e^x+x)}{\sqrt{x}}$.

$\boxed{\textbf{3.7}}$ **[♦♦♦]**

1. Étudier les variations de $f : x \mapsto \sqrt[3]{x} - \sqrt[3]{x+1}$.
2. Des deux nombres $\sqrt[3]{2} + \sqrt[3]{4}$ et $\sqrt[3]{24}$, lequel est le plus grand ?

$\boxed{\textbf{3.8}}$ **[♦♦◇]**

1. Soit α un réel et $x > -1$. Comparer $(1+x)^\alpha$ et $1 + \alpha x$ (on discutera selon les valeurs de α).
2. Soit $\alpha \in [0,1]$ et $n \in \mathbb{N}^*$. Montrer que

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

$\boxed{\textbf{3.9}}$ **[♦♦◇]** [Unicité de la fonction exponentielle comme solution d'un problème de Cauchy]

On dit qu'une fonction $y : \mathbb{R} \to \mathbb{R}$ satisfait le problème $(*)$ si

$$y \text{ est dérivable sur } \mathbb{R}, \qquad y(0) = 1, \qquad \forall x \in \mathbb{R} \;\; y'(x) = y(x).$$

1. Soit f une fonction satisfaisant le problème $(*)$ et $u : x \mapsto f(x)f(-x)$.
   Démontrer que u est constante sur $\mathbb{R}$. En déduire que f ne s'annule pas sur $\mathbb{R}$.
2. Soient f et g deux fonctions satisfaisant le problème $(*)$.
   En considérant le quotient des deux fonctions, démontrer que $f = g$.

---

1 Cosinus et sinus d'un réel, via le cercle.

On munit le plan d'un repère orthonormé (O, I, J).

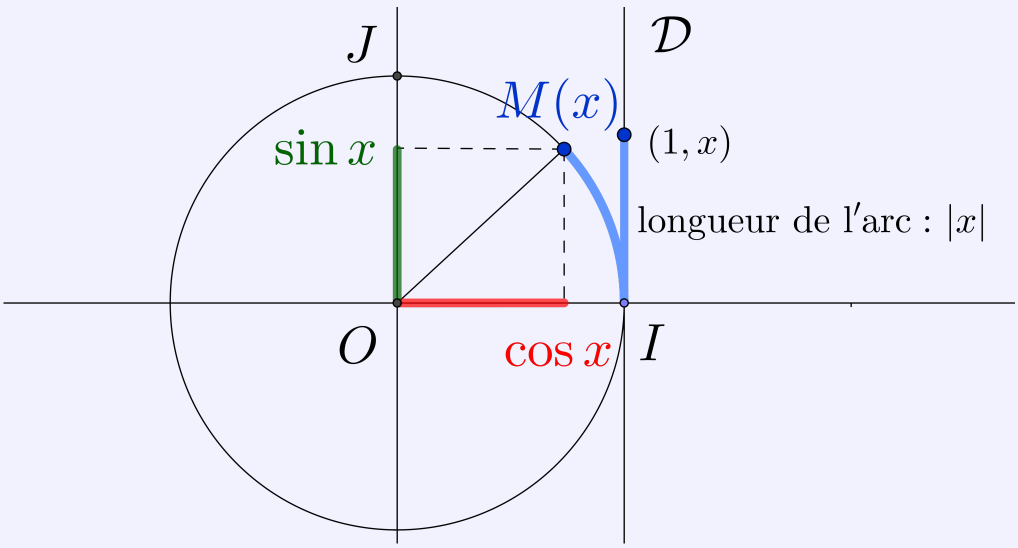
Le cercle de centre O et de rayon 1 est appelé **cercle trigonométrique**.

Soit $\mathcal{D}$ la droite parallèle à l'axe des ordonnées et passant par le point I. À tout un réel x, on associe le point $(1, x)$ sur $\mathcal{D}$. Notamment, le réel 0 est identifié à $I \in \mathcal{D}$.

On « enroule » alors la droite $\mathcal{D}$ sur le cercle : les réels positifs vont l'être dans le sens direct (antihoraire), et les réels négatifs dans le sens indirect. Pour un réel x, on notera $M(x)$ le point du cercle sur lequel a été enroulé le point $(1, x)$. Le cercle étant de périmètre 2π et la droite infinie, il va falloir faire plusieurs tours...

Définition 1.

Soit $x \in \mathbb{R}$ et $M(x)$ le point correspondant sur le cercle trigonométrique, obtenu par enroulement. On appelle **cosinus** de x son abscisse et **sinus** de x son ordonnée, notés $\cos x$ et $\sin x$.



Par définition, on a $\boxed{\forall x \in \mathbb{R} \quad \begin{array}{l} -1 \leq \cos x \leq 1 \\ -1 \leq \sin x \leq 1 \end{array}}$ c'est-à-dire $\boxed{\forall x \in \mathbb{R} \quad \begin{array}{l} |\cos x| \leq 1 \\ |\sin x| \leq 1 \end{array}}$

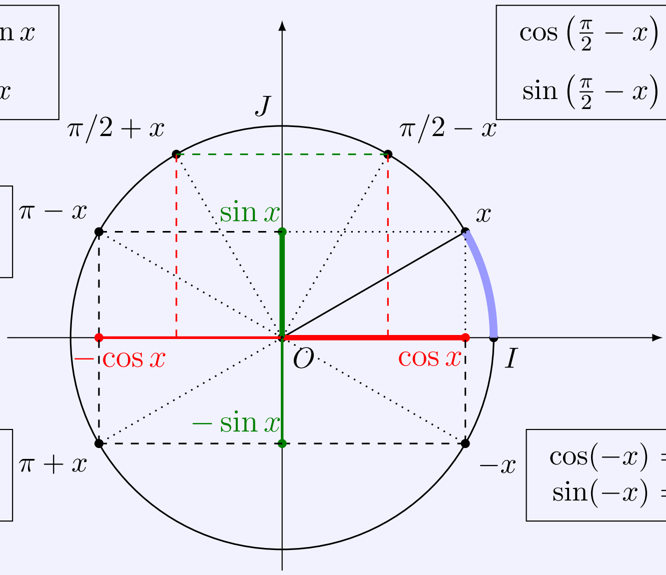
2 Formulaire de trigonométrie.

Proposition 2 (Les symétries de cos et sin)**.**

$$\cos\left(\frac{\pi}{2}+x\right) = -\sin x \qquad \sin\left(\frac{\pi}{2}+x\right) = \cos x$$

$$\cos\left(\frac{\pi}{2}-x\right) = \sin x \qquad \sin\left(\frac{\pi}{2}-x\right) = \cos x$$

$$\cos(\pi - x) = -\cos x \qquad \sin(\pi - x) = \sin x$$

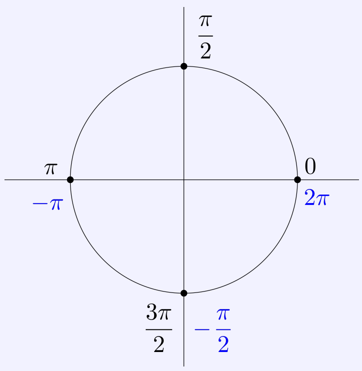


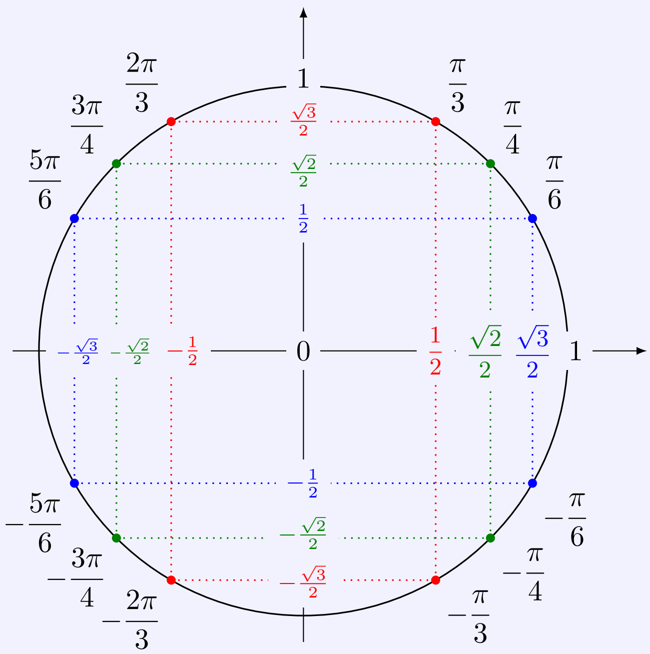
$$\cos(\pi + x) = -\cos x \qquad \sin(\pi + x) = -\sin x$$

$$\cos(-x) = \cos x \qquad \sin(-x) = -\sin x$$

Proposition 3 (Valeurs notables)**.**

x	0	$\frac{\pi}{2}$	π	$\frac{3\pi}{2}$
$\cos x$	1	0	-1	0
$\sin x$	0	1	0	-1





Proposition 4 (Une conséquence du théorème de Pythagore).

$$\forall x \in \mathbb{R} \quad \cos^2 x + \sin^2 x = 1.$$

Proposition 5 (Formules d'addition).

Pour tous réels $a, b \in \mathbb{R}$,

$$\begin{aligned} \cos(a-b) &= \cos a \cos b + \sin a \sin b & \qquad \sin(a-b) &= \sin a \cos b - \sin b \cos a \\ \cos(a+b) &= \cos a \cos b - \sin a \sin b & \qquad \sin(a+b) &= \sin a \cos b + \sin b \cos a \end{aligned}$$

Corollaire 6 (Formules de duplication).

Pour tout $a \in \mathbb{R}$,

$$\cos 2a = 2\cos^2 a - 1 = 1 - 2\sin^2 a \quad \text{et} \quad \sin 2a = 2 \cos a \sin a.$$

La première identité donne les *linéarisations* $\cos^2 a = \frac{1+\cos 2a}{2}$ et $\sin^2 a = \frac{1-\cos 2a}{2}$.

Exemple 7.

- Calculer $\cos(\pi/12)$ et $\sin(\pi/12)$.
- Étant donné un entier $n \in \mathbb{N}^*$, simplifier $\displaystyle\prod_{k=1}^{n} \cos\left(\frac{\pi}{2^{k+1}}\right)$.

Corollaire 8 (Produit de deux cosinus, de deux sinus).

Pour tous réels a, b, $\begin{cases} \cos a \cos b &= \frac{1}{2}\left(\cos(a-b) + \cos(a+b)\right) \\ \sin a \sin b &= \frac{1}{2}\left(\cos(a-b) - \cos(a+b)\right) \\ \sin a \cos b &= \frac{1}{2}\left(\sin(a+b) + \sin(a-b)\right) \end{cases}$

Proposition 9 (Somme et différence de deux cosinus, de deux sinus).

Pour tous réels p, q,

$$\begin{aligned} \cos p + \cos q &= 2\cos\left(\tfrac{p-q}{2}\right)\cos\left(\tfrac{p+q}{2}\right) & \qquad \sin(p) + \sin(q) &= 2\cos\left(\tfrac{p-q}{2}\right)\sin\left(\tfrac{p+q}{2}\right) \\ \cos p - \cos q &= -2\sin\left(\tfrac{p-q}{2}\right)\sin\left(\tfrac{p+q}{2}\right) & \qquad \sin(p) - \sin(q) &= 2\sin\left(\tfrac{p-q}{2}\right)\cos\left(\tfrac{p+q}{2}\right) \end{aligned}$$

Remarque. Dans le cours sur les nombres complexes, on apprendra comment retrouver simplement ces formules en utilisant les nombres e^{ip} et e^{iq}.

3 Égalité de deux cosinus, de deux sinus.

Définition 10 (Congruence modulo α)**.**

On dit que deux réels a et b sont **congrus** (ou plus simplement égaux) modulo α, et on note

$$a \equiv b\ [\alpha]$$

si a et b diffèrent d'un multiple entier de α. Cette définition se récrit

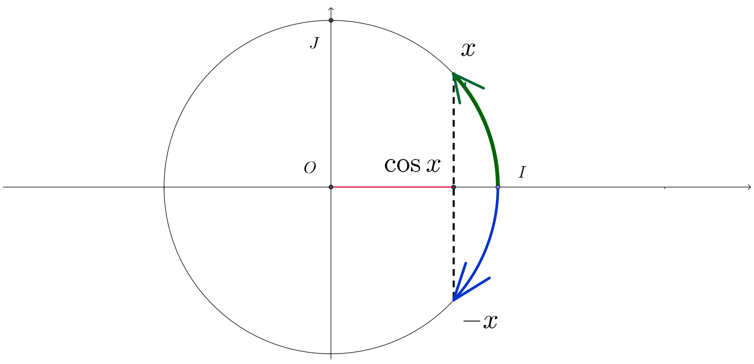
$$a \equiv b\ [\alpha] \iff \exists k \in \mathbb{Z} : a = b + k\alpha.$$

Remarque. Deux réels égaux modulo 2π seront *enroulés* sur le même point : ils représentent le même *angle*.

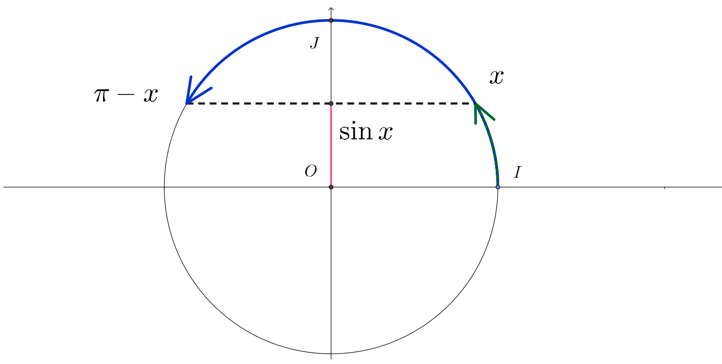
Proposition 11.

Soient x et y deux nombres réels. On a

$$\cos x = \cos y \iff \left\{ \begin{array}{c} x \equiv y\ [2\pi] \\ \text{ou} \\ x \equiv -y\ [2\pi] \end{array} \right. \qquad \text{et} \qquad \sin x = \sin y \iff \left\{ \begin{array}{c} x \equiv y\ [2\pi] \\ \text{ou} \\ x \equiv \pi - y\ [2\pi] \end{array} \right.$$



Égalité de deux cosinus.



Égalité de deux sinus.

Exemple 12.

Résoudre les équations ci-dessous. Représenter les solutions sur un cercle.

$$\sin(2x) = \frac{\sqrt{2}}{2}, \qquad \cos(3x) = \sin x \qquad \cos x + \sqrt{3} \sin x = 1.$$

Exemple 13.

Résoudre l'inéquation $\sin x \geq \dfrac{1}{2}$.

Exercices

$\boxed{\mathbf{4.1}}$ **[♦◊◊]** Résoudre les équations suivantes sur $\mathbb{R}$. Représenter les solutions sur le cercle trigonométrique.

$$\text{a) } \sin 2x = \frac{\sqrt{2}}{2}; \qquad \text{b) } \sin^2(x) = \frac{3}{2}\cos x \qquad \text{c) } \cos x + \sin x = 1$$

$\boxed{\mathbf{4.2}}$ **[♦◊◊]** Résoudre

$$\cos(2x) + \sin(x) > 1.$$

$\boxed{\mathbf{4.3}}$ **[♦♦◊]** Trouver tous les couples (x, y) de $\mathbb{R}^2$ tels que

$$\begin{cases} \sin x \cos y &= \frac{3}{4} \\ \cos x \sin y &= \frac{1}{4} \end{cases}$$

$\boxed{\mathbf{4.4}}$ **[♦♦◊]** Soit n un entier naturel non nul. On pose

$$S_n = \sum_{k=0}^{n} \cos^2\left(\frac{k\pi}{2n}\right).$$

1. À l'aide du changement d'indice $j = n - k$, donner une autre expression de la somme S_n, faisant intervenir la fonction sin.
2. Calculer $S_n + S_n$ et en déduire S_n.

$\boxed{\mathbf{4.5}}$ **[♦♦◊]** Pour $n \in \mathbb{N}^*$, on pose

$$u_n = \sqrt{2 + \sqrt{2 + \cdots \sqrt{2}}} \qquad (n \text{ fois le symbole } \sqrt{\cdot})$$

1. Montrer que $\forall n \in \mathbb{N}^*\ u_n = 2\cos\left(\frac{\pi}{2^{n+1}}\right)$.
2. En déduire $\lim u_n$.

$\boxed{\mathbf{4.6}}$ **[♦♦◊]** Soient α, β et γ les angles au sommet d'un triangle ABC. On suppose que

$$\cos^2\alpha + \cos^2\beta + \cos^2\gamma = 1.$$

Démontrer que ABC est un triangle rectangle.

$\boxed{\mathbf{4.7}}$ **[♦♦♦]** Calculer $\cos\frac{\pi}{7}\cos\frac{2\pi}{7}\cos\frac{4\pi}{7}$.

$\boxed{\mathbf{4.8}}$ **[♦♦♦]**

1. Soit un réel θ et un entier $n \in \mathbb{N}$. Calculer à l'aide d'un télescopage le nombre
$$\sin\left(\frac{\theta}{2}\right)\sum_{k=0}^{n}\cos(k\theta).$$
2. Factoriser la somme $\sum\limits_{k=0}^{n}\cos(k\theta)$ (on distinguera selon les valeurs de θ).

---

5 Nombres complexes

0 Le corps des nombres complexes.

On admet l'existence d'un ensemble de nombres noté $\mathbb{C}$ ainsi que d'une *addition* et d'un *produit* $+$ et $\cdot$:

$$+ : \left\{ \begin{array}{ccc} \mathbb{C}^2 & \to & \mathbb{C} \\ (z,z') & \mapsto & z+z' \end{array} \right. \quad \text{et} \quad \cdot : \left\{ \begin{array}{ccc} \mathbb{C}^2 & \to & \mathbb{C} \\ (z,z') & \mapsto & z \cdot z' \end{array} \right. .$$

Les éléments de $\mathbb{C}$ sont appelés **nombres complexes**.

La construction de $(\mathbb{C}, +, \cdot)$ n'est pas très difficile (ce qui est dur, c'est de construire $\mathbb{R}$!) mais elle est hors-programme. La liste des propriétés ci-dessous est donc admise.

- Les nombres réels sont des nombres complexes : $\mathbb{R} \subset \mathbb{C}$. Dans $\mathbb{C}$, il existe un nombre i tel que

$$i^2 = -1.$$

  Ainsi, l'équation $x^2 = -1$, qui n'a *pas de solutions* dans $\mathbb{R}$, en possède une (au moins...) dans $\mathbb{C}$.

- Tout nombre complexe z s'écrit sous la forme $\boxed{z = a + ib}$, avec $(a, b) \in \mathbb{R}^2$.
  Cette écriture est unique (voir plus bas) : on dit que $a + ib$ est la **forme algébrique** du nombre z.
- Les lois $+$ et $\cdot$ sont commutatives :

$$\forall z, z' \in \mathbb{C} \qquad z + z' = z' + z \quad \text{et} \quad z \cdot z' = z' \cdot z.$$

- Les lois $+$ et $\cdot$ sont associatives :
$$\forall z_1, z_2, z_3 \in \mathbb{C} \qquad (z_1+z_2)+z_3 = z_1+(z_2+z_3) \quad \text{et} \quad (z_1 \cdot z_2)\cdot z_3 = z_1 \cdot (z_2 \cdot z_3).$$
- La loi $\cdot$ est distributive par rapport à $+$:
$$\forall z_1, z_2, z \in \mathbb{C} \qquad (z_1+z_2)\cdot z = z_1 \cdot z + z_2 \cdot z = z \cdot (z_1+z_2).$$
- 0 est neutre pour l'addition et 1 est neutre pour la multiplication :
$$\forall z \in \mathbb{C} \quad 0+z = z = z+0 \quad \text{et} \quad z \times 1 = z = 1 \times z.$$

Méthode (Un premier calcul dans $\mathbb{C}$)**.**

$$(a+ib)\cdot(c+id) = \qquad .$$

- L'ensemble $\mathbb{C} \setminus \{0\}$ sera noté $\mathbb{C}^*$.
Pour tout nombre complexe z non nul, il existe un unique nombre complexe ω tel que $\omega z = z\omega = 1$. Ce nombre sera appelé **inverse** de z et noté z^{-1}. Comme dans $\mathbb{R}$, 0 n'a pas d'inverse dans $\mathbb{C}$.
- Le quotient de deux nombres complexes est défini ainsi : si $(z, z') \in \mathbb{C}^* \times \mathbb{C}$,
$$\frac{z'}{z} := z' \cdot (z)^{-1}.$$
Les égalités suivantes sont vraies pour tous nombres z_1, z_2, z_3 non nuls :
$$\left(\frac{z_1}{z_2}\right)^{-1} = \frac{z_2}{z_1} \qquad \frac{z_1+z_2}{z_3} = \frac{z_1}{z_3} + \frac{z_2}{z_3} \qquad \frac{z_1 \cdot z_2}{z_3} = z_1 \cdot \frac{z_2}{z_3}.$$
- Un produit de nombres complexes est nul si et seulement si l'un des facteurs est nul :
$$\forall z, z' \in \mathbb{C} \quad z \cdot z' = 0 \iff \big(z = 0 \ \text{ ou } \ z' = 0\big).$$
- Un nombre complexe n'a pas de signe. Une inégalité entre nombres complexes non réels n'a <u>aucun sens</u>.
- Les identités démontrées dans le cours Sommes et produits sont vraies pour les nombres complexes (toutes les preuves fonctionnent de la même façon). On a notamment

$$\forall z \in \mathbb{C} \qquad \forall n \in \mathbb{N} \qquad \sum_{k=0}^{n} z^k = \begin{cases} \dfrac{1-z^{n+1}}{1-z} & \text{si } z \neq 1 \\ n+1 & \text{si } z = 1 \end{cases}$$

$$\forall (\alpha,\beta) \in \mathbb{C}^2 \qquad \forall n \in \mathbb{N}^* \qquad \alpha^n - \beta^n = (\alpha-\beta)\sum_{k=0}^{n-1} \alpha^{n-1-k}\beta^k$$

$$\forall (\alpha,\beta) \in \mathbb{C}^2 \qquad \forall n \in \mathbb{N} \qquad (\alpha+\beta)^n = \sum_{k=0}^{n} \binom{n}{k} \alpha^k \beta^{n-k}.$$

Exemple 1.

1. $\forall p \in \mathbb{Z} \quad i^{2p} = (-1)^p$ et $i^{2p+1} = (-1)^p i$. En particulier, $\boxed{\frac{1}{i} = -i}$.
2. Calcul de
$$1+2i+3i^2+4i^3+5i^4, \qquad (1+2i)^2, \qquad (1+i)^3.$$

Exemple 2 (Calcul de l'inverse).

1. Soient $(a,b) \in \mathbb{R}^2 \setminus \{(0,0)\}$. Vérifier que $\dfrac{1}{a+ib} = \dfrac{a-ib}{a^2+b^2}$.
   Le nombre $a-ib$ sera appelé plus loin le conjugué de de $a+ib$ et $\sqrt{a^2+b^2}$ son module.
2. Donner la forme algébrique des nombres $\dfrac{1}{1+i}$ et $\dfrac{2-i}{1-3i}$.

1 Forme algébrique d'un nombre complexe.

1.1 Partie réelle, partie imaginaire.

Proposition-Définition 3.

Soient $a, a', b, b' \in \mathbb{R}$. L'unicité de l'écriture de la forme algébrique d'un nombre complexe donne

$$\boxed{a+ib = a'+ib' \iff \left(a = a' \text{ et } b = b'\right).}$$

$$\text{En particulier,} \qquad a+ib = 0 \iff (a = 0 \text{ et } b = 0)\,.$$

Soit $z = a+ib$ un nombre complexe, avec (a,b) tel que $z = a+ib$.
Le réel a est appelé **partie réelle** de z et noté $\mathrm{Re}(z)$.
Le réel b est appelé **partie imaginaire** de z et noté $\mathrm{Im}(z)$.

Proposition 4 (Réels et imaginaires purs).

$$\forall z \in \mathbb{C} \quad z \in \mathbb{R} \iff \mathrm{Im}(z) = 0.$$

La nullité de la partie réelle de z caractérise quant à elle l'appartenance de z à l'ensemble des **imaginaires purs**, ensemble parfois noté $i\mathbb{R}$.

Proposition 5.

Pour tous $z, z' \in \mathbb{C}$, pour tout $\lambda \in \mathbb{R}$ réel, on a

$$\mathrm{Re}\left(z+z'\right) = \mathrm{Re}(z) + \mathrm{Re}(z') \quad \text{et} \quad \mathrm{Re}\left(\lambda z\right) = \lambda \mathrm{Re}(z).$$

$$\mathrm{Im}\left(z+z'\right) = \mathrm{Im}(z) + \mathrm{Im}(z') \quad \text{et} \quad \mathrm{Im}\left(\lambda z\right) = \lambda \mathrm{Im}(z).$$

Plus généralement, si $z_1, \ldots, z_n \in \mathbb{C}$,

$$\mathrm{Re}\left(\sum_{k=1}^{n} z_k\right) = \sum_{k=1}^{n} \mathrm{Re}(z_k) \quad \text{et} \quad \mathrm{Im}\left(\sum_{k=1}^{n} z_k\right) = \sum_{k=1}^{n} \mathrm{Im}(z_k).$$

« La partie réelle de la somme, c'est la somme des parties réelles ». Idem pour la partie imaginaire.

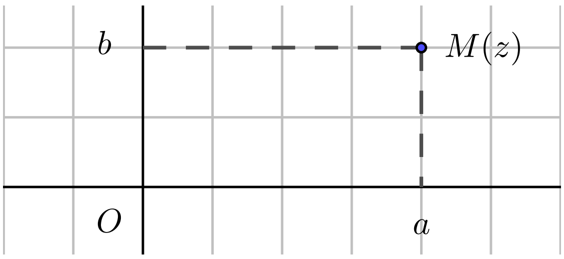
1.2 Représentation : le plan complexe.

On travaille dans cette partie avec un repère orthonormé du plan $(O, \vec{i}, \vec{j})$.

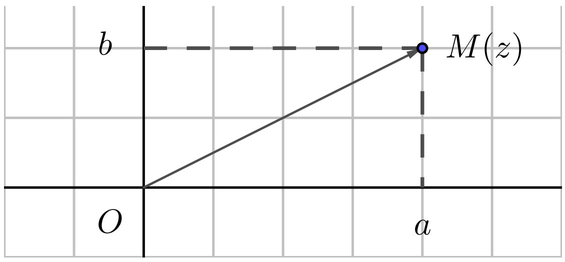
Définition 6.

Soient a et b deux réels.

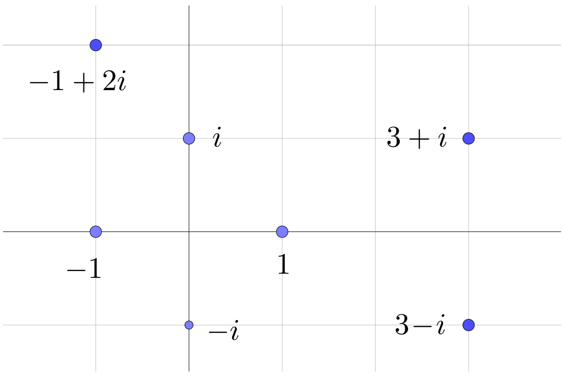
1. Si M est le point du plan de coordonnées (a, b), le nombre $a + ib$ est appelé l'**affixe** de M. Réciproquement, si $z = a + ib$, le point M de coordonnées (a, b) est l'unique point du plan d'affixe z. On pourra le noter $M(z)$.
2. Cette correspondance bijective $z \mapsto M(z)$ entre nombres complexes et points du plan permet d'identifier $\mathbb{C}$ à $\mathbb{R}^2$: on parle de **plan complexe**.
3. L'affixe d'un vecteur $\vec{u}(a, b)$ est le nombre complexe $a + ib$.



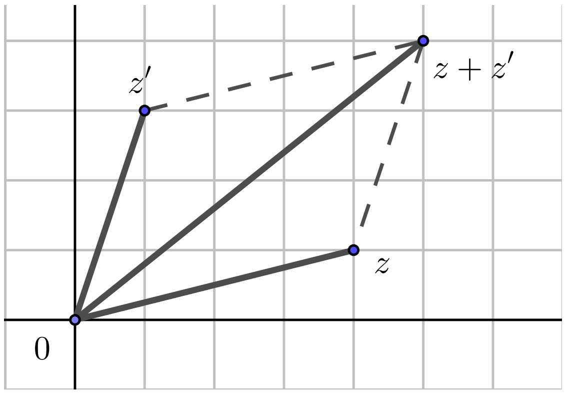
Point d'affixe $z = a + ib$



Vecteur d'affixe $z = a + ib$

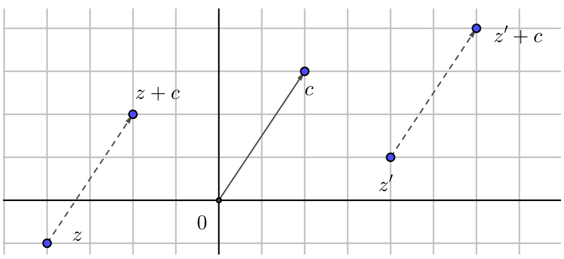


Exemples, en confondant points et affixes

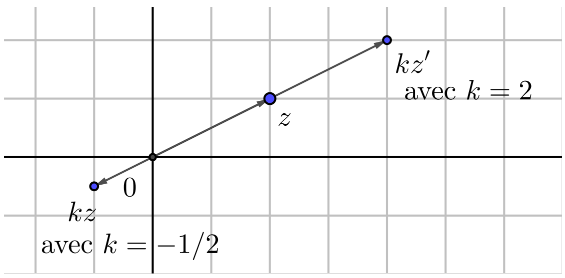


Somme et parallélogramme

Soit $c \in \mathbb{C}$ un nombre complexe. L'application $z \mapsto z + c$ est appelée **translation** de vecteur c.
Soit k un nombre réel. L'application $z \mapsto kz$ est appelée **homothétie** de rapport k.



Translation de vecteur c

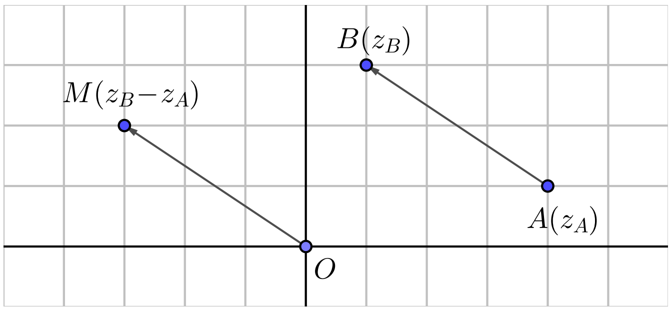


Homothétie de rapport k

Proposition 7.

Si A a pour affixe z_A et B pour affixe z_B, le vecteur $\overrightarrow{AB}$ a pour affixe $z_B - z_A$.

Si $\overrightarrow{u}$ et $\overrightarrow{v}$ sont deux vecteurs d'affixes respectives z et z', et λ et μ deux réels, le vecteur $\lambda\overrightarrow{u}+\mu\overrightarrow{v}$ a pour affixe $\lambda z + \mu z'$.



1.3 Conjugué d'un nombre complexe.

Définition 8.

On appelle **conjugué** d'un nombre complexe z, et on note $\overline{z}$ le nombre

$$\overline{z} := \mathrm{Re}(z) - i\mathrm{Im}(z).$$

Autrement dit,

$$\forall (a,b) \in \mathbb{R} \quad \overline{a+ib} = a - ib.$$

Figure. Soit un point M d'affixe z.
Le point M', d'affixe $\overline{z}$, est le symétrique de M par rapport à l'axe des abscisses.

Proposition 9.

Pour tout $z \in \mathbb{C}$,

$$z + \overline{z} = 2\mathrm{Re}(z) \qquad \text{et} \qquad z - \overline{z} = 2i\mathrm{Im}(z).$$

Ceci permet d'obtenir les caractérisations suivantes :

$$z \in \mathbb{R} \iff z = \overline{z} \qquad \text{et} \qquad z \in i\mathbb{R} \iff z = -\overline{z}.$$

Proposition 10 (Conjugaison et opérations)**.**

Pour tous nombres complexes z et z', on a

a) $\overline{\overline{z}} = z$ c) $\overline{z \cdot z'} = \overline{z} \cdot \overline{z'}$

b) $\overline{z + z'} = \overline{z} + \overline{z'}$ d) si $z' \neq 0$, $\overline{\left(\frac{z}{z'}\right)} = \frac{\overline{z}}{\overline{z'}}$.

Par conséquent, l'application $z \mapsto \overline{z}$ est $\mathbb{R}$-linéaire, c'est à dire que pour tous nombres $z, z' \in \mathbb{C}$, et tous <u>réels</u> λ, μ, on a

$$\overline{\lambda z + \mu z'} = \lambda \overline{z} + \mu \overline{z'}.$$

« Le conjugué de la somme, c'est la somme des conjugués ». Marche avec le produit et le quotient.

1.4 Module d'un nombre complexe.

Définition 11.

Pour tout nombre complexe z, on appelle **module** de z et on note $|z|$ le nombre réel positif

$$|z| := \sqrt{\mathrm{Re}(z)^2 + \mathrm{Im}(z)^2}.$$

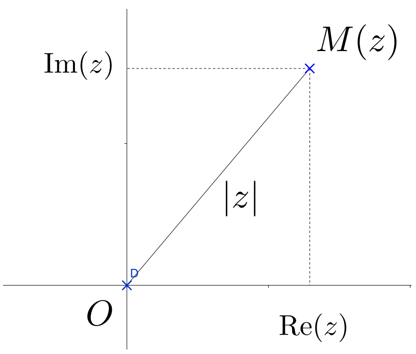
Exemple 12.

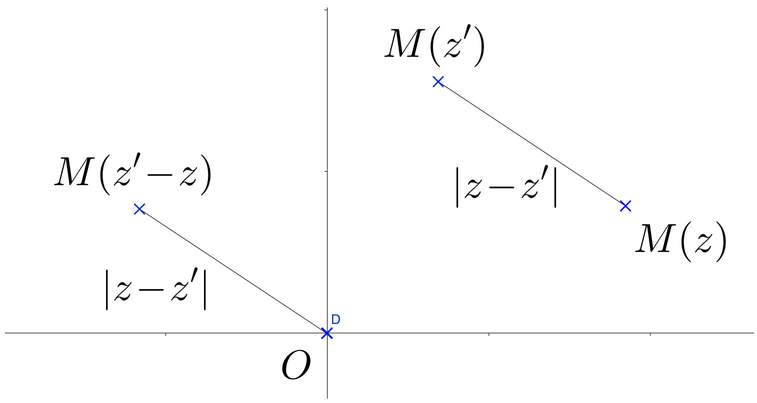
$|i| =$ $|2 + 3i| =$.

Le module d'un nombre réel a vaut $\sqrt{a^2 + 0^2}$: c'est sa valeur absolue.

Figure.

- Si M est un point du plan d'affixe z, alors $|z|$ est la longueur du segment $[OM]$.
- Si M et M' sont deux points du plan d'affixes z et z', alors $|z - z'|$ est la distance entre M et M'.





Confondons le point et son affixe pour énoncer l'idée importante suivante :

$$\boxed{\text{pour } z, z' \in \mathbb{C},\ |z - z'| \text{ est la } \textbf{distance} \text{ entre } z \text{ et } z'.}$$

Continuons de confondre point et affixe. Soit $a \in \mathbb{C}$ et r un nombre réel positif. Les ensembles

$$\{z \in \mathbb{C} \mid |z-a| = r\} \qquad \text{et} \qquad \{z \in \mathbb{C} \mid |z-a| \leq r\}$$

sont respectivement le **cercle** et le **disque** de centre a et de rayon r.

Exemple 13 (Module, cercles et disques)**.**

Représenter l'ensemble

$$\{z \in \mathbb{C} \mid |z-1| = 1 \ \text{ et } \ |z+1| \leq 2\}.$$

Proposition 14.

Pour tout nombre complexe z,

a) $|z| = 0 \iff z = 0$.

b) $|-z| = |z| = |\overline{z}|$.

c) $|\mathrm{Re}(z)| \leq |z|$ et $|\mathrm{Im}(z)| \leq |z|$.

d) $\mathrm{Re}(z) = |z| \iff z \in \mathbb{R}_+$.

Proposition 15 (Propriétés multiplicatives du module)**.**

Pour tous nombres complexes z et z', on a

a) $|z|^2 = z \cdot \overline{z}$ *b)* $|z \cdot z'| = |z| \cdot |z'|$, *c)* si $z' \neq 0$, $\left|\dfrac{z}{z'}\right| = \dfrac{|z|}{|z'|}$ *d)* si $z \neq 0$, $\dfrac{1}{z} = \dfrac{\overline{z}}{|z|^2}$.

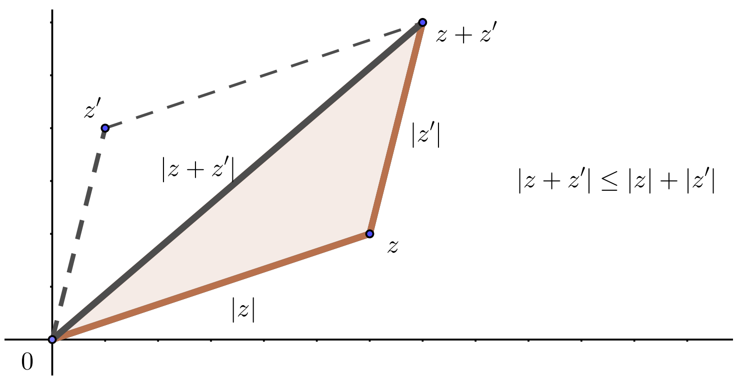
« Le module du produit, c'est le produit des modules ». Idem pour le quotient mais... attention à la somme !

Théorème 16 (Inégalité triangulaire)**.**

Pour tous nombres complexes z et z', on a

$$|z+z'| \leq |z| + |z'|.$$

Il y a égalité si et seulement si $z = 0$ ou il existe un nombre réel <u>positif</u> λ tel que $z' = \lambda z$.



Corollaire 17.

1. $\forall (z,z') \in \mathbb{C}^2 \quad |z - z'| \leq |z| + |z'|$.
2. $\forall (z,z') \in \mathbb{C}^2 \quad ||z| - |z'|| \leq |z - z'|$.
3. $\forall n \in \mathbb{N}^*, \quad \forall (z_1, \dots, z_n) \in \mathbb{C}^n, \qquad \left|\sum_{k=1}^{n} z_k\right| \leq \sum_{k=1}^{n} |z_k|$.

2 Forme trigonométrique d'un nombre complexe.

2.1 Paramétrisation du cercle trigonométrique.

Définition 18.

On note $\mathbb{U}$ l'ensemble des nombres complexes de module 1 :

$$\mathbb{U} = \{\omega \in \mathbb{C} \mid |\omega| = 1.\}.$$

Si on identifie $\mathbb{C}$ avec le plan muni d'un repère orthonormé, alors $\mathbb{U}$ est le cercle trigonométrique.

Proposition 19.

Tous les nombres de $\mathbb{U}$ sont non nuls, donc inversibles, et

$$\forall \omega \in \mathbb{U} \quad \omega^{-1} = \overline{\omega}.$$

Définition 20.

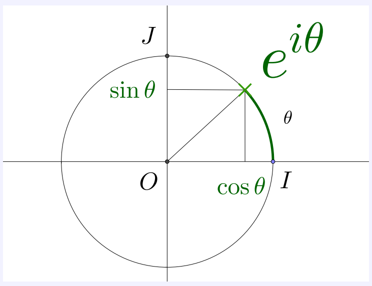
Soit $\theta \in \mathbb{R}$. On note $e^{i\theta}$ (« exponentielle de $i\theta$ ») le nombre complexe de module 1 suivant :

$$\boxed{e^{i\theta} := \cos\theta + i \sin\theta.}$$

Par définition même de $e^{i\theta}$, on a $\cos\theta = \mathrm{Re}\left(e^{i\theta}\right)$ et $\sin\theta = \mathrm{Im}\left(e^{i\theta}\right)$.

Proposition 21 (Paramétrisation de $\mathbb{U}$).

$$\forall z \in \mathbb{C} \quad z \in \mathbb{U} \iff \exists \theta \in \mathbb{R} \ z = e^{i\theta}.$$



Par conséquent,

$$\mathbb{U} = \left\{ e^{i\theta} \mid \theta \in \mathbb{R} \right\}.$$

Exemple 22 (Valeurs notables)**.**

$$-1 = e^{i\pi}, \qquad 1 = e^{i0} = e^{2i\pi}, \qquad i = e^{i\frac{\pi}{2}}, \qquad -i = e^{-i\frac{\pi}{2}}$$
$$\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i = e^{i\frac{\pi}{4}}, \qquad \frac{1}{2} + \frac{\sqrt{3}}{2}i = e^{i\frac{\pi}{3}}, \qquad \frac{\sqrt{3}}{2} + \frac{1}{2}i = e^{i\frac{\pi}{6}}.$$

Le rapport entre les nombres $e^{i\theta}$ qui viennent d'être définis et la fonction exponentielle définie sur $\mathbb{R}$ restera floue dans ce cours, faute d'une définition rigoureuse de l'exponentielle comme somme de série. Nous démontrons néanmoins dans la proposition ci-dessous que que ces deux applications

$$: \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R}_+^* \\ x & \mapsto & e^x \end{array} \right. \qquad \text{et} \qquad : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{U} \\ \theta & \mapsto & e^{i\theta} \end{array} \right. .$$

possèdent un point commun : la propriété de morphisme.

Proposition 23 (Propriété de morphisme pour $e^{i\cdot}$)**.**

$$\boxed{\forall \theta, \theta' \in \mathbb{R} \qquad e^{i(\theta+\theta')} = e^{i\theta} \cdot e^{i\theta'}}.$$

Par conséquent, pour tout θ, θ' réels

$$\left(e^{i\theta}\right)^{-1} = e^{-i\theta} = \overline{e^{i\theta}}, \quad e^{i(\theta-\theta')} = \frac{e^{i\theta}}{e^{i\theta'}} \quad \text{et} \quad \forall k \in \mathbb{Z} \quad (e^{i\theta})^k = e^{ik\theta}.$$

Proposition 24.

$$\forall (\theta, \theta') \in \mathbb{R}^2 \quad e^{i\theta} = e^{i\theta'} \iff \theta = \theta' \ [2\pi].$$

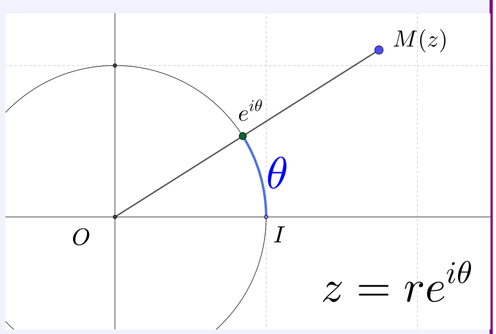
2.2 Forme trigonométrique d'un nombre complexe non nul.

Proposition-Définition 25.

Tout nombre complexe z non nul peut s'écrire sous la forme

$$\boxed{z = re^{i\theta},} \text{ où } r \in \mathbb{R}_+^* \text{ et } \theta \in \mathbb{R}.$$

- Le nombre r est le module de z,
- et on appelle θ *un* **argument** de z.
- On dit alors que z est écrit **sous forme trigonométrique**.



Dans le plan muni d'un repère orthonormé direct, si O, I et M sont les points d'affixes 0, 1, z ($z \neq 0$), et si θ est *un* argument de z, alors peut être considéré comme une **mesure de l'angle orienté** $(\overrightarrow{OI}, \overrightarrow{OM})$.

Méthode (Passer de la forme algébrique à la forme trigonométrique).

Pour mettre un nombre complexe non nul sous forme trigonométrique il suffit de mettre son module en facteur. On va peut-être reconnaître un argument connu ($\frac{\pi}{3}, \frac{\pi}{4}$...).

Exemple 26.

1. Mettre les nombres suivants sous forme trigonométrique (on précisera bien le module et un argument)

$$1+i, \qquad 1-i, \qquad \sqrt{3}+i, \qquad -2.$$

2. Justifier que $1+2i$ possède un argument dans l'intervalle $[\frac{\pi}{3}, \frac{\pi}{2}]$.

Proposition 27 (Égalité de formes trigonométriques : presque-unicité de l'écriture).

$$\forall r, r' \in \mathbb{R}_+^* \;\; \forall \theta, \theta' \in \mathbb{R} \qquad re^{i\theta} = r'e^{i\theta'} \iff \begin{cases} r = r' \\ \theta \equiv \theta' \; [2\pi] \end{cases}$$

Exemple 28 (Résoudre un problème multiplicatif avec la forme trigonométrique).

Résoudre sur $\mathbb{C}$ l'équation

$$z^3 = -4|z|.$$

Définition 29.

Parmi l'infinité d'arguments d'un même nombre complexe non nul, un seul appartient à l'intervalle $]-\pi, \pi]$. On l'appelle **argument principal** de z et on le note $\arg(z)$.

Proposition 30.

Soit $z \in \mathbb{C}^*$. Alors

$$z \in \mathbb{R} \iff (\arg(z) = 0 \;\text{ ou }\; \arg(z) = \pi)\,; \qquad z \in i\mathbb{R} \iff \left(\arg(z) = \pm\frac{\pi}{2}\right).$$

Proposition 31.

Soient z et z' dans $\mathbb{C}^*$. On a

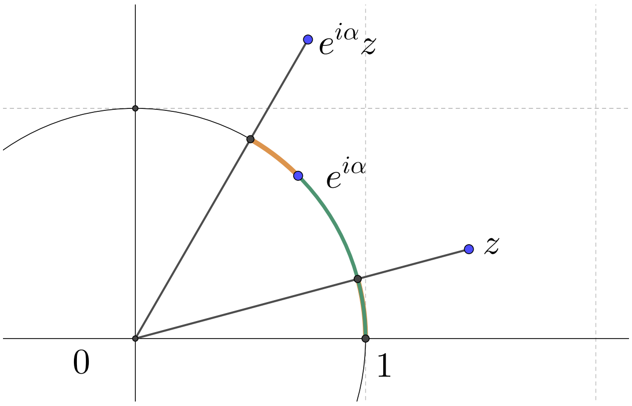
$$\arg(zz') \equiv \arg(z) + \arg(z') \; [2\pi] \qquad \text{et} \qquad \arg\left(\frac{z}{z'}\right) \equiv \arg(z) - \arg(z') \; [2\pi]$$

Soient $r > 0$ et $\theta, \alpha \in \mathbb{R}$. Multiplions le nombre $z = re^{i\theta}$ par $e^{i\alpha}$. On obtient $re^{i(\theta+\alpha)}$.
On voit que l'application $z \mapsto e^{i\alpha}z$ est la **rotation** d'angle α et de centre 0 (dessin plus bas).

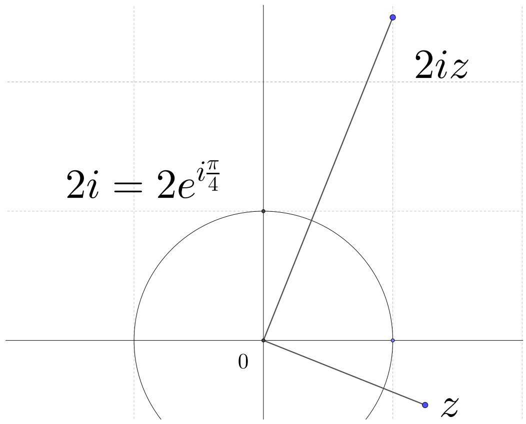
Plus généralement, on est désormais capable d'interpréter géométriquement le produit de deux nombres complexes. La proposition ci-dessous est énoncée en confondant les points et leurs affixes.

Proposition 32.

Soit $(r, \alpha) \in \mathbb{R}_+^* \times \mathbb{R}$ et $a = re^{i\alpha}$. L'application $z \mapsto az$ est la composée (commutative) de
- l'homothétie de centre 0 et de rapport r,
- la rotation de centre 0 et de rapport α.



Effet d'une multiplication par $e^{i\alpha}$



Effet d'une multiplication par $2i$

2.3 Applications à la trigonométrie

Certains des résultats du paragraphe 2.1 se récrivent sous la forme de formules que nous donnons ci-dessous.

Proposition 33 (Formule d'Euler/Formule de Moivre)**.**

Les identités suivantes sont appelées *formules d'Euler* :

$$\forall \theta \in \mathbb{R} \qquad \cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2} \qquad \sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}.$$

La relation suivante est appelée *formule de Moivre* :

$$\forall \theta \in \mathbb{R} \quad \forall n \in \mathbb{N} \quad (\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta).$$

Preuve.
Les formules d'Euler découlent directement de la définition de $e^{i\theta}$, pour θ réel :

$$e^{i\theta} + e^{-i\theta} = e^{i\theta} + \overline{e^{i\theta}} = 2\mathrm{Re}(e^{i\theta}) = 2\cos(\theta) \qquad e^{i\theta} - e^{-i\theta} = e^{i\theta} - \overline{e^{i\theta}} = 2i\mathrm{Im}(e^{i\theta}) = 2i\sin(\theta).$$

Quant à la formule de Moivre, il s'agit juste de la propriété de morphisme : pour $\theta \in \mathbb{R}$ et $n \in \mathbb{N}$

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

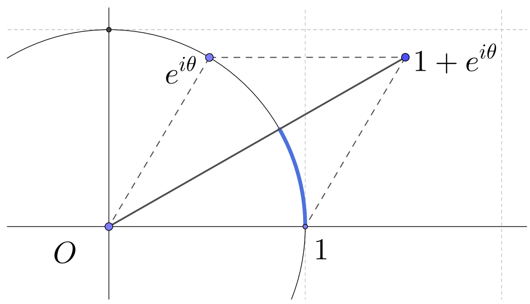
et on écrit la définition de $e^{i\theta}$ et $e^{in\theta}$. $\square$

Méthode (Factorisation par l'argument moitié).

Cette factorisation permet de faire apparaître une formule d'Euler :

$$1+e^{i\theta}=e^{i\frac{\theta}{2}}\big(\underbrace{e^{-i\theta/2}+e^{i\theta/2}}_{=2\cos\frac{\theta}{2}}\big)=2\cos\left(\frac{\theta}{2}\right)e^{i\frac{\theta}{2}}.$$

$$1-e^{i\theta}=e^{i\frac{\theta}{2}}\big(\underbrace{e^{-i\theta/2}-e^{i\theta/2}}_{=-2i\sin\frac{\theta}{2}}\big)=-2i\sin\left(\frac{\theta}{2}\right)e^{i\frac{\theta}{2}}.$$



L'argument moitié sur un dessin

Méthode (Généralisation : factorisation par l'argument moyen).

Pour factoriser la somme ou la différence de e^{ia} et e^{ib}, retenons qu'on peut factoriser par $e^{i\frac{a+b}{2}}$.

$$e^{ia}+e^{ib}=e^{i\frac{a+b}{2}}\big(\underbrace{e^{i\frac{a-b}{2}}+e^{i\frac{b-a}{2}}}_{=2\cos\frac{a-b}{2}}\big)=2\cos\left(\frac{a-b}{2}\right)e^{i\frac{a+b}{2}}.$$

$$e^{ia}-e^{ib}=e^{i\frac{a+b}{2}}\big(\underbrace{e^{i\frac{a-b}{2}}-e^{i\frac{b-a}{2}}}_{=2i\sin\frac{a-b}{2}}\big)=2i\sin\left(\frac{a-b}{2}\right)e^{i\frac{a+b}{2}}.$$

Exemple 34 (Somme de cos, somme de sin).

Soient $p,q\in\mathbb{R}$. On retrouve les égalités :

$$\begin{aligned}\cos p+\cos q &= 2\cos\left(\tfrac{p-q}{2}\right)\cos\left(\tfrac{p+q}{2}\right) & \sin(p)+\sin(q) &= 2\cos\left(\tfrac{p-q}{2}\right)\sin\left(\tfrac{p+q}{2}\right)\\ \cos p-\cos q &= -2\sin\left(\tfrac{p-q}{2}\right)\sin\left(\tfrac{p+q}{2}\right) & \sin(p)-\sin(q) &= 2\sin\left(\tfrac{p-q}{2}\right)\cos\left(\tfrac{p+q}{2}\right)\end{aligned}$$

Exemple 35.

Pour $\theta\in\mathbb{R}\setminus\{2k\pi,k\in\mathbb{Z}\}$, on établit les formules

$$\sum_{k=0}^{n}\cos(k\theta)=\frac{\sin\left(\frac{(n+1)\theta}{2}\right)\cos\left(\frac{n\theta}{2}\right)}{\sin\left(\frac{\theta}{2}\right)}\quad\text{et}\quad\sum_{k=0}^{n}\sin(k\theta)=\frac{\sin\left(\frac{(n+1)\theta}{2}\right)\sin\left(\frac{n\theta}{2}\right)}{\sin\left(\frac{\theta}{2}\right)}$$

Méthode (Linéarisation des puissances de cos et sin).

Soient p et q deux entiers naturels. Pour *linéariser* $(\cos\theta)^p\,(\sin\theta)^q$, on peut toujours :
- transformer $\cos\theta$ et $\sin\theta$ par les formules d'Euler ;
- développer grâce à la formule du binôme de Newton ;
- regrouper les exponentielles conjuguées $e^{ik\theta}$ et $e^{-ik\theta}$;
- reconnaître des termes $\cos(k\theta)$ et $\sin(k\theta)$ $(k \in \mathbb{N})$ par les formules d'Euler.

On peut ainsi transformer $(\cos\theta)^p\,(\sin\theta)^q$ en une combinaison linéaire de termes $\cos(k\theta)$ et $\sin(k\theta)$, où $k \in \mathbb{N}$.

Exemple 36.

Linéariser $(\cos\theta)^4$, $(\sin\theta)^3$ et $(\cos\theta)^3\sin\theta$. Calculer $\displaystyle\int_0^\pi (\cos x)^4 \mathrm{d}x$.

Méthode (« Délinéarisation » : exprimer $\cos(n\theta)$ et $\sin(n\theta)$ en fonction de $\cos\theta$ et $\sin\theta$).

On peut toujours
- écrire la formule de Moivre :

$$\cos(n\theta) + i\sin(n\theta) = (\cos\theta + i\sin\theta)^n\,.$$

- développer par la formule du binôme de Newton ;
- identifier les parties réelles et imaginaires.

On exprime ainsi $\cos(n\theta)$ et $\sin(n\theta)$ en fonction de $\cos\theta$ et $\sin\theta$.

En utilisant la relation $\cos^2\theta + \sin^2\theta = 1$, on poursuit les simplifications.

On obtiendra toujours deux polynômes T_n et U_{n-1} tels que

$$\begin{aligned}\cos(n\theta) &= T_n(\cos\theta)\\ \sin(n\theta) &= (\sin\theta)U_{n-1}(\cos\theta).\end{aligned}$$

Exemple 37.

Exprimer $\cos 3\theta$ et $\sin 5\theta$ en fonction de $\cos\theta$ et de $\sin\theta$.

On termine par une dernière application de la formule d'Euler.

Méthode (Amplitude et retard de phase d'une combinaison linéaire de signaux).

Transformation de $a\cos t + b\sin t$ en $A\cos(t+\varphi)$, où $A = \sqrt{a^2+b^2}$.
- On écrit $a\cos t + b\sin t$ sous la forme $ze^{it} + \overline{z}e^{-it}$ (formules d'Euler).
- On écrit z sous forme trigonométrique : $z = \rho e^{i\varphi}$.
- Encore la formule d'Euler pour faire apparaître $\cos(t+\varphi)$.

2.4 Exponentielle d'un nombre complexe.

Définition 38.

Soit $z \in \mathbb{C}$. On appelle **exponentielle** du nombre z et on note $\exp(z)$ ou e^z le nombre complexe

$$\exp(z) := e^{\mathrm{Re}(z)} \cdot e^{i\mathrm{Im}(z)}.$$

Proposition 39.

$$\forall z \in \mathbb{C} \qquad |e^z| = e^{\mathrm{Re}(z)} \quad \text{et} \quad \arg(e^z) = \mathrm{Im}(z)\ [2\pi].$$

Pour tout z, on déduit de la proposition précédente que e^z n'est jamais nul (son module est strictement positif). On peut donc voir l'exponentielle complexe comme l'application

$$\exp : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C}^* \\ z & \mapsto & e^z \end{array} \right.$$

Proposition 40.

$$\forall z, z' \in \mathbb{C} \qquad \exp(z+z') = \exp(z)\exp(z'),$$

ce qui justifie la notation "puissance" $\exp(z) = e^z$.

Par conséquent, pour tout z, z' complexes

$$\overline{e^z} = e^{\overline{z}}, \qquad (e^z)^{-1} = e^{-z}, \qquad e^{z-z'} = \frac{e^z}{e^{z'}}.$$

$$\forall z, z' \in \mathbb{C} \quad e^z = e^{z'} \iff z - z' \in 2i\pi\mathbb{Z}.$$

Exemple 41.

Soit $a \in \mathbb{C}^*$. Résolution de l'équation $e^z = a$.

Preuve.
On résout l'équation en se ramenant à l'égalité de deux formes trigonométrique.
Écrivons $a = \rho e^{i\alpha}$, avec $(\rho, \alpha) \in \mathbb{R}_+^* \times \mathbb{R}$ et considérons un nombre $z \in \mathbb{C}$. On a

$$e^z = a \iff e^{\mathrm{Re}(z)} \cdot e^{i\mathrm{Im}(z)} = \rho e^{i\alpha} \iff \left\{ \begin{array}{l} e^{\mathrm{Re}(z)} = \rho \\ \mathrm{Im}(z) \equiv \alpha\ [2\pi] \end{array} \right. \iff \left\{ \begin{array}{l} \mathrm{Re}(z) = \ln(\rho) \\ \exists k \in \mathbb{Z} \mid \mathrm{Im}(z) = \alpha + 2k\pi \end{array} \right.$$

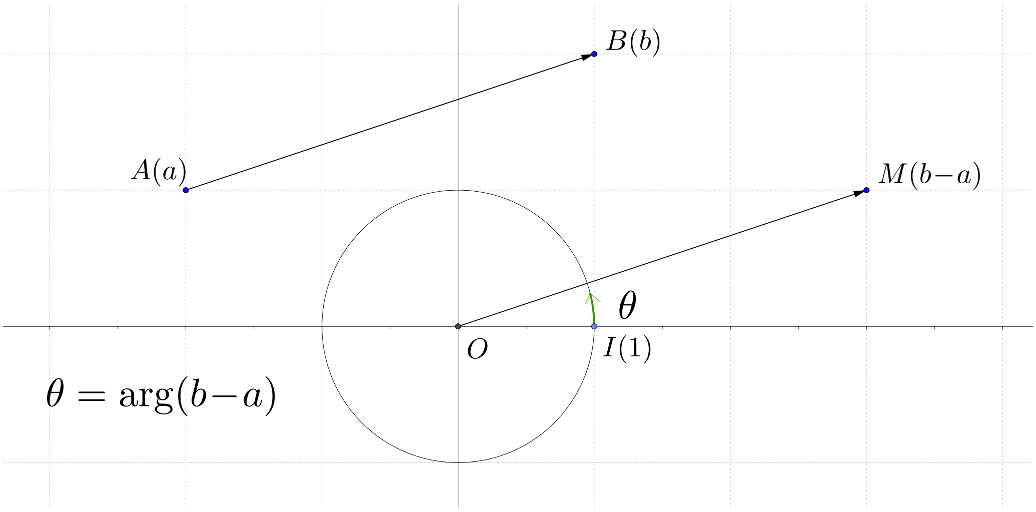
L'ensemble des solutions de l'équation est donc

$$\{\ln(\rho) + i\alpha + 2ik\pi \mid k \in \mathbb{Z}\}.$$

□

2.5 Compléments de géométrie.

On travaille ici dans le plan muni d'un repère orthonormé direct $(O, \vec{i}, \vec{j})$. Le point O a pour affixe 0 et on note I le point d'affixe 1. On rappelle que si A et B sont deux points du plan d'affixes respectives a et b, on appelle **affixe du vecteur** $\overrightarrow{AB}$ le nombre complexe $b-a$. Il s'agit de l'affixe du point M tel que $\overrightarrow{OM} = \overrightarrow{AB}$.



$$\|\overrightarrow{AB}\| = |b-a|,$$

$\arg(b-a)$ est une mesure de l'angle orienté $(\overrightarrow{OI}, \overrightarrow{OM})$.

Alignement, parallélisme, orthgonalité.

Proposition 42 (Quatre points dans le plan)**.**

Soient A, B, C, D quatre points du plan distincts deux à deux, d'affixes respectives a, b, c et d.

$$\left|\frac{d-c}{b-a}\right| = \frac{\|\overrightarrow{CD}\|}{\|\overrightarrow{AB}\|}$$

Le nombre $\arg\left(\frac{d-c}{b-a}\right)$ est une mesure de l'angle orienté $(\overrightarrow{AB}, \overrightarrow{CD})$.

Corollaire 43.

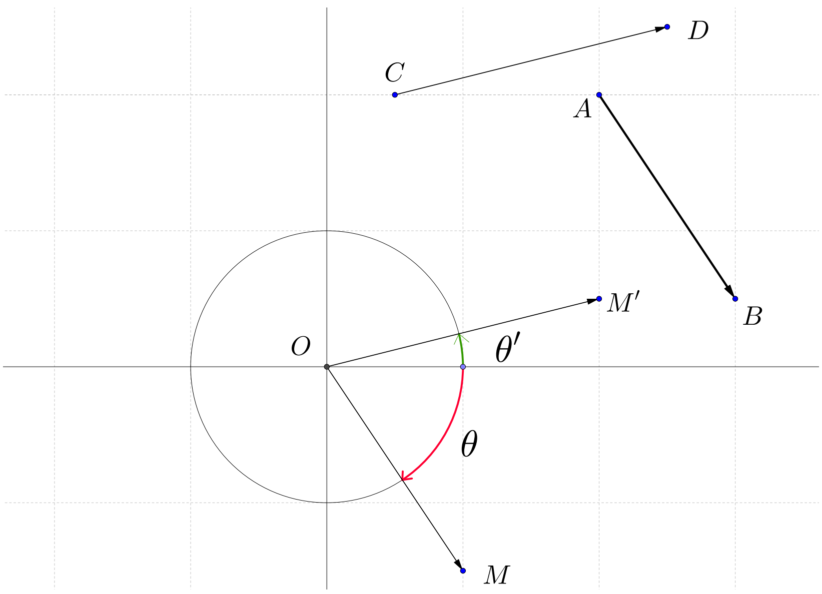
Soient A, B, C, D quatre points du plan distincts deux à deux d'affixes a, b, c et d.

- $(AB) /\!/ (CD) \iff \dfrac{d-c}{b-a} \in \mathbb{R}$.
- En particulier A, B et C sont alignés ssi $\dfrac{c-a}{b-a} \in \mathbb{R}$.
- $(AB) \perp (CD) \iff \dfrac{d-c}{b-a} \in i\mathbb{R}$.

Preuve de la proposition 42. Il faudrait mettre le mot preuve entre guillemets ici puisque la notion d'angle orienté n'a pas été définie rigoureusement...

Notons $\theta = \arg(b-a)$. C'est une mesure de l'angle orienté $(\overrightarrow{OI}, \overrightarrow{OM})$ où $\overrightarrow{OM} = \overrightarrow{AB}$.
Notons $\theta' = \arg(d-c)$. C'est une mesure de l'angle orienté $(\overrightarrow{OI}, \overrightarrow{OM'})$ où $\overrightarrow{OM'} = \overrightarrow{CD}$.
Le nombre $\theta' - \theta$ est (cf. figure) une mesure de l'angle $(\overrightarrow{OM}, \overrightarrow{OM'})$, donc de l'angle $(\overrightarrow{AB}, \overrightarrow{CD})$ On peut désormais conclure en écrivant

$$\theta' - \theta = \arg(d-c) - \arg(b-a) \equiv \arg\left(\frac{d-c}{b-a}\right) [2\pi].$$



$\square$

Preuve du corollaire 43.

Les droites (AB) et (CD) sont parallèles si et seulement si $\overrightarrow{AB}$ et $\overrightarrow{CD}$ sont colinéaires. Cela arrive si et seulement si 0 est une mesure de l'angle orienté $(\overrightarrow{AB}, \overrightarrow{CD})$ (vecteurs colinéaires, de même sens) ou si π en est une (vecteurs colinéaires, de sens opposé). On a donc

$$(AB) \mathbin{/\!/} (CD) \iff \arg\left(\frac{d-c}{b-a}\right) = 0 \ \text{ ou } \pi \iff \frac{d-c}{b-a} \in \mathbb{R}.$$

En particulier, ceci donne une condition d'alignement pour trois points A, B et C distincts deux à deux, car A, B, C sont alignés ssi $(AB) \mathbin{/\!/} (AC)$.

Et pour l'orthogonalité ? Les droites (AB) et (CD) sont perpendiculaires si et seulement si les vecteurs $\overrightarrow{AB}$ et $\overrightarrow{CD}$ sont orthogonaux, c'est à dire si $\frac{\pi}{2}$ ou $-\frac{\pi}{2}$ est une mesure de l'angle orienté $(\overrightarrow{AB}, \overrightarrow{CD})$. On a donc

$$(AB) \perp (CD) \iff \arg\left(\frac{d-c}{b-a}\right) = \frac{\pi}{2} \ \text{ ou } -\frac{\pi}{2} \iff \frac{d-c}{b-a} \in i\mathbb{R}.$$

$\square$

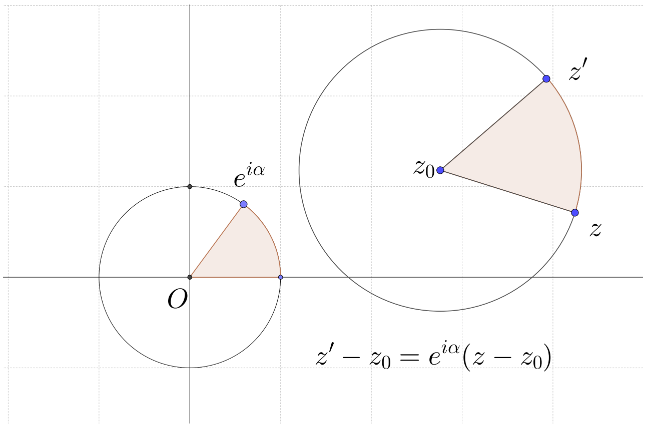
Rotations.

Proposition 44.

Soit M_0 un point du plan d'affixe $z_0 \in \mathbb{C}$ et $\alpha \in \mathbb{R}$.
Soient M et M' deux points du plan d'affixes respectives z et z'.

Le point M' est l'image de M par la rotation de centre M_0 et d'angle α si et seulement si

$$z' - z_0 = e^{i\alpha}(z - z_0).$$



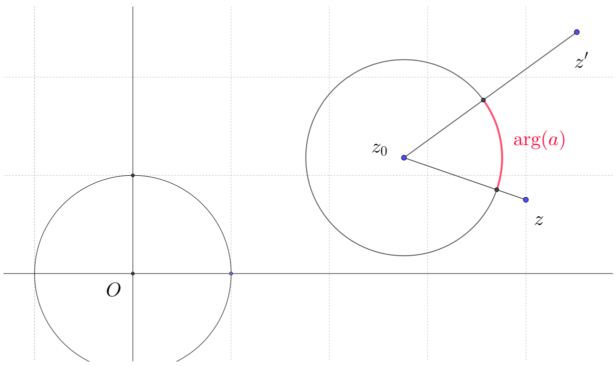
Simitudes directes du plan.

Méthode (Étude de $z \mapsto az + b$ lorsque $a \notin \{0,1\}$.)**.**

Soient a et b deux nombres complexes. On suppose <u>a non nul et différent de 1</u>.
Soit $f : z \mapsto az + b$. Elle possède un unique *point fixe* $z_0 = \frac{b}{1-a}$.
Pour tout $z, z' \in \mathbb{C}$, on a

$$z' = az + b \iff z' - z_0 = a(z - z_0).$$

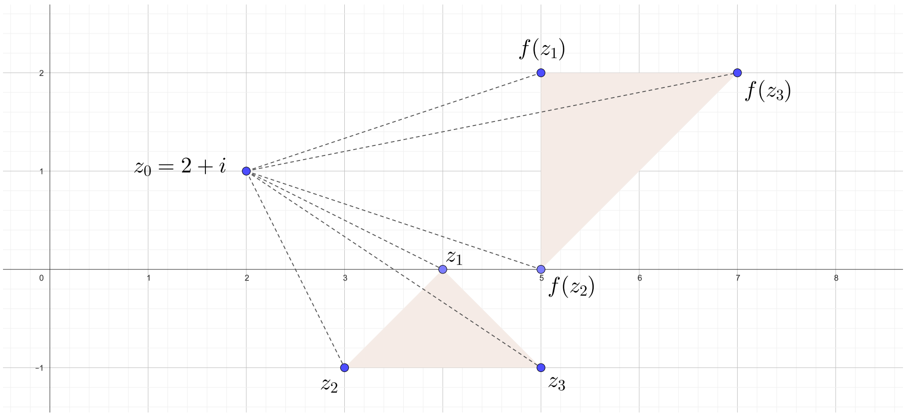
Le point z' se déduit donc de z par la composée de l'homothétie de centre z_0 et de rapport $|a|$ avec la rotation de centre z_0 et d'angle $\arg(a)$.



Remarque. Pour $b \in \mathbb{C}$ donné, l'application $z \mapsto z + b$ est sans point fixe si $b \neq 0$. C'est translation de vecteur b.

Exemple 45.

Étude de $f : z \mapsto (1+i)z + (1-2i)$.



Solution.
Déterminons d'abord le point fixe de f. L'équation $f(z) = z$ a pour unique solution le complexe $z_0 = 2+i$. Puisque $1+i = \sqrt{2}e^{i\frac{\pi}{4}}$, la transformation f se comprend comme la composée de l'homothétie de rapport $\sqrt{2}$ et de centre z_0, et de la rotation de centre z_0 et d'angle $\frac{\pi}{4}$.

□

Remarque.

- Les applications de la forme $z \mapsto az+b$ avec $a \neq 0$ sont appelées **similitudes directes**. Ce sont les applications qui transforment les figures du plan en une figure *semblable* de même "forme" en agrandissant ou rétrécissant sa taille, et en conservant son orientation (d'où le *directe*).
- Les applications de la forme $z \mapsto a\overline{z}+b$, avec $a \neq 0$, sont appelées similitudes indirectes. Elles transforment une figure en une figure semblable, en changeant l'orientation (la conjugaison correspondant à une symétrie). On n'en dira pas plus : seules les similitudes directes figurent à notre programme.

Ci-dessous, des figures, dont certaines sont *semblables* (from Wikipedia).

Effet d'une similiture directe ou indirecte

3 Équations algébriques.

Soient $n \in \mathbb{N}$ et $a_0, \dots, a_n$ des nombres complexes. L'équation

$$\boxed{a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0 = 0},$$

d'inconnue $z \in \mathbb{C}$, est appelée **équation algébrique** : elle s'écrit seulement avec des sommes et des produits. On parle aussi d'équation **polynomiale** puisque l'application $z \mapsto \sum_{k=0}^{n} a_k z^k$ est appelée polynôme.

Dans le cours sur les polynômes, nous énoncerons le théorème de d'Alembert-Gauss (ou théorème fondamental de l'algèbre) qui affirme que si $a_1, \dots, a_n$ ne sont pas tous nuls, l'équation ci-dessus possède au moins une solution dans $\mathbb{C}$.

Prenons par exemple l'équation $x^6 + 2x^2 + 3 = 0$. On peut vite voir qu'elle ne possède pas de solution réelle. En effet, pour tout x réel, $x^6 + 2x^2 + 3 \geq 3 > 0$. Le théorème de d'Alembert-Gauss nous apprend que dans $\mathbb{C}$, il y a une solution. Mais il ne nous dit pas comment la trouver ! Il n'existe d'ailleurs pas de méthode générale.

Dans cette partie, on va s'intéresser à des équations algébriques particulières et importantes, pour lesquelles on a une méthode de résolution.

3.1 Racines carrées d'un nombre complexe.

Rappelons que <u>la</u> racine carrée d'un nombre réel positif a est <u>le</u> nombre réel positif dont le carré vaut a. Il est noté $\sqrt{a}$. On réservera le symbole $\sqrt{\ }$ pour la racine carrée d'un nombre *réel positif*.

Définition 46.

Soit $a \in \mathbb{C}$. Une **racine carrée** de a est un nombre complexe z tel que $z^2 = a$.

Exemple. Racines carrées d'un nombre réel positif. Racines carrées d'un nombre réel négatif.

Proposition 47.

Tout nombre complexe non nul a exactement deux racines carrées et elles sont opposées.

⚠ Une écriture du type « $\sqrt{1+i}$ » n'a <u>aucun sens</u> : le symbole radical est réservé pour les nombres réels positifs comme rappelé plus haut.

Méthode (Recherche des racines carrées sous forme trigonométrique)**.**

Soit l'équation $z^2 = a$ (d'inconnue z, avec $a \in \mathbb{C}^*$ fixé).
On écrit a sous forme trigonométrique : $a = \rho e^{i\alpha}$ ($\rho \in \mathbb{R}_+^*$, $\alpha \in \mathbb{R}$).
Les racines carrées de a sont

$$\sqrt{\rho} e^{i\alpha/2} \quad \text{et} \quad -\sqrt{\rho} e^{i\alpha/2}.$$

Méthode (Recherche des racines carrées sous forme algébrique)**.**

Soit l'équation $z^2 = a$ (d'inconnue z, avec $a \in \mathbb{C}$ fixé).
On écrit z et a sous forme algébrique : $z = x + iy$, $(x, y \in \mathbb{R})$ et $a = \alpha + i\beta$ $(\alpha, \beta \in \mathbb{R})$.
On a $z^2 = x^2 - y^2 + 2ixy$. Ainsi,

$$z^2 = a \iff \begin{cases} |z|^2 & = |a| \\ z^2 & = a \end{cases} \iff \begin{cases} x^2 + y^2 & = & \sqrt{\alpha^2 + \beta^2} \\ x^2 - y^2 & = & \alpha \\ 2xy & = & \beta \end{cases}$$

Les deux premières lignes permettent de calculer x^2 et y^2 et donc x et y au signe près.
La dernière ligne permet de savoir si x et y sont de même signe ou de signes opposés.

Exemple 48.

Calculer les racines carrées de $-4i$, ainsi que celles du nombre $3 - 4i$.

3.2 Racines n-èmes de l'unité et équation $z^n = a$.

Définition 49.

Soit $n \in \mathbb{N}^*$. On appelle **racine $n$ème de l'unité** toute solution complexe de l'équation

$$z^n = 1.$$

On note $\mathbb{U}_n$ l'ensemble des racines $n$èmes de l'unité.

Soit $n \in \mathbb{N}^*$.

- Remarquons que $1 \in \mathbb{U}_n$. À quelle condition a-t-on $-1 \in \mathbb{U}_n$?
- Démontrer que $\mathbb{U}_n$ est stable par conjugaison : $\forall z \in \mathbb{C} \quad z \in \mathbb{U}_n \Longrightarrow \overline{z} \in \mathbb{U}_n$.

Théorème 50 (Description des racines $n$èmes de l'unité)**.**

Soit $n \in \mathbb{N}^*$. On a

$$\mathbb{U}_n = \left\{ e^{\frac{2ik\pi}{n}},\ k \in [\![0, n-1]\!] \right\} \qquad \text{(ensemble de cardinal } n\text{)}.$$

Proposition 51 (Propriétés algébriques des racines $n$èmes de 1)**.**

Soit $n \in \mathbb{N}^*$. Les racines $n$èmes de l'unité forment une progression géométrique de raison $\omega = e^{\frac{2i\pi}{n}}$:

$$\mathbb{U}_n = \left\{ 1, \omega, \omega^2, \dots, \omega^{n-1} \right\}.$$

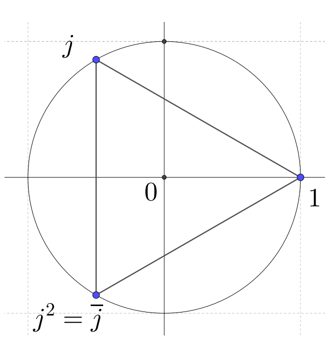
Les nombres $\omega, \omega^2 \dots, \omega^{n-1}$ sont les $n - 1$ solutions de l'équation $\sum_{k=0}^{n-1} x^k = 0$.
Si $n \geq 2$, alors la somme des racines $n$èmes de l'unité est nulle.

Corollaire 52 (Cas particulier important : racines troisième de l'unité)**.**

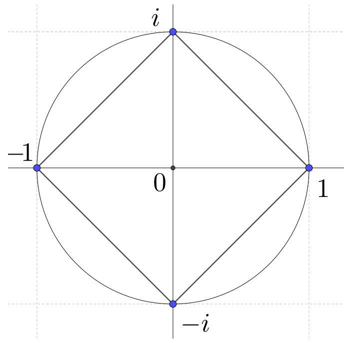
Notons $\boxed{j = e^{\frac{2i\pi}{3}}}$. L'équation $z^3 = 1$ a pour solutions les trois éléments de $\mathbb{U}_3 = \{1, j, j^2\}$.

$$j = e^{\frac{2i\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \qquad \text{et} \qquad j^2 = e^{\frac{4i\pi}{3}} = j^{-1} = \overline{j}$$

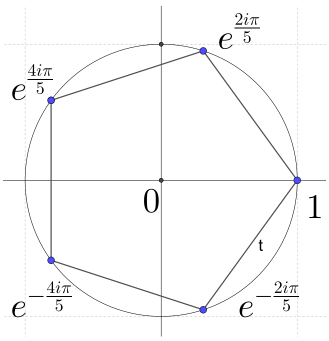
Les nombres j et j^2 sont les solutions de l'équation $x^2 + x + 1 = 0$.



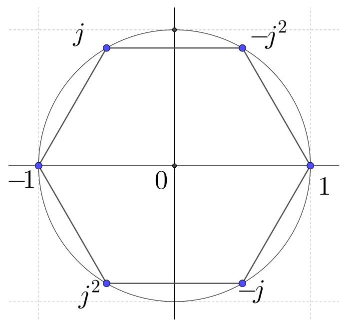
$\mathbb{U}_3 = \{1, j, j^2\}$



$\mathbb{U}_4 = \{1, i, -1, -i\}$



$\mathbb{U}_5$



$\mathbb{U}_6$

Méthode (Résoudre $z^n = a$, avec $a \in \mathbb{C}^*$ quelconque)**.**

Soit $a \in \mathbb{C}^*$. On peut l'écrire $a = \rho e^{i\alpha}$, avec $\rho \in \mathbb{R}_+^*$ et $\alpha \in \mathbb{R}$.
Le nombre $z_0 := \rho^{\frac{1}{n}} e^{\frac{i\alpha}{n}}$ est une solution de l'équation $z^n = a$. Ainsi, pour $z \in \mathbb{C}$,

$$z^n = a \iff z^n = z_0^n \iff \left(\frac{z}{z_0}\right)^n = 1 \iff \frac{z}{z_0} \in \mathbb{U}_n.$$

L'ensemble des solutions de $z^n = a$ est donc $\left\{ z_0 e^{\frac{2ik\pi}{n}},\ k \in [\![0, n-1]\!] \right\}$.
Les points dont l'affixe est solution de l'équation forment un polygone régulier à n sommets.

Exemple 53.

Résolution de $z^3 = 8i$.

3.3 Équations du second degré.

Définition 54.

On appelle **équation du second degré** toute équation de la forme

$$az^2 + bz + c = 0,$$

où $a, b, c \in \mathbb{C}$ avec $a \neq 0$. Les solutions de l'équation sont appelées ses **racines**.

Proposition 55 (Équations du second degré, coefficients complexes)**.**

Soient $a, b, c \in \mathbb{C}$ avec $a \neq 0$. On considère l'équation

$$az^2 + bz + c = 0$$

et on note Δ le nombre complexe $b^2 - 4ac$, qu'on appelle **discriminant** de l'équation.

- Si $\Delta \neq 0$, alors Δ a exactement deux racines carrées que l'on note δ et $-\delta$. L'équation a alors exactement deux racines : $r_1 = \dfrac{-b-\delta}{2a}$ et $r_2 = \dfrac{-b+\delta}{2a}$.
- Si $\Delta = 0$, l'équation a une racine "double" : $r_1 = r_2 = -\dfrac{b}{2a}$.

<u>Factorisation</u> du trinôme : pour tout $z \in \mathbb{C}$,

$$\boxed{az^2 + bz + c = a\left(z - r_1\right)\left(z - r_2\right)}.$$

Proposition 56 (Équations du second degré, coefficients réels)**.**

Soient $a, b, c \in \mathbb{R}$ avec $a \neq 0$. On considère l'équation

$$az^2 + bz + c = 0$$

et on note $\Delta = b^2 - 4ac$ son discriminant.

- Si $\Delta > 0$, alors Δ a pour racines carrées $\sqrt{\Delta}$ et $-\sqrt{\Delta}$ et l'équation a deux racines réelles distinctes
$$r_1 = \frac{-b-\sqrt{\Delta}}{2a} \quad \text{et} \quad r_2 = \frac{-b+\sqrt{\Delta}}{2a}.$$
- Si $\Delta = 0$, l'équation a une racine "double" : $r = -\dfrac{b}{2a}$.
- Si $\Delta < 0$, alors Δ a pour racines carrées $i\sqrt{|\Delta|}$ et $-i\sqrt{|\Delta|}$ et l'équation a deux racines complexes conjuguées
$$r_1 = \frac{-b-i\sqrt{|\Delta|}}{2a} \quad \text{et} \quad r_2 = \frac{-b+i\sqrt{|\Delta|}}{2a}.$$

Proposition 57 (Relations coefficients-racines)**.**

Soient $a, b, c \in \mathbb{C}$ avec $a \neq 0$ et z_1 et z_2 deux nombres complexes. Les nombres z_1 et z_2 sont deux racines, éventuellement égales, de $az^2 + bz + c = 0$ si et seulement si

$$z_1 + z_2 = -\frac{b}{a} \quad \text{et} \quad z_1 z_2 = \frac{c}{a}.$$

Remarque. Ainsi, si S et P sont deux nombres complexes, le système

$$\begin{cases} z_1 + z_2 & = & S \\ z_1 z_2 & = & P \end{cases}$$

a deux solutions dans $\mathbb{C}^2$: les couples (r_1, r_2) et (r_2, r_1), où r_1 et r_2 sont les racines de l'équation

$$z^2 - Sz + P = 0.$$

Exemple 58.

Soit $z \in \mathbb{C}$, $r \in \mathbb{R}_+^*$ et $\theta \in \mathbb{R}$. Factoriser à vue les expressions

$$z^2 + 2z - 3, \qquad 2z^2 + z - 1, \qquad z^2 - 2r\cos(\theta)z + r^2.$$

Exercices

Forme algébrique, conjugué, module.

$\boxed{\textbf{5.1}}$ **[♦◇◇]** Résoudre $4z^2 + 8|z|^2 - 3 = 0$.

$\boxed{\textbf{5.2}}$ **[♦◇◇]** Soient a et b deux nombres complexes non nuls. Montrer que :

$$\left| \frac{a}{|a|^2} - \frac{b}{|b|^2} \right| = \frac{|a-b|}{|a||b|}.$$

$\boxed{\textbf{5.3}}$ **[♦◇◇]** Soient ω et ω' deux éléments de $\mathbb{U}$ tels que $\omega + \omega' \neq 0$.
Démontrer que

$$\frac{\omega + \omega'}{1 - \omega\omega'} \in \mathbb{R}.$$

$\boxed{\textbf{5.4}}$ **[♦♦◇]** Soient z_1, z_2,... z_n des nombres complexes non nuls de même module. Démontrer que

$$\frac{(z_1+z_2)(z_2+z_3)\cdots(z_{n-1}+z_n)(z_n+z_1)}{z_1 z_2 \cdots z_n} \in \mathbb{R}.$$

$\boxed{\textbf{5.5}}$ **[♦♦◇]** Si $z \in \mathbb{C} \setminus \{1\}$, montrer que :

$$\frac{1+z}{1-z} \in i\mathbb{R} \iff |z| = 1.$$

$\boxed{\textbf{5.6}}$ **[♦♦◇]** Soient a, b deux nombres complexes tels que $\overline{a}b \neq 1$ et $c = \dfrac{a-b}{1-\overline{a}b}$. Montrer que

$$(|c| = 1) \iff (|a| = 1 \text{ ou } |b| = 1).$$

$\boxed{\textbf{5.7}}$ **[♦♦♦]** Pour $n \in \mathbb{N}^\star$, calculer $R^2 + S^2$ où

$$R = \sum_{0 \leq 2k \leq n} (-1)^k \binom{n}{2k} \quad \text{et} \quad S = \sum_{0 \leq 2k+1 \leq n} (-1)^k \binom{n}{2k+1}.$$

$\boxed{\textbf{5.8}}$ **[♦♦♦]** Soit $ABCD$ un parallélogramme.
Montrer que $AC^2 + BD^2 = AB^2 + BC^2 + CD^2 + DA^2$.

Forme trigonométrique

$\boxed{\textbf{5.9}}$ **[♦◇◇]** Calculer $(1+i)^{2024}$.

$\boxed{\textbf{5.10}}$ **[♦♦◇]** Soient trois réels x, y, z tels que $e^{ix} + e^{iy} + e^{iz} = 0$. Montrer que $e^{2ix} + e^{2iy} + e^{2iz} = 0$.

$\boxed{\textbf{5.11}}$ **[♦◇◇]**

1. Déterminer les formes algébriques et trigonométriques du nombre

$$\frac{1+i\sqrt{3}}{2-2i}.$$

2. En déduire l'expression de $\cos\frac{7\pi}{12}$ et de $\sin\frac{7\pi}{12}$ à l'aide de radicaux.

$\boxed{\textbf{5.12}}$ **[♦◇◇]** Soit un réel θ. Linéariser $(\cos\theta)^5$ et $(\sin\theta)^6$.

$\boxed{\textbf{5.13}}$ **[♦♦◇]**

1. Soit x un réel. Exprimer $\cos(5x)$ comme un polynôme en $\cos x$.
2. Montrer que $\cos^2\left(\frac{\pi}{10}\right)$ est racine du trinôme $x \mapsto 16x^2 - 20x + 5$.
3. En déduire l'égalité $\cos\left(\frac{\pi}{5}\right) = \frac{1+\sqrt{5}}{4}$.
4. (*) Pourquoi ceci démontre-t-il que le pentagone régulier est constructible à la règle et au compas ?

$\boxed{\textbf{5.14}}$ **[♦♦◇]** Soit $x \in \mathbb{R}$ et $n \in \mathbb{N}$. Calculer

$$\sum_{k=0}^{n} \binom{n}{k} \cos(kx), \qquad \text{et} \qquad \sum_{k=0}^{n} \binom{n}{k} \sin(kx).$$

$\boxed{\textbf{5.15}}$ **[♦♦◇]** Noyaux de Dirichlet et de Féjer.
Soit $n \in \mathbb{N}^*$ et $x \in \mathbb{R} \setminus \{2k\pi, k \in \mathbb{Z}\}$. On note

$$D_n(x) = \sum_{k=-n}^{n} e^{ikx} \qquad \text{et} \qquad F_n(x) = \frac{1}{n}\sum_{k=0}^{n-1} D_k(x).$$

La fonction $x \mapsto D_n(x)$ est appelée noyau de Dirichlet ; elle intervient notamment dans le cadre de l'analyse de Fourier. La fonction $x \mapsto F_n(x)$, moyenne arithmétique des n premiers noyaux de Dirichlet, est appelée noyau de Féjer.

1. Montrer que $D_n(x) = \dfrac{\sin\left((n+\frac{1}{2})x\right)}{\sin\frac{x}{2}}$.
2. Montrer que $F_n(x) = \dfrac{1}{n}\left(\dfrac{\sin\left(\frac{nx}{2}\right)}{\sin\frac{x}{2}}\right)^2$.

$\boxed{\textbf{5.16}}$ **[♦♦♦]** Soient un quadrilatère $ABCD$ du plan. On construite les points E, F, G, H à l'extérieur du quadrilatère tels que les triangles EBA, FCB, GDC et HAD soient des triangles directs, isocèles et rectangles en E, F, G, H. Démontrer que

$$\overrightarrow{EG} \perp \overrightarrow{FH} \quad \text{et} \quad EG = FH.$$

$\boxed{\textbf{5.17}}$ **[♦♦♦]** Trouver les nombres complexes d'affixe $z \in \mathbb{C}$ tels que $1, z^2$ et z^4 sont alignés.

Équations algébriques

$\boxed{5.18}$ [♦◇◇]

1. Calculer les racines carrées du nombre $-8i$.
   On donnera ces nombres sous forme algébrique et sous forme trigonométrique.
2. Résoudre dans $\mathbb{C}$ l'équation
$$z^2 - 4z + 4 + 2i = 0.$$

$\boxed{5.19}$ [♦◇◇] Résoudre $iz^2 + (4-i)z - 5 - 5i = 0$. *Indication :* $13^2 = 169$.

$\boxed{5.20}$ [♦◇◇] Soit $n \in \mathbb{N}$, $n \geq 2$. Calcul de $\displaystyle\sum_{z \in \mathbb{U}_n} z$ et $\displaystyle\prod_{z \in \mathbb{U}_n} z$.

$\boxed{5.21}$ [♦♦◇] Donner une expression du périmètre du polygone régulier formé par les nombres de $\mathbb{U}_n$.
Que conjecture-t-on géométriquement sur la limite du périmètre lorsque $n \to +\infty$?
Essayer de prouver votre conjecture.

$\boxed{5.22}$ [♦◇◇] Soit $\omega \in \mathbb{U}_7$, une racine 7e de l'unité différente de 1.

1. Justifier que $1 + \omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6 = 0$.
2. Calculer le nombre
$$\frac{\omega}{1+\omega^2} + \frac{\omega^2}{1+\omega^4} + \frac{\omega^3}{1+\omega^6}.$$
   Indication : La réponse est un entier négatif.

$\boxed{5.23}$ [♦♦◇] Dans cet exercice, n est un entier naturel supérieur ou égal à 2.

1. Rappel de définition : quand dit-on qu'un nombre réel θ est un *argument* d'un nombre complexe z ?
2. Soit $k \in [\![0, n-1]\!]$. Donner le module et un argument de $e^{\frac{2ik\pi}{n}} - 1$.
3. Établir l'égalité
$$\sum_{z \in \mathbb{U}_n} |z - 1| = \frac{2}{\tan\left(\frac{\pi}{2n}\right)}.$$

$\boxed{5.24}$ [♦♦◇] Soit θ un nombre réel appartenant à $]0, \pi[$. Résoudre l'équation
$$z^2 - 2e^{i\theta}z + 2ie^{i\theta}\sin\theta = 0.$$
On écrira les solutions sous forme algébrique <u>et</u> sous forme trigonométrique.

$\boxed{5.25}$ [♦♦◇] Soit $n \in \mathbb{N}^*$

1. Résoudre dans $\mathbb{C}$ l'équation $z^2 - 2\cos(\theta)z + 1 = 0$.
2. Résoudre dans $\mathbb{C}$ l'équation $z^{2n} - 2\cos(\theta)z^n + 1 = 0$.

$\boxed{5.26}$ [♦♦◇] Résoudre.
$$\left(\frac{z+i}{z-i}\right)^3 + \left(\frac{z+i}{z-i}\right)^2 + \left(\frac{z+i}{z-i}\right) + 1 = 0.$$

$\boxed{5.27}$ [♦♦♦] Résoudre dans $\mathbb{C}$ l'équation $(z+1)^n = z^n$.

$\boxed{5.28}$ [♦♦♦] Soient $n \in \mathbb{N}^*$ et $z \in \mathbb{C}$ tels que $z^n = (1+z)^n = 1$.
Montrer que n est un multiple de 6 et que $z^3 = 1$.

$\boxed{5.29}$ [♦♦♦] Résoudre dans $\mathbb{C}^2$ le système
$$\begin{cases} u^2 + v^2 &= -1 \\ uv &= 1 \end{cases}$$

Dans ce cours, les lettres E, F, G et H désigneront des ensembles.

1 Vocabulaire.

1.1 Définitions.

Définition 1.

Une **application** f de E dans F est un procédé qui à tout élément x de E associe un unique élément dans F, que l'on note $f(x)$. Cet objet est aussi appelé **fonction**, et décrit à l'aide de la notation

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

L'ensemble E est alors appelé **ensemble de départ** F **ensemble d'arrivée**.

Soient $x \in E$ et $y \in F$ tels que

$$y = f(x);$$

On dit que y est l'**image** de x par f et que x est un **antécédent** de y par f.

Figure : deux patates et des flèches (important !)

Une application sert à faire un lien entre deux ensembles (éventuellement égaux). On a beaucoup manipulé au lycée les fonctions de la variable réelle, telles que la fonction logarithme népérien :

$$\ln : \left\{ \begin{array}{ccc} \mathbb{R}_+^* & \to & \mathbb{R} \\ x & \mapsto & \ln(x) \end{array} \right. .$$

Mais les applications ne seront pas définies seulement entre des ensembles de nombres : elles vont nous permettre de donner une existence mathématique à certaines opérations. Prenons l'exemple du passage au complémentaire dans un ensemble E donné : il peut être vu comme une application :

$$\psi : \left\{ \begin{array}{ccc} \mathcal{P}(E) & \to & \mathcal{P}(E) \\ A & \mapsto & \overline{A} \end{array} \right. .$$

Définition 2 (Des applications simples à définir).

On appelle application **identité** sur E et on note id_E l'application

$$\mathrm{id}_E : \left\{ \begin{array}{ccc} E & \to & E \\ x & \mapsto & x \end{array} \right. .$$

Soit $a \in F$; on appelle **application constante** égale à a la fonction

$$: \left\{ \begin{array}{ccc} E & \to & F \\ x & \mapsto & a \end{array} \right. .$$

Notation.

L'ensemble des applications de E dans F est noté F^E ou bien $\mathcal{F}(E,F)$.

Proposition 3 (Égalité de deux fonctions).

Deux applications sont égales si et seulement si elles sont *égales en tout point* :

$$\forall (f,g) \in (\mathcal{F}(E,F))^2 \qquad f = g \quad \Longleftrightarrow \quad \forall x \in E \quad f(x) = g(x).$$

Définissons l'ensemble des images par une application : cela nous permettra de bien comprendre la différence avec l'ensemble d'arrivée.

Définition 4.

Soit $f \in \mathcal{F}(E,F)$ une application. On appelle **image** de f (ou plus précisément ensemble des images par f) et on note $\mathrm{Im}(f)$ ou encore $f(E)$ l'ensemble

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

On peut écrire aussi

$$\mathrm{Im}(f) = \{y \in F \mid \exists x \in E \quad y = f(x)\}.$$

Considérons l'application

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

Nous savons que son (ensemble des) images est $\mathrm{Im}(f) = \mathbb{R}_+^*$. Il est différent de l'ensemble $\mathbb{R}$, qui a été déclaré comme ensemble d'arrivée. On peut d'ailleurs changer l'ensemble d'arrivée sans vraiment changer la fonction et écrire

$$\exp : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R}_+^* \\ x & \mapsto & \exp(x) \end{array} \right. .$$

1.2 Fonctions indicatrices.

Définition 5.

Soit A une partie de E. La **fonction indicatrice** de A est l'application notée $\mathbf{1}_A$, définie par

$$\mathbf{1}_A : \left\{ \begin{array}{ccl} E & \to & \{0,1\} \\ x & \mapsto & \mathbf{1}_A(x) := \left\{ \begin{array}{ll} 1 & \text{si } x \in A, \\ 0 & \text{si } x \notin A. \end{array} \right. \end{array} \right.$$

Par exemple, $\mathbb{Q}$ étant une partie de $\mathbb{R}$, on considère $\mathbf{1}_{\mathbb{Q}}$, fonction indicatrice de $\mathbb{Q}$, définie sur $\mathbb{R}$.

$$\mathbf{1}_{\mathbb{Q}}\left(\frac{2}{3}\right) = 1 \qquad \text{et} \qquad \mathbf{1}_{\mathbb{Q}}\left(\sqrt{2}\right) = 0.$$

Proposition 6 (Une partie est caractérisée par sa fonction indicatrice)**.**

$$\forall (A,B) \in (\mathcal{P}(E))^2 \quad A = B \iff \mathbf{1}_A = \mathbf{1}_B.$$

Proposition 7.

Soit E un ensemble et $A, B \in \mathcal{P}(E)$. Les égalités qui suivent sont des égalités entre applications.

Si A et B sont disjoints ($A \cap B = \emptyset$) alors $\mathbf{1}_{A\cup B} = \mathbf{1}_A + \mathbf{1}_B$.

Plus généralement,

$$\mathbf{1}_{A\setminus B} = \mathbf{1}_A - \mathbf{1}_{A\cap B}, \qquad \mathbf{1}_{A\cap B} = \mathbf{1}_A \cdot \mathbf{1}_B \qquad \mathbf{1}_{A\cup B} = \mathbf{1}_A + \mathbf{1}_B - \mathbf{1}_{A\cap B}.$$

1.3 Restriction, prolongement.

Définition 8.

Soit $f \in \mathcal{F}(E,F)$ et $A \in \mathcal{P}(E)$. On appelle **restriction** de f à A, et on note $f_{|A}$ l'application

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

Définition 9.

Soit A une partie de E et $g \in \mathcal{F}(A,F)$.
On appelle **prolongement** de g sur E toute application $f \in \mathcal{F}(E,F)$ telle que $f_{|A} = g$.

Exemple 10.

Soit g la fonction constante égale à 1 sur $\mathbb{R}^*$. Définir deux prolongements différents de g sur $\mathbb{R}$.

2 Composition.

Définition 11.

Soient E, F, G trois ensembles. Soient deux applications

$$f : E \to F \quad \text{et} \quad g : F \to G.$$

La **composée** de f par g, notée $g \circ f$ est l'application

$$g \circ f : \left\{ \begin{array}{ccc} E & \to & G \\ x & \mapsto & g \circ f(x) := g(f(x)) \end{array} \right. .$$

Aussi important que la définition : le dessin avec les trois patates.

Exemple 12.

Soient

$$f : x \mapsto \ln(x-3), \qquad g : x \mapsto \sqrt{x^2-4}, \qquad h : x \mapsto \sqrt{\ln(x)}.$$

Écrire chacune comme la composée de deux fonctions "simples" (en précisant bien sûr chaque fois les ensembles de départ et d'arrivée).

Exemple 13 (Pour des fonctions de la variable réelle, à valeurs réelles)**.**

La composée de deux fonctions décroissantes est croissante.

Proposition 14 (L'identité est neutre pour la composition)**.**

Pour tout application $f \in \mathcal{F}(E, F)$, on a

$$\mathrm{id}_F \circ f = f \quad \text{et} \quad f \circ \mathrm{id}_E = f.$$

Proposition 15 (Associativité de la composition)**.**

Si $f : E \to F$, $g : F \to G$, $h : G \to H$, alors,

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

Définition 16 (extension)**.**

Soient E, F, E' et F' quatre ensembles. Soient deux applications

$$f : E \to F \quad \text{et} \quad g : E' \to F',$$

telles que $\underline{\mathrm{Im}(f) \subset E'}$. On appelle alors composée $g \circ f$ l'application $g \circ f = \left(g_{|\mathrm{Im}(f)}\right) \circ f$.

3 Bijections (premier contact).

Définition 17.

On dit qu'une application $f : E \to F$ est une **bijection** de E vers F si tout élément de F possède un unique antécédent dans E par f, ce qui s'écrit

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

Définition 18.

Soit $f : E \to F$ une bijection. Tout élément $y \in F$ possède un unique antécédent dans E par f ; notons-le $f^{-1}(y)$. Ceci définit la fonction **réciproque** de f.

$$f^{-1} : \begin{cases} F & \to & E \\ y & \mapsto & f^{-1}(y) \end{cases}.$$

Exemple. $\exp : \mathbb{R} \to \mathbb{R}_+^*$ est une bijection et $\ln : \mathbb{R}_+^* \to \mathbb{R}$ est sa réciproque.

Proposition 19 (découle de la définition de f^{-1})**.**

Soit $f : E \to F$ une bijection et $f^{-1} : F \to E$ sa réciproque. On a

$$\forall x \in E \quad f^{-1}(f(x)) = x \qquad \text{et} \qquad \forall y \in F \quad f\left(f^{-1}(y)\right) = y.$$

Ceci se récrit

$$f^{-1} \circ f = \mathrm{id}_E, \qquad \text{et} \qquad f \circ f^{-1} = \mathrm{id}_F.$$

Dans le second cours sur les applications, le concept de bijectivité sera décomposé en deux sous-concepts : l'injectivité et la surjectivité.

Complément : Famille d'éléments d'un ensemble.

Définition 20.

Soient E et I deux ensembles (le second étant celui des indices).

Une **famille d'éléments de E indexée par I** est une fonction $a \colon I \to E$.

Pour $i \in I$, on note $a_i = a(i)$. La famille a est alors notée $a = (a_i)_{i \in I}$.

L'ensemble des familles d'éléments de E indexées par I sera notée E^I.

L'idée : a_i est un élément de E « étiqueté » à l'aide d'une étiquette i prise dans l'ensemble des indices I.

Définition 21.

On appelle **suite** d'éléments de E une famille d'éléments de E indexée par $\mathbb{N}$.

L'ensemble des suites à termes dans E est donc $E^{\mathbb{N}}$. Une suite $u \in E^{\mathbb{N}}$ est donc notée $u = (u_n)_{n\in\mathbb{N}}$.

Proposition 22 (admis)**.**

Soit $f : E \to E$ et $a \in E$. Alors il existe une unique suite $(u_n)_{n\in\mathbb{N}} \in E^{\mathbb{N}}$ telle que

$$\begin{cases} u_0 = a \\ \forall n \in \mathbb{N} \quad : \quad u_{n+1} = f(u_n). \end{cases}$$

Exercices

$\boxed{\textbf{6.1}}$ **[♦♦◇]** À l'aide de notions croisées dans les cours précédents, donner des exemples d'applications *involutives*, c'est-à-dire des applications du type

$$f : E \to E \quad | \quad f \circ f = \mathrm{id}_E.$$

$\boxed{\textbf{6.2}}$ **[♦♦◇]** À l'aide de notions croisées dans les cours précédents, donner des exemples d'applications *idempotentes*, c'est-à-dire des applications du type

$$f : E \to E \quad | \quad f \circ f = f.$$

où E est un ensemble que vous préciserez.

$\boxed{\textbf{6.3}}$ **[♦♦◇]** Exhibez deux applications $f : \mathbb{N} \to \mathbb{N}$ et $g : \mathbb{N} \to \mathbb{N}$ telles que

$$g \circ f = \mathrm{Id}_{\mathbb{N}} \quad \text{et} \quad f \circ g \neq \mathrm{Id}_{\mathbb{N}}.$$

$\boxed{\textbf{6.4}}$ **[♦♦◇]** On veut démontrer qu'il n'existe aucune fonction $f : \mathbb{N} \to \mathbb{N}$ telle que

$$\forall n \in \mathbb{N} \quad f(f(n)) = n + 1.$$

On va raisonner par l'absurde. On suppose donc qu'il existe une telle fonction f.

1. Démontrer que pour tout entier $n \in \mathbb{N}$, on a $f(n+1) - f(n) = 1$.
   Indication : on pourra considérer $f \circ f \circ f$.
2. Démontrer alors que pour tout entier naturel n, on a $f(n) = n + f(0)$.
3. Conclure.

$\boxed{\textbf{6.5}}$ **[♦♦◇]** Associativité de la différence symétrique.
Soit E un ensemble. Pour X et Y deux parties de E, on note $X \Delta Y = (X \cup Y) \setminus (X \cap Y)$.
Soient A, B, C trois parties de E. Développer $1_{(A\Delta B)\Delta C}$. En déduire que $(A\Delta B)\Delta C = A\Delta(B\Delta C)$.

---

7 Outils pour l'étude des fonctions

Ce cours se donne pour but de définir un vocabulaire rigoureux pour l'étude des fonctions de la variable réelle. On souhaite aussi présenter (sans preuve) un certain nombre de résultats que nous utiliserons dès maintenant, et qui seront établis dans le (vrai) cours d'analyse.

Dans tout ce cours, la lettre $\mathbb{K}$ pourra être remplacée par $\mathbb{R}$ ou $\mathbb{C}$.

Les lettres I et J désigneront des intervalles de $\mathbb{R}$ non vides et non réduits à un point.

La lettre X désignera quant à elle une partie quelconque de $\mathbb{R}$. Dans la pratique, il s'agira souvent d'un intervalle, mais cela pourra être aussi une réunion d'intervalles. La lettre Y sera une partie quelconque de $\mathbb{K}$.

1 Propriétés de $\mathbb{R}$.

1.1 Relation $\leq$.

Rappel ($\leq$ est une relation d'ordre sur $\mathbb{R}$).

- $\forall x \in \mathbb{R} \quad x \leq x.$ (Réflexivité)
- $\forall (x,y) \in \mathbb{R}^2 \quad (x \leq y \text{ et } y \leq x) \Longrightarrow x = y.$ (Antisymétrie)
- $\forall (x,y,z) \in \mathbb{R}^3 \quad (x \leq y \text{ et } y \leq z) \Longrightarrow x \leq z.$ (Transitivité)

Rappel (C'est une relation d'ordre totale).

On peut toujours comparer deux réels : pour tout couple (x,y) de $\mathbb{R}^2$, on a $x \leq y$ ou $y \leq x$.

Rappel (Élémentaire mais fondamental).

On peut comparer deux réels en examinant le signe de leur différence :

$$\forall (x,y) \in \mathbb{R}^2 \qquad x \leq y \iff y - x \geq 0.$$

Exemple 1 (Inégalité arithmético-géométrique .).

Établir l'inégalité $\sqrt{xy} \leq \dfrac{x+y}{2}$ pour deux réels x et y positifs. Dans quel cas a-t-on égalité ?

Rappel ($\leq$ et somme).

On peut *sommer des inégalités*. Pour tous réels x, x', y, y',

$$\left\{\begin{array}{ccc} x & \leq & y \\ & \text{et} & \\ x' & \leq & y' \end{array}\right. \qquad \Longrightarrow \qquad x + x' \leq y + y'.$$

Si $(x_i)_{i\in I}$ et $(y_i)_{i\in I}$ sont des familles finies de nombres réels,

$$(\forall i \in I \quad x_i \leq y_i) \quad \Longrightarrow \quad \sum_{i\in I} x_i \leq \sum_{i\in I} y_i.$$

Proposition 2 (Somme nulle de termes positifs).

Soient $x_1, \ldots, x_n$ des réels $\boxed{\text{positifs}}$ tels que

$$\sum_{i=1}^{n} x_i = 0 \quad \Longrightarrow \quad \forall i \in [\![1,n]\!] \quad x_i = 0.$$

Rappel ($\leq$ et produit)**.**

Soient x et y deux réels tels que $x \leq y$.
- Si a est un réel positif alors $ax \leq ay$.
- Si a est un réel négatif alors $ax \geq ay$.

On peut *multiplier des inégalités* dont les membres sont positifs. Pour tous réels x, x', y, y',

$$\begin{cases} 0 \leq x \leq y \\ \text{et} \\ 0 \leq x' \leq y' \end{cases} \implies x \times x' \leq y \times y'.$$

Rappel ($\leq$ et quotient)**.**

$$\forall x, y \in \mathbb{R} \qquad 0 < x \leq y \implies 0 \leq \frac{1}{y} < \frac{1}{x}.$$

1.2 Intervalles.

Définition 3 (Les deux infinis)**.**

On ajoute à l'ensemble $\mathbb{R}$ les deux éléments $+\infty$ et $-\infty$ pour former l'ensemble

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

en prenant la convention que pour tout x réel, $x \leq +\infty$ et $-\infty \leq x$.

Définition 4.

On appelle **intervalle** de $\mathbb{R}$ une partie de $\mathbb{R}$ ayant l'une des formes décrites ci-dessous :

- Segment $[a, b] = \{x \in \mathbb{R} : a \leq x \text{ et } x \leq b\}$ où $a, b \in \mathbb{R}$.
- Intervalles ouverts $]a, b[= \{x \in \mathbb{R} : a < x \text{ et } x < b\}$ où $a \in \mathbb{R} \cup \{-\infty\}, b \in \mathbb{R} \cup \{+\infty\}$.
- Intervalles semi-ouverts $]a, b] = \{x \in \mathbb{R} : a < x \text{ et } x \leq b\}$ où $a \in \mathbb{R} \cup \{-\infty\}, b \in \mathbb{R}$, ou bien $[a, b[= \{x \in \mathbb{R} : a \leq x \text{ et } x < b\}$ où $a \in \mathbb{R}, b \in \mathbb{R} \cup \{+\infty\}$.

Remarque. Les parties décrites ci-dessus peuvent être vides. Par exemple, $]5, 3] = \emptyset$.

Figures. Représentation des intervalles $[1, 2[$ et $]5, +\infty[$.

Exemple 5.

Les intervalles sont des parties « convexes » de $\mathbb{R}$: si I est un intervalle,

$$\forall (x,y) \in I^2 \quad [x,y] \subset I.$$

L'ensemble des réels non nuls $\mathbb{R}^*$ n'est **pas** un intervalle (il n'est pas convexe).
C'est néanmoins une réunion d'intervalles :

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

1.3 Partie entière.

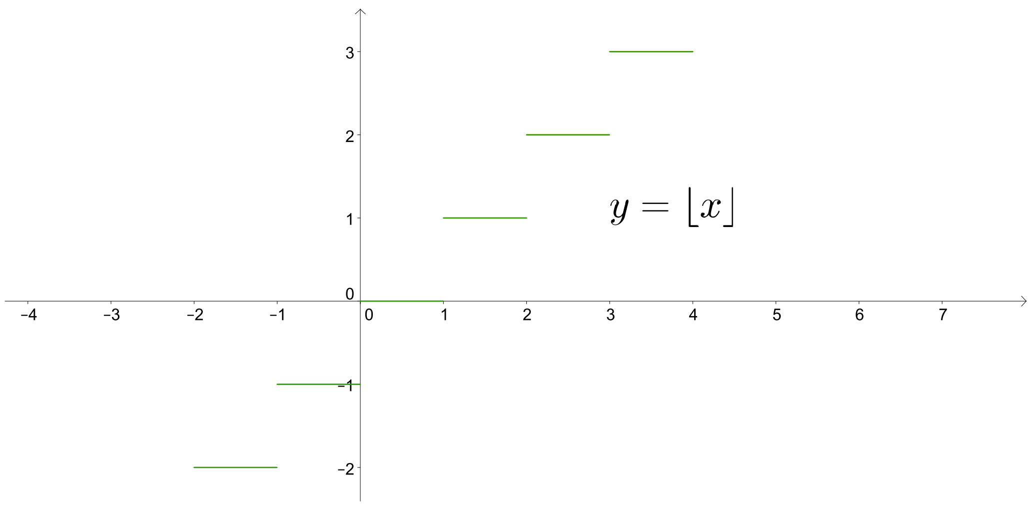
Définition 6.

Pour tout nombre réel x, on appelle **partie entière** de x, et on note $\lfloor x \rfloor$ le plus grand entier relatif inférieur à x :

$$\lfloor x \rfloor = \max \{k \in \mathbb{Z} \mid k \leq x\}.$$

Remarque. La définition ci-dessus a un sens en admettant que toute partie non vide et majorée de $\mathbb{Z}$ possède un plus grand élément.

Exemple. $\lfloor \pi \rfloor = 3$, $\lfloor -\pi \rfloor = -4$.



Proposition 7 (Partie entière et encadrements)**.**

Pour tout nombre réel x,

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1.$$

En « croisant » les inégalités, ceci implique notamment que pour tout $x \in \mathbb{R}$,

$$x - 1 < \lfloor x \rfloor \leq x.$$

1.4 Valeur absolue.

Définition 8.

Soit $x \in \mathbb{R}$. On appelle **valeur absolue** de x et on note $|x|$ le nombre réel *positif* donné par

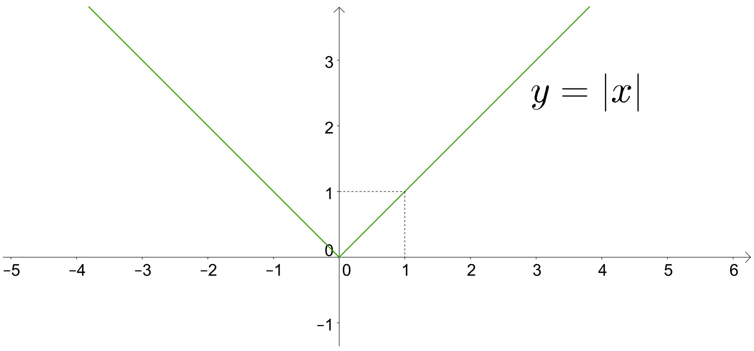
$$|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0. \end{cases}$$

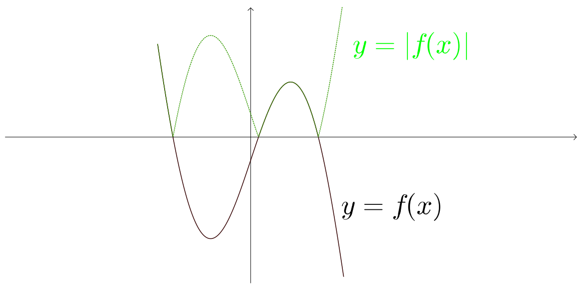
Proposition 9 (Propriétés élémentaires)**.**

Pour tout x réel,

$$|x| = \max(x, -x) \qquad x \leq |x|, \quad -x \leq |x| \quad \text{et} \quad -|x| \leq x \leq |x|$$

$$|-x| = |x| \qquad |x| = 0 \iff x = 0$$





Proposition 10 (Valeurs absolues et produits)**.**

1. $\forall x \in \mathbb{R} \quad |x|^2 = x^2$ et $|x| = \sqrt{x^2}$.
2. La valeur absolue du produit, c'est le produit des valeurs absolues
$$\forall x, y \in \mathbb{R} \quad |x \cdot y| = |x| \cdot |y|.$$
3. $\forall x \in \mathbb{R}\ \forall y \in \mathbb{R}^* \quad \left|\dfrac{x}{y}\right| = \dfrac{|x|}{|y|}$.

Comme nous l'avons montré dans le cas plus général du module, la valeur absolue de la somme n'est **pas** la somme des valeurs absolues. Dans $\mathbb{C}$, on pouvait dessiner le triangle.

Proposition 11 (Inégalité triangulaire)**.**

Pour tous nombres réels x et y, on a

$$|x + y| \leq |x| + |y|$$

Corollaire 12.

1. $\forall (x,y) \in \mathbb{R}^2 \quad |x-y| \leq |x|+|y|$.
2. $\forall (x,y) \in \mathbb{R}^2 \quad ||x|-|y|| \leq |x-y|$.
3. Soit $n \in \mathbb{N}^*$. Pour tous nombres réels $x_1, \ldots, x_n$, on a l'inégalité $\left|\sum_{k=1}^{n} x_k\right| \leq \sum_{k=1}^{n} |x_k|$.

⚠ On notera que dans la première inégalité, on a écrit un $-$ à gauche mais il y toujours un $+$ à droite !

Une notion de distance sur $\mathbb{R}$. On l'a déjà compris avec le module : pour x et y deux réels,

$$\boxed{|x-y| \text{ est la } \textbf{distance} \text{ entre } x \text{ et } y.}$$

Proposition 13.

$$\forall x, a \in \mathbb{R} \quad \forall b \in \mathbb{R}_+ \qquad \begin{array}{lcl} |x-a| \leq b & \iff & x \in [a-b, a+b] \\ |x-a| \geq b & \iff & x \geq a+b \ \text{ ou } \ x \leq a-b. \end{array}$$

$$\text{En particulier,} \qquad \forall x \in \mathbb{R} \qquad \forall b \in \mathbb{R}_+ \quad |x| \leq b \iff -b \leq x \leq b.$$

2 Description des fonctions.

Soit X une partie de $\mathbb{R}$ (quelconque) et Y une partie de $\mathbb{K}$. On rappelle qu'une fonction (ou application)

$$f : \left\{ \begin{array}{ccc} X & \to & Y \\ x & \mapsto & f(x) \end{array} \right. .$$

est un procédé qui a tout élément x de X associe un unique élément $f(x)$ appartenant à Y.

Si $x \in X$ et $y = f(x)$, on rappelle que y est l'**image** de x et que x est *un* **antécédent** de y.

Puisqu'ici la variable x est un nombre réel, on dit que la fonction est de la **variable réelle**.

Lorsque toutes les images par la fonction f sont des nombres réels, alors f est dite **à valeurs réelles** (dans la pratique, ce sera le cas dans l'immense majorité des cas considérés).

Rappel.

« La fonction $f(x)$ » ou « La fonction f » ?

La bonne réponse, c'est la deuxième !

Pour $f : X \to \mathbb{K}$, l'objet $f(x)$ est un <u>nombre</u> (de $\mathbb{K}$), bien défini si x est un élément de l'ensemble X.

Prenons les bonnes habitudes dès maintenant si on veut être capable de comprendre un jour la différence entre convergence simple et convergence uniforme d'une suite de fonctions...

2.1 Ensemble de définition.

L'**ensemble de définition** d'une fonction f est l'ensemble des réels x tel que $f(x)$ a un sens.

Exemple 14.

Donner l'ensemble de définition de

$$f : x \mapsto \sqrt{x(x-2)}, \qquad g : x \mapsto \ln\left(x(x-2)\right), \qquad h : x \mapsto \ln(x) + \ln(x-2).$$

2.2 Représentation graphique d'une fonction à valeurs réelles.

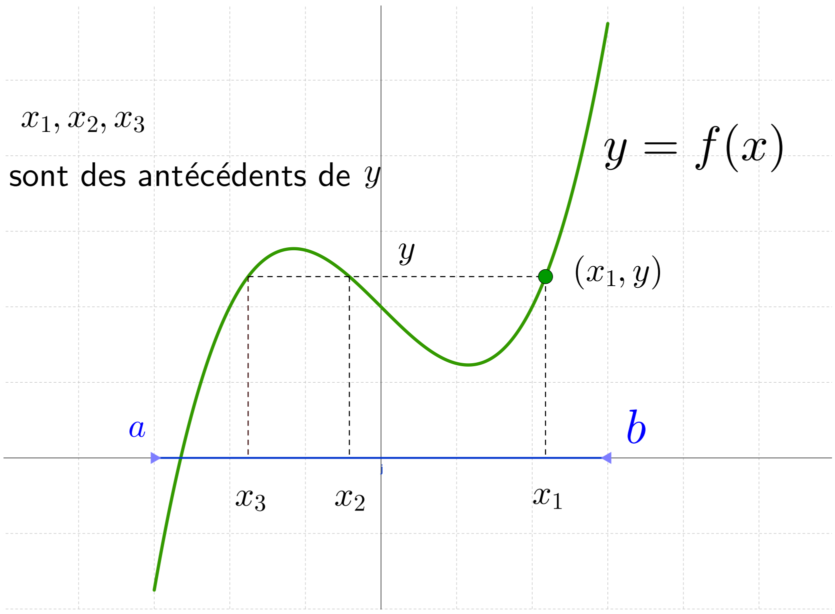
Définition 15.

Soit $f : X \to \mathbb{R}$ une fonction réelle de la variable réelle et à valeurs réelles.
On appelle **graphe** de f la partie de $\mathbb{R}^2$ suivante :

$$\{(x, f(x)), \quad x \in X\}$$

$$\text{qui peut aussi s'écrire} \qquad \left\{(x,y) \in \mathbb{R}^2 : x \in X \text{ et } y = f(x)\right\}.$$

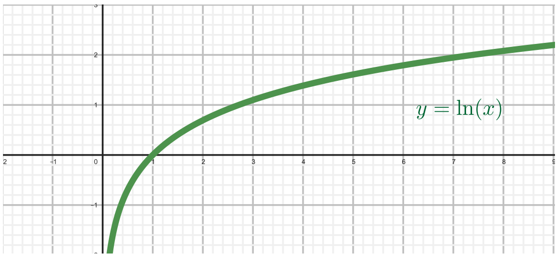
Supposons le plan muni d'un repère orthonormé $(O, \overrightarrow{i}, \overrightarrow{j})$. À chaque élément du graphe correspond alors un point du plan. Déposons une goutte d'encre sur chacun de ces points (ou noircissons le pixel correspondant). Le résultat est appelé **courbe représentative** de la fonction. Dans la pratique, on confond graphe et courbe représentative.

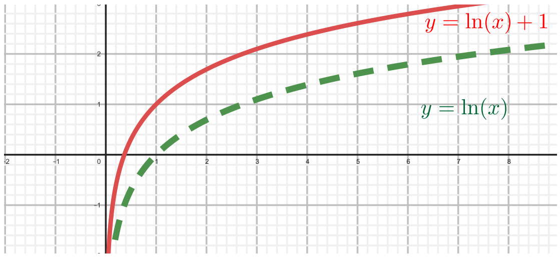


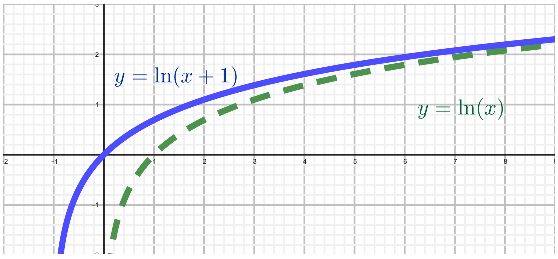
Graphe d'une fonction définie sur un segment $[a, b]$.

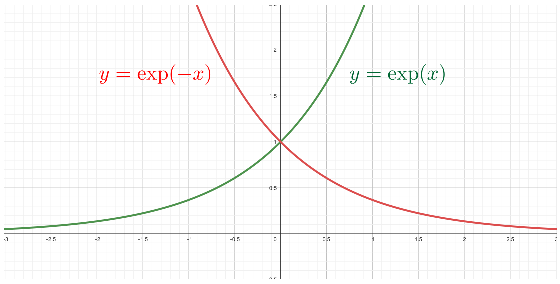
Remarque. Chaque fois qu'on représentera un graphe de fonctions dans la suite, il faudra bien sûr comprendre qu'il s'agit d'une fonction à valeurs réelles.

• Quelques graphes déduits de graphes de fonctions usuelles.

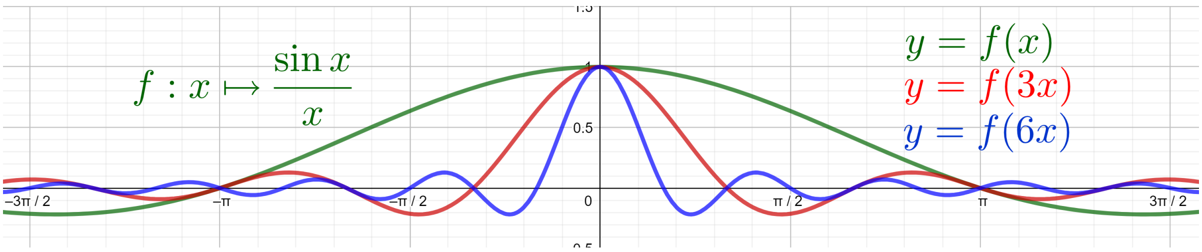








• Quel lien entre le graphe de f et celui de $x \mapsto f(ax)$, avec $a > 0$?

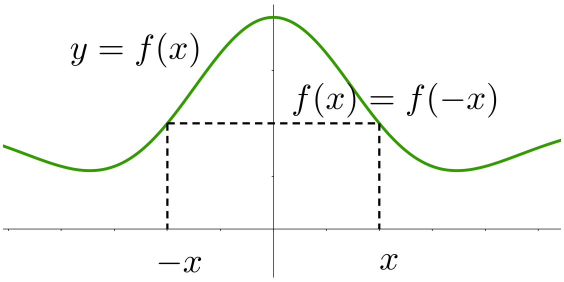


2.3 Parité, imparité.

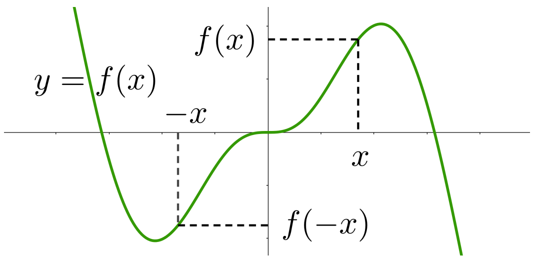
Définition 16.

Soit X une partie de $\mathbb{R}$. Une fonction $f : X \to \mathbb{K}$ est dite

• **paire** si $\forall x \in X \begin{cases} -x \in X \\ f(-x) = f(x) \end{cases}$ • **impaire** si $\forall x \in X \begin{cases} -x \in X \\ f(-x) = -f(x) \end{cases}$



Graphe d'une fonction paire.



Graphe d'une fonction impaire.

2.4 Périodicité.

Définition 17.

Soit $T > 0$ et X une partie de $\mathbb{R}$. Une fonction $f : X \to \mathbb{K}$ est dite T-**périodique** si

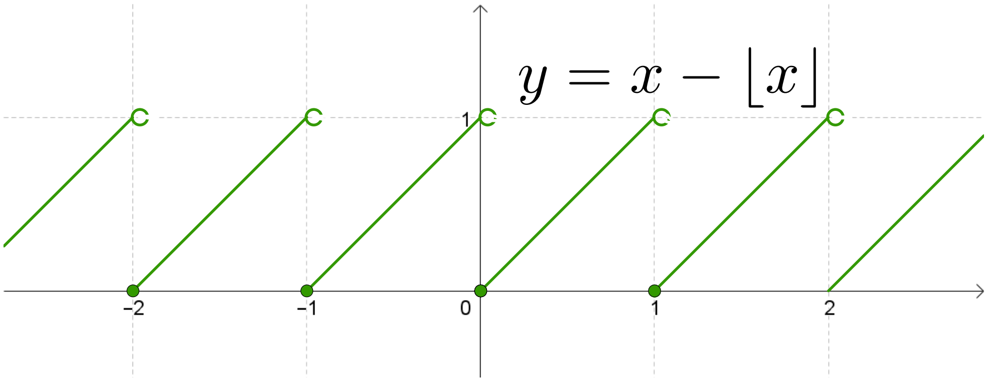
$$\forall x \in X \begin{cases} x + T \in X \\ f(x+T) = f(x) \end{cases}$$

On peut aussi dire que f « admet T pour période ».

Une fonction sera dite périodique si elle admet une certaine période $T \in \mathbb{R}_+^*$.

Exemples. cos et sin sont 2π-périodiques. La fonction tan est π-périodique sur son ensemble de définition. Un exemple de fonction à valeurs complexes : $t \mapsto e^{it}$, 2π-périodique.

Ci-dessous, le graphe de $x \mapsto x - \lfloor x \rfloor$, qui est 1-périodique.



Exemple 18.

Soit $f : \mathbb{R} \to \mathbb{K}$ une fonction T-périodique, où T est un réel strictement positif.

Montrer que $g : x \mapsto f(-x)$ est T-périodique.

Soit $a > 0$. Prouver que $h : x \mapsto f(ax)$ est T'-périodique, en précisant T'.

Méthode (Réduction de l'intervalle d'étude)**.**

Soit $f : X \to \mathbb{R}$.

- Si f est T périodique, son graphe est laissé invariant par la translation de vecteur $T\overrightarrow{i}$. Il suffit donc d'étudier une fonction T-périodique sur un intervalle de longueur T, le plus souvent $[0, T]$ ou $[-\frac{T}{2}, \frac{T}{2}]$. On obtient le reste du graphe par translations.
- Si f est paire, son graphe est symétrique par rapport à l'axe des ordonnées. Si f est impaire, il est invariant par la symétrie centrale de centre O. Il suffit alors d'étudier f sur $X \cap \mathbb{R}_+$. L'étude sur $X \cap \mathbb{R}_-$ vient par symétrie.

2.5 Monotonie.

Définition 19.

Soit $f : X \to \mathbb{R}$. Elle est dite

- **croissante** si $\quad \forall x \in X\ \forall x' \in X \quad x \leq x' \Longrightarrow f(x) \leq f(x')$.
- **décroissante** si $\quad \forall x \in X\ \forall x' \in X \quad x \leq x' \Longrightarrow f(x) \geq f(x')$.
- **strictement croissante** si $\quad \forall x \in X\ \forall x' \in X \quad x < x' \Longrightarrow f(x) < f(x')$.
- **strictement décroissante** si $\quad \forall x \in X\ \forall x' \in X \quad x < x' \Longrightarrow f(x) > f(x')$.

Lorsqu'une fonction a l'une des propriétés ci-dessus, elle est dite **monotone** (strictement monotone dans les deux derniers cas).

En bref et en français : une fonction est croissante si elle conserve les inégalités larges, strictement croissante si elle conserve les inégalités strictes.

Si $f : X \to \mathbb{R}$ et que $A \subset X$, on dira que f est **monotone** « sur A » si la restriction $f_{|A}$ est monotone.

Exemple 20.

Soit f une fonction paire sur $\mathbb{R}$ et croissante sur $\mathbb{R}_+$. Montrer que f est décroissante sur $\mathbb{R}_-$.

Proposition 21.

La fonction partie entière est croissante sur $\mathbb{R}$.

Exemple 22 (Un peu de logique)**.**

Soit f une fonction strictement croissante sur un intervalle I et $x, y \in I$. Démontrer l'équivalence

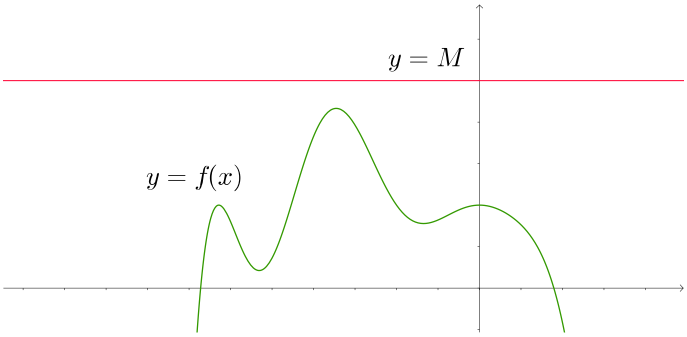
$$x < y \Longleftrightarrow f(x) < f(y).$$

2.6 Fonctions bornées.

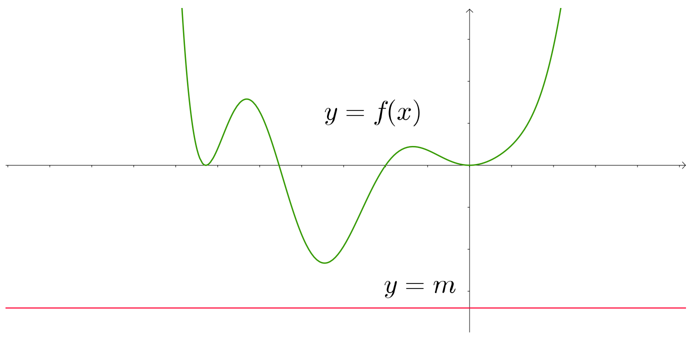
Définition 23.

Une fonction $f : X \to \mathbb{R}$ est dite

- **majorée** s'il existe $M \in \mathbb{R}$ tel que $\quad \forall x \in X\ f(x) \leq M$,
  (M étant alors appelé un **majorant** de f)
- **minorée** s'il existe $m \in \mathbb{R}$ tel que $\quad \forall x \in X\ f(x) \geq m$,
  (m étant alors appelé un **minorant** de f)
- **bornée** si elle est majorée et minorée.



Une fonction f majorée par un réel M.



Une fonction f minorée par un réel m.

Proposition 24 (Caractérisation des fonctions bornées)**.**

Soit $f : X \to \mathbb{R}$ une fonction.

$$f \text{ est bornée} \quad \iff \quad \exists \mu \in \mathbb{R}_+ \ \forall x \in X \quad |f(x)| \leq \mu.$$

Un slogan : « être borné, c'est être majoré en valeur absolue ».

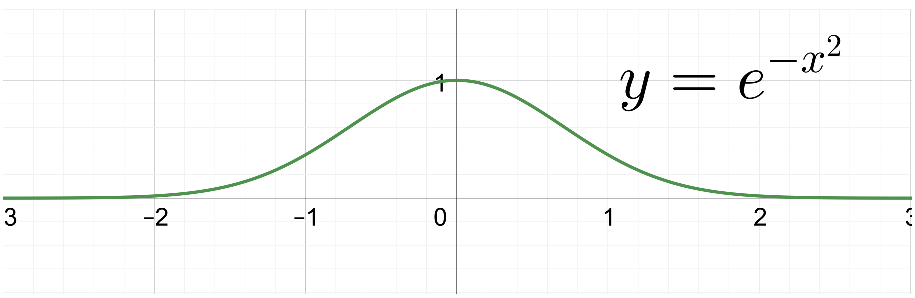
Définition 25.

Soit une fonction $f : X \to \mathbb{R}$ et $a \in X$. On dit que

- f admet (ou atteint) un **maximum** en a si $\forall x \in X \ f(x) \leq f(a)$,
- f admet (ou atteint) un **minimum** en a si $\forall x \in X \ f(x) \geq f(a)$,
- un **extremum** est un minimum ou un maximum.

Dans la définition précédente, $f(a)$ est le maximum de la partie de $\mathbb{R}$ $\{f(x), x \in X\}$, qui est l'ensemble de toutes les images par f. Il y a unicité de ce maximum, comme on l'a montré dans le cours de logique.

En revanche, ce maximum unique peut être atteint en plusieurs points ! Par exemple, la fonction cos admet un maximum (qui vaut 1) et ce maximum est atteint en tous les multiples de 2π.



La fonction $x \mapsto e^{-x^2}$ possède un maximum en 0, qui vaut 1. La fonction est minorée (par 0) mais ne possède pas de minimum. En effet, puisque la fonction est strictement décroissante sur $\mathbb{R}_+$, aucun minimum ne peut être atteint sur cet intervalle, idem pour $\mathbb{R}_-$.

2.7 Somme et produit de fonctions.

Définition 26.

Soient f et g définies sur un même ensemble $X \subset \mathbb{R}$, à valeurs réelles.
La **somme** de f et g est la fonction définie par

$$f+g : \left\{ \begin{array}{ccl} X & \to & \mathbb{K} \\ x & \mapsto & (f+g)(x) := f(x)+g(x) \end{array} \right. .$$

Définition 27.

Soient f et g définies sur un même ensemble $X \subset \mathbb{R}$, à valeurs réelles.
Le **produit** et le **quotient** de f et g sont les fonctions définies par

$$f \cdot g : \left\{ \begin{array}{ccl} X & \to & \mathbb{K} \\ x & \mapsto & (f \cdot g)(x) := f(x)g(x) \end{array} \right. \quad \text{et} \quad f/g : \left\{ \begin{array}{ccl} X & \to & \mathbb{K} \\ x & \mapsto & (f/g)(x) := \dfrac{f(x)}{g(x)} \end{array} \right. .$$

(pour que la définition du quotient ait un sens, il est nécessaire que g ne s'annule pas sur X).

Notation.

Si $f : X \mapsto \mathbb{K}$, la notation f^2 désignera la fonction $f \times f$. Ainsi,

$$\forall x \in X \quad f^2(x) = (f(x))^2 .$$

Exemple 28.

Montrer que le produit de deux fonctions impaires est une fonction paire.

Exemple 29.

Soient deux fonctions bornées f et g définies sur un même ensemble X.
Montrer que leur somme $f+g$ et leur produit fg sont des fonctions bornées.

Exemple 30 (Une preuve par analyse-synthèse)**.**

Démontrer le résultat ci-dessous.

Toute fonction définie sur $\mathbb{R}$ s'écrit de manière unique comme somme
d'une fonction paire et d'une fonction impaire.

Solution dans la partie 3 chapitre 0.

2.8 Bijections.

On rappelle la définition d'une bijection (donnée dans le cours sur les applications).

Rappel.

On dit qu'une fonction $f : I \to J$ est une **bijection** de I vers J si tout élément de J possède un unique antécédent dans I par f, ce qui s'écrit

$$\forall y \in J \quad \exists! x \in I \quad y = f(x).$$

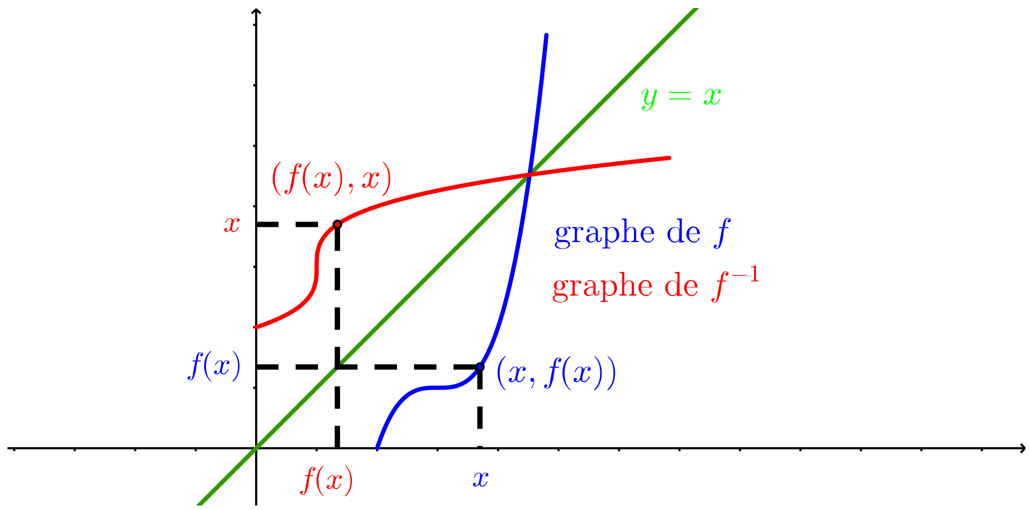
Si f est une bijection de I vers J, pour tout élément $y \in J$, on note $f^{-1}(y)$ son unique antécédent dans I par f. Ceci définit la **réciproque** de f :

$$f^{-1} : \left\{ \begin{array}{ccc} J & \to & I \\ y & \mapsto & f^{-1}(y) \end{array} \right. .$$

Exemple. $\exp : \mathbb{R} \to \mathbb{R}_+^*$ est une bijection et $\ln : \mathbb{R}_+^* \to \mathbb{R}$ est sa réciproque.

Proposition 31.

Soit $f : I \to J$ une bijection de I vers J.
Le graphe de $f^{-1} : J \to I$ est le symétrique de celui de f par rapport à la droite d'équation $y = x$.



Proposition 32.

Soit $f : I \to J$ une bijection.

1. Si f est strictement croissante (resp. strictement décroissante) sur I, alors f^{-1} est strictement croissante (resp. strictement décroissante sur J).
2. Si f est impaire, alors $f^{-1} : J \to I$ l'est aussi.

3 Continuité et applications.

Un cours sera consacré à la continuité, une fois définie rigoureusement la notion de limite. On se contente ici de quelques définitions et de résultats importants dont la preuve est différée.

3.1 Définition.

Définition 33.

Soit $f : I \to \mathbb{K}$ et $a \in I$. La fonction f est **continue en** a si

$$f(x) \underset{x \to a}{\longrightarrow} f(a).$$

Si f est continue en tout point de I, elle est dite **continue sur** I.

Exemple 34.

La plupart des fonctions usuelles sont continues sur leur intervalle de définition.
La fonction partie entière est continue (constante !) sur tous les intervalles de forme $]p, p+1[$ avec $p \in \mathbb{Z}$. Elle n'est continue en aucun point $p \in \mathbb{Z}$.

3.2 Continuité et opérations.

Proposition 35.

Si f et g sont continues sur I, alors leur somme et leur produit sont continus sur I.
Si f et g sont continues sur I et que g ne s'annule pas sur I, leur quotient est continu sur I.

Proposition 36.

Soient deux fonctions $f : I \to J$ et $g : J \to \mathbb{K}$.
Si f est continue sur I et g est continue sur J, alors la composée $g \circ f$ est continue sur I.

3.3 Théorème des valeurs intermédiaires.

Théorème 37 (des valeurs intermédiaires)**.**

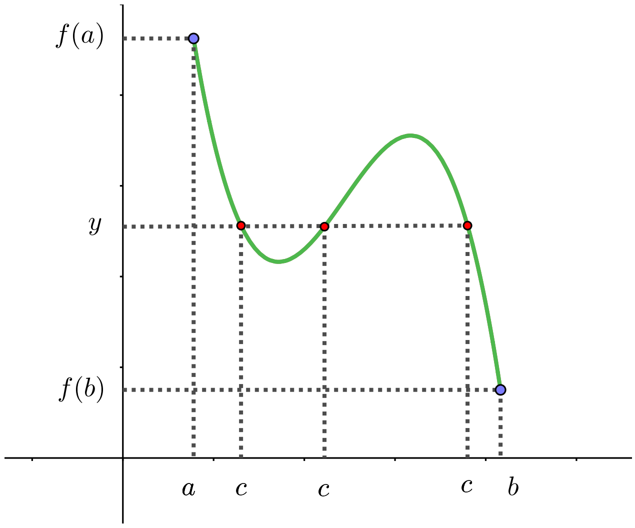
Soient deux réels $a \leq b$ et $f : [a, b] \to \mathbb{R}$ continue. Alors, pour tout réel y entre $f(a)$ et $f(b)$,

$$\exists c \in [a, b] \quad y = f(c).$$

Corollaire 38 (Changement de signe d'une fonction continue)**.**

Si une fonction continue sur un intervalle y change de signe, alors elle s'annule sur cet intervalle.

Autrement dit, toute *valeur intermédiaire* entre $f(a)$ et $f(b)$ possède (au moins) un antécédent par f. Comme on le voit dans l'illustration ci-dessous, il n'y a pas forcément unicité de l'antécédent.



Le TVI pourra donc être utilisé pour prouver l'existence d'une solution à une équation. Ceci est illustré par le corollaire suivant, qui revient à prouver l'existence d'une solution à une équation de forme $f(x) = 0$. Voici maintenant un corollaire où l'hypothèse de stricte monotonie est ajoutée. Il pourra être utilisé pour prouver l'existence et l'unicité d'une solution à une équation.

Corollaire 39 (TVI strictement monotone).

Soit $f : [a, b] \to \mathbb{R}$ continue et strictement monotone sur $[a, b]$. Pour tout réel y entre $f(a)$ et $f(b)$,

$$\exists! c \in [a, b] \quad y = f(c).$$

Théorème 40 (Théorème de la bijection continue).

Soit I un intervalle de $\mathbb{R}$ et $f : I \to \mathbb{R}$ une fonction.

Si f est strictement monotone et continue sur I, alors elle réalise une bijection de I dans $f(I)$.

On rappelle que la notation $f(I)$ désigne l'ensemble de toutes les images par f des éléments de I :

$$f(I) = \{f(x), x \in I\} = \{y \in J \mid \exists x \in I : y = f(x)\}.$$

Dans le cours sur la continuité, on démontrera de surcroît que

- L'ensemble $f(I)$ est un intervalle.
- Sur cet intervalle, f^{-1} est strictement monotone, de même monotonie que f.
- Sur cet intervalle, la réciproque f^{-1} est continue.

Dans la pratique, l'intervalle $f(I)$ est déterminé à partir de la forme de I et des limites aux bornes de f :

$f(I)$ dans les huit cas :

I	$[a, b]$	$]a, b]$	$[a, b[$	$]a, b[$
$f \nearrow$	$[f(a), f(b)]$	$]\lim\limits_{a} f, f(b)]$	$[f(a), \lim\limits_{b} f[$	$]\lim\limits_{a} f, \lim\limits_{b} f[$
$f \searrow$	$[f(b), f(a)]$	$[f(b), \lim\limits_{a} f[$	$]\lim\limits_{b} f, f(a)]$	$]\lim\limits_{b} f, \lim\limits_{a} f[$

4 Dérivabilité et applications.

4.1 Définitions.

Un cours sera consacré à la dérivabilité, une fois définie rigoureusement la notion de limite. On se contente ici de quelques définitions et de résultats importants dont la preuve est différée.

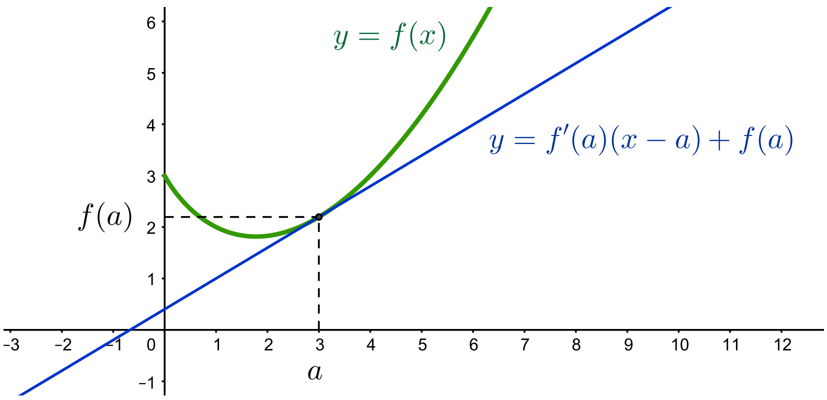
Définition 41.

Soit $f : I \to \mathbb{K}$ et $a \in I$. La fonction f est **dérivable en** a si

$$\frac{f(x) - f(a)}{x - a} \qquad (x \neq a)$$

a une limite finie lorsque x tend vers a. On note alors $f'(a) = \lim\limits_{x \to a} \frac{f(x)-f(a)}{x-a}$.

Si f est dérivable en tout point de I, elle est dite **dérivable sur** I.
La fonction $f' : \left\{ \begin{array}{ccc} I & \to & \mathbb{K} \\ x & \mapsto & f'(x) \end{array} \right.$, est alors appelée **dérivée** de f.



Tangente en un point au graphe de f.

Figure. Par les points $(a, f(a))$ et $(x, f(x))$ passe une droite appelée corde, de pente $\frac{f(x)-f(a)}{x-a}$.

Lorsque x se rapproche de a, cette corde "tend" vers une droite qui effleure la courbe de f en a : c'est la tangente. La pente de la corde tend vers celle de la tangente : $f'(a)$.

L'équation de la tangente est $\boxed{y = f'(a)(x - a) + f(a).}$

Exemple 42.

Continuité et dérivabilité de la fonction $x \mapsto \sqrt{x}$.

Proposition 43.

Si une fonction est dérivable, alors elle est continue. La réciproque est fausse.

Tableau des dérivées usuelles : (X est l'ensemble où la fonction f est dérivable)

$f(x)$	$f'(x)$	X
$x^n (n \in \mathbb{N})$	nx^{n-1}	$\mathbb{R}$
$x^p (p \in \mathbb{Z})$	px^{p-1}	$\mathbb{R}^*$
$\frac{1}{x}$	$-\frac{1}{x^2}$	$\mathbb{R}^*$
$x^a (a \in \mathbb{R})$	ax^{a-1}	$\mathbb{R}_+^*$
$\sqrt{x}$	$\frac{1}{2\sqrt{x}}$	$\mathbb{R}_+^*$
e^x	e^x	$\mathbb{R}$
$\ln(x)$	$\frac{1}{x}$	$\mathbb{R}_+^*$

$f(x)$	$f'(x)$	X
$\mathrm{ch}(x)$	$\mathrm{sh}(x)$	$\mathbb{R}$
$\mathrm{th} x$	$\begin{cases} 1 - \mathrm{th}^2 x \\ \frac{1}{\mathrm{ch}^2 x} \end{cases}$	$\mathbb{R}$
$\mathrm{sh}(x)$	$\mathrm{ch}(x)$	$\mathbb{R}$
$\cos x$	$-\sin x$	$\mathbb{R}$
$\sin x$	$\cos x$	$\mathbb{R}$
$\tan x$	$\begin{cases} 1 + \tan^2 x \\ \frac{1}{\cos^2 x} \end{cases}$	$D_{\tan}$

4.2 Dérivabilité et opérations.

Proposition 44 (Dérivée d'une somme, d'un produit, d'un quotient)**.**

Soient deux fonctions $f, g : I \to \mathbb{K}$, dérivables sur l'intervalle I. Soit $\lambda \in \mathbb{R}$.

- La fonction $f + g$ est dérivable sur I et $(f + g)' = f' + g'$.
- La fonction λf est dérivable sur I et $(\lambda f)' = \lambda f'$.
- La fonction fg est dérivable sur I et $(fg)' = f'g + fg'$.
- Si g ne s'annule pas sur I, la fonction fonction f/g est dérivable sur I et $\left(\frac{f}{g}\right)' = \frac{gf' - fg'}{g^2}$.

Théorème 45 (Dérivée d'une composée)**.**

Soient deux fonctions $f : I \to J$ et $g : J \to \mathbb{K}$.
Si f est dérivable sur I, et si g est dérivable sur J, alors la composée $g \circ f$, est dérivable sur I et

$$\boxed{(g \circ f)' = f' \cdot (g' \circ f)} \quad \text{i.e.} \quad \forall x \in I \quad (g \circ f)'(x) = f'(x) \cdot g'(f(x)).$$

Méthode (Justifier qu'une composée est dérivable)**.**

« La fonction f est dérivable sur I et $\forall x \in I$ $f(x) \in J$. De plus, la fonction g est dérivable sur J. D'après le théorème de dérivation des composées, $g \circ f$ est dérivable sur I. »

Noter qu'on a vérifié les trois hypothèses du théorème :

1. la dérivabilité de f sur l'intervalle I considéré,
2. la dérivabilité de g sur l'intervalle J considéré,
3. le fait que les images par f des éléments de I sont des éléments de J.

Un premier cas particulier : si g est une fonction dérivable sur $\mathbb{R}$, alors pour tous a et b réels, puisque $x \mapsto ax+b$ est dérivable sur $\mathbb{R}$, la fonction composée $x \mapsto g(ax+b)$ l'est aussi par théorème. On a

$$\frac{\mathrm{d}}{dx} g(ax+b) = \frac{\mathrm{d}}{\mathrm{d}x}(ax+b) \cdot g'(ax+b) \qquad \text{soit} \quad \boxed{\frac{\mathrm{d}}{dx} g(ax+b) = a \cdot g'(ax+b).}$$

Par exemple,

$$\frac{\mathrm{d}}{\mathrm{d}x}\sin(3x) = 3\cos(3x) \qquad\qquad \frac{\mathrm{d}}{\mathrm{d}x}\sqrt{7x+1} = \frac{7}{2\sqrt{7x+1}}.$$

Corollaire 46 (Cas particuliers courants)**.**

Soit $u : I \to \mathbb{R}$, dérivable sur I, alors

- la fonction e^u est dérivable sur I et $\boxed{(e^u)' = u'e^u}$.
- u^n est dérivable sur I et $(u^n)' = nu'u^{n-1}$.

Si de surcroît,

- $u : I \to \mathbb{R}^*$, alors la fonction $1/u$ est dérivable sur I et $\boxed{\left(\frac{1}{u}\right)' = -\frac{u'}{u^2}}$.
- $u : I \to \mathbb{R}_+^*$, alors pour tout réel a, u^a est dérivable sur I, et $\boxed{(u^a)' = au'u^{a-1}}$.

  Notamment, $\boxed{(\sqrt{u})' = \frac{u'}{2\sqrt{u}}}$.
- $u : I \to \mathbb{R}_+^*$, la fonction $\ln(u)$ est dérivable sur I et $\boxed{(\ln(u))' = \frac{u'}{u}}$.

Remarque. À quoi sert de regarder des cas particuliers puisqu'on a une formule simple dans le cas général ? La réponse est à chercher du côté du calcul de primitives : nous aurons besoin de savoir « dériver à l'envers » : il est donc utile de bien connaître la forme des dérivées de composées dans les cas courants.

4.3 Dérivée d'une réciproque.

Théorème 47 (Dérivée d'une réciproque)**.**

Soit une bijection $f : I \to J$, dérivable sur I.
Sa réciproque f^{-1} est dérivable sur J si et seulement si f' ne s'annule pas sur I. On a alors

$$\boxed{\left(f^{-1}\right)' = \frac{1}{f' \circ f^{-1}}} \qquad \text{i.e.} \qquad \forall y \in J \quad \left(f^{-1}\right)'(y) = \frac{1}{f'(f^{-1}(y))}.$$

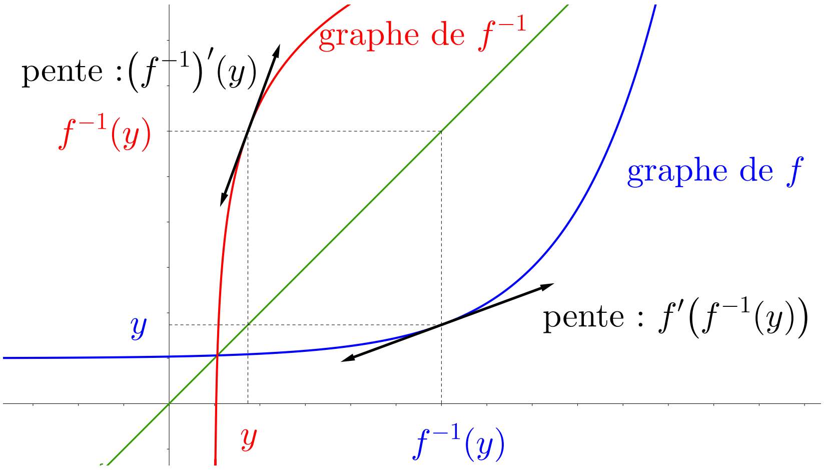
Exemple 48.

Donner un exemple de bijection entre deux intervalles I et J, dérivable sur I et dont la réciproque n'est pas dérivable sur J. Illustrer.

Exemple 49.

Appliquer le théorème pour retrouver le résultat connu sur la dérivée de ln.

Les nombres $f'\left(f^{-1}(y)\right)$ et $\left(f^{-1}\right)'(y)$ sont les pentes respectivement d'une tangente à la courbe de f et d'une tangente à la courbe de f^{-1}. Symétriques par rapport à $y = x$, leurs pentes sont inverses l'une de l'autre.



Ceci n'est pas une preuve.

4.4 Variations des fonctions dérivables.

Théorème 50 (Caractérisation des fonctions monotones parmi les fonctions dérivables)**.**

Soit I un intervalle, et $f : I \to \mathbb{R}$ une fonction dérivable sur I.

- f est croissante sur I si et seulement si f' est positive sur I.
- f est décroissante sur I si et seulement si f' est négative sur I.
- f est constante sur I si et seulement si f' est nulle sur I.

Proposition 51 (Caract. des fonctions strict. monotones parmi les fonctions dérivables)**.**

Soit I un intervalle et $f : I \to \mathbb{R}$, dérivable sur I.
La fonction f est strictement croissante sur I si et seulement si f' est positive (ou nulle) sur I et n'est identiquement nulle sur aucun intervalle $[a, b]$ inclus dans I avec $a < b$.

Corollaire 52 (Dans la pratique)**.**

Soit I un intervalle, et $f : I \to \mathbb{R}$ une fonction dérivable sur I.

- Si f' est strictement positive sur I, alors f y est strictement croissante. Réciproque fausse.
- Si f' est strictement négative sur I, alors f y est strictement décroissante. Réciproque fausse.

L'implication demeure vraie si f' ne s'annule qu'en un nombre fini de points de I.

Méthode (Conseils pour l'étude d'une fonction).

- Déterminer son ensemble de définition.
- Détecter une éventuelle parité/imparité/périodicité et réduire en conséquence le domaine d'étude.
- Pour l'étude des variations, on ne se rue pas sur la dérivation si la fonction est une somme ou une composée de fonctions croissantes, par exemple !
- Dans le cas où on dérive, on justifie sur quel ensemble et pourquoi on peut le faire, soigneusement.
- Calcul de la dérivée. Puisque c'est son signe qui nous intéressera, on cherche à la **factoriser** le plus possible !
- Étude du signe de la dérivée : il suffira la plupart du temps de résoudre l'**inéquation** $f'(x) \geq 0$.
- Tableau de signe pour la dérivée, de variations pour la fonction.
- Calcul des limites aux bords. Si on détecte une incohérence, il est encore temps de se relire !
- Esquisser un graphe résumant l'étude. Ne pas hésiter à y souligner des valeurs, ou des tangentes notables.

4.5 Dériver une fonction à valeurs complexes.

Définition 53.

Soit $f : I \to \mathbb{C}$ une fonction. On dit que f est **dérivable** sur I si les fonctions $\mathrm{Re}(f) : x \mapsto \mathrm{Re}(f(x))$ et $\mathrm{Im}(f) : x \mapsto \mathrm{Im}(f(x))$ sont toutes deux dérivables sur I.

La **dérivée** de f est alors définie comme la fonction $f' : \begin{cases} I & \to & \mathbb{C} \\ x & \mapsto & \mathrm{Re}(f)'(x) + i\mathrm{Im}(f)'(x) \end{cases}$.

Remarque. Par définition même de f', les égalités ci-dessous sont vraies dès qu'elles ont un sens

$$(\mathrm{Re}(f))'(x) = \mathrm{Re}\left(f'(x)\right) \qquad \text{et} \qquad (\mathrm{Im}(f))'(x) = \mathrm{Im}\left(f'(x)\right)$$

Proposition 54.

Soit $\varphi : I \to \mathbb{C}$ une fonction dérivable sur I. Soit $f : t \mapsto e^{\varphi(t)}$.
La fonction f est dérivable sur I et

$$\forall t \in I \quad f'(t) = \varphi'(t)e^{\varphi(t)}.$$

Preuve. Notons $a : t \mapsto \mathrm{Re}(\varphi(t))$ et $b : t \mapsto \mathrm{Im}(\varphi(t))$, définies sur I. On a,

$$\forall t \in I \quad f(t) = e^{a(t)}e^{ib(t)} = e^{a(t)}\left(\cos(b(t)) + i\sin(b(t))\right).$$

On a donc que $\mathrm{Re}(f) = e^a \cos b$ et $\mathrm{Im}(f) = e^a \sin b$. La fonction a est dérivable sur I, exp l'est sur $\mathbb{R}$ donc la composée $e^a : I \to \mathbb{R}$ est dérivable sur I. De même, les deux fonction à valeurs réelles $\cos b$ et $\sin b$ sont des composées dérivables sur I. Par produit, on obtient que $\mathrm{Re}(f)$ et $\mathrm{Im}(f)$ sont dérivables sur I. On peut donc dire, conformément à la dernière définition, que f est dérivable sur I. On a

$$\begin{aligned} f' = \mathrm{Re}(f)' + i\mathrm{Im}(f)' &= (a'e^a \cos b - b'e^a \sin b) + i\,(a'e^a \sin b + b'e^a \cos b) \\ &= e^a\left[a'(\cos b + i\sin b) + ib'(\cos b + i\sin b)\right] \\ &= (a' + ib')e^a e^{ib} = \varphi' e^{\varphi} \end{aligned}$$

□

Solutions des exercices donnés comme exemples.

Exemple 1. Inégalité arithmético-géométrique.

Soit $(x, y) \in \mathbb{R}^2$ un réel.

$$\begin{aligned}\frac{x+y}{2} - \sqrt{xy} &= \frac{1}{2}\left((x+y) - 2\sqrt{xy}\right) \\ &= \frac{1}{2}\left((\sqrt{x})^2 + (\sqrt{y})^2 - 2\sqrt{x}\sqrt{y}\right) \\ &= \frac{1}{2}\left((\sqrt{x} - \sqrt{y})^2\right)\end{aligned}$$

Cette différence est positive, ceci prouve l'inégalité.

$$\boxed{\sqrt{xy} \leq \frac{x+y}{2}}$$

Il y a égalité si et seulement si la différence est nulle, ce qui arrive si et seulement si $x = y$.

Exemple 14. Ensembles de définition.

- Pour x réel, l'expression définissant $f(x)$ a un sens si et seulement si $x(x-2)$ est positif, c'est-à-dire si x appartient à $\boxed{]-\infty, 0] \cup [2, +\infty[}$.
- Pour x réel, l'expression définissant $g(x)$ a un sens, si et seulement si $x(x-2)$ est strictement positif, c'est-à-dire si x appartient à $\boxed{]-\infty, 0[\cup]2, +\infty[}$.
- Pour x réel, l'expression définissant $h(x)$ a un sens, si et seulement si x et $(x-2)$ sont strictement positifs, c'est-à-dire si x appartient à $\boxed{]2, +\infty[}$.

Exemple 18. $f : \mathbb{R} \to \mathbb{K}$ est T-périodique.

- Montrons que $g : x \mapsto f(-x)$ est T-périodique.
  Soit $x \in \mathbb{R}$. Bien sûr, $x + T \in \mathbb{R}$. On a

  $$g(x+T) = f(-(x+T)) = f(-x+T) \underset{(*)}{=} f(-x-T+T) = f(-x) = g(x),$$

  où on utilise la T-périodicité de f pour écrire $(*)$.
- Montrons que $h : x \mapsto f(ax)$ est $\frac{T}{a}$-périodique. Soit $x \in \mathbb{R}$. Bien sûr $x + \frac{T}{a} \in \mathbb{R}$. On a

  $$h\left(x + \frac{T}{a}\right) = f\left(a(x + \frac{T}{a})\right) = f(ax+T) \underset{(*)}{=} f(x).$$

Exemple 20. f est une fonction paire et croissante sur $\mathbb{R}_+$. Il s'agit de montrer que f est décroissante sur $\mathbb{R}_-$.

Soit $(x, y) \in (\mathbb{R}_-)^2$. On suppose que $x \leq y$.
Ramenons-nous sur $\mathbb{R}_+$ en multipliant par -1. On avait $x \leq y \leq 0$, on a $0 \leq -y \leq -x$. Par croissance de f sur $\mathbb{R}_+$, on a $f(-y) \leq f(-x)$. Par parité de f, on obtient $f(y) \leq f(x)$.

Exemple 21. Soit $f : I \to \mathbb{R}$ strictement croissante, $(x, y) \in I$.

- L'implication $x < y \Longrightarrow f(x) < f(y)$ est vraie par définition de la stricte croissance de f.
- Montrons que $f(x) < f(y) \Longrightarrow x < y$ par contraposée. Supposons que l'inégalité $x < y$ est fausse, c'est-à-dire supposons que $x \geq y$. Puisque f est croissante, on a $f(x) \geq f(y)$. L'inégalité $f(x) < f(y)$ est donc fausse.

Exemple 28. Produit de deux fonctions impaires.
Soient deux fonctions impaires définies sur une même partie X de $\mathbb{R}$. Soit $x \in X$. Par hypothèse sur f, $-x \in X$. De plus,

$$(f \cdot g)(-x) = f(-x) \cdot g(-x) = (-f(x))(-g(x)) = (-1)^2 f(x)g(x) = (f \cdot g)(x).$$

La fonction $f \cdot g$ est bien paire.

Exemple 29. Soient deux fonctions bornées f et g définies sur un même ensemble X.

- Montrons que leur somme $f + g$ est bornée sur X. Notons m et M respectivement un minorant et un majorant de f, et m' et M' respectivement un minorant et un majorant de g.
  Soit $x \in X$. On a
  $$\begin{cases} m \leq f(x) \leq M \\ m' \leq g(x) \leq M' \end{cases}$$
  Sommons ces inégalités ! On obtient
  $$m + m' \leq (f + g)(x) \leq M + M'.$$
  Ceci démontre que $f + g$ est bornée : elle est minorée par $m + m'$ et majorée par $M + M'$.
- Montrons que leur somme $f + g$ est borné sur X. On ne peut pas faire le produit des inégalités écrites plus haut pour la somme car on ne sait pas quel est le signe des réels comparés. On va donc utiliser la caractérisation des fonctions bornées utilisant une valeur absolue. Puisque f et g sont bornées, elles sont majorées en valeurs absolue. Notons μ et μ' deux majorants respectifs de $|f|$ et $|g|$. Soit $x \in X$. On a
  $$\begin{cases} 0 \leq |f(x)| \leq \mu \\ 0 \leq |g(x)| \leq \mu' \end{cases}$$
  On peut faire le produit de ces inégalités dont les membres sont positifs :
  $$|f(x)| \cdot |g(x)| \leq \mu \cdot \mu' \quad \text{soit} \quad |(fg)(x)| \leq \mu\mu'.$$
  La fonction fg est majorée en valeur absolue : elle est bien bornée.

Exercices

Partie entière, valeur absolue.

$\boxed{7.1}$ **[♦♦◇]** Démontrer que

$$\forall x \in \mathbb{R}_+ \quad \lfloor \sqrt{\lfloor x \rfloor} \rfloor = \lfloor \sqrt{x} \rfloor.$$

$\boxed{7.2}$ **[♦♦♦]** Démontrer que

$$\forall x, y \in \mathbb{R} \quad \lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1.$$

$\boxed{7.3}$ **[♦◇◇]** Résoudre l'équation

$$\ln|x| + \ln|x+1| = 0.$$

$\boxed{7.4}$ **[♦♦◇]** Résoudre l'inéquation

$$|2x+1| < |x+2|.$$

$\boxed{7.5}$ **[♦♦◇]** Résoudre l'inéquation

$$|2x+1| < x+2.$$

$\boxed{7.6}$ **[♦◇◇]** Soit x un réel. Démontrer que :

$$\forall n \in \mathbb{N} \quad |\sin(nx)| \leq n|\sin x|.$$

$\boxed{7.7}$ **[♦♦◇]**

1. Étudier les variations de $f : x \mapsto \dfrac{x}{1+x}$ sur $[0, +\infty[$.
2. Prouver que

$$\forall x, y \in \mathbb{R} \quad \frac{|x+y|}{1+|x+y|} \leq \frac{|x|}{1+|x|} + \frac{|y|}{1+|y|}.$$

Vocabulaire sur les fonctions

$\boxed{7.8}$ **[♦◇◇]** Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction 2 périodique et 3-périodique. Montrer que f est 1-périodique.

$\boxed{7.9}$ **[♦♦◇]** Soit $f : X \to \mathbb{R}$. Démontrer que si f est bornée sur X, alors $x \mapsto \lfloor f(x) \rfloor$ l'est aussi.

$\boxed{7.10}$ **[♦♦♦]** Déterminer toutes les fonctions croissantes $f : \mathbb{R} \to \mathbb{R}$ telles que

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

$\boxed{7.11}$ **[♦◇◇]** Considérons la fonction $f : \begin{cases}]1, +\infty[& \to & \mathbb{R} \\ x & \mapsto & \exp\left(-\frac{1}{\ln(x)}\right) \end{cases}$

1. Démontrer que f réalise une bijection de $]1, +\infty[$ dans un intervalle que l'on précisera.
2. Expliciter la réciproque de f. Peut-on écrire en conclusion que $f^{-1} = f$?

Étude de fonctions.

$\boxed{7.12}$ **[♦◇◇]** [S'entraîner tout seul à dériver.]
Pour chacune des fonctions ci-dessous, donner un ou plusieurs intervalles sur lesquels la fonction est dérivable, et préciser sa dérivée (réponses ci-dessous).

$$A : x \mapsto x^{\pi}, \quad B : x \mapsto \pi^{x}, \quad C : x \mapsto \cos(5x), \quad D : x \mapsto \ln(1+x^3),$$

$$E : x \mapsto \cos\left(\sqrt{\ln(x)}\right), \quad F : x \mapsto \frac{1}{\sqrt{3x-1}}, \quad G : x \mapsto \sin|x+1|,$$

Réponses pour le premier exercice.

- La fonction A est dérivable sur $\mathbb{R}_+^*$ (cours : fonction usuelle).
  On a $\forall x \in \mathbb{R}_+^*$ $A'(x) = \pi x^{\pi-1}$.
- Par définition : $B : x \mapsto e^{x\ln(\pi)}$. Cette fonction est clairement dérivable sur $\mathbb{R}$
  et $\forall x \in \mathbb{R}$ $B'(x) = \ln(\pi)e^{x\ln(\pi)} = \ln(\pi)\pi^x$.
- C est dérivable sur $\mathbb{R}$ et $\forall x \in \mathbb{R}$ $C'(x) = -5\sin(5x)$.
- D est dérivable sur $\mathbb{R} \setminus \{-1\}$, c'est-à-dire sur $]-\infty,-1[$ et sur $]-1,+\infty[$.
  $\forall x \in \mathbb{R} \setminus \{-1\}$ $E'(x) = \frac{3x^2}{1+x^3}$.
- E est dérivable sur $]1,+\infty[$ et $\forall x \in]1,+\infty[$ $F'(x) = -\frac{\sin(\sqrt{\ln(x)})}{2x\sqrt{\ln(x)}}$.
- On a $F : x \mapsto (3x-1)^{-1/2}$. Sur $]\frac{1}{3},+\infty[$, $F'(x) = -\frac{3}{2}(3x-1)^{-3/2}$.
- Sur $]-1,+\infty[$, $G(x) = \sin(x+1)$ et $G'(x) = \cos(x+1)$.
  Sur $]-\infty,-1[$, $G(x) = \sin(-x-1)$ et $G'(x) = -\cos(-x-1)$.

$\boxed{7.13}$ **[♦♦◇]**

1. Démontrer que
$$\forall x \in]-1,+\infty[\quad \frac{x}{1+x} \leq \ln(1+x) \leq x.$$
2. À l'aide du théorème des gendarmes, calculer $\lim\limits_{x\to 0} \dfrac{\ln(1+x)}{x}$.
3. Retrouver ce résultat en faisant apparaître un taux d'accroissement.

$\boxed{7.14}$ **[♦♦◇]** Démontrer l'inégalité

$$\forall x \in]0,1[\quad x^x(1-x)^{1-x} \geq \frac{1}{2}.$$

$\boxed{7.15}$ **[♦♦◇]** Soit la fonction $f : x \mapsto \ln\left(\sqrt{x^2+1}-x\right)$.

1. Donner le domaine de définition de f.
2. Montrer que f est impaire.
3. Étudier ses variations et donner le tableau correspondant.

$\boxed{7.16}$ **[♦♦◇]** Notons a le nombre $\sqrt[3]{20+14\sqrt{2}} + \sqrt[3]{20-14\sqrt{2}}$.

1. Montrer que $a^3 = 6a + 40$.
2. En déduire la valeur de a.

$\boxed{7.17}$ **[♦♦♦]** Soit $(a,b) \in \mathbb{R}^2$ tel que $b \geq a > 0$.

1. Étudier sur $\mathbb{R}_+^*$ les variations de la fonction $f : x \longmapsto \dfrac{\ln(1+ax)}{\ln(1+bx)}$.
   Indication : le signe de la dérivée n'est pas évident... ne pas hésiter à refaire une étude de fonction !
2. En déduire que
$$\ln\left(1+\frac{a}{b}\right) \times \ln\left(1+\frac{b}{a}\right) \leq \ln^2(2).$$

Neuf fonctions usuelles

1 Fonctions circulaires : cos, sin, tan.

Proposition 1.

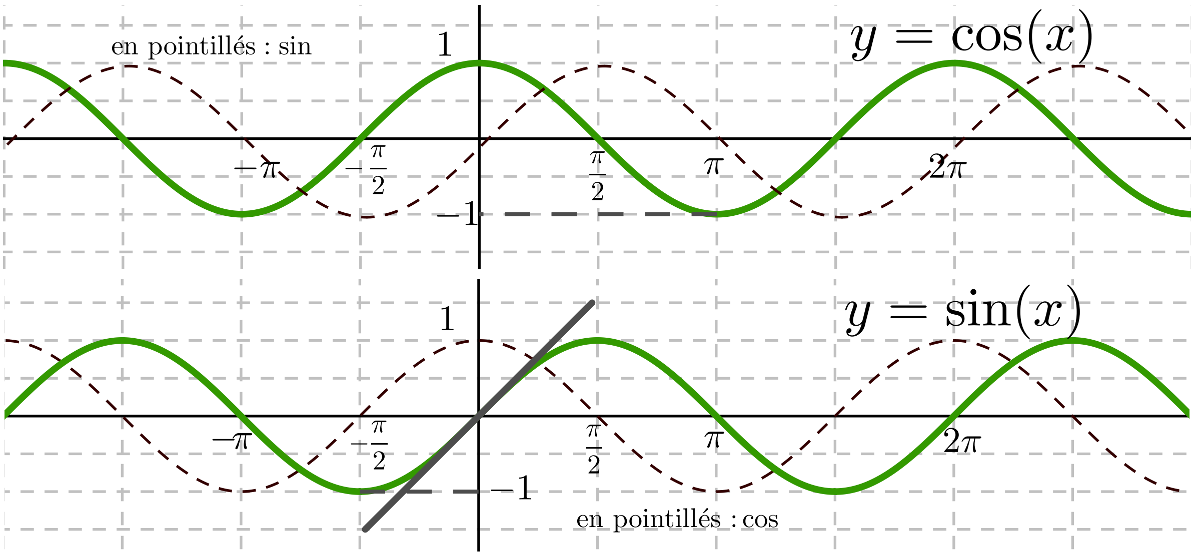
La fonction cos est paire, et la fonction sin impaire. Elles sont toutes deux 2π-périodiques.
Le graphe de sin se déduit de celui de cos par la translation de vecteur $\frac{\pi}{2}\overrightarrow{i}$.

Proposition 2.

Les fonctions cosinus et sinus sont dérivables sur $\mathbb{R}$, de dérivées

$$\cos' = -\sin \qquad \text{et} \qquad \sin' = \cos\,.$$

Preuve : en annexe, à la fin.



Proposition 3.

$$\forall x \in \mathbb{R} \quad |\sin(x)| \leq |x|.$$

Définition 4.

On appelle fonction **tangente** et on note tan la fonction définie par

$$\tan : \left\{ \begin{array}{ccc} D_{\tan} & \to & \mathbb{R} \\ x & \mapsto & \tan(x) := \dfrac{\sin x}{\cos x} \end{array} \right. \qquad \text{où} \quad D_{\tan} = \mathbb{R} \setminus \left\{ \frac{\pi}{2} + k\pi, k \in \mathbb{Z} \right\}.$$

L'écriture de $D_{\tan}$ comme réunion d'intervalles disjoints de longueur π :

$$D_{\tan} = \bigcup_{k \in \mathbb{Z}} \left] -\frac{\pi}{2} + k\pi, \frac{\pi}{2} + k\pi \right[.$$

Proposition 5.

Sur $D_{\tan}$, la fonction tangente est impaire et π-périodique.

La π-périodicité permet de réduire l'étude à un intervalle de longueur π, ce qui est le cas de $]-\frac{\pi}{2}, \frac{\pi}{2}[$.

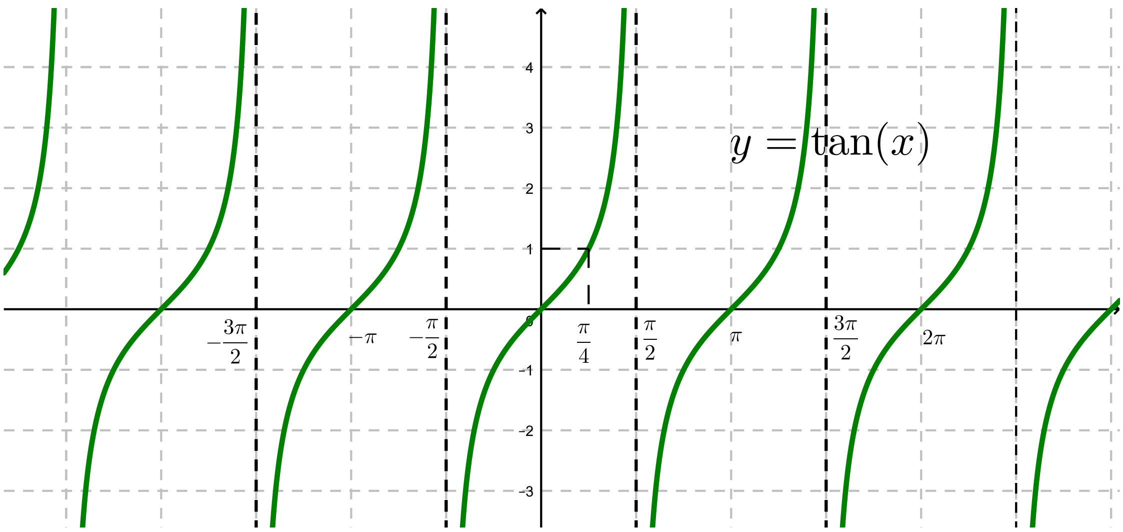
Proposition 6 (Valeurs et limites notables)**.**

$$\tan(0) = 0, \qquad \tan\left(\frac{\pi}{4}\right) = 1, \qquad \tan\left(\frac{\pi}{3}\right) = \sqrt{3}, \qquad \lim_{\substack{x \to \frac{\pi}{2} \\ x < \frac{\pi}{2}}} \tan(x) = +\infty, \qquad \lim_{\substack{x \to -\frac{\pi}{2} \\ x > -\frac{\pi}{2}}} \tan(x) = -\infty$$

Proposition 7.

La fonction tangente est dérivable sur $D_{\tan}$ et

$$\forall x \in D_{\tan} \quad \tan'(x) = \frac{1}{\cos^2(x)} = 1 + \tan^2(x).$$



Proposition 8 (Formules d'addition)**.**

Pour tous réels a et b tels que les nombres ci-dessous ont un sens,

$$\tan(a+b) = \frac{\tan a + \tan b}{1 - \tan a \tan b}, \qquad \tan(a-b) = \frac{\tan a - \tan b}{1 + \tan a \tan b}, \qquad \tan(2a) = \frac{2\tan a}{1 - \tan^2 a}.$$

Corollaire 9 (Identités à savoir retrouver)**.**

Soit $a \in \mathbb{R}\backslash\{\pi+2k\pi, k \in \mathbb{Z}\}$, c'est-à-dire que a est un réel tel que $\frac{a}{2} \in D_{\tan}$. En notant $t = \tan\left(\frac{a}{2}\right)$,

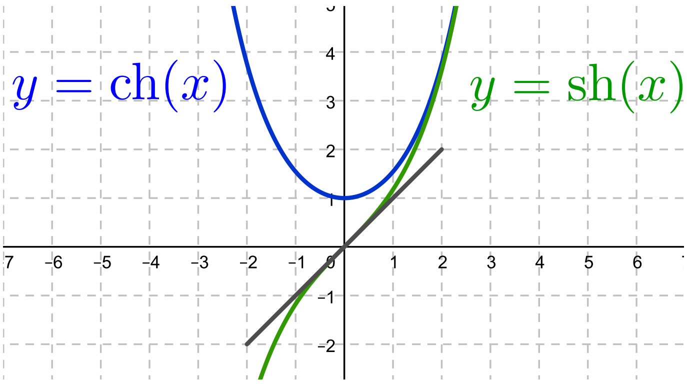
$$\cos a = \frac{1-t^2}{1+t^2}, \qquad \text{et} \qquad \sin a = \frac{2t}{1+t^2}.$$

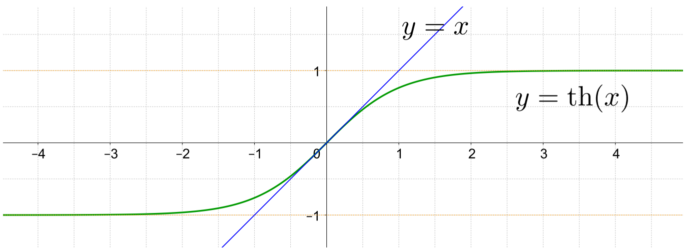
2 Fonctions hyperboliques ch, sh, th.

Définition 10.

Les fonctions **cosinus, sinus et tangente hyperbolique** sont définies sur $\mathbb{R}$ par

$$\mathrm{ch} : x \mapsto \frac{e^x + e^{-x}}{2}, \qquad \mathrm{sh} : x \mapsto \frac{e^x - e^{-x}}{2}, \qquad \mathrm{th} : x \mapsto \frac{\mathrm{sh}(x)}{\mathrm{ch}(x)}.$$





Pourquoi *cosinus* et *sinus* ? Cela vient de l'analogie avec les formules d'Euler pour les "vrais" cos et sin :

$$\forall t \in \mathbb{R} \qquad \cos t = \frac{e^{it} + e^{-it}}{2} \qquad \sin t = \frac{e^{it} - e^{-it}}{2i}.$$

Pourquoi *hyperbolique* ?
Pour les "vrais" cosinus et sinus, on a $\cos^2 + \sin^2 = 1$ et l'ensemble $\{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ est un cercle. Avec ch et sh, on va voir que $\mathrm{ch}^2 - \mathrm{sh}^2 = 1$ et l'ensemble

$$\{(x,y) \in \mathbb{R}^2 : x^2 - y^2 = 1\}$$

est appelé une hyperbole en géométrie.

Proposition 11.

- La fonction ch est paire et les fonctions sh et th sont impaires.
- $\forall x \in \mathbb{R} \quad \begin{cases} e^x & = & \mathrm{ch}(x) + \mathrm{sh}(x) \\ e^{-x} & = & \mathrm{ch}(x) - \mathrm{sh}(x) \end{cases}$
- Une formule de trigonométrie hyperbolique :

$$\forall x \in \mathbb{R} \quad \mathrm{ch}^2(x) - \mathrm{sh}^2(x) = 1.$$

- Des limites :

$$\lim_{x \to +\infty} \mathrm{ch}(x) = \lim_{x \to +\infty} \mathrm{sh}(x) = +\infty \quad \text{et} \quad \lim_{x \to +\infty} \mathrm{th}(x) = 1.$$

- Toutes les trois sont dérivables sur $\mathbb{R}$ et

$$\forall x \in \mathbb{R} \qquad \mathrm{ch}'(x) = \mathrm{sh}(x), \quad \mathrm{sh}'(x) = \mathrm{ch}(x), \quad \mathrm{th}'(x) = \frac{1}{\mathrm{ch}^2(x)} = 1 - \mathrm{th}^2(x).$$

- Les tangentes aux courbes de sh et th en 0 sont d'équation $y = x$. De plus,

$$\forall x \in \mathbb{R}_+ \quad \mathrm{sh}(x) \geq x \quad \text{et} \quad \mathrm{th}(x) \leq x.$$

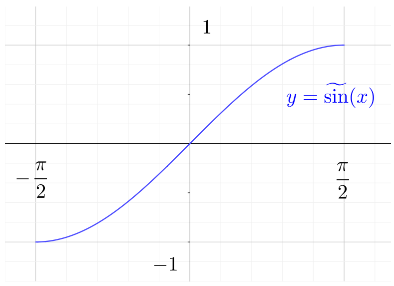
3 Fonctions circulaires réciproques : arcsin, arccos, arctan.

La fonction $\sin : \mathbb{R} \to \mathbb{R}$ n'est (grossièrement) pas bijective. Par exemple, on pourra remarquer que 2 ne possède pas d'antécédent par sin, ou encore que 1 en possède une infinité.

En revanche, la fonction

$$\widetilde{\sin} : \begin{cases} [-\frac{\pi}{2}, \frac{\pi}{2}] & \to & [-1, 1] \\ x & \mapsto & \sin x \end{cases}$$

est continue et strictement croissante sur $[-\frac{\pi}{2}, \frac{\pi}{2}]$, et $\widetilde{\sin}\left([-\frac{\pi}{2}, \frac{\pi}{2}]\right) = [-1, 1]$.



Le théorème de la bijection continue légitime alors la définition ci-dessous.

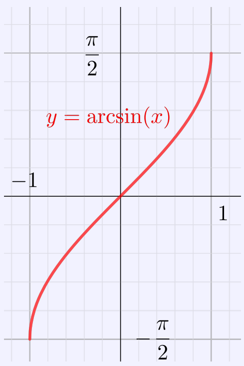
Définition 12.

On appelle fonction **arcsinus** et on note

$$\arcsin : [-1, 1] \to [-\frac{\pi}{2}, \frac{\pi}{2}]$$

la réciproque de la bijection $\widetilde{\sin} : [-\frac{\pi}{2}, \frac{\pi}{2}] \to [-1, 1]$.

Pour tout y dans $[-1, 1]$, $\arcsin(y)$ est l'unique antécédent de y par sin dans $[-\frac{\pi}{2}, \frac{\pi}{2}]$.



Proposition 13.

La fonction arcsin est strictement croissante sur $[-1, 1]$ et elle est impaire.

Proposition 14.

$$\forall x \in [-1, 1] \quad \sin(\arcsin(x)) = x \qquad\qquad \forall x \in [-\frac{\pi}{2}, \frac{\pi}{2}] \quad \arcsin(\sin x) = x$$

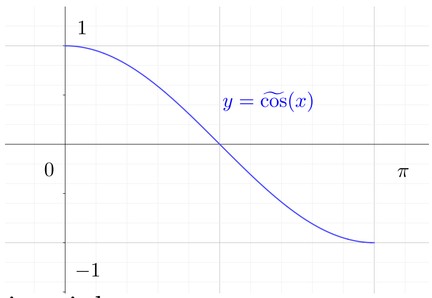
Exemple 15.

Que valent $\arcsin(0)$, $\arcsin(1)$, $\arcsin(\frac{1}{2})$? Et $\arcsin\left(\sin(\frac{2\pi}{3})\right)$?

La fonction

$$\widetilde{\cos} : \left\{ \begin{array}{ccc} [0, \pi] & \to & [-1, 1] \\ x & \mapsto & \cos x \end{array} \right.$$

est continue et strictement décroissante sur $[0, \pi]$,
et $\widetilde{\cos}\,([0, \pi]) = [-1, 1]$.



Le théorème de la bijection continue légitime alors la définition ci-dessous

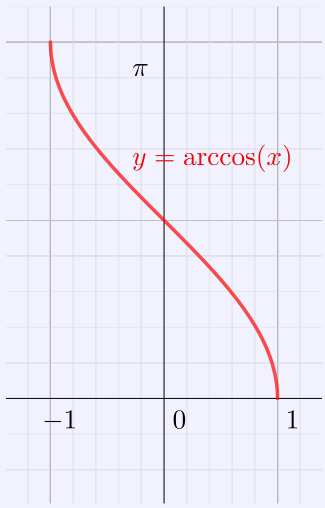
Définition 16.

On appelle fonction **arccosinus** et on note

$$\arccos : [-1, 1] \to [0, \pi]$$

la réciproque de la bijection $\widetilde{\cos} : [0, \pi] \to [-1, 1]$.

Pour tout y dans $[-1, 1]$, $\arccos(y)$ est l'unique antécédent de y par cos dans $[0, \pi]$.



Comme réciproque d'une fonction strictement décroissate, arccos est strictement décroissante sur $[-1, 1]$.

Proposition 17.

$$\forall x \in [-1,1] \quad \cos(\arccos(x)) = x \qquad\qquad \forall x \in [0,\pi] \quad \arccos(\cos x) = x$$

Exemple 18.

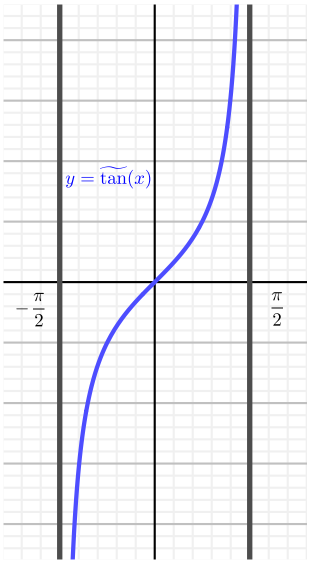
Que valent $\arccos(0)$, $\arccos(1)$, $\arccos(-1)$, $\arccos(\frac{\sqrt{3}}{2})$? Et $\arccos\left(\cos(\frac{5\pi}{3})\right)$?

La fonction

$$\widetilde{\tan} : \begin{cases}]-\frac{\pi}{2},\frac{\pi}{2}[& \to & \mathbb{R} \\ x & \mapsto & \tan x \end{cases}$$

est continue et strictement croissante sur $]-\frac{\pi}{2},\frac{\pi}{2}[$, et $\widetilde{\tan}\left(]-\frac{\pi}{2},\frac{\pi}{2}[\right) = \mathbb{R}$.

Le théorème de la bijection continue légitime alors la définition ci-dessous



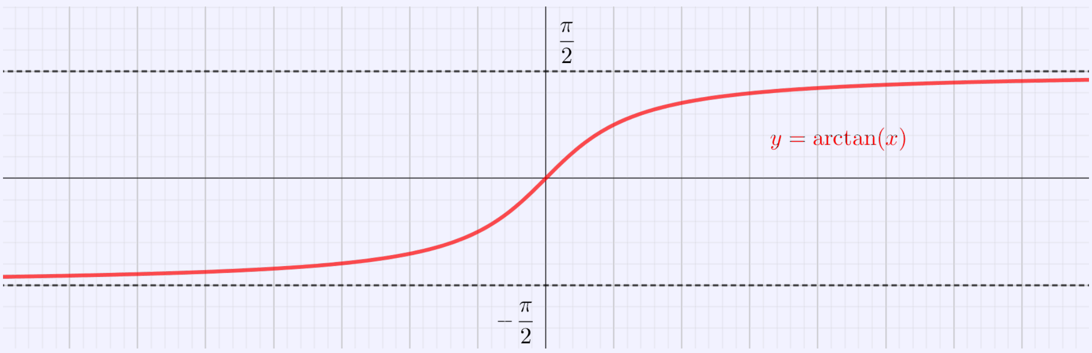
Définition 19.

On appelle fonction **arctangente** et on note

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

la réciproque de la bijection $\widetilde{\tan} :]-\frac{\pi}{2},\frac{\pi}{2}[\to \mathbb{R}$.

Pour tout y dans $\mathbb{R}$, $\arctan(y)$ est l'unique antécédent de y par tan dans $]-\frac{\pi}{2},\frac{\pi}{2}[$.



Proposition 20.

La fonction arctan est strictement croissante sur $\mathbb{R}$ et elle est impaire.

$$\lim_{x\to+\infty} \arctan(x) = \frac{\pi}{2} \quad \text{et} \quad \lim_{x\to-\infty} \arctan(x) = -\frac{\pi}{2}.$$

Proposition 21.

$$\forall x \in \mathbb{R} \quad \tan(\arctan(x)) = x \qquad\qquad \forall x \in]-\frac{\pi}{2}, \frac{\pi}{2}[\quad \arctan(\tan x) = x$$

Exemple 22.

Que valent $\arctan(0)$? $\arctan(1)$? $\arctan(\sqrt{3})$? Et $\arctan(\tan(\pi))$?

Lemme 23.

$$\forall x \in [-1,1] \quad \cos(\arcsin(x)) = \sqrt{1-x^2} = \sin(\arccos(x)).$$

$$\forall x \in \mathbb{R} \quad \cos(\arctan(x)) = \frac{1}{\sqrt{1+x^2}}.$$

Proposition 24.

Les fonctions arcsin et arccos sont dérivables sur $]-1,1[$ et

$$\forall x \in]-1,1[\qquad \arcsin'(x) = \frac{1}{\sqrt{1-x^2}} \quad \text{et} \quad \arccos'(x) = -\frac{1}{\sqrt{1-x^2}}.$$

La fonction arctan est dérivable sur $\mathbb{R}$, et

$$\forall x \in \mathbb{R} \qquad \arctan'(x) = \frac{1}{1+x^2}.$$

Proposition 25 (Lien entre arccos et arcsin)**.**

$$\forall x \in [-1,1] \qquad \arccos(x) = \frac{\pi}{2} - \arcsin(x).$$

Proposition 26.

$$\forall x \in \mathbb{R}^* \qquad \arctan(x) + \arctan\left(\frac{1}{x}\right) = \begin{cases} \frac{\pi}{2} & \text{si } x > 0 \\ -\frac{\pi}{2} & \text{si } x < 0. \end{cases}$$

Annexe.

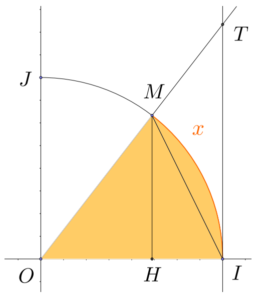
Preuve de la proposition 2 : on prouve que cos et sin sont des fonctions dérivables sur $\mathbb{R}$ et que leurs dérivées sont respectivement $-\sin$ et cos.

Lemme.

$$\forall x \in \left]0, \frac{\pi}{2}\right] \quad \cos x \leq \frac{\sin(x)}{x} \leq 1.$$

Preuve. Soit $x \in \left]0, \frac{\pi}{2}\right]$. On note $M = M(x)$ le point du cercle trigonométrique associé à x par enroulement. Notons $\mathcal{C}(x)$ la portion de disque délimitée par O, I et M (pleine sur la figure suivante). On lit sur la figure l'inégalité

$$Aire(OIM) \leq Aire\left(\mathcal{C}(x)\right) \leq Aire(OIT). \quad (\star)$$



• Le disque de rayon 1 est d'aire π donc le quart de disque $\mathcal{C}(\frac{\pi}{2})$ est d'aire $\frac{\pi}{4}$. Une règle de trois nous donne que $\mathcal{C}(x)$ est d'aire $\frac{x}{2}$.

• Le triangle OIM est de base $OI = 1$ et de hauteur $HM = \sin(x)$. On a donc $Aire(OIM) = \frac{1 \times \sin(x)}{2}$.

• Le théorème de Thalès donne $\frac{IT}{HM} = \frac{OI}{OH}$ d'où $IT = \frac{HM \times OI}{OH} = \frac{\sin x}{\cos x}$. On a donc $Aire(OIT) = \frac{\tan x}{2}$.

Les inégalités $(\star)$ donnent donc

$$\frac{\sin x}{2} \leq \frac{x}{2} \leq \frac{\sin x}{2 \cos x}.$$

ce qui fournit bien l'inégalité

$$\cos(x) \leq \frac{\sin(x)}{x} \leq 1.$$

□

Preuve de la proposition 2.

• Soit $x \in \mathbb{R}$. On va dériver la fonction sin en x c'est à dire s'intéresser au taux d'accroissement

$$\frac{\sin(x+h) - \sin x}{h}.$$

Il nous faut montrer que ce dernier a pour limite $\cos x$ lorsque h tend vers 0.

L'utilisation des formules d'addition amène, pour tout $h \neq 0$,

$$\frac{\sin(x+h) - \sin x}{h} = \frac{\sin x \cos h + \cos x \sin h - \sin x}{h} = \cos x \frac{\sin h}{h} + \sin x \frac{\cos h - 1}{h}.$$

Ainsi, la proposition est démontrée si on prouve

$$\frac{\sin h}{h} \underset{h \to 0}{\longrightarrow} 1 \quad \text{et} \quad \frac{1 - \cos h}{h} \underset{h \to 0}{\longrightarrow} 0.$$

La première limite découle du lemme précédent grâce au théorème des gendarmes.

Pour la seconde, on calcule

$$\frac{(1+\cos h)(1-\cos h)}{h} = \frac{1 - \cos^2 h}{h} = \frac{\sin^2(h)}{h} = \sin h \times \frac{\sin h}{h},$$

d'où

$$\frac{1 - \cos h}{h} = \frac{\sin h}{1 + \cos h} \times \frac{\sin h}{h} \underset{h \to 0}{\longrightarrow} \frac{0}{2} \times 1 = 0.$$

On a donc bien

$$\frac{\sin(x+h) - \sin x}{h} \underset{h \to 0}{\longrightarrow} \cos(x) \times 1 + 0 = \cos(x).$$

Ceci achève de démontrer que sin est dérivable en x, de dérivée $\cos x$.

• Rappelons que pour tout $x \in \mathbb{R}$,

$$\cos(x) = \sin\left(\frac{\pi}{2} - x\right).$$

Ainsi, cos est dérivable sur $\mathbb{R}$ comme composée de fonctions dérivables sur $\mathbb{R}$ et

$$\forall x \in \mathbb{R} \quad \cos'(x) = (-1)\sin'\left(\frac{\pi}{2} - x\right) = -\cos\left(\frac{\pi}{2} - x\right) = -\sin(x).$$

□

Exercices

Trigonométrie. Fonctions circulaires.

$\boxed{8.1}$ **[♦♦◇]**

1. Soit $f : x \mapsto \sin^2(x)\sin(2x)$. Déterminer son maximum sur $[0,\pi]$ puis sur $\mathbb{R}$.
2. Démontrer pour tout réel x et tout entier $n \geq 1$, on a
$$\prod_{k=0}^{n} \sin(2^k x) \leq \left(\frac{\sqrt{3}}{2}\right)^n.$$

$\boxed{8.2}$ **[♦◇◇]** Calculer $\tan(\frac{\pi}{8})$.

$\boxed{8.3}$ **[♦◇◇]** Résoudre
$$|\tan(x)| = 1.$$

Fonctions hyperboliques.

$\boxed{8.4}$ **[♦◇◇]** Trigonométrie hyperbolique.

1. Montrer que pour tous réels a et b, on a
   (a) $\mathrm{ch}(a+b) = \mathrm{ch}(a)\mathrm{ch}(b) + \mathrm{sh}(a)\mathrm{sh}(b)$.
   (b) $\mathrm{sh}(a+b) = \mathrm{sh}(a)\mathrm{ch}(b) + \mathrm{ch}(a)\mathrm{sh}(b)$.
   (c) Trouver une identité pour $\mathrm{th}(a+b)$.
2. Pour x réel, on pose $t = \mathrm{th}(\frac{x}{2})$. Montrer que
$$(a)\ \mathrm{ch}(x) = \frac{1+t^2}{1-t^2} \qquad (b)\ \mathrm{sh}(x) = \frac{2t}{1-t^2} \qquad (c)\ \mathrm{th}(x) = \frac{2t}{1+t^2}.$$

$\boxed{8.5}$ **[♦◇◇]** Résoudre l'équation $\mathrm{ch}(x) = 2$. Que dire des solutions ?

$\boxed{8.6}$ **[♦♦◇]** Soient a et b deux réels tels que $b \neq 0$. Résoudre l'équation
$$a\,\mathrm{ch}(x) + b\,\mathrm{sh}(x) = 0.$$

$\boxed{8.7}$ **[♦♦◇]**

1. Justifier que sh réalise une bijection de $\mathbb{R}$ dans $\mathbb{R}$.
2. Expliciter sa réciproque, puis calculer la dérivée de cette réciproque.
3. Retrouver le dernier résultat en appliquant le théorème de dérivation d'une réciproque.

$\boxed{8.8}$ **[♦♦♦]**

1. Montrer que th est une bijection de $\mathbb{R}$ dans $]-1,1[$ et déterminer une expression explicite de sa réciproque, qu'on notera argth.
2. De deux façons différentes, montrer que argth est dérivable sur son intervalle de définition et calculer sa dérivée.
3. Montrer que pour tout $x \in \mathbb{R}$, $\mathrm{argth}\left(\dfrac{1+3\mathrm{th}x}{3+\mathrm{th}x}\right) = x + \ln\sqrt{2}$.

Fonctions circulaires réciproques.

$\boxed{\textbf{8.9}}$ **[♦◇◇]** Montrer que $\forall x \in \mathbb{R}_+ \; x - \dfrac{x^3}{3} \leq \arctan(x) \leq x$.

$\boxed{\textbf{8.10}}$ **[♦♦◇]** Montrer que

$$\arctan(1/2) + \arctan(1/3) = \frac{\pi}{4}.$$

$\boxed{\textbf{8.11}}$ **[♦♦◇]** Soit l'équation

$$\arcsin(x) + \arcsin\left(\frac{x}{2}\right) = \frac{\pi}{4}.$$

1. Justifier que l'équation admet une unique solution sur $[-1, 1]$.
2. Donner une expression de cette solution.

$\boxed{\textbf{8.12}}$ **[♦♦◇]** Dans cet exercice, on considère la fonction

$$f : x \mapsto \arcsin\left(\operatorname{th}(x)\right)$$

1. Justifier soigneusement que f est dérivable sur $\mathbb{R}$ et prouver que $f' = \dfrac{1}{\operatorname{ch}}$.
2. Démontrer que
$$\forall x \in \mathbb{R} \quad f(x) = 2\arctan(e^x) - \frac{\pi}{2}.$$

$\boxed{\textbf{8.13}}$ **[♦♦◇]** Soit

$$f : x \mapsto \arcsin\left(\frac{x}{\sqrt{1+x^2}}\right).$$

1. Démontrer que pour tout $x \in \mathbb{R}$, $\frac{x}{\sqrt{1+x^2}} \in]-1, 1[$.
2. Montrer que f est dérivable sur $\mathbb{R}$ et calculer sa dérivée.
3. En déduire une expression plus simple de la fonction f.
4. Retrouver ce résultat par une preuve directe.

$\boxed{\textbf{8.14}}$ **[♦♦♦]** Pour $a < x < b$, montrer que $\arcsin\sqrt{\dfrac{x-a}{b-a}} = \arctan\sqrt{\dfrac{x-a}{b-x}}$.

---

9 Calcul de primitives et d'intégrales

Ce cours a deux parties. Dans la première, on explique que primitiver, c'est dériver à l'envers. On s'entraîne donc à voir une fonction comme la dérivée d'une fonction usuelle (1.1), ou d'une composée de fonctions usuelles (1.2). Dans le cas où on ne reconnaît rien, la seconde partie nous propose un lien entre les primitives des fonctions continues et leurs intégrales (2.2). On donnera deux outils fondamentaux pour calculer ces intégrales : l'intégration par parties (2.3) et le changement de variable (2.4).

1 Définition et calculs directs.

1.1 Définition.

Définition 1.

Soit I un intervalle de $\mathbb{R}$ et $f : I \to \mathbb{K}$ une fonction.
On dit qu'une fonction $F : I \to \mathbb{K}$ est une **primitive** de f sur I si elle est dérivable sur I et si

$$\forall x \in I, \quad F'(x) = f(x).$$

Par exemple on a $x \mapsto \frac{x^2}{2}$ et $x \mapsto \frac{x^2}{2} + 3$ sont des primitives de $x \mapsto x$ sur $\mathbb{R}$.

On va prouver que si F et G sont deux primitives de f sur I, alors elles sont égales sur I à une constante additive près.

Proposition 2 (Ensemble des primitives d'une même fonction sur un intervalle)**.**

Soit $f : I \to \mathbb{K}$ une fonction définie sur un intervalle I et $\mathcal{P}_f$ l'ensemble des primitives de f sur I, dont on suppose ici qu'il est <u>non vide</u>. Soit F une primitive de f, alors

$$\mathcal{P}_f = \{F + c,\ c \in C_I\},$$

où C_I est l'ensemble des fonctions constantes sur I.

Proposition 3 (Primitives usuelles).

Fonction	**Paramètre**	**Une primitive**	**Intervalle déf.**
$x \mapsto x^n$	$n \in \mathbb{N}$	$x \mapsto \dfrac{x^{n+1}}{n+1}$	$\mathbb{R}$
$x \mapsto x^p$	$p \in \mathbb{Z}, p < -1,$	$x \mapsto \dfrac{x^{p+1}}{p+1}$	$\mathbb{R}_+^*$ ou $\mathbb{R}_-^*$
$x \mapsto x^\alpha$	$\alpha \in \mathbb{R} \setminus \{-1\},$	$x \mapsto \dfrac{x^{\alpha+1}}{\alpha+1}$	$\mathbb{R}_+^*$
$x \mapsto \dfrac{1}{x}$		$x \mapsto \ln\lvert x\rvert$	$\mathbb{R}_+^*$ ou $\mathbb{R}_-^*$
$x \mapsto \sqrt{x}$		$x \mapsto \frac{2}{3}x^{3/2}$	$\mathbb{R}_+^*$
$x \mapsto \dfrac{1}{\sqrt{x}}$		$x \mapsto 2\sqrt{x}$	$\mathbb{R}_+^*$

Fonction	**Une primitive**	**Intervalle déf.**
$x \mapsto \cos x$	$x \mapsto \sin x$	$\mathbb{R}$
$x \mapsto \sin x$	$x \mapsto -\cos x$	$\mathbb{R}$
$x \mapsto \tan x$	$x \mapsto -\ln\lvert\cos x\rvert$	$]-\frac{\pi}{2}+k\pi, \frac{\pi}{2}+k\pi[; k \in \mathbb{Z}$
$x \mapsto \mathrm{ch} x$	$x \mapsto \mathrm{sh} x$	$\mathbb{R}$
$x \mapsto \mathrm{sh} x$	$x \mapsto \mathrm{ch} x$	$\mathbb{R}$
$x \mapsto e^x$	$x \mapsto e^x$	$\mathbb{R}$
$x \mapsto \ln(x)$	$x \mapsto x\ln(x) - x$	$\mathbb{R}_+^*$
$x \mapsto \dfrac{1}{\sqrt{1-x^2}}$	$x \mapsto \arcsin(x)$	$]-1, 1[$
$x \mapsto \dfrac{1}{1+x^2}$	$x \mapsto \arctan(x)$	$\mathbb{R}$

Fonction	**Paramètre**	**Une primitive**	**Intervalle déf.**
$x \mapsto e^{\lambda x}$	$\lambda \in \mathbb{C}^*$	$x \mapsto \dfrac{e^{\lambda x}}{\lambda}$	$\mathbb{R}$
$x \mapsto \dfrac{1}{x^2+a^2}$	$a \in \mathbb{R}^*$	$x \mapsto \frac{1}{a}\arctan\left(\frac{x}{a}\right)$	$\mathbb{R}$

Proposition 4.

Soient $f : I \to \mathbb{K}$ et $g : I \to \mathbb{K}$. Soient F et G des primitives respectivement des fonctions f et g sur I, et deux nombres $\alpha, \beta \in \mathbb{K}$. Alors,

$$\text{la fonction } \alpha F + \beta G \text{ est une primitive de la fonction } \alpha f + \beta g \text{ sur } I.$$

Exemple 5.

Soit une fonction polynomiale $f : x \mapsto \sum_{k=0}^{n} a_k x^k$, où $n \in \mathbb{N}$ et $a_0, \ldots, a_n \in \mathbb{K}$.
La fonction $F : x \mapsto \displaystyle\sum_{k=0}^{n} a_k \frac{x^{k+1}}{k+1}$ en est une primitive.

1.2 Fonctions composées.

Proposition 6 (Primitive et composée)**.**

Soient deux fonctions $u : I \to J$, dérivable sur I, et $F : J \to \mathbb{K}$, dérivable sur J.
Alors, la fonction

$$F \circ u \text{ est une primitive de } u' \times F' \circ u \text{ sur } I.$$

En particulier, si F est une primitive de f sur $\mathbb{R}$, pour $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$, $x \mapsto \frac{1}{a}F(ax+b)$ est une primitive de $x \mapsto f(ax+b)$.

Soit $u : I \to J$ une fonction dérivable sur I. Voici une liste de cas particuliers de la proposition 6 où F est une fonction usuelle dérivable sur l'intervalle J qui n'est pas précisé ici (on fait confiance au lecteur !)

Fonction	**Une primitive**
$u'u$	$\frac{1}{2}u^2$
$u'u^\alpha$ $(\alpha \neq -1)$	$\dfrac{1}{\alpha+1}u^{\alpha+1}$
$u'e^u$	e^u

Fonction	**Une primitive**
$\dfrac{u'}{\sqrt{u}}$	$2\sqrt{u}$
$\dfrac{u'}{u}$	$\ln(\lvert u\rvert)$
$\dfrac{u'}{1+u^2}$	$\arctan(u)$

Exemple 7.

Calculer pour chacune des fonctions ci-dessous une primitive (on précisera sur quel intervalle).

$x \mapsto \sin(3x)$ $\quad$ $x \mapsto \cos x \sin x$ $\quad$ $x \mapsto xe^{x^2}$ $\quad$ $x \mapsto \tan x$ $\quad$ $x \mapsto \dfrac{x}{1+x^2}$ $\quad$ $x \mapsto \dfrac{x}{\sqrt{1-x^2}}$

1.3 Inverse de trinôme.

Soient a, b, c dans $\mathbb{R}$ avec $a \neq 0$. Il s'agit ici de proposer une primitive de

$$f : x \mapsto \frac{1}{ax^2 + bx + c}.$$

Trois cas se présentent.

- Le trinôme a une racine double γ.
  On peut écrire
  $$\frac{1}{ax^2 + bx + c} = \frac{1}{a(x - \gamma)^2}.$$
  En voici une primitive :
  $$F : x \mapsto -\frac{1}{a} \cdot \frac{1}{x - \gamma} \qquad x \in]-\infty, \gamma[\text{ ou }]\gamma, +\infty[.$$

- Le trinôme possède deux racines distinctes α et β. On peut alors réaliser une décomposition en éléments simples, c'est-à-dire trouver deux constantes A et B (voir méthode de calcul plus bas) telles que
  $$f(x) = \frac{1}{ax^2 + bx + c} = \frac{1}{a(x - \alpha)(x - \beta)} = \frac{A}{x - \alpha} + \frac{B}{x - \beta}.$$
  On connaît $\boxed{\frac{1}{x - \alpha} = \frac{\mathrm{d}}{\mathrm{d}x} \ln|x - \alpha|}$.
  $$F : x \mapsto A \ln|x - \alpha| + B \ln|x - \beta| \qquad x \in]-\infty, \alpha[\text{ ou }]\alpha, \beta[\text{ ou }]\beta, +\infty[.$$
  Comme on le verra dans la méthode de calcul, on a toujours $B = -A$, ce qui permet d'écrire la primitive sous la forme $x \mapsto A \ln\left|\frac{x-\alpha}{x-\beta}\right|$.

- Le trinôme n'a pas de racines réelles. On sait alors mettre le trinôme sous forme canonique : il existe deux constantes A et B telles que
  $$\frac{1}{ax^2 + bx + c} = \frac{1}{a\left((x + A)^2 + B^2\right)}.$$
  On connaît $\boxed{\frac{1}{a^2 + x^2} = \frac{\mathrm{d}}{\mathrm{d}x} \left(\frac{1}{a} \arctan \frac{x}{a}\right)}$. On a donc la primitive :
  $$F : x \mapsto \frac{1}{aB} \arctan\left(\frac{x + A}{B}\right) \qquad x \in \mathbb{R}.$$

Méthode.

Soient α et β deux réels distincts. Il existe deux constantes A et B réelles telles que

$$\forall x \in \mathbb{R} \setminus \{\alpha, \beta\} \quad \frac{1}{(x - \alpha)(x - \beta)} = \frac{A}{x - \alpha} + \frac{B}{x - \beta}.$$

Cette écriture est appelée **décomposition en éléments simples**.
On donne en classe deux méthodes pour trouver A et B (qui sont opposés).

Méthode.

Mise sous forme canonique : pour $a \neq 0$, $b, c \in \mathbb{R}$ et $x \in \mathbb{R}$,

$$ax^2 + bx + c = a\,(\underbrace{x^2 + \frac{b}{a}x}_{\text{début de } (x+\frac{b}{2a})^2} + \frac{c}{a}) = a\left((x + \frac{b}{2a})^2 - (\frac{b}{2a})^2 + \frac{c}{a}\right) = a\left(\left(x + \frac{b}{2a}\right)^2 + \frac{4ac - b^2}{4a^2}\right)$$

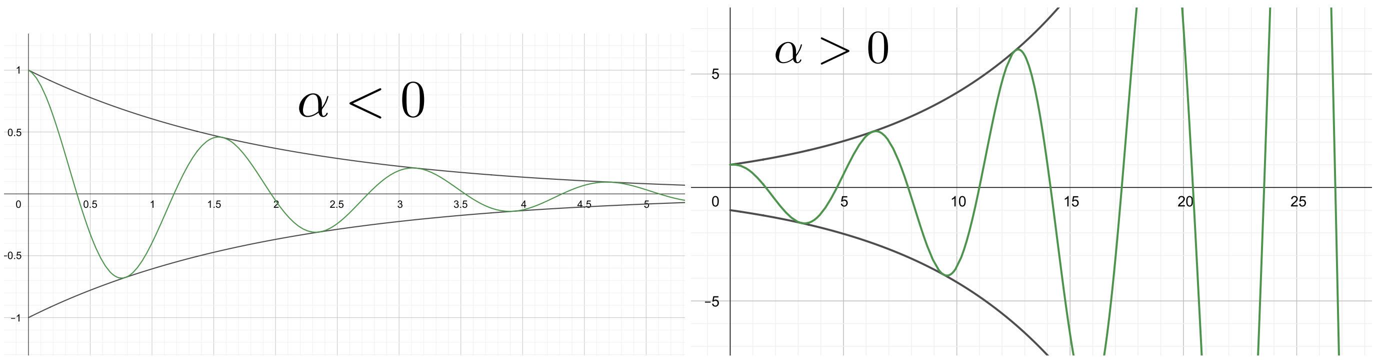
Exemple 8.

Calculer une primitive des fonctions $f : x \mapsto \dfrac{1}{x^2 + 3x + 2}$ et $g : x \mapsto \dfrac{1}{x^2 + x + 1}$.

1.4 Primitive d'une fonction $t \mapsto e^{\alpha t}\cos(\omega t)$ ou $t \mapsto e^{\alpha t}\sin(\omega t)$.

Soit $\alpha \in \mathbb{R}$ et $\omega \in \mathbb{R}_+^*$. On veut calculer une primitive pour chacune des deux fonctions

$$f : t \mapsto e^{\alpha t}\cos(\omega t) \quad \text{et} \quad g : t \mapsto e^{\alpha t}\sin(\omega t) \qquad \text{avec } \alpha \in \mathbb{R}, \omega \in \mathbb{R}^*.$$



$\boxed{\text{Méthode}}$: passer dans $\mathbb{C}$. Pour t réel, on a

$$e^{\alpha t}\cos(\omega t) = e^{\alpha t}\mathrm{Re}\left(e^{i\omega t}\right) = \mathrm{Re}\left(e^{(\alpha+i\omega)t}\right) \qquad \text{et} \qquad e^{\alpha t}\sin(\omega t) = e^{\alpha t}\mathrm{Im}\left(e^{i\omega t}\right) = \mathrm{Im}\left(e^{(\alpha+i\omega)t}\right).$$

Or, $t \mapsto \dfrac{1}{\alpha + i\omega}e^{(\alpha+i\omega)t}$ est une primitive de $t \mapsto e^{(\alpha+i\omega)t}dt$ sur $\mathbb{R}$. On peut alors calculer

$$\begin{cases} F(t) & := & \mathrm{Re}\left(\frac{1}{\alpha+i\omega}e^{(\alpha+i\omega)t}\right) \underset{calcul}{=} \dfrac{e^{\alpha t}}{\alpha^2 + \omega^2}\left(\alpha\cos(\omega t) + \omega\sin(\omega t)\right). \\ G(t) & := & \mathrm{Im}\left(\frac{1}{\alpha+i\omega}e^{(\alpha+i\omega)t}\right) \underset{calcul}{=} \dfrac{e^{\alpha t}}{\alpha^2 + \omega^2}\left(\alpha\sin(\omega t) - \omega\cos(\omega t)\right). \end{cases}$$

La fonction F est une primitive de f et la fonction G est une primitive de g.

Exemple 9.

Calculer une primitive sur $\mathbb{R}$ de la fonction $x \mapsto e^{3x}\cos(2x)$.

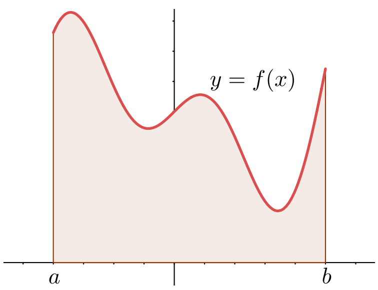
2 Calcul intégral et primitives.

2.1 Propriétés de l'intégrale.

Soit f une fonction continue sur un intervalle I et à valeurs réelles, et a et b deux réels de I. Pour une telle fonction, la construction de l'intégrale de Riemann au second semestre donnera un sens au nombre $\boxed{\int_a^b f(t)\mathrm{d}t}$.

Rappelons brièvement quelques propriétés entrevues au lycée ; elles seront démontrées en fin d'année.

0. Intégrale d'une constante. Si f est constante égale à C sur I, alors $\int_a^b C\mathrm{d}x = C(b-a)$.
1. Positivité. Si f est une fonction continue et positive sur $[a,b]$ (avec $a \leq b$) alors $\int_a^b f(t)\mathrm{d}t$ est un nombre positif. Il représente l'aire sous la courbe de f entre a et b :



2. Croissance. Si f et g sont deux fonctions continues sur $[a,b]$ (avec $a \leq b$) et telles que $\forall x \in [a,b]\ f(x) \leq g(x)$, alors $\int_a^b f(t)\mathrm{d}t \leq \int_a^b g(t)\mathrm{d}t$.
3. Relation de Chasles. Si f est une fonction continue sur $[a,b]$, par définition, $\int_b^a f(t)\mathrm{d}t = -\int_a^b f(t)\mathrm{d}t$. Notamment, $\int_a^a f(t)\mathrm{d}t = 0$.
   Si maintenant a, b, c sont trois points d'un intervalle I sur lequel f est continue, alors
   $$\int_a^b f(t)\mathrm{d}t = \int_a^c f(t)\mathrm{d}t + \int_c^b f(t)\mathrm{d}t.$$
4. Linéarité. Si f et g sont deux fonctions continues sur I et que a et b sont deux réels de I, alors
   $$\int_a^b (f(t)+g(t))\,\mathrm{d}t = \int_a^b f(t)\mathrm{d}t + \int_a^b g(t)\mathrm{d}t \quad \text{et} \quad \int_a^b \lambda f(t)\mathrm{d}t = \lambda \int_a^b f(t)\mathrm{d}t.$$
   En combinant les opérations somme et multiplication par un scalaire, on forme des combinaisons linéaires de fonctions. Pour λ, μ deux réels, alors
   $$\int_a^b (\lambda f(t) + \mu g(t))\,\mathrm{d}t = \lambda \int_a^b f(t)\mathrm{d}t + \mu \int_a^b g(t)\mathrm{d}t.$$
5. Inégalité triangulaire. Si f est une fonction continue sur $[a,b]$ (avec $a \leq b$) alors
   $$\left| \int_a^b f(t)\mathrm{d}t \right| \leq \int_a^b |f(t)|\mathrm{d}t.$$
6. Valeurs complexes. Si $f : [a,b] \to \mathbb{C}$ est continue, alors $\mathrm{Re}(f)$ et $\mathrm{Im}(f)$ sont continues sur $[a,b]$ et
   $$\int_a^b f(x)\mathrm{d}x := \int_a^b \mathrm{Re}\,(f(x))\,\mathrm{d}x + i \int_a^b \mathrm{Im}\,(f(x))\,\mathrm{d}x.$$

2.2 Intégrales et primitives d'une fonction continue.

Le théorème suivant énonce que sous certaines conditions, la dérivation et l'intégration, deux opérations fondamentales en analyse, sont réciproques l'une de l'autre. Ce théorème sera démontré au second semestre dans le cours d'intégration.

Théorème 10 (Théorème fondamental de l'analyse)**.**

Soit I un intervalle de $\mathbb{R}$, a un élément de I et $f : I \to \mathbb{K}$ une fonction continue sur I. La fonction

$$F : x \mapsto \int_a^x f(t)\mathrm{d}t$$

est une primitive de f sur I (c'est la primitive de f qui s'annule en a.)

Corollaire 11.

Si une fonction est continue sur un intervalle I, elle y admet des primitives.

Exemple 12.

Exprimer à l'aide du symbole intégrale une primitive de $f : x \mapsto e^{-x^2}$ et de $g : x \mapsto \ln^2(x)$.

Proposition 13 (Calculer une intégrale grâce à une primitive)**.**

Soit $f : [a, b] \to \mathbb{K}$ une fonction continue et F *une* primitive de f sur $[a, b]$. Alors

$$\int_a^b f(t)\mathrm{d}t = F(b) - F(a).$$

Rappel : pour une fonction F définie sur $[a, b]$, on note $\big[F\big]_a^b = F(b) - F(a)$.

Exemple 14.

Calcul de $I_1 = \displaystyle\int_0^{\frac{1}{2}} t^3\mathrm{d}t \qquad I_2 = \int_0^{\frac{\pi}{2}} \cos t \sin^3 t\mathrm{d}t \qquad I_3 = \int_0^{\frac{\pi}{4}} \tan^2(x)\mathrm{d}x.$

Exemple 15.

Domaine de définition et variations de $x \mapsto \displaystyle\int_x^{x^2} \frac{1}{\ln(t)}\mathrm{d}t.$

Notation.

Le lien qui vient d'être fait entre primitives et intégrale amène certain·e·s auteur·e·s à utiliser la notation

$$\int^x f(t)\mathrm{d}t$$

pour désigner *une* primitive de f. Exemple : $\int^x \sin t\mathrm{d}t = -\cos x$.
Avantage : évite d'introduire une nouvelle lettre pour désigner la primitive.
Inconvénient : peut amener à des confusions entre nombres et fonctions.

2.3 Intégration par parties.

Pour les intégrales, l'intégration par parties (souvent abrégée en "IPP") est le pendant de la formule de dérivée d'un produit :

$$(uv)' = u'v + uv', \quad \text{i.e.} \quad u'v = (uv)' - uv'.$$

Faisons des hypothèses qui nous permettent d'écrire l'intégrale des fonctions ci-dessus. Pour assurer que des fonctions du type $u'v$ ou uv' sont *continues*, on va choisir u et v parmi les fonctions dérivables **dont la dérivée est continue**, ce qui motive la définition suivante.

Définition 16.

On dit qu'une fonction $f : I \to \mathbb{K}$ est **de classe $\mathcal{C}^1$** sur un intervalle I si $\underline{f \text{ est dérivable sur } I}$ et si sa dérivée $\underline{f' \text{ est continue}}$ sur I.

Théorème 17 (Intégration par parties)**.**

Soient u et v deux fonctions de classe $\mathcal{C}^1$ sur un intervalle I et $a, b \in I$. On a

$$\int_a^b u'(x)v(x)\mathrm{d}x = [uv]_a^b - \int_a^b u(x)v'(x)\mathrm{d}x.$$

Exemple 18.

Calculer les intégrales $\displaystyle\int_0^{\frac{\pi}{2}} x\cos x\mathrm{d}x$ et $\displaystyle\int_0^{\pi} \mathrm{ch}(x)\sin(x)\mathrm{d}x$ (double IPP pour cette dernière).

Exemple 19.

Calculer des primitives pour les fonctions :

$$f : x \mapsto \sqrt{x}\ln(x) \text{ et } g : x \mapsto \arctan(x).$$

2.4 Changement de variable.

Théorème 20 (Changement de variable).

Soit $\varphi : I \to J$, de classe $\mathcal{C}^1$ sur I et $f : J \to \mathbb{K}$ continue sur J. Pour tous $a, b \in I$, on a

$$\int_{\varphi(a)}^{\varphi(b)} f(x)\mathrm{d}x = \int_a^b f(\varphi(t))\, \varphi'(t)\mathrm{d}t.$$

Les physiciens ont un moyen pour se souvenir de la formule : ils posent $\boxed{\begin{cases} x &= \varphi(t) \\ \mathrm{d}x &= \varphi'(t)\mathrm{d}t \end{cases}}$

En remplaçant formellement, on a bien

$$\int f(x)\mathrm{d}x = \int f(\varphi(t))\, \varphi'(t)\mathrm{d}t,$$

et il n'y a plus qu'à écrire les bonnes bornes.

Exemple 21 (Appliquer la formule "dans les deux sens").

1. En posant $x = \sin t$, calculer $\displaystyle\int_0^{\frac{1}{2}} \sqrt{1 - x^2}\mathrm{d}x$.
2. À l'aide du changement de variable de votre choix, calculer $\displaystyle\int_0^1 \frac{e^{2t}}{e^t + 1}\mathrm{d}t$.

Exemple 22.

1. Calcul d'une primitive de $\dfrac{1}{\mathrm{ch}}$ sur $\mathbb{R}$.
2. Calcul d'une primitive de $\dfrac{1}{\sin}$ sur $]0, \pi[$ en posant $u = \cos x$.

Corollaire 23 (Intégrale d'une fonction paire, d'une fonction impaire).

Soit a un réel positif et f une fonction continue sur $[-a, a]$.

$$\text{Si } f \text{ est paire, } \int_{-a}^{a} f(t)\mathrm{d}t = 2\int_0^a f(t)\mathrm{d}t. \qquad \text{Si } f \text{ est impaire, } \int_{-a}^{a} f(t)\mathrm{d}t = 0.$$

Corollaire 24.

Soit f une fonction continue sur $\mathbb{R}$ et T périodique, avec T un réel strictement positif.

$$\forall a \in \mathbb{R} \quad \int_a^{a+T} f(t)\mathrm{d}t = \int_0^T f(t)\mathrm{d}t.$$

Exercices

$\boxed{9.1}$ **[♦◇◇]** Donner les primitives des fonctions suivantes (on précisera l'intervalle que l'on considère).

$$a : x \mapsto \cos x e^{\sin x}\,; \quad b : x \mapsto \frac{\cos x}{\sin x}\,; \quad c : x \mapsto \frac{\cos x}{\sqrt{\sin x}}\,; \quad d : x \mapsto \frac{1}{3x+1}\,;$$
$$e : x \mapsto \frac{\ln(x)}{x}\,; \quad f : x \mapsto \frac{1}{x\ln(x)}\,; \quad g : x \mapsto \sqrt{3x+1}\,; \quad h : x \mapsto \frac{x+x^2}{1+x^2}.$$

$\boxed{9.2}$ **[♦◇◇]** [Issu du cahier de calcul]
On rappelle que $\int_a^b f(x)\mathrm{d}x$ est l'aire algébrique entre la courbe représentative de f et l'axe des abscisses.

1. Sans chercher à les calculer, donner le signe des intégrales suivantes.
$$\int_{-2}^{3} e^{-x^2}\mathrm{d}x; \qquad \int_{5}^{-3} |\sin x|\mathrm{d}x; \qquad \int_{1}^{a} \ln^7(x)\mathrm{d}x \ (a \in \mathbb{R}_+^*).$$
2. En vous ramenant à des aires, calculer de tête
$$\int_1^3 7\mathrm{d}x; \qquad \int_0^7 3x\mathrm{d}x; \qquad \int_{-2}^{1} |x|\mathrm{d}x.$$

$\boxed{9.3}$ **[♦◇◇]** Calculer les intégrales ci-dessous :

$$I_1 = \int_0^1 x\sqrt{x}\mathrm{d}x, \qquad I_2 = \int_{-1}^1 2^x\mathrm{d}x \qquad I_3 = \int_1^e \frac{\ln^3(t)}{t}\mathrm{d}t \qquad I_4 = \int_0^1 \frac{x}{2x^2+3}\mathrm{d}x, \qquad I_5 = \int_0^1 \frac{1}{2x^2+3}\mathrm{d}x,$$
$$I_6 = \int_0^{\frac{\pi}{2}} \cos^2 x\mathrm{d}x \qquad I_7 = \int_0^{\pi} |\cos x|\mathrm{d}x \qquad I_8 = \int_0^{\frac{\pi}{2}} \cos^3 x\mathrm{d}x, \qquad I_9 = \int_0^{\frac{\pi}{4}} \tan^3 x\mathrm{d}x.$$

$\boxed{9.4}$ **[♦◇◇]** Calculer le nombre $\displaystyle\int_1^2 \frac{\ln(x)}{\sqrt{x}}\mathrm{d}x$

1. À l'aide d'une IPP.
2. À l'aide du changement de variable $x = t^2$.

$\boxed{9.5}$ **[♦◇◇]** Calculer
$$\int_1^3 \frac{1}{(t+1)\sqrt{t}}\mathrm{d}t \qquad \text{en posant } t = u^2.$$

$\boxed{9.6}$ **[♦◇◇]** Calculer
$$\int_0^1 \frac{t^9}{t^5+1}\mathrm{d}t \qquad \text{en posant } u = t^5.$$

$\boxed{9.7}$ **[♦♦◇]** En posant le changement de variable $u = \tan(x)$, calculer l'intégrale
$$\int_0^{\frac{\pi}{4}} \frac{1}{1+\cos^2(x)}\mathrm{d}x.$$

$\boxed{9.8}$ **[♦◇◇]** On pose

$$C = \int_0^{\frac{\pi}{2}} \frac{\cos x}{\sin x + \cos x} \mathrm{d}x \quad \text{et} \quad S = \int_0^{\frac{\pi}{2}} \frac{\sin x}{\sin x + \cos x} \mathrm{d}x.$$

1. À l'aide du changement de variable $u = \frac{\pi}{2} - x$, prouver que $C = S$.
2. Calculer $C + S$, en déduire la valeur commune de ces deux intégrales.

$\boxed{9.9}$ **[♦♦♦]** On considère les deux intégrales suivantes

$$I = \int_0^{\pi/2} \frac{\cos(t)}{\sqrt{1 + \sin(2t)}}\, dt \quad J = \int_0^{\pi/2} \frac{\sin(t)}{\sqrt{1 + \sin(2t)}}\, dt$$

1. A l'aide du changement de variable $u = \frac{\pi}{4} - t$ calculer $I + J$.
2. A l'aide du changement de variable $u = \frac{\pi}{2} - t$ montrer que $I = J$.
3. En déduire I et J.

$\boxed{9.10}$ **[♦◇◇]** Que vaut

$$\int_{-666}^{666} \ln\left(\frac{1 + e^{\arctan(x)}}{1 + e^{-\arctan(x)}}\right) \mathrm{d}x \ ?$$

$\boxed{9.11}$ **[♦♦◇]** Le but de cet exercice est de calculer les intégrales

$$I = \int_0^1 \sqrt{1 + x^2} \mathrm{d}x \quad \text{et} \quad J = \int_0^1 \frac{1}{\sqrt{1 + x^2}} \mathrm{d}x.$$

1. Justifier que l'équation $\mathrm{sh}(x) = 1$ possède une unique solution réelle que l'on notera dans la suite α. Exprimer α à l'aide de la fonction ln.
2. Calculer J en posant $x = \mathrm{sh}(t)$. On exprimera le résultat en fonction de α.
3. À l'aide d'une intégration par parties, obtenir une équation reliant I et J.
4. En déduire une expression de I en fonction de α.

$\boxed{9.12}$ **[♦♦♦]** Calculer $\displaystyle\int_0^1 \arctan(x^{1/3}) \mathrm{d}x$ en posant d'abord $x = t^3$.

$\boxed{9.13}$ **[♦♦♦]** Calculer l'intégrale $I = \displaystyle\int_0^{\pi/4} \ln(1 + \tan x)\, dx$ en posant $x = \frac{\pi}{4} - u$.

$\boxed{9.14}$ **[♦♦◇]** Les intégrales de Wallis : attention, grand classique !
On définit, pour tout entier $n \in \mathbb{N}$ le nombre

$$W_n = \int_0^{\pi/2} \sin^n(x) \mathrm{d}x.$$

1. À l'aide d'une intégration par parties, montrer que

$$\forall n \in \mathbb{N} \quad W_{n+2} = \frac{n+1}{n+2} W_n.$$

2. Démontrer les égalités suivantes pour $n \in \mathbb{N}$:

$$W_{2n} = \frac{(2n)!}{2^{2n}(n!)^2} \cdot \frac{\pi}{2} \quad \text{et} \quad W_{2n+1} = \frac{2^{2n}(n!)^2}{(2n+1)!}.$$

$\boxed{9.15}$ **[♦♦◇]** Pour tous entiers naturels p et q, on note

$$I(p,q) := \int_0^1 t^p(1-t)^q \mathrm{d}t.$$

1. Soit $(p,q) \in \mathbb{N}^2$.
   Avec un changement de variable, démontrer que $I(p,q) = I(q,p)$.
2. À l'aide de l'intégration par parties, démontrer

$$\forall p,q \in \mathbb{N} \quad (p+1)I(p,q+1) = (q+1)I(p+1,q).$$

3. (a) Calculer $I(p,0)$, pour un entier p donné.
   (b) Démontrer enfin que

$$\forall p,q \in \mathbb{N} \quad I(p,q) = \frac{p!q!}{(p+q+1)!}.$$

$\boxed{9.16}$ **[♦♦◇]** Pour tout entier naturel n, on pose $I_n = \displaystyle\int_1^e x(\ln x)^n \mathrm{d}x$.

1. Calculer I_0 et I_1.
2. Montrer que $J_n = 2I_n + nI_{n-1}$ est indépendant de n. Déterminer sa valeur.
3. Montrer que la suite (I_n) est décroissante puis, en utilisant la question **2.**, démontrer l'encadrement

$$\frac{e^2}{n+3} \leq I_n \leq \frac{e^2}{n+2} \, .$$

4. En déduire $\lim\limits_{n\to+\infty} I_n$ et $\lim\limits_{n\to+\infty} nI_n$.

$\boxed{9.17}$ **[♦♦♦]** Calculer, pour tout entier naturel n, le nombre $I_n = \int_0^1 x^n\sqrt{1-x}\mathrm{d}x$.

Petits systèmes linéaires

1 Droites et plans.

Droites

Définition 1.

Soit $(a, b) \in \mathbb{R}^2 \setminus \{(0,0)\}$ et $c \in \mathbb{R}$.

L'ensemble des couples (x, y) de $\mathbb{R}^2$ qui sont solutions de l'équation linéaire

$$ax + by = c$$

est une **droite affine** de $\mathbb{R}^2$.

La droite d'équation $ax + by = 0$ est dite **vectorielle**. Parallèle à la première, elle contient $(0, 0)$.

Proposition 2.

Soit $(a, b) \in \mathbb{R}^2 \setminus \{(0,0)\}$ et $c \in \mathbb{R}$. On considère les droites

$$D = \left\{(x, y) \in \mathbb{R}^2 \mid ax + by = c\right\} \quad \text{et} \quad D_0 = \left\{(x, y) \in \mathbb{R}^2 \mid ax + by = 0\right\}.$$

Considérons
- $\overrightarrow{u}$ un *vecteur* (couple) (α, β) non nul de D_0 (une solution non nulle de $ax + by = 0$) ;
- M_p un couple (x_p, y_p) de D (une solution particulière de $ax + by = c$).

On a

$$D_0 = \{(\lambda\alpha, \lambda\beta) \mid \lambda \in \mathbb{R}\} = \{\lambda\overrightarrow{u} \mid \lambda \in \mathbb{R}\}.$$

$$D = \{(x_p + \lambda\alpha, y_p + \lambda\beta) \mid \lambda \in \mathbb{R}\} = \{M_p \oplus \lambda\overrightarrow{u} \mid \lambda \in \mathbb{R}\}.$$

On appelle ces écritures des **représentations paramétriques** de D_0 et D, le réel λ étant un *paramètre*. L'addition $\oplus$ est ici celle des couples, coordonnée par coordonnée.

Exemple 3.

Droite d'équation $x - y = 2$. Représentation(s) paramétrique(s). Droite vectorielle associée.

Exemple 4 (Système linéaire 2×2 : l'intersection de droites sous-jacente)**.**

Soient (a, b, c) et (a', b', c') trois triplets de réels, tels que $(a, b) \neq (0, 0)$ et $(a', b') \neq (0, 0)$.
On considère le système linéaire ci-dessous :

$$\left\{ \begin{array}{cccc} ax & + & by & = c \\ a'x & + & b'y & = c' \end{array} \right.$$

En raisonnant en termes d'intersection de droites, discuter la forme que peut avoir l'ensemble des solutions dans $\mathbb{R}^2$.

Exemple 5 (Notre système linéaire 2×2 préféré : somme et différence)**.**

Soient $(x, y) \in \mathbb{R}^2$ et $(a, b) \in \mathbb{R}^2$. On a

$$\left\{ \begin{array}{ccc} x + y & = & a \\ x - y & = & b \end{array} \right. \qquad \Longleftrightarrow \qquad \left\{ \begin{array}{ccc} x & = & \frac{a+b}{2} \\ y & = & \frac{a-b}{2} \end{array} \right.$$

Plans

Définition 6.

Soit $(a, b, c) \in \mathbb{R}^3 \setminus \{(0, 0, 0)\}$ et $d \in \mathbb{R}$.

L'ensemble des triplets (x, y, z) de $\mathbb{R}^3$ qui sont solutions de l'équation linéaire

$$ax + by + cz = d$$

est un plan affine de $\mathbb{R}^3$.

Le plan d'équation $ax + by + cz = 0$ est dit **vectoriel**, il contient le triplet $(0, 0, 0)$.

Proposition 7.

Soit $(a, b, c) \in \mathbb{R}^3 \setminus \{(0, 0, 0)\}$ et $d \in \mathbb{R}$. On considère les plans

$$P = \left\{ (x, y, z) \in \mathbb{R}^3 \;\middle|\; ax + by + cz = d \right\} \quad \text{et} \quad P_0 = \left\{ (x, y, z) \in \mathbb{R}^3 \;\middle|\; ax + by + cz = 0 \right\}.$$

Considérons
- $\overrightarrow{u}$ et $\overrightarrow{v}$ deux *vecteurs* (triplets) non colinéaires de P_0 ;
- M_p un triplet de P.

On a

$$P_0 = \left\{ \lambda \overrightarrow{u} + \mu \overrightarrow{v} \;\middle|\; (\lambda, \mu) \in \mathbb{R}^2 \right\} \qquad \text{et} \qquad P = \left\{ M_p + \lambda \overrightarrow{u} + \mu \overrightarrow{v} \;\middle|\; (\lambda, \mu) \in \mathbb{R}^2 \right\}.$$

On appelle ces écritures des **représentations paramétriques** de P_0 et P, les réels λ et μ étant des *paramètres*. L'addition $+$ est ici celle des triplets, coordonnée par coordonnée.

Exemple 8.

Plan d'équation $x - y - z = 3$. Représentation(s) paramétrique(s). Plan vectoriel associé.

Exemple 9 (Système linéaire 2×3 : l'intersection de plans sous-jacente)**.**

Soient (a, b, c, d) et (a', b', c', d') trois 4-uplets de réels, tels que (a, b, c) et (a', b', c') sont différents de $(0, 0, 0)$. On considère le système linéaire ci-dessous :

$$\left\{ \begin{array}{ccccccl} ax & + & by & + & cz & = d \\ a'x & + & b'y & + & c'z & = d' \end{array} \right.$$

En réfléchissant en termes d'intersection de plans, discuter la forme que peut avoir l'ensemble de solutions dans $\mathbb{R}^3$.

2 L'algorithme du pivot, par l'exemple.

Exemple 10.

Donner l'ensemble des triplets $(x, y, z) \in \mathbb{R}^3$ solutions de

$$\left\{ \begin{array}{ccccccl} x & + & y & + & z & = 1 \\ 2x & - & y & + & 11z & = -1 \\ 3x & + & 4y & + & z & = 1 \end{array} \right.$$

Exemple 11.

Donner l'ensemble des triplets $(x, y, z) \in \mathbb{R}^3$ solutions de

$$\left\{ \begin{array}{ccccccl} 2x & + & 3y & + & 7z & = 6 \\ x & + & y & + & 2z & = 2 \\ 3x & + & 4y & + & 9z & = 8 \end{array} \right.$$

Exemple 12.

Discuter selon les valeurs de $m \in \mathbb{R}$ l'ensemble des solutions du système suivant.

$$\left\{ \begin{array}{cccl} x & + & (m+1)y & = (m+2) \\ mx & + & (m+4)y & = 8 \end{array} \right.$$

Interpréter en termes d'intersection de droites.

Définition 13.

On appelle **opération élémentaire** sur les lignes d'un système l'une des opérations suivantes :

1. Échange des $i$èmes et $j$èmes lignes. On note $L_i \leftrightarrow L_j$.
2. Multiplication d'une ligne par un scalaire λ non nul. On note $L_i \leftarrow \lambda L_i$.
3. Ajout à la ligne L_i d'une ligne L_j $(i \neq j)$ multipliée par un scalaire μ. On note $L_i \leftarrow L_i + \mu L_j$.

Proposition 14 (admise)**.**

Si on passe d'un système linéaire à un autre par un nombre fini d'opérations élémentaires, les deux systèmes ont le même ensemble de solutions.

Définition 15.

Un système linéaire ayant des solutions est dit compatible.
Un système linéaire ayant une unique solution est dit de **Cramer**.

Exercices

10.1 **[♦◇◇]** [Un système de Cramer bête et méchant]
Résoudre le système suivant dans $\mathbb{R}^3$ (si vous ne trouvez pas une unique solution $(3,5,2)$, recommencez).

$$\begin{cases} 3x + y - 2z = 10 \\ 2x - y + z = 3 \\ x - y + 2z = 2 \end{cases}$$

10.2 **[♦◇◇]** Résoudre le système suivant dans $\mathbb{R}^3$.

$$\begin{cases} x + 2y - z = 2 \\ x - 2y + 3z = -2 \\ 3x - 2y + 5z = -2 \end{cases}$$

10.3 **[♦♦◇]** Soit $(a,b,c) \in \mathbb{R}^3$, $a \neq b$, $a \neq c$, $b \neq c$. Résoudre :

$$\begin{cases} x + ay + a^2z = a^3 \\ x + by + b^2z = b^3 \\ x + cy + c^2z = c^3 \end{cases}$$

10.4 **[♦♦♦]** Soit λ un paramètre réel et le système :

$$\begin{cases} (2-\lambda)x + y + z = 0 \\ x + (2-\lambda)y + z = 0 \\ x + y + (2-\lambda)z = 0 \end{cases}$$

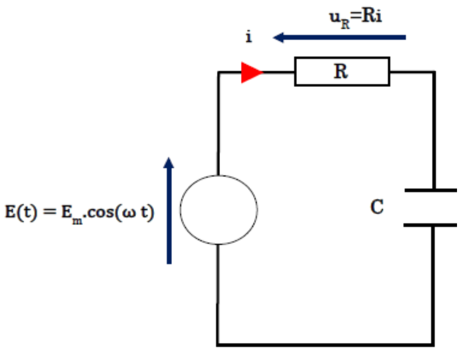
Le résoudre, en discutant selon les valeurs de λ.

---

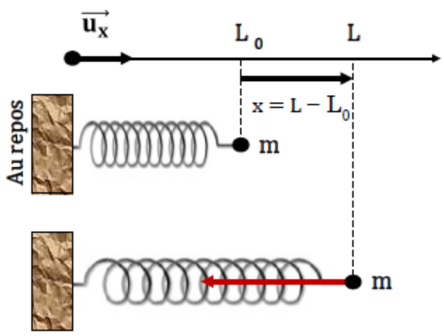
11 Équations différentielles linéaires d'ordre 1

Dans ce cours, $\mathbb{K}$ désignera $\mathbb{R}$ ou $\mathbb{C}$ et I un intervalle de $\mathbb{R}$.

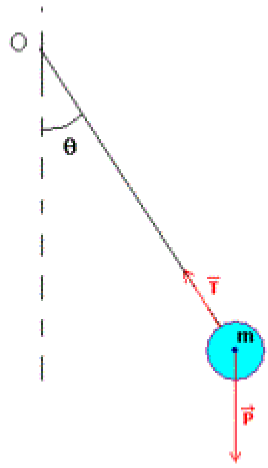
0 Notion d'équation différentielle.



Circuit RC série.



Ressort



Pendule

En physique, en chimie, en économie... on étudie parfois l'évolution, au sein d'un système, d'une quantité d'intérêt Q, dépendant d'un paramètre t (par exemple le temps). On va donc être amené à s'interroger sur la *fonction* $Q : t \mapsto Q(t)$. Les contraintes s'exerçant sur le système sont traduites à travers des équations, qui peuvent faire intervenir Q mais aussi ses dérivées successives.

Considérons trois exemples issus de la physique.

Exemple 1. Circuit RC série.

Soient une résistance R et un condensateur de capacité C branchés en série à un générateur de tension sinusoïdal imposant à ses bornes une tension $E(t) = E_m \cos(\omega t)$. On étudie la tension u aux bornes du condensateur. Si on note i le courant traversant le circuit, la loi des mailles amène $E = u + Ri$. Or, on a $i = C\frac{\mathrm{d}u}{\mathrm{d}t}$. D'où, pour $t \geq 0$,

$$RC\frac{\mathrm{d}u}{\mathrm{d}t}(t) + u(t) = E_m \cos(\omega t) \tag{1}$$

Exemple 2. Masse attachée à un ressort.
Soit une masse m, attachée à un ressort ayant un coefficient de rappel k. La masse se déplace sur une surface plane, avec un coefficient de frottement fluide λ. On étudie la position x de la masse au cours du temps. Notons $\overrightarrow{a}$ son accélération. Le principe fondamental de la dynamique donne

$$m\overrightarrow{a} = \overrightarrow{P} + \overrightarrow{N} + \overrightarrow{F}_{rappel} + \overrightarrow{F}_{frott}.$$

En dehors du poids $\overrightarrow{P}$ et de la réaction normale du support $\overrightarrow{N}$, la masse est soumise à la force de rappel $\overrightarrow{F}_{rappel} = -kx(t)\overrightarrow{u_x}$, et à une force de frottement fluide $\overrightarrow{F}_{frott} = -\lambda\overrightarrow{v} = -\lambda\frac{\mathrm{d}x}{\mathrm{d}t}\overrightarrow{u_x}$. Son accélération est $\overrightarrow{a} = \frac{\mathrm{d}^2x}{\mathrm{d}t^2}\overrightarrow{u_x}$. Ainsi, en projetant l'égalité vectorielle sur $\overrightarrow{e_1}$, on obtient pour tout $t \geq 0$:

$$m\frac{\mathrm{d}^2x}{\mathrm{d}t^2}(t) + \lambda\frac{\mathrm{d}x}{\mathrm{d}t}(t) + kx(t) = 0. \tag{2}$$

Exemple 3. Pendule simple, sans frottement.
Une masse attachée à un fil non élastique, et non pesant, de longueur ℓ. La force de tension $\overrightarrow{T}$, orthogonale au vecteur vitesse, ne travaille pas, contrairement au poids $\overrightarrow{P}$. On étudie l'angle $\theta(t)$ entre la position à l'instant t et celle de repos. En dérivant une expression de l'énergie mécanique, constante ici, on peut obtenir la relation suivante, pour $t \geq 0$.

$$\frac{\mathrm{d}^2\theta}{\mathrm{d}t^2}(t) + \frac{g}{\ell}\sin(\theta(t)) = 0, \tag{3}$$

où g est l'accélération de la pesanteur.

Les relations (1), (2) et (3) sont des **équations différentielles**. Le plus haut degré de dérivation mis en jeu dans l'équation est appelé **ordre** de l'équation. L'équation (1) est d'ordre 1 car seule la première dérivée y figure. Les équations (2) et (3) sont, elles, d'ordre 2.

On dit d'une équation différentielle qu'elle est **linéaire** si elle se présente sous la forme

$$\sum_{k=0}^{n} a_k y^{(k)} = b,$$

où $a_0, a_1, \ldots, a_n$ et b sont des fonctions. Les équations (1) et (2) sont linéaires, ce qui n'est pas le cas pour (3) à cause du sinus.

La forme générale d'une équation différentielle linéaire d'ordre 1 est donc

$$a_1(t)y'(t) + a_0(t)y(t) = b(t).$$

Quitte à diviser par a_1 et résoudre l'équation sur des intervalles où elle ne s'annule pas, on peut se ramener à une équation pour laquelle la fonction devant y' est constante égale à 1. C'est ainsi que dans ce cours on résoudra les équations de la forme

$$y'(t) + a(t)y(t) = b(t),$$

où a et b sont des fonctions continues sur un intervalle de $\mathbb{R}$. On se restreint donc à l'étude de (certaines) équations différentielles linéaires d'ordre 1.

1 Ensemble des solutions d'une ED linéaire d'ordre 1.

Définition 1.

Soient $a, b : I \to \mathbb{K}$ deux applications continues sur I. On considère l'équation différentielle

$$y' + a(x)y = b(x) \qquad (E)$$

- On dit que $y : I \to \mathbb{K}$ est **solution** de (E) sur I si elle est dérivable sur I et si elle est telle que $\forall x \in I \ y'(x) + a(x)y(x) = b(x)$.
- La fonction b est souvent appelée **second membre** de l'équation.
- L'**équation homogène** associée à (E) (ou équation "sans second membre") est

$$y' + a(x)y = 0 \qquad (E_0)$$

Ci-dessous, S et S_0 désignent respectivement les ensembles de solutions de (E) et (E_0).

Proposition 2 (Lien entre S et S_0)**.**

Si S est non vide, alors, en considérant $z_p \in S$ (une « solution particulière » de l'équation), on a

$$S = \{z_p + y, \quad y \in S_0\}.$$

Pour connaître *toutes* les solutions de (E), il suffit donc de

- connaître *toutes* les solutions de (E_0) $\longrightarrow$ partie 2 du cours.
- connaître *une* solution de (E) $\longrightarrow$ partie 3 du cours.

2 Résolution de l'équation homogène.

On va donner $\boxed{\text{toutes}}$ les solutions de

$$y' + a(x)y = 0 \qquad (E_0)$$

Cas particulier (Terminale) : le cas où a est une fonction constante (égale à $a \in \mathbb{K}$). On a vu que les solutions de $y' + ay = 0$ sont les fonctions de la forme $x \mapsto \lambda e^{-ax}$, où λ est une constante quelconque de $\mathbb{K}$.

Ci-dessous, on traite le cas général pour une fonction $a : I \to \mathbb{K}$.

Théorème 3.

Soit (E_0) l'équation $y' + a(x)y = 0$, où $a : I \to \mathbb{K}$ est une fonction continue sur l'intervalle I.
Soit A une primitive de a sur I. L'ensemble S_0 des solutions de (E_0) sur I est

$$S_0 = \left\{x \mapsto \lambda e^{-A(x)} \quad | \ \lambda \in \mathbb{K}\right\}.$$

On dit aussi que $x \mapsto \lambda e^{-A(x)}$, où $\lambda \in \mathbb{K}$, est la *solution générale* de (E_0).

Exemple 4.

Résoudre sur $]0,1[$ l'équation $t(1-t)y' + y = 0$.

Lemme 5 (Une remarque intéressante)**.**

Si a est continue sur I, la seule solution de $y'+a(x)y=0$ qui s'annule sur I, c'est la fonction nulle.

3 Équation générale : obtenir une solution particulière.

Il s'agit ici de trouver $\boxed{\text{une}}$ solution de l'équation

$$y' + a(x)y = b(x) \qquad (E)$$

3.1 Trouver une solution à vue.

Lorsque a et b sont des fonctions constantes (a non nulle), notre équation a une solution constante. On a déjà croisé ce genre de situation en physique en regardant un circuit RC soumis à un échelon de tension.

Plus précisément,

$$\boxed{\text{L'équation } y' + ay = b \text{ a pour solution particulière la fonction constante } z_p : x \mapsto \frac{b}{a}.}$$

Plus généralement, lorsque b sera une fonction polynomiale de degré n, on pourra chercher une solution polynomiale de degré n.

Exemple 6.

Deviner une solution pour les équations ci-dessous

$$(1)\ y' + 2y = 1 \qquad (2)\ y' + 2y = e^x \qquad (3)\ y' + y = x.$$

3.2 Principe de superposition.

Pratique lorsque le second membre se présente comme somme de deux fonctions.

Proposition 7 (Principe de superposition)**.**

Soient a, b_1, b_2 trois fonctions continues sur I. Si
- y_1 est solution sur I de $y' + a(x)y = b_1(x) \quad (E_1)$,
- y_2 est solution sur I de $y' + a(x)y = b_2(x) \quad (E_2)$,

alors $y_1 + y_2$ est solution sur I de l'équation $y' + a(x)y = b_1(x) + b_2(x) \quad (E_3)$.

Exemple 8.

Trouver une solution de l'équation $y' + 2y = 1 + e^x$.

3.3 Méthode générale : variation de la constante.

Proposition 9 (Variation de la constante).

Si a et b sont continues sur I, l'équation $y' + a(x)y = b(x)$ possède une solution z de la forme $z = \lambda u$ où u est une solution non nulle de l'équation homogène, et λ une fonction dérivable sur I.

Preuve. (a valeur de méthode en pratique).

On cherche une solution de (E) de la forme $z : x \mapsto \lambda(x)u(x)$, où u est une solution (non nulle) de l'équation homogène (E_0) et λ une fonction dérivable sur I à choisir.

La fonction z étant dérivable sur I comme produit, on a

$$\begin{aligned} z' + az &= (\lambda u)' + a(\lambda u) \\ &= \lambda' u + \lambda u' + \lambda a u \\ &= \lambda' u + \underbrace{\lambda\,(u' + au)}_{=0}, \end{aligned}$$

où on a utilisé à la dernière ligne que u est solution de (E_0). Ainsi,

$$\begin{array}{rcll} z \text{ est solution de } (E) & \iff & z' + az = b & \text{sur } I \\ & \iff & \lambda' u = b & \text{sur } I. \end{array}$$

Nous avons vu plus haut que, puisque u est une solution de (E_0) qui n'est pas la fonction nulle, elle ne s'annule nulle part sur I. On peut donc écrire

$$z \text{ est solution de } (E) \quad \iff \quad \lambda' = b/u \quad \text{sur } I.$$

Notre fonction z sera donc solution si et seulement si λ est choisie parmi les primitives de b/u.

□

Exemple 10.

Résolution de $x^4 y' + 3x^3 y = 1$ sur $\mathbb{R}_+^*$.

4 Synthèse.

Théorème 11 (de synthèse).

Soient $a : I \to \mathbb{K}$ et $b : I \to \mathbb{K}$ deux fonctions continues. L'équation

$$y' + a(x)y = b(x) \quad (E)$$

a des solutions. Si z_p est une telle solution (« particulière ») et A une primitive de a sur I, alors l'ensemble des solutions de (E) est

$$S = \left\{ x \mapsto z_p(x) + \lambda e^{-A(x)}, \lambda \in \mathbb{K} \right\}.$$

Définition 12.

Soient $x_0 \in I$ et $y_0 \in \mathbb{R}$. On appelle **problème de Cauchy** la donnée d'une équation différentielle et d'une condition initiale (valeur imposée en un point)

$$\left\{ \begin{array}{rcl} y' + a(x)y & = & b(x) \\ y(x_0) & = & y_0 \end{array} \right. .$$

Théorème 13 (de Cauchy-Lipschitz, cas linéaire)**.**

Soient $a, b : I \to \mathbb{K}$ continues, $x_0 \in I$ et $y_0 \in \mathbb{K}$.

Le problème de Cauchy $\left\{ \begin{array}{rcl} y' + a(x)y & = & b(x) \\ y(x_0) & = & y_0 \end{array} \right.$ admet une unique solution sur I.

Preuve. D'après le théorème précédent, l'équation différentielle admet des solutions. On en fixe une que l'on note z_p. Si A une primitive fixée de a sur I, alors les solutions sont les fonctions de la forme

$$y : x \mapsto z_p(x) + \lambda e^{-A(x)}.$$

Parmi ces fonctions, on veut distinguer celles qui satisfont la condition initiale. On écrit donc

$$\begin{aligned} y(x_0) = y_0 &\iff z_p(x_0) + \lambda e^{-A(x_0)} = y_0 \\ &\iff \lambda = e^{A(x_0)} \left(y_0 - z_p(x_0) \right). \end{aligned}$$

Il existe donc une unique valeur pour λ pour laquelle $y(x_0) = y_0$; notons-la λ_0.
Le problème de Cauchy possède une unique solution : la fonction $y = z_p + \lambda_0 e^{-A}$. □

Exercices

11.1 [♦◇◇] Résoudre les équations différentielles ci-dessous

1. $y' - 2y = 2$ sur $\mathbb{R}$
2. $(x^2+1)y' + xy = x$
3. $y' + \tan(x)y = \sin(2x)$ sur $]-\frac{\pi}{2}, \frac{\pi}{2}[$
4. $y' - \ln(x)y = x^x$ sur $\mathbb{R}_+^*$
5. $(1-x)y' - y = \dfrac{1}{1-x}$ sur $]-\infty, 1[$

11.2 [♦◇◇] Résoudre sur $\mathbb{R}_+^*$ le problème de Cauchy $\left\{ \begin{array}{rcl} y' - \dfrac{2}{x}y & = & x^2 \cos x \\ y(\pi) & = & 0 \end{array} \right.$

11.3 [♦♦◇] Trouver toutes les fonctions f dérivables sur $\mathbb{R}$ telles que

$$\forall x \in \mathbb{R} \quad f'(x) + f(x) = \int_0^1 f(t)\mathrm{d}t.$$

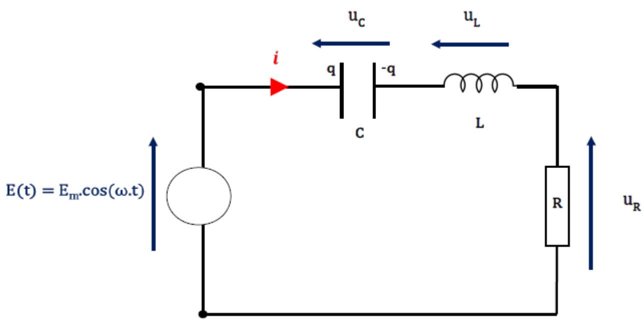
11.4 [♦♦♦] [« Recollement »]
Soit l'équation différentielle $x^2y' - y = 0$.

1. Résoudre sur $\mathbb{R}_+^*$ et sur $\mathbb{R}_-^*$.
2. Trouver toutes les solutions définies sur $\mathbb{R}$.

---

12 Équations différentielles linéaires d'ordre 2 à coefficients constants

Introduction



Oscillateur harmonique amorti, soumis à une excitation périodique.

On considère, branchés en série, une résistance R, un condensateur de capacité C, une bobine d'inductance L, et un générateur de tension sinusoïdale. Soit q la charge aux bornes du condensateur ; on a $i = \frac{\mathrm{d}q}{\mathrm{d}t}$. Exprimons toutes les tensions en fonction de q : $u_R = Ri = R\frac{\mathrm{d}q}{\mathrm{d}t}$, $u_L = L\frac{\mathrm{d}i}{\mathrm{d}t} = L\frac{\mathrm{d}^2q}{\mathrm{d}t^2}$ et $u_C = \frac{q}{C}$. En appliquant la loi des mailles, on obtient $\frac{q}{C} + R\frac{\mathrm{d}q}{\mathrm{d}t} + L\frac{\mathrm{d}^2q}{\mathrm{d}t^2} = E_m\cos(\omega t)$, que l'on récrit

$$\frac{\mathrm{d}^2q}{\mathrm{d}t^2} + 2\lambda\frac{\mathrm{d}q}{\mathrm{d}t} + \omega_0^2 q = \frac{E_m}{L}\cos(\omega t) \qquad (\varphi)$$

où $\lambda = \frac{R}{2L}$ et $\omega_0 = (\sqrt{LC})^{-1}$. Le paramètre λ, on le verra, est un facteur d'*amortissement*, homogène à l'inverse d'un temps. Le paramètre ω_0 est appelé *pulsation propre* de l'oscillateur dans le cas d'un amortissement négligeable ($\lambda = 0$) et en l'absence d'excitation ($U_0 = 0$), q sera sinusoïdal de pulsation ω_0. L'équation (φ) modélise aussi bien des oscillateurs mécaniques, et elle sera étudiée et utilisée en physique et en SII.

Dans ce cours, on s'intéresse aux équations différentielles linéaires d'ordre 2 de la forme

$$y'' + ay' + by = f(x) \qquad (E),$$

où $(a, b) \in \mathbb{K}^2$ (les coefficients sont *constants*, ce ne sont pas des fonctions) et où $f : \mathbb{R} \to \mathbb{K}$ appartient à une classe de fonctions utile pour les applications.

1 Ensemble des solutions d'une ED linéaire d'ordre 2.

Définition 1.

Soient $a, b \in \mathbb{K}$ deux constantes et $f : I \to \mathbb{K}$. On considère l'équation différentielle

$$y'' + ay' + by = f(x) \qquad (E)$$

On appelle **solution** de (E) sur $\mathbb{R}$, à valeurs dans $\mathbb{K}$ toute fonction $y : \mathbb{R} \to \mathbb{K}$, deux fois dérivable, et telle que $\forall x \in \mathbb{R}\ y''(x) + ay'(x) + by(x) = f(x)$.

On appelle **équation homogène** associée à (E) l'équation différentielle

$$y'' + ay' + by = 0 \qquad (E_0).$$

Ci-dessous, S et S_0 désignent respectivement les ensembles de solutions de (E) et (E_0).

Proposition 2 (Structure de S_0)**.**

S_0 contient la fonction nulle et est stable par combinaisons linéaires.

Preuve. Soient y_1 et y_2 deux solutions de (E_0) et λ et μ deux scalaires de $\mathbb{K}$. Par définition, y_1 et y_2 sont donc deux fois dérivables et il en va de même de $\lambda y_1 + \mu y_2$. On a donc

$$\begin{aligned}
&(\lambda y_1 + \mu y_2)'' + a(\lambda y_1 + \mu y_2)' + b(\lambda y_1 + \mu y_2)\\
&\qquad = (\lambda y_1'' + \mu y_2'') + a(\lambda y_1' + \mu y_2') + b(\lambda y_1 + \mu y_2)\\
&\qquad = \lambda\underbrace{(y_1'' + ay_1' + by_1)}_{=0 \text{ car } y_1 \in S_0} \;+\; \mu\underbrace{(y_2'' + ay_2' + by_2)}_{=0 \text{ car } y_2 \in S_0}\\
&\qquad = \lambda \cdot 0 + \mu \cdot 0 = 0.
\end{aligned}$$

On a donc montré que $(\lambda y_1 + \mu y_2) \in S_0$. □

Proposition 3 (Lien entre S et S_0)**.**

Si S est non vide, alors, en considérant $z_p \in S$ (une « solution particulière » de l'équation), on a

$$S = \{z_p + y, \quad y \in S_0\}.$$

Preuve. Soit z une fonction deux fois dérivable sur $\mathbb{R}$. On a

$$\begin{aligned}
z \in S \quad &\iff \quad z'' + az' + bz = f\\
&\iff \quad z'' + az' + bz = z_p'' + az_p' + bz_p\\
&\iff \quad (z - z_p)'' + a(z - z_p)' + b(z - z_p) = 0\\
&\iff \quad z - z_p \in S_0\\
&\iff \quad \exists y \in S_0 \ \ z - z_p = y.
\end{aligned}$$

□

Remarque. Tout ce qui précède reste valable, sans changer la preuve, lorsque a et b sont des fonctions.

Pour connaître *toutes* les solutions de (E), il suffit donc de

- connaître *toutes* les solutions de (E_0) $\longrightarrow$ partie 2 du cours
- connaître *une* solution de (E) $\longrightarrow$ partie 3 (dans des cas particuliers)

2 Résolution de l'équation homogène.

Dans ce paragraphe, on souhaite déterminer S_0, ensemble des solutions de l'équation homogène

$$y'' + ay' + by = 0 \qquad (E_0)$$

Commençons par chercher des solutions à l'équation, de la forme $u : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{C} \\ x & \mapsto & e^{rx} \end{array} \right.$, où $r \in \mathbb{C}$.

La fonction u est deux fois dérivable sur $\mathbb{R}$: $u' = ru$ et $u'' = r^2 u$. On a donc

$$u'' + au' + bu = (r^2 + ar + b)u \qquad \text{et donc} \qquad u \in S_0 \iff r^2 + ar + b = 0.$$

Ceci motive la définition suivante.

Définition 4.

On appelle **équation caractéristique** associée à (E_0) l'équation

$$x^2 + ax + b = 0,$$

où a et b sont les coefficients constants de (E_0).

Remarque. On rappelle qu'une telle équation a deux racines r_1 et r_2, avec $r_1 + r_2 = -a$.
On a $r_1 = r_2$ (racine « double ») si et seulement si elles valent toutes les deux $-a/2$.

Lemme 5 (Des solutions de E_0)**.**

Soit l'équation caractéristique $x^2 + ax + b = 0$ associée à (E_0) et r une racine de cette équation.

- la fonction $x \mapsto e^{rx}$ est solution de (E_0).
- Si r est une racine double, $x \mapsto xe^{rx}$ est solution de (E_0).

Théorème 6 (Solutions complexes de l'équation homogène)**.**

Soit $(a, b) \in \mathbb{C}^2$ et (E_0) l'équation $y'' + ay' + by = 0$.
Soit Δ le discriminant de l'équation caractéristique $x^2 + ax + b = 0$.
On note $S_0^{\mathbb{C}}$ l'ensemble des solutions de (E_0) à valeurs complexes.

- Si $\Delta \neq 0$, l'équation caractéristique a deux racines distinctes dans $\mathbb{C}$, disons r_1 et r_2, et

$$S_0^{\mathbb{C}} = \left\{ x \mapsto \lambda e^{r_1 x} + \mu e^{r_2 x},\ (\lambda, \mu) \in \mathbb{C}^2 \right\}.$$

- Si $\Delta = 0$, l'équation caractéristique a une racine double dans $\mathbb{C}$, disons r, et

$$S_0^{\mathbb{C}} = \left\{ x \mapsto \lambda x e^{rx} + \mu e^{rx},\ (\lambda, \mu) \in \mathbb{C}^2 \right\}.$$

Preuve. Pour $r_1, r_2, r \in \mathbb{C}$, on note

$$\Gamma^{\mathbb{C}}(r_1,r_2) = \left\{x \mapsto \lambda e^{r_1 x} + \mu e^{r_2 x},\ (\lambda,\mu) \in \mathbb{C}^2\right\} \quad \text{et} \quad \widetilde{\Gamma}^{\mathbb{C}}(r) = \left\{x \mapsto (\lambda x + \mu)e^{rx},\ (\lambda,\mu) \in \mathbb{C}^2\right\}.$$

Partie 1. "Les inclusions $\supset$".

• Si $\Delta \neq 0$, alors, l'équation caractéristique a deux racines distinctes que l'on note r_1 et r_2. D'après le Lemme 5, les fonctions $y_1 : x \mapsto e^{r_1 x}$ et $y_2 : x \mapsto e^{r_2 x}$ sont solutions de (E_0). D'après la proposition **??** toutes les combinaisons linéaires de la forme $\lambda y_1 + \mu y_2$ sont encore des solutions de (E_0). Ceci montre que $S_0^{\mathbb{C}} \supset \Gamma^{\mathbb{C}}(r_1,r_2)$.

• Si $\Delta = 0$. Alors, l'équation caractéristique a une racine double que l'on note r. D'après le Lemme 5, les fonctions $y_1 : x \mapsto xe^{rx}$ et $y_2 : x \mapsto e^{rx}$ sont solutions de (E_0). D'après la proposition **??** toutes les combinaisons linéaires de la forme $(\lambda y_1 + \mu y_2) : x \mapsto \lambda x e^{rx} + \mu e^{rx}$ sont encore des solutions de (E_0). Ceci montre que $S_0^{\mathbb{C}} \supset \widetilde{\Gamma}^{\mathbb{C}}(r)$.

Partie 2. "Les inclusions $\subset$".

Soit $y \in S_0^{\mathbb{C}}$ une solution de (E_0) à coefficients complexes. Soit r une solution complexe de l'équation caractéristique ; on définit la fonction $z : x \mapsto e^{-rx}y(x)$. La fonction z est deux fois dérivable par produit. Notons $u : x \mapsto e^{rx}$. On a

$$\begin{aligned} y &= uz, \\ y' &= u'z + uz', \\ y'' &= u''z + u'z' + u'z' + uz''. \end{aligned}$$

Dans ce qui suit, les équivalences sont inutiles, et seules les implications directes nous servent. On a tout de même conservé les équivalences car si on cherchait à écrire une preuve plus courte, on pourrait les utiliser pour se dispenser de la partie 1.

$$\begin{aligned} y \text{ est solution de } (E_0) &\iff y'' + ay' + by = 0 \\ &\iff (u''z + u'z' + u'z' + uz'') + a(u'z + uz') + buz = 0 \\ &\iff uz'' + (2\underbrace{u'}_{=ru} + au)z' + (\underbrace{u'' + au' + bu}_{=0 \text{ car } u \in S_0^{\mathbb{C}}})z = 0 \\ &\iff uz'' + u(2r+a)z' = 0 \end{aligned}$$

Rappelons que pour tout x réel, $u(x) = e^{rx} \neq 0$ (ce nombre complexe étant de module non nul...) On peut alors diviser par u pour obtenir

$$y \text{ est solution de } (E_0) \iff z' \text{ est solution de } Y' + (2r+a)Y \overset{(*)}{=} 0.$$

On a supposé y est solution de (E_0). En résolvant $(*)$, on en déduit qu'il existe $\lambda \in \mathbb{C}$ tel que

$$\forall x \in \mathbb{R} \quad z'(x) = \lambda e^{-(2r+a)x}.$$

• Si $\Delta = 0$, alors r est racine double et $2r + a = 0$. On a donc que z' est constante égale à λ donc il existe μ telle que

$$\forall x \in \mathbb{R} \quad z(x) = \lambda x + \mu,$$

d'où

$$\forall x \in \mathbb{R} \quad y(x) = e^{rx}z(x) = (\lambda x + \mu)e^{rx}.$$

On a bien montré ici que $y \in \widetilde{\Gamma}^{\mathbb{C}}(r)$.

• Si $\Delta \neq 0$, alors, l'équation caractéristique a deux racines distinctes r_1 et r_2. Mettons que $r = r_2$. Alors, $r_1 = -r - a$, et comme $r_1 \neq r_2$, on a $2r + a \neq 0$. Connaissant z', on connait z : il existe une constante μ telle que

$$\forall x \in \mathbb{R} \quad z(x) = -\frac{\lambda}{2r+a}e^{-(2r+a)x} + \mu,$$

d'où

$$\forall x \in \mathbb{R} \quad y(x) = e^{rx}z(x) = \underbrace{-\frac{\lambda}{2r+a}}_{:=\tilde{\lambda}} e^{(-\cancel{2}r-a+\cancel{r})x} + \mu e^{rx} = \tilde{\lambda}e^{r_1 x} + \mu e^{r_2 x}.$$

On a bien montré ici que $y \in \Gamma^{\mathbb{C}}(r_1,r_2)$.

$\square$

Théorème 7 (Solutions réelles de l'équation homogène).

Soit $(a,b) \in \mathbb{R}^2$ et (E_0) l'équation $y'' + ay' + by = 0$. Soit Δ le discriminant de l'équation caractéristique $x^2 + ax + b = 0$. Notons $S_0^{\mathbb{R}}$ l'ensemble des solutions de (E_0) à valeurs réelles.

- Si $\Delta > 0$, l'équation caractéristique a deux racines *réelles* distinctes, disons r_1 et r_2 et

$$S_0^{\mathbb{R}} = \left\{t \mapsto \lambda e^{r_1 t} + \mu e^{r_2 t},\ (\lambda,\mu) \in \mathbb{R}^2\right\}.$$

- Si $\Delta = 0$, l'équation caractéristique a une racine double dans $\mathbb{R}$, disons r et

$$S_0^{\mathbb{R}} = \left\{t \mapsto \lambda t e^{rt} + \mu e^{rt},\ (\lambda,\mu) \in \mathbb{R}^2\right\}.$$

- Si $\Delta < 0$, l'équation caractéristique a deux racines *complexes conjuguées*.
  On les note $r_1 = \gamma + i\omega$ et $r_2 = \gamma - i\omega$, avec $(\gamma,\omega) \in \mathbb{R}^2$. On a alors

$$S_0^{\mathbb{R}} = \left\{t \mapsto e^{\gamma t}\left(\alpha\cos(\omega t) + \beta\sin(\omega t)\right),\ (\alpha,\beta) \in \mathbb{R}^2\right\}.$$

  On peut aussi écrire $S_0^{\mathbb{R}} = \left\{t \mapsto Ae^{\gamma t}\cos(\omega t + \varphi),\ (A,\varphi) \in \mathbb{R}^2\right\}$.

Remarque. Une idée clé : toute solution à valeurs réelles de (E_0) est a fortiori une solution à valeurs complexes de cette même équation. Ceci peut s'énoncer à l'aide de l'inclusion :

$$S_0^{\mathbb{R}} \subset S_0^{\mathbb{C}}.$$

Preuve. du cas $\Delta < 0$. L'équation caractéristique a deux racines complexes conjuguées $r_1 = \gamma + i\omega$ et $r_2 = \gamma - i\omega$, avec $(\gamma,\omega) \in \mathbb{R}^2$. Soit $y \in S_0^{\mathbb{R}}$. A fortiori, $y \in S_0^{\mathbb{C}}$. D'après le théorème 6, il existe donc deux nombres **complexes** λ et μ tels que

$$\forall t \in \mathbb{R} \quad y(t) = \lambda e^{r_1 t} + \mu e^{r_2 t} \qquad (*)$$

On laisse ici les calculs au lecteur : puisque y est à valeurs réelles on a en particulier $\overline{y(0)} = y(0)$ et $\overline{y'(0)} = y'(0)$. En se rappelant que $r_2 = \overline{r_1}$, ceci conduit au système $\begin{cases} (\lambda - \overline{\mu}) + (\mu - \overline{\lambda}) & = & 0 & (L_1) \\ r_1(\lambda - \overline{\mu}) + \overline{r_1}(\mu - \overline{\lambda}) & = & 0 & (L_2) \end{cases}$

L'opération $L_2 \leftarrow L_2 - r_1 L_1$ amène que $\boxed{\mu = \overline{\lambda}}$. On a donc, en revenant à $(*)$,

$$\forall t \in \mathbb{R} \quad y(t) = e^{\gamma t}\left(\overline{\lambda} e^{i\omega t} + \overline{\lambda} e^{-i\omega t}\right) = e^{\gamma t} \cdot 2\mathrm{Re}\left(\lambda e^{i\omega t}\right).$$

Écrivons λ sous forme géométrique : $\lambda = re^{i\varphi}$. On a donc

$$\forall t \in \mathbb{R} \quad y(t) = 2e^{\gamma t}\mathrm{Re}\left(e^{i\varphi}e^{i\omega t}\right) = 2re^{\gamma t}\cos\left(\omega t + \varphi\right),$$

ce qui est bien de la forme donnée par le théorème, en posant $A = 2r$. On vient de montrer l'inclusion

$$S_0^{\mathbb{R}} \subset \left\{t \mapsto Ae^{\gamma t}\cos(\omega t + \varphi),\ (A,\varphi) \in \mathbb{R}^2\right\}.$$

On peut aussi écrire

$$\forall t \in \mathbb{R} \quad y(t) = 2re^{\gamma t}\left(\cos(\varphi)\cos(\omega t) - \sin(\varphi)\sin(\omega t)\right),$$

ce qui montre l'inclusion

$$S_0^{\mathbb{R}} \subset \left\{t \mapsto e^{\gamma t}\left(\alpha\cos(\omega t) + \beta\sin(\omega t)\right),\ (\alpha,\beta) \in \mathbb{R}^2\right\}.$$

Les inclusions réciproques sont plus simples. □

Exemple 8.

Pour chacune des équations ci-dessous, on écrit l'ensemble des solutions réelles :

1) $y'' - 2y' - 3y = 0$; 2) $y'' - 6y' + 9y = 0$; 3) $y'' + y' + y = 0$.

Exemple (L'équation $y'' + \omega^2 y = 0$: oscillateur harmonique non amorti)**.**

Soit, pour $\omega \in \mathbb{R}_+^*$ l'équation $y'' + \omega^2 y = 0$.

L'équation caractéristique est $x^2 + \omega^2 = 0$, qui a pour racines $i\omega$ et $-i\omega$ (partie réelle nulle : pas d'amortissement).

L'ensemble des solutions est $\boxed{S_0 = \{t \mapsto \alpha \cos(\omega t) + \beta \sin(\omega t) \mid \alpha, \beta \in \mathbb{R}\}}$

3 Équation générale : obtenir une solution particulière.

Il s'agit ici de trouver *une* solution de l'équation

$$y'' + ay' + by = f(x) \qquad (E)$$

3.1 Trouver une solution à vue.

Lorsque le second membre f est une fonction constante, l'équation a une solution constante (cas particulier courant en physique). Plus précisément, si $a, b, c \in \mathbb{K}$ avec $b \neq 0$,

$$\boxed{\text{L'équation } y'' + ay' + by = c \text{ a pour solution particulière la fonction constante } z_p : x \mapsto \tfrac{c}{b}.}$$

Plus généralement, lorsque b sera une fonction polynomiale de degré n, on pourra chercher une solution polynomiale de degré n.

3.2 Principe de superposition.

Comme pour les ED linéaires d'ordre 1, on a un principe de superposition lorsque le second membre se présente comme somme de deux fonctions.

Proposition 9 (Principe de superposition)**.**

Soient $a, b \in \mathbb{K}$. Si
- y_1 est solution sur $\mathbb{R}$ de $y'' + ay' + by = f_1(x) \quad (E_1)$,
- y_2 est solution sur $\mathbb{R}$ de $y'' + ay' + by = f_2(x) \quad (E_2)$,

alors $y_1 + y_2$ est solution sur I de l'équation $y'' + ay' + by = f_1(x) + f_2(x) \quad (E_3)$.

Preuve. Soient y_1 et y_2 deux solutions, respectivement de (E_1) et (E_2). Elles sont par définition deux fois dérivables sur $\mathbb{R}$. La fonction $y_1 + y_2$ l'est donc aussi. Pour $x \in \mathbb{R}$,

$$\begin{aligned}(y_1+y_2)''(x) + a(y_1+y_2)'(x) + b(y_1+y_2)(x) &= \Big(\underbrace{y_1'' + ay_1' + by_1}_{=f_1(x) \text{ car } y_1 \text{ sol. de } E_1} \Big) + \Big(\underbrace{y_2'' + ay_2' + by_2}_{=f_2(x) \text{ car } y_2 \text{ sol. de } E_2} \Big) \\ &= f_1(x) + f_2(x).\end{aligned}$$

Les deux « paquets », l'un dépendant de y_1, l'autre de y_2 ont pu être formés en tirant parti de la linéarité de l'équation.

□

3.3 Obtenir une solution pour des seconds membres particuliers.

En première année, on limite l'étude des équations non-homogènes à des exemples importants pour les applications : on considère dans ce qui suit des seconds membres de la forme

$$x \mapsto Ae^{\alpha x}, \text{ avec } (A, \alpha) \in \mathbb{C}^2 \quad \text{et} \quad t \mapsto A\cos(\omega t) \quad \text{ou} \quad t \mapsto A\sin(\omega t), \text{ avec } (A, \omega) \in \mathbb{R}^2.$$

Proposition 10.

Soient $a, b, A, \alpha \in \mathbb{K}$. L'équation

$$y'' + ay' + by = Ae^{\alpha x}$$

admet une solution particulière de la forme

- $x \mapsto Be^{\alpha x}$ si α n'est pas racine de l'équation caractéristique,
- $x \mapsto Bxe^{\alpha x}$ si α est une racine simple de l'équation caractéristique,
- $x \mapsto Bx^2e^{\alpha x}$ si α est racine double de l'équation caractéristique,

où B est une constante (de $\mathbb{K}$) à déterminer.

Preuve. On va chercher une solution particulière de la forme

$$y : x \mapsto z(x)e^{\alpha x},$$

où z est une fonction deux fois dérivable sur $\mathbb{R}$ à déterminer. Notons $u : x \mapsto e^{\alpha x}$. La fonction u est deux fois dérivable : on a $u' = \alpha u$ et $u'' = \alpha^2 u$. La fonction y est deux fois dérivable comme produit :

$$\begin{aligned} y &= zu, \\ y' &= zu' + z'u = (\alpha z + z')u, \\ y'' &= zu'' + z'u' + z'u' + z''u = (\alpha^2 z + 2\alpha z' + z'')u \end{aligned}$$

On a, u ne s'annulant pas,

$$\begin{aligned} y \text{ est solution de } (E_0) \quad &\iff \quad y'' + ay' + by = Au \\ &\iff \quad (\alpha^2 z + 2\alpha z' + z'')\cancel{u} + a(\alpha z + z')\cancel{u} + bz\cancel{u} = A\cancel{u} \\ &\iff \quad z'' + (2\alpha + a)z' + (\alpha^2 + a\alpha + b)z \underset{(*)}{=} A \end{aligned}$$

• Si α n'est pas racine de l'équation caractéristique, il suffit de prendre z constante égale à $B := A/(\alpha^2 + a\alpha + b)$ pour satisfaire $(*)$. Cela donne bien une solution particulière du type $y : x \mapsto z(x)e^{\alpha x} = Be^{\alpha x}$.
• Si α est racine simple de l'équation caractéristique, on a $\alpha^2 + a\alpha + b = 0$ et $2\alpha + a \neq 0$. Il faut donc choisir z telle que

$$z'' + (2\alpha + a)z' \underset{(*)}{=} A.$$

On prend z' constante égale à $B := A/(2\alpha + a)$ et pour cela on choisit $z : x \mapsto Bx$. Cela donne bien une solution particulière du type $y : x \mapsto z(x)e^{\alpha x} = Bxe^{\alpha x}$.
• Si α est racine double de l'équation caractéristique, on a $\alpha^2 + a\alpha + b = 0$ et $2\alpha + a = 0$. Il faut donc choisir z telle que

$$z'' \underset{(*)}{=} A,$$

ce que l'on fait en prenant $z : x \mapsto \frac{A}{2}x^2$. Cela donne bien une solution particulière du type $y : x \mapsto z(x)e^{\alpha x} = Bx^2e^{\alpha x}$ (en posant $B = A/2$). On remarque que si a, b, α et A sont des nombres réels, dans les trois cas, B est réel. □

Cas particulier important pour les applications : celui où le second membre est de la forme $t \mapsto A\cos(\omega t)$, ou $t \mapsto A\sin(\omega t)$. Physiquement, il s'agit de l'équation d'un oscillateur harmonique excité périodiquement. On va voir que l'on peut se ramener à une équation du type de celles de la proposition 10.

Méthode.

Soient $a, b, A \in \mathbb{R}$ et $\omega \in \mathbb{R}_+^*$. Soit (E) une équation du type

$$y'' + ay' + by = A\cos(\omega t) \quad \text{ou} \quad y'' + ay' + by = A\sin(\omega t).$$

Pour tout $t \in \mathbb{R}$,

$$\cos(\omega t) = \mathrm{Re}\left(e^{i\omega t}\right) \quad \text{et} \quad \sin(\omega t) = \mathrm{Im}\left(e^{i\omega t}\right).$$

On sait trouver une solution particulière de l'équation auxiliaire complexe

$$y'' + ay' + by = Ae^{i\omega t} \quad (E_{\mathbb{C}}).$$

Reste à sélectionner la partie réelle ou la partie imaginaire pour obtenir une solution de (E).

- Si $i\omega$ n'est pas racine de l'équation caractéristique, on obtiendra une solution particulière de $(E_{\mathbb{C}})$ de la forme $t \mapsto Be^{i\omega t}$ avec $B \in \mathbb{C}$. En sélectionnant la partie réelle/imaginaire, on obtient une solution du type
$$z : t \mapsto \alpha\cos(\omega t) + \beta\sin(\omega t), \qquad (\alpha, \beta) \in \mathbb{R}^2$$
- Si $i\omega$ est racine de l'équation caractéristique, alors son conjugué aussi et l'équation caractéristique est $(x + i\omega)(x - i\omega) = x^2 + \omega^2$. L'équation complexe associée à (E) est de la forme
$$y'' + \omega^2 y = Ae^{i\omega t}$$
C'est celle d'un oscillateur harmonique non amorti excité à sa pulsation propre. On obtiendra une solution particulière de $(E_{\mathbb{C}})$ de la forme $t \mapsto Bte^{i\omega t}$ avec $B \in \mathbb{C}$.
En sélectionnant la partie réelle/imaginaire, on obtient une solution du type
$$z : t \mapsto t\left(\alpha\cos(\omega t) + \beta\sin(\omega t)\right), \qquad (\alpha, \beta) \in \mathbb{R}^2$$
Le facteur t dans traduit que le système entre en *résonance* (vidéo). Voir l'exercice 8.4.

4 Synthèse.

Méthode (Conseils pour la résolution des EDL2 à coefficients constants)**.**

- Résoudre l'équation homogène (E_0) associée. Pour cela, commencer par poser l'équation caractéristique.
- Rechercher une solution particulière de (E) avec second membre. Le cours nous apprend à le faire lorsque ce dernier est de la forme $Ae^{\alpha x}$. Il va falloir discuter selon que α est racine ou pas de l'EC.
- Si le second membre est de la forme $A\cos(\omega t)$ ou $A\sin(\omega t)$, on se ramène à un second membre exponentiel en posant une équation auxiliaire complexe.
- Exprimer l'ensemble des solutions de (E) à l'aide de la solution particulière et des solutions de (E_0).
- Conditions initiales. La notion de problème de Cauchy n'a pas été définie pour des EDL2. On vérifiera dans la pratique que pour une équation (E) donnée, il existe une unique solution de (E) satisfaisant une condition initiale du type $(y(t_0) = y_0 \ \text{ et } \ y'(t_0) = v_0)$.

Exercices

12.1 Résoudre :

$$\begin{cases} y'' + 2y' + 10y = 5 \\ y(0) = 1 \quad y'(0) = 0 \end{cases}$$

12.2 Résoudre :

$$y'' - y' - 2y = 2\mathrm{ch}(x).$$

12.3 Résoudre :

$$y'' + 2y' + y = \cos(2t) \quad (E).$$

12.4 Résonance... ou pas

1. Excitation à une pulsation quelconque. Résoudre

$$y'' + 4y = \cos t.$$

2. Excitation à la pulsation propre : résonance. Résoudre

$$y'' + 4y = \cos(2t).$$

12.5 Soit $\alpha \in \mathbb{R}$. Résoudre l'équation différentielle

$$2y'' + \alpha y' + \alpha y = 0.$$

On discutera la réponse en fonction du paramètre α, bien entendu.

12.6 Soit $a \in \mathbb{R}$. En discutant selon la valeur de a, résoudre

$$y'' - 2ay' + (1 + a^2)y = \sin x.$$

12.7 On considère l'équation différentielle à coefficients *non constants* ci-dessous :

$$(E) \qquad t^2 y'' + 4ty' + (2 + t^2)y = 1 \quad \text{sur } \mathbb{R}_+^*.$$

Soient y une fonction définie sur $\mathbb{R}_+^*$ et $z : t \mapsto t^2 y(t)$.

1. Justifier que y est deux fois dérivable sur $\mathbb{R}_+^*$ si et seulement si z est deux fois dérivable sur $\mathbb{R}_+^*$.
2. Démontrer que y est solution de l'équation si et seulement si z est solution d'une équation différentielle très simple que l'on précisera.
3. Donner l'ensemble des solutions de (E).

12.8 Trouver toutes les fonctions f dérivables sur $\mathbb{R}$ et telles que

$$\forall x \in \mathbb{R} \quad f'(x) = f(\pi - x).$$

---

13 Suites : la pratique

Ce chapitre sera complété par le cours **Suites : la théorie**, dans lequel sera donnée une définition rigoureuse de la notion de suite convergente, ainsi que des preuves pour les théorème énoncés ici. On souhaite d'abord focaliser sur les méthodes et les exemples, et notamment sur les deux outils fondamentaux que sont le théorème d'encadrement (des « gendarmes »), et le théorème de convergence monotone.

0 Qu'est-ce qu'une suite ?

Définition 1.

On appelle **suite numérique** une application de $\mathbb{N}$ dans $\mathbb{K}$.
Une suite réelle est une fonction de $\mathbb{N}$ dans $\mathbb{R}$. Ainsi, $\mathbb{R}^{\mathbb{N}}$ est l'ensemble des suites réelles.

Une suite numérique est donc une suite de *nombres*. On s'intéressera un jour à des suites de matrices, des suites de fonctions...

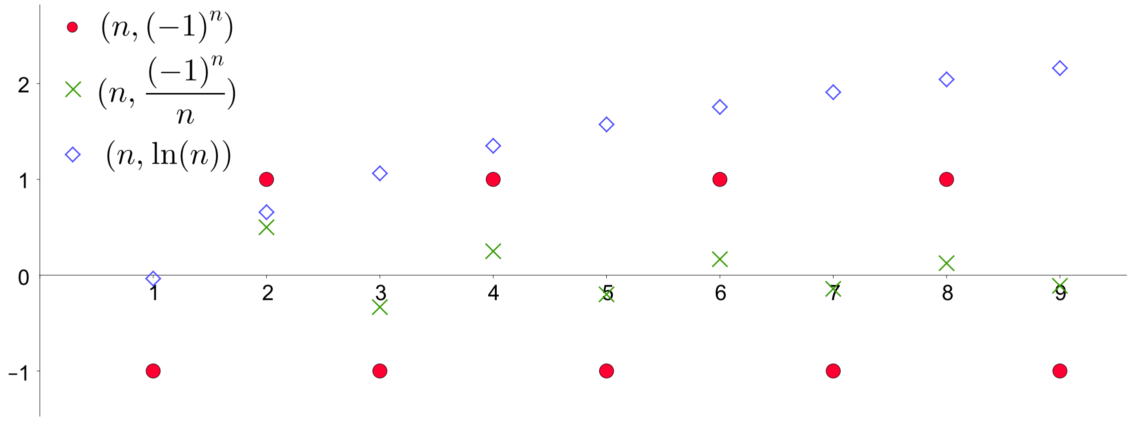
Notation.

Soit une suite $u : \mathbb{N} \to \mathbb{K}$. Pour tout $n \in \mathbb{N}$, le nombre $u(n)$ est noté u_n et appelé **terme général** de la suite, ou terme de rang n. La suite u est notée $(u_n)_{n\geq 0}$, $(u_n)_{n\in\mathbb{N}}$ ou plus simplement (u_n).

Remarque. On peut considérer des suites définies seulement sur une partie de $\mathbb{N}$ de la forme $[n_0, +\infty[\cap\mathbb{N}$ dans $\mathbb{K}$, où $n_0 \in \mathbb{N}$. On notera alors $(u_n)_{n\geq n_0}$ une telle suite.

On pourra voir la variable n comme une variable de temps (discret), où u_n donne l'état du système observé au temps n. Pour une suite réelle, on peut représenter cette évolution en donnant le graphe de l'application u :

$$\{(n, u_n), n \in \mathbb{N}\}.$$



Trois graphes de suites

1 Calculs de limites.

1.1 Limites usuelles.

Proposition 2 (Limite d'une puissance de n)**.**

Soit $\alpha \in \mathbb{R}$. La suite $(n^\alpha)_{n\in\mathbb{N}^*}$ a une limite, qui vaut

$$\lim n^\alpha = \begin{cases} +\infty & \text{si } \alpha > 0 \\ 1 & \text{si } \alpha = 0 \\ 0 & \text{si } \alpha < 0. \end{cases}$$

Proposition 3 (Limite d'une suite géométrique)**.**

Soit $q \in \mathbb{R}$. On a

$$\lim_{n\to+\infty} q^n = \begin{cases} +\infty & \text{si } q > 1 \\ 1 & \text{si } q = 1 \\ 0 & \text{si } q \in]-1, 1[\\ \text{n'existe pas} & \text{si } q \leq -1. \end{cases}$$

Proposition 4 (Croissances comparées)**.**

Soit $a \in \mathbb{R}_+^*$, $p > 1$ et $q \in]-1, 1[$. On a les limites suivantes.

$$\lim_{n\to+\infty} \frac{n^a}{p^n} = 0, \quad \text{et} \quad \lim_{n\to+\infty} n^a q^n = 0.$$

Une suite géométrique l'emporte toujours sur une puissance de n

1.2 Opérations algébriques et limites.

Pour énoncer les propositions suivantes, on se donne (u_n) et (v_n) des suites réelles admettant une limite, finie ou infinie, ainsi que deux réels ℓ et ℓ'. Les tableaux donnent les limites de suites construites par opérations sur (u_n) et (v_n). La mention F.I. (« forme indéterminée ») signale que l'on ne peut rien dire en général.

Proposition 5 (Limite d'une somme).

Si (u_n) (v_n) sont deux suites convergentes, alors $(u_n + v_n)$ l'est aussi et la limite de la somme est la somme des limites.
Ce résultat correspond à la première colonne du tableau ci-dessous, où ℓ et ℓ' sont des réels.

$\lim u_n$	ℓ	$+\infty$	$-\infty$	$+\infty$
$\lim v_n$	ℓ'	ℓ' ou $+\infty$	ℓ' ou $-\infty$	$-\infty$
$\lim(u_n + v_n)$	$\ell + \ell'$	$+\infty$	$-\infty$	F.I.

Proposition 6 (Limite d'un produit).

$\lim u_n$	ℓ	$+\infty$	$+\infty$	$+\infty$	$-\infty$	$-\infty$	$-\infty$
$\lim v_n$	ℓ'	$\ell'>0$ ou $+\infty$	$\ell'<0$ ou $-\infty$	0	$\ell'>0$ ou $+\infty$	$\ell'<0$ ou $-\infty$	0
$\lim u_n v_n$	$\ell\ell'$	$+\infty$	$-\infty$	F.I.	$-\infty$	$+\infty$	F.I.

En prenant (v_n) constante égale à λ, on en déduit ce qu'il faut sur les limites et la multiplication par un scalaire. Par exemple, si (u_n) tend vers $\ell \in \mathbb{R}$, $\lambda u_n \to \lambda\ell$; si $u_n \to +\infty$ et $\lambda < 0$, $\lambda u_n \to -\infty$, etc...

On rappelle la notation courante ci-dessous : on écrit

- $u_n \to 0_+$ lorsque (u_n) tend vers 0 en restant strictement positive à.p.d.c.r.
- $u_n \to 0_-$ lorsque (u_n) tend vers 0 en restant strictement négative à.p.d.c.r.

Proposition 7 (Limite et inverse).

Dans tous les cas ci-dessous, la suite (u_n) ne s'annule pas à partir d'un certain rang.

$\lim u_n$	$\ell \in \mathbb{R}^*$	0_+	0_-	$+\infty$	$-\infty$
$\lim \frac{1}{u_n}$	$\frac{1}{\ell}$	$+\infty$	$-\infty$	0_+	0_-

Un quotient $\dfrac{u_n}{v_n}$ s'écrit $u_n \cdot \dfrac{1}{v_n}$. En combinant les propositions 6 et 7, on obtient

Proposition 8 (Limite et quotient).

On suppose si besoin que (v_n) ne s'annule pas à partir d'un certain rang.

$\lim u_n$	ℓ	ℓ	ℓ	ℓ	0	$+\infty$	$+\infty$	$\pm\infty$
$\lim v_n$	$\ell' \in \mathbb{R}^*$	$\pm\infty$	0_+	0_-	0	$\ell > 0$ ou 0_+	$\ell < 0$ ou 0_-	$\pm\infty$
$\lim \frac{u_n}{v_n}$	$\frac{\ell}{\ell'}$	0	$+\infty$	$-\infty$	F.I.	$+\infty$	$-\infty$	F.I.

2 Existence d'une limite : deux outils fondamentaux.

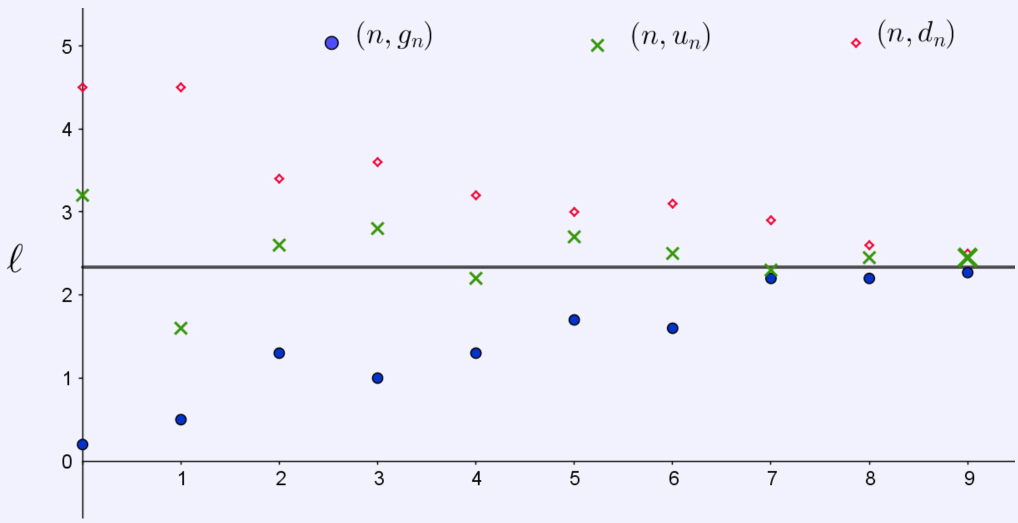
Dans cette partie, on énonce et on illustre les deux outils principaux qui pourront être mobilisés dans la pratique pour prouver qu'une suite converge : le théorème d'encadrement, et le théorème de la limite monotone. Ces résultats reposent sur des inégalités : toutes les suites ici seront **réelles**.

2.1 L'encadrement.

Théorème 9 (d'encadrement, ou des gendarmes)**.**

Soient trois suites réelles (g_n), (u_n), (d_n) telles que $\forall n \in \mathbb{N} \quad g_n \leq u_n \leq d_n$.
Si de surcroît, (g_n) et (d_n) convergent vers la même limite $\ell \in \mathbb{R}$, alors

$$(u_n) \text{ est convergente} \quad \text{et} \quad \lim u_n = \ell.$$



Exemple 10 (utiliser le théorème d'encadrement)**.**

Montrer que la suite de terme général $\dfrac{\lfloor \sqrt{n} - 1 \rfloor}{\lfloor \sqrt{n} + 1 \rfloor}$ converge et préciser sa limite.

Méthode (Majorer la distance par une suite qui tend vers 0)**.**

Pour montrer qu'une suite (u_n) tend vers un réel ℓ, il suffit d'obtenir une majoration du type

$$|u_n - \ell| \leq v_n$$

où (v_n) est une suite qui tend vers 0.

En particulier, pour montrer qu'une suite tend vers 0, il suffit de majorer sa valeur absolue par une suite qui tend vers 0.

Méthode (Encadrer une somme, une intégrale).

Pour encadrer une somme,
- on propose un encadrement pour chaque terme,
- puis on somme les inégalités.

Parfois intéressant : majorer/minorer chaque terme par le plus grand/petit d'entre eux.

Pour encadrer une intégrale,
- on propose un encadrement pour la fonction intégrée,
- puis intègre l'inégalité (croissance de l'intégrale : bornes bien rangées parmi les hypothèses).

L'inégalité triangulaire est un outil pour majorer la valeur absolue d'une somme ou d'une intégrale.

Exemple 11 (Montrer qu'une suite tend vers 0 en écrasant sa valeur absolue).

Démontrer que les suites de terme général ci-dessous tendent vers 0 :

$$u_n = \frac{n\sin(n)}{n+2^n}; \qquad v_n = \sum_{k=n+1}^{2n} \frac{(-1)^k}{k^2}; \qquad w_n = \int_0^1 x^n \sin(nx)\arctan(n^x)\mathrm{d}x$$

Exemple 12 (utiliser le théorème d'encadrement avec des sommes).

Convergence et limite des suites u et v de terme général

$$u_n = n\sum_{k=n+1}^{2n} \frac{1}{n^2+k} \quad \text{et} \quad v_n = \frac{1}{n^2}\sum_{k=1}^{n} \lfloor k\pi \rfloor.$$

Proposition 13 (de minoration, de majoration).

Soient (u_n) et (v_n) deux suites réelles.
- Si $\forall n \in \mathbb{N}\ u_n \leq v_n$ et $u_n \to +\infty$, alors $v_n \to +\infty$.
- Si $\forall n \in \mathbb{N}\ u_n \leq v_n$ et $v_n \to -\infty$, alors $u_n \to -\infty$.

Exemple 14.

Pour $n \in \mathbb{N}^*$, on pose $u_n = \displaystyle\sum_{k=n+1}^{2n} \frac{1}{\sqrt{k}}$. Démontrer que $u_n \to +\infty$.

Exemple 15 (La série harmonique).

Pour $n \in \mathbb{N}^*$, on note $H_n = \displaystyle\sum_{k=1}^{n} \frac{1}{k}$.

1. Pour $k \in \mathbb{N}^*$, justifier que $\ln\left(1+\frac{1}{k}\right) \leq \frac{1}{k}$.
2. Démontrer que $H_n \to +\infty$.

2.2 La monotonie.

Définition 16.

Une suite réelle $(u_n)_{n\geq 0}$ est dite

croissante si $\forall n \in \mathbb{N},\ u_{n+1} \geq u_n$, **décroissante** si $\forall n \in \mathbb{N},\ u_{n+1} \leq u_n$,

monotone si elle est croissante ou décroissante.

Méthode.

Soit un entier n. Pour comparer deux termes consécutifs u_n et u_{n+1} d'une suite u, on pourra

- Examiner le signe de $u_{n+1} - u_n$. C'est bête à dire mais

$$u_{n+1} \geq u_n \iff u_{n+1} - u_n \geq 0.$$

- Dans le cas où la suite est strictement positive, comparer le quotient $\frac{u_{n+1}}{u_n}$ à 1, puisqu'alors

$$u_{n+1} \geq u_n \iff \frac{u_{n+1}}{u_n} \geq 1.$$

Définition 17.

Une suite réelle $(u_n)_{n\geq 0}$ est

majorée si $\exists M \in \mathbb{R}\ \forall n \in \mathbb{N}\ u_n \leq M.$, **minorée** si $\exists m \in \mathbb{R}\ \forall n \in \mathbb{N}\ u_n \geq m$,

bornée si elle est majorée et minorée.

Remarque au cas où... Une suite majorée, c'est une suite dont les termes sont majorés par une constante.

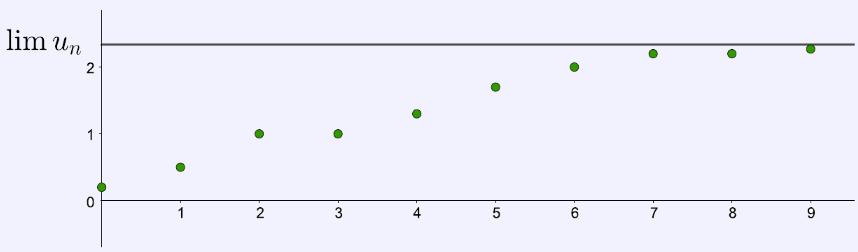
Proposition 18 (Caractérisation des suites bornées)**.**

Une suite réelle (u_n) est bornée si et seulement si la suite $(|u_n|)$ est majorée.

Remarque. On dira d'une suite complexe qu'elle est bornée si elle majorée en module.

Théorème 19 (de convergence monotone)**.**

Toute suite croissante et majorée converge vers une limite finie.
Toute suite croissante et non majorée diverge vers $+\infty$.



Corollaire 20.

Toute suite décroissante et minorée converge vers une limite finie.
En particulier, toute suite positive est convergente.
Toute suite décroissante et non minorée diverge vers $-\infty$.

Exemple 21.

Établir la convergence des suites u et v définies pour tout n par $u_n = \sum_{k=0}^{n} \frac{1}{k!}$ et $v_n = 2^{-2n}\binom{2n}{n}$.

Définition 22.

On dit que deux suites (u_n) et (v_n) sont **adjacentes** lorsque

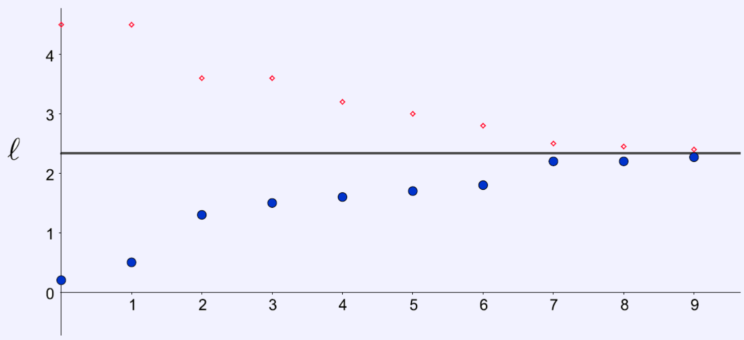
- (u_n) et (v_n) sont monotones de monotonie opposée,
- $v_n - u_n \to 0$.

Théorème 23 (Convergence des suites adjacentes)**.**

Deux suites adjacentes convergent vers une même limite finie.

Plus précisément, si (u_n) et (v_n) sont deux suites adjacentes (u croissante et v décroissante), alors elles convergent vers une même limite finie $\ell \in \mathbb{R}$. De plus,

$$\forall n \in \mathbb{N} \quad u_n \leq \ell \leq v_n.$$



Exemple 24.

oient les suites réelles $(u_n)_{n\geq 1}$ et $(v_n)_{n\geq 1}$ définies par

$$\forall n \geq 1 \quad u_n = \sum_{k=0}^{n} \frac{1}{k!} \quad \text{et} \quad v_n = \sum_{k=0}^{n} \frac{1}{k!} + \frac{1}{nn!}$$

1. Démontrer que (u_n) et (v_n) convergent vers une même limite finie.
2. On admet que $e = \lim u_n$. Démontrer que $e \notin \mathbb{Q}$.

3 Suites particulières.

Dans ce qui suit, les suites considérées sont à valeurs réelles ou complexes.

3.1 Suites stationnaires

Définition 25.

Une suite (u_n) est dite **stationnaire** si elle est constante *à partir d'un certain rang*, c'est-à-dire qu'il existe $n_0 \in \mathbb{N}$ tel que $\forall n \geq n_0,\ u_n = u_{n_0}$.

Exemple 26.

Soit p un entier naturel.
Pour $n \geq 0$, on pose $u_n = \cos\left(\frac{2\pi n!}{p!}\right)$. Justifier que la suite $(u_n)_{n\geq 0}$ est stationnaire.

Exemple 27.

Montrer que l'ensemble des suites stationnaires est stable par combinaisons linéaires.

3.2 Suites arithmético-géométriques.

Définition 28.

Soit $r \in \mathbb{K}$ et $n_0 \in \mathbb{N}$. On dit qu'une suite $(u_n)_{n\geq n_0}$ est **arithmétique** de raison r si

$$\forall n \geq n_0 \quad u_{n+1} = u_n + r.$$

Proposition 29.

Le terme général d'une suite $(u_n)_{n\geq n_0}$ arithmétique de raison $r \in \mathbb{K}$ est donné par

$$\forall n \geq n_0 \quad u_n = u_{n_0} + (n - n_0)r.$$

Définition 30.

Soit $q \in \mathbb{K}$ et $n_0 \in \mathbb{N}$. On dit qu'une suite $(u_n)_{n\geq n_0}$ est **géométrique de raison** q si

$$\forall n \geq n_0 \quad u_{n+1} = q \cdot u_n.$$

Proposition 31.

Le terme général d'une suite $(u_n)_{n\geq n_0}$ géométrique de raison $q \in \mathbb{K}$ est donné par

$$\forall n \geq n_0 \quad u_n = q^{n-n_0} u_{n_0}.$$

Définition 32.

On dit qu'une suite $(u_n)_{n\geq n_0}$ est **arithmético-géométrique** s'il existe a et b dans $\mathbb{K}$ tels que

$$\forall n \geq n_0 \quad u_{n+1} = au_n + b \quad (*)$$

Fixons a et b dans $\mathbb{K}$. La suite constante égale à $\alpha \in \mathbb{K}$ satisfait $(*)$ si et seulement si $\alpha = a\alpha + b$. On peut alors dire que α est un *point fixe* pour la fonction $x \mapsto ax + b$.

Méthode (Calcul du terme général d'une suite satisfaisant $(*)$, avec $a \neq 1$)**.**

On pose l'équation au point fixe

$$ax + b = x.$$

Notons α l'unique solution de cette solution. Alors, pour tout n, $\begin{cases} u_{n+1} & = & au_n + b \\ \alpha & = & a\alpha + b \end{cases}$

En faisant la différence de ces deux lignes, on obtient, pour tout n,

$$u_{n+1} - \alpha = a(u_n - \alpha),$$

Notons $v_n := u_n - \alpha$. Ceci définit une suite auxiliaire (v_n) dont on vient de montrer qu'elle est géométrique. On sait donc exprimer le terme général de (v_n), puis de (u_n).

Exemple 33.

Calculer le terme général à l'ordre n de la suite définie par

$$\begin{cases} u_0 = 5 \\ \forall n \in \mathbb{N} \quad u_{n+1} = 3u_n - 4. \end{cases}$$

3.3 Suites récurrentes linéaires d'ordre 2.

Définition 34.

On dit qu'une suite (u_n) est **récurrente linéaire d'ordre** 2 s'il existe $a, b \in \mathbb{K}$ avec $b \neq 0$ tels que

$$\forall n \in \mathbb{N} \quad u_{n+2} = au_{n+1} + bu_n. \quad (**)$$

On cherche une suite particulière qui satisfait $(**)$. Soit $r \in \mathbb{C}$ et (u_n) la suite de terme général $u_n = r^n$.

$$\begin{aligned} (u_n) \text{ satisfait } (**) \quad & \iff \quad \forall n \in \mathbb{N} \quad u_{n+2} = au_{n+1} + bu_n \\ & \iff \quad \forall n \in \mathbb{N} \quad r^{n+2} = ar^{n+1} + br^n \\ & \iff \quad \forall n \in \mathbb{N} \quad r^n\left(r^2 - ar - b\right) = 0. \\ & \iff \quad r^2 - ar - b = 0 \end{aligned}$$

(on a pris $n = 0$ pour obtenir la dernière implication directe.)

Définition 35.

Soit (u_n) une suite récurrente linéaire d'ordre 2 définie d'après la relation $(**)$ ci-dessus.
On appelle **équation caractéristique** associée l'équation du second ordre.

$$x^2 - ax - b = 0.$$

Proposition 36 (Terme général dans le cas complexe)**.**

Soit (u_n) une suite *complexe* récurrente linéaire d'ordre 2 définie d'après la relation $(**)$ (déf. 34), où a et b sont complexes, avec $b \neq 0$.

- Si l'équation caractéristique a deux solutions distinctes r_1 et r_2, alors il existe un unique couple $(\lambda, \mu) \in \mathbb{C}^2$ tels que
$$\forall n \in \mathbb{N} \quad u_n = \lambda r_1^n + \mu r_2^n.$$
- Si l'équation caractéristique a une unique solution r, alors il existe un unique couple $(\lambda, \mu) \in \mathbb{C}^2$ tels que
$$\forall n \in \mathbb{N} \quad u_n = \lambda n r^n + \mu r^n.$$

Ceci sera prouvé au second semestre, dans le cours d'algèbre linéaire.

Proposition 37 (Terme général dans le cas réel)**.**

Soit (u_n) une suite *réelle* récurrente linéaire d'ordre 2 définie d'après la relation $(**)$ (déf. 34), où a et b sont réels, avec $b \neq 0$.

- Si l'équation caractéristique a deux solutions réelles distinctes r_1 et r_2, alors il existe un unique couple $(\lambda, \mu) \in \mathbb{R}^2$ tels que
$$\forall n \in \mathbb{N} \quad u_n = \lambda r_1^n + \mu r_2^n.$$
- Si l'équation caractéristique a une unique solution r, alors il existe un unique couple $(\lambda, \mu) \in \mathbb{R}^2$ tels que
$$\forall n \in \mathbb{N} \quad u_n = \lambda n r^n + \mu r^n.$$
- Si l'équation caractéristique n'a pas de solutions dans $\mathbb{R}$, alors elle a deux solutions complexes conjuguées distinctes de la forme $\rho e^{i\theta}$ et $\rho e^{-i\theta}$. Il existe un unique couple $(\lambda, \mu) \in \mathbb{R}^2$ tel que
$$\forall n \in \mathbb{N} \quad u_n = \rho^n \left(\lambda \cos(n\theta) + \mu \sin(n\theta)\right).$$

Exemple 38 (La suite de Fibonacci)**.**

Soit (F_n), définie par récurrence par $\left\{ \begin{array}{l} F_0 = 0, \quad F_1 = 1 \\ \forall n \geq 0 \quad F_{n+2} = F_{n+1} + F_n. \end{array} \right.$.

1. Calculer son terme général.
2. Démontrer que pour tout $n \in \mathbb{N}$, $F_n \in \mathbb{N}$.

4 Modes de définition.

Dans les exemples étudiés jusqu'ici, on disposait d'une expression **explicite** du terme général d'une suite. On peut établir une éventuelle convergence en se ramenant à des limites usuelles (partie 1 de ce cours) ou en s'appuyant sur l'un des deux outils fondamentaux rappelés en partie 2 : l'encadrement, ou l'exploitation de la monotonie. Mentionnons que le calcul de limite sera renforcé au second semestre avec l'étude des développements limités.

On peut aussi définir une suite de manière **implicite** : pour tout entier n, le nombre u_n est défini comme solution d'une équation du type « $F(u_n, n) = 0$ ». On donne un exemple dans le paragraphe à suivre.

Une autre façon classique pour définir une suite est d'utiliser une **relation de récurrence**. Les termes de la suites étant supposés bien définis jusqu'à un certain rang n, le terme suivant u_{n+1} est défini comme une fonction de n et des termes précédents :

$$u_{n+1} = f(n, u_0, u_2, \dots, u_n).$$

On se concentrera dans le second paragraphe de cette partie sur les relations du type « $u_{n+1} = f(u_n)$ ».

4.1 Définition implicite.

Exemple 39.

1. Pour $n \in \mathbb{N}^*$, montrer que l'équation $x^n \ln(x) = 1$ possède une unique solution x_n. Ceci définit une suite $(x_n)_{n\in\mathbb{N}^*}$.
2. Montrer que pour tout $n \in \mathbb{N}^*$, $x_n > 1$.
3. Étudier la monotonie de la suite et la convergence de cette suite.

4.2 Définition par une relation de type « $u_{n+1} = f(u_n)$ ».

Exemple 40.

Le système $\begin{cases} u_0 = e^2 \\ \forall n \in \mathbb{N}\ u_{n+1} = \ln(u_n) \end{cases}$ ne définit **pas** une suite réelle. Pourquoi ?

Pour qu'une suite u soit bien définie par une relation $u_{n+1} = f(u_n)$, il faut que les termes de la suite *restent* dans l'intervalle de définition de f. On donne dans ce qui suit une condition suffisante sur f pour que cela arrive.

Proposition 41.

Soit une fonction f définie sur une partie X de $\mathbb{R}$. On dit que X est **stable** par f si $f(X) \subset X$, c'est-à-dire que pour tout $x \in X$, on a $f(x) \in X$. Dans ces conditions, une contrainte du type

$$\begin{cases} u_0 = a \in X \\ \forall n \in \mathbb{N} \quad u_{n+1} = f(u_n). \end{cases}$$

définit correctement une unique suite $(u_n)_{n\in\mathbb{N}}$.

Méthode (Monotonie des suites définies à partir de $u_{n+1} = f(u_n)$: utilisation de $x \mapsto f(x) - x$).

Pour tout $n \in \mathbb{N}$, $u_{n+1} - u_n = f(u_n) - u_n$. L'étude du signe de $x \mapsto f(x) - x$ permet de déterminer la monotonie de f.

1. Si $x \mapsto f(x) - x$ est *positive* sur une partie $X' \subset X$ stable par f et que $u_0 \in X'$, alors $\forall n \in \mathbb{N}\ u_n \in X'$ et $\forall n \in \mathbb{N}\ u_{n+1} - u_n \geq 0$: (u_n) est *croissante.*
2. Si $x \mapsto f(x) - x$ est *négative* sur un intervalle $J \subset I$ stable par f, et que $u_0 \in J$, alors $\forall n \in \mathbb{N}\ u_n \in X'$ et $\forall n \in \mathbb{N}\ u_{n+1} - u_n \leq 0$: (u_n) est *décroissante.*

Méthode (Monotonie des suites définies à partir de $u_{n+1} = f(u_n)$: cas où f est croissante).

Si f est croissante, sur I, alors (u_n) est **monotone**. Plus précisément, il est clair que les propriétés « $u_n \leq u_{n+1}$ », ainsi que « $u_n \geq u_{n+1}$ » sont héréditaires. Ainsi,

- Si $u_0 \leq u_1$, on peut montrer par récurrence que (u_n) est croissante.
- Si $u_0 \geq u_1$, on peut montrer par récurrence que (u_n) est décroissante.

Méthode (Oscillations dans le cas où f est décroissante).

Si f est décroissante sur I alors les suites extraites (u_{2n}) et (u_{2n+1}) sont monotones, de monotonie contraire. En effet,

$$\forall n \in \mathbb{N} \quad u_{2n+2} = f \circ f(u_{2n}) \quad \text{et} \quad u_{2n+3} = f \circ f(u_{2n+1}),$$

où $f \circ f$ est une fonction *croissante*. Par décroissance de f, si $u_0 \leq u_1$, alors $u_1 \geq u_2$ et inversement.

Proposition 42.

Soit $f : X \to X$ et u une suite satisfaisant $\forall n \in \mathbb{N}\ u_{n+1} = f(u_n)$.

Si (u_n) converge vers une limite ℓ, que $\ell \in X$ et que f est continue en ℓ, alors ℓ est un *point fixe* de f, c'est à dire que $\boxed{f(\ell) = \ell}$

Exemple 43.

Étude de la suite (u_n) définie par $\begin{cases} u_0 \in [-2, +\infty[\\ \forall n \in \mathbb{N} \quad u_{n+1} = \sqrt{2 + u_n}. \end{cases}$

Exemple 44.

Étude de la suite (u_n) définie par $\begin{cases} u_0 \leq 2 \\ \forall n \in \mathbb{N} \quad u_{n+1} = \sqrt{2 - u_n}. \end{cases}$

Exercices

Avant de parler de convergence.

$\boxed{\textbf{13.1}}$ **[♦◇◇]** Une suite croissante est une fonction croissante sur $\mathbb{N}$.
Démontrer que le titre de l'exercice dit vrai, c'est-à-dire, pour une suite réelle $(u_n)_{n\in\mathbb{N}}$ l'équivalence entre

1. $\forall n \in \mathbb{N} \quad u_{n+1} \geq u_n$.
2. $\forall (n,p) \in \mathbb{N}^2 \quad n \leq p \implies u_n \leq u_p$.

$\boxed{\textbf{13.2}}$ **[♦♦◇]** Soit a un réel supérieur à 1 et $(u_n)_{n\geq 0}$ la suite définie par $\forall n \in \mathbb{N} \quad u_n = \frac{a^n}{n!}$.
Démontrer que l'ensemble des termes de la suite possède un maximum, qu'on exprimera en fonction de a.

$\boxed{\textbf{13.3}}$ **[♦◇◇]** Pour $n \in \mathbb{N}$, on pose

$$u_n = \sum_{k=n+1}^{2n} \frac{k \sin k}{k^2+1}$$

Prouver que la suite (u_n) est bornée.

$\boxed{\textbf{13.4}}$ **[♦◇◇]** Soit $\alpha \in]0,1[$ et (u_n) la suite définie par $\begin{cases} u_0 = \alpha(1-\alpha) \\ \forall n \geq 0 \quad u_{n+1} = (1-\alpha)u_n + \alpha(1-\alpha) \end{cases}$

1. Exprimer le terme général de la suite en fonction de α et n.
2. Donner $\lim u_n$.

$\boxed{\textbf{13.5}}$ **[♦♦◇]** Soit θ un réel.

1. Donner la forme du terme général d'une suite $(u_n)_{n\in\mathbb{N}}$ de $\mathbb{R}^{\mathbb{N}}$ telle que
$$\forall n \in \mathbb{N} \quad u_{n+2} - 2\cos(\theta)u_{n+1} + u_n = 0.$$
2. Supposons dans cette question que $\theta \notin \pi\mathbb{Z}$. Donner sous forme factorisée le terme général de l'unique suite (u_n) satisfaisant la relation ci-dessus et telle que $u_0 = u_1 = 1$.

$\boxed{\textbf{13.6}}$ **[♦♦◇]** Soit (u_n), définie par récurrence par $\begin{cases} u_0 = 1 \\ \forall n \geq 0 \quad u_{n+1} = 3u_n + 2^n \quad (*). \end{cases}$.

1. Prouver qu'il existe une suite (a_n) géométrique de raison 2 qui satisfait la relation de récurrence $(*)$.
2. Donner le terme général de (u_n).

$\boxed{\textbf{13.7}}$ **[♦♦◇]** Soit la suite (u_n), définie par $\begin{cases} u_0 > 0; u_1 > 0 \\ \forall n \geq 0 \quad u_{n+2} = \sqrt{u_{n+1}u_n} \end{cases}$. Exprimer le terme général de (u_n) et montrer qu'elle converge vers une limite que l'on exprimera en fonction de u_0 et de u_1.

Encadrement.

$\boxed{\textbf{13.8}}$ **[♦◇◇]** Soit $a > 1$. Pour $n \geq 1$, on définit $u_n = (\lfloor a^n \rfloor)^{1/n}$.
Montrer que (u_n) est convergente et donner sa limite.

$\boxed{\textbf{13.9}}$ **[♦♦◇]** Pour tout $n \in \mathbb{N}^*$, on note $u_n = \displaystyle\prod_{k=1}^{n}\left(1 + \frac{k}{n^2}\right)$.

1. Montrer que pour tout $x > 0$, $x - \frac{x^2}{2} \leq \ln(1+x) \leq x$.
2. Montrer que u converge et déterminer sa limite.

$\boxed{\textbf{13.10}}$ **[♦♦♦]** Étudier la convergence de la suite de terme général $\dfrac{1! + 2! + \ldots + n!}{n!}$.

Monotonie.

$\boxed{\textbf{13.11}}$ **[♦◇◇]** Pour $n \in \mathbb{N}$, on pose $I_n = \displaystyle\int_0^{\frac{\pi}{4}} (\arctan(x))^n \, dx$. Justifier que (I_n) est une suite convergente.

$\boxed{\textbf{13.12}}$ **[♦◇◇]** Soit α un réel de $]0,1[$. Pour tout $n \in \mathbb{N}^*$, on pose $u_n = \displaystyle\prod_{k=1}^{n} (1+\alpha^k)$.

1. Justifier brièvement que $\forall x \in \mathbb{R} \quad 1 + x \leq e^x$.
2. Démontrer que (u_n) est une suite convergente, et que $\lim u_n \leq \exp(\frac{\alpha}{1-\alpha})$.

$\boxed{\textbf{13.13}}$ **[♦◇◇]** Soient (u_n) et (v_n) deux suites définies par

$$\forall n \in \mathbb{N}^* \qquad u_n = \sum_{k=n+1}^{2n} \frac{1}{k} \quad \text{et} \quad v_n = u_n + \frac{1}{n}.$$

Démontrer que (u_n) et (v_n) convergent vers une même limite.

$\boxed{\textbf{13.14}}$ **[♦♦◇]** Soient (u_n) et (v_n) deux suites définies par $u_0 > v_0 > 0$ et

$$u_{n+1} = \frac{u_n + v_n}{2}; \quad v_{n+1} = \frac{2u_n v_n}{u_n + v_n}.$$

Montrer que ces deux suites convergent vers une limite commune. En examinant la suite $(u_n v_n)$, exprimer cette limite en fonction de u_0 et v_0.

$\boxed{\textbf{13.15}}$ **[♦♦◇]** Pour $n \in \mathbb{N}^*$

$$u_n = \sum_{k=1}^{n} \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \quad \text{et} \quad v_n = \sum_{k=1}^{n} \frac{1}{k^2} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2}.$$

1. Pour chacune des deux suites u et v, faire un pronostic : convergente ou divergente ?
2. Justifier que pour tout entier k supérieur à 2, on a $\frac{1}{k^2} \leq \frac{1}{k(k-1)} = \frac{1}{k-1} - \frac{1}{k}$.
   En déduire que la suite (v_n) est majorée puis qu'elle converge vers une limite finie.
3. (a) Montrer que pour tout $n \in \mathbb{N}^*$, $u_{2n} - u_n \geq 1/2$.
   (b) Démontrer par l'absurde que (u_n) tend vers $+\infty$.

$\boxed{\textbf{13.16}}$ **[♦♦♦]** Soit la suite (u_n) définie par

$$\forall n \in \mathbb{N} \quad u_n = \sqrt{a_1 + \sqrt{a_2 + \cdots + \sqrt{a_n}}}.$$

où a_n est la $n$ème décimale de π. Étudier la convergence de (u_n).

Modes de définition particulier d'une suite

$\boxed{\textbf{13.17}}$ **[♦♦◇]** Étudier la suite u définie par $\begin{cases} u_0 \in \mathbb{R} \\ \forall n \in \mathbb{N} \quad u_{n+1} = \frac{1}{3}(4 - u_n^2). \end{cases}$

$\boxed{\textbf{13.18}}$ **[♦♦♦]**
Prouver que pour tout $n \in \mathbb{N}^*$, il existe un unique $x_n > 0$ tel que $x_n^n + x_n = 3$. Prouver que (x_n) converge et déterminer sa limite.

Applications

2/2 : Images et antécédents

Les lettres E et F désigneront des ensembles.

1 Images par une application.

1.1 Image directe.

Définition 1.

Soit $f : E \to F$ une application et A une partie de E.
On appelle **image** (directe) de A par f, et on note $f(A)$ la partie de F ci-dessous

$$f(A) = \{f(x) \mid x \in A\} = \{y \in F \mid \exists x \in A \ y = f(x)\}.$$

Lorsque c'est l'image de E tout entier que l'on considère, on peut noter

$$\mathrm{Im}(f) = f(E).$$

Exemple 2.

1. Que vaut $\mathrm{Im}(\arctan)$?
2. Soit $\exp : z \mapsto e^z; \quad \mathbb{C} \to \mathbb{C}^*$ l'exponentielle complexe. Que valent $\exp(\mathbb{R})$ et $\exp(i\mathbb{R})$?

Proposition 3.

Soit $f : E \to F$ une application. Soient A et B deux parties de E. On a

$$f(A \cup B) = f(A) \cup f(B) \quad \text{et} \quad f(A \cap B) \subset f(A) \cap f(B).$$

Exemple 4.

Soit $f : x \mapsto x^2$, définie sur $\mathbb{R}$. Considérons $A = [2, +\infty[$, et $B =]-\infty, -2]$. Montrer que

$$f(A \cap B) \neq f(A) \cap f(B).$$

1.2 Image réciproque.

Définition 5.

Soient E et F deux ensembles non vides et $f : E \to F$ une application. Soit A une partie de F. On appelle **image réciproque** de A par f, et on note $f^{-1}(A)$ la partie de E ci-dessous

$$f^{-1}(A) = \{x \in E \mid f(x) \in A\}.$$

En particulier, si $y_0 \in F$, $f^{-1}(\{y_0\})$ est l'ensemble des antécédents de y_0 par f dans E.

La notation $f^{-1}(A)$ peut prêter à confusion.
Si $f : E \to F$, n'est pas bijective, **l'application f^{-1} n'est pas définie**, contrairement à l'ensemble $f^{-1}(A)$. Bref, sauf dans le cas où la réciproque existe, l'image réciproque n'est pas l'image par la réciproque...

Exemple 6.

1. La fonction tan étant définie sur l'ensemble que l'on sait, déterminer $\tan^{-1}(\mathbb{R}_+)$?
2. Soit $f : \left\{ \begin{array}{ccc} \mathbb{R}^2 & \to & \mathbb{R} \\ (x, y) & \mapsto & xy \end{array} \right.$. Que valent $f^{-1}(\mathbb{R}_+)$ et $f^{-1}(\{0\})$?

Proposition 7.

Soit $f : E \to F$ une application. Soient A et B deux parties de F. On a

$$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B) \quad \text{et} \quad f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B).$$

2 Applications injectives, surjectives, bijectives.

2.1 Injectivité

Définition 8.

Une application $f : E \to F$ est dite **injective** si tout élément de F a au plus un antécédent dans E, ce qui s'écrit :

$$\forall x, x' \in E \quad f(x) = f(x') \implies x = x'.$$

Méthode.

1. Pour démontrer qu'une application $f : E \to F$ **est** injective :
   - On considère deux éléments x et x' de E,
   - on suppose que $f(x) = f(x')$,
   - on démontre que $x = x'$.
2. Pour démontrer qu'une application $f : E \to F$ **n'est pas** injective, il suffit d'exhiber une paire $\{x, x'\}$ d'éléments de E tels que $x \neq x'$ et $f(x) = f(x')$.

D'une application $f : E \to F$ injective, on peut dire aussi que c'est une **injection** de E vers F.

Exemples 9.

1. La fonction $\sin : \mathbb{R} \to \mathbb{R}$ est-elle injective ? Comment la « rendre injective » ?
2. Soient
$$f : \left\{ \begin{array}{ccc} \mathbb{Z}^2 & \to & \mathbb{R} \\ (p,q) & \mapsto & p + \sqrt{2}q \end{array} \right. \quad \text{et} \quad g : \left\{ \begin{array}{ccc} \mathbb{R}^2 & \to & \mathbb{R} \\ (x,y) & \mapsto & xy \end{array} \right. .$$
Montrer que f est injective et que g ne l'est pas.

Exemple 10.

Soit $f : X \to \mathbb{R}$, où $X \in \mathcal{P}(\mathbb{R})$. Montrer que si f est strictement monotone, alors elle est injective.

Proposition 11.

La composée de deux applications injectives est injective.

Proposition 12 (Une réciproque partielle)**.**

Soient deux applications $f : E \to F$ et $g : F \to G$.
$$g \circ f \text{ est injective} \quad \Longrightarrow \quad f \text{ est injective.}$$

2.2 Surjectivité.

Définition 13.

Une application $f : E \to F$ est dite **surjective** si tout élément de F a au moins un antécédent dans E, ce qui s'écrit :
$$\forall y \in F \quad \exists x \in E \quad y = f(x).$$

Méthode.

1. Pour démontrer qu'une application $f : E \to F$ **est** surjective :
   - On considère un élément y de F,
   - on trouve/prouve l'existence de $x \in E$ tel que $y = f(x)$.
2. Pour démontrer qu'une application $f : E \to F$ **n'est pas** surjective, il suffit d'exhiber un élément de F n'ayant pas d'antécédent dans E par f.

D'une application $f : E \to F$ surjective, on peut dire aussi que c'est une **surjection** de E vers F.

Proposition 14 (Vision ensembliste de la surjectivité).

Soit $f : E \to F$ une application. On a

$$f \text{ surjective} \iff \operatorname{Im}(f) = F.$$

Exemples 15.

1. La fonction $\sin : \mathbb{R} \to \mathbb{R}$ est-elle surjective ?
2. Soient
$$f : \left\{ \begin{array}{ccc} \mathbb{Z}^2 & \to & \mathbb{R} \\ (p,q) & \mapsto & p + \sqrt{2}q \end{array} \right. \quad \text{et} \quad g : \left\{ \begin{array}{ccc} \mathbb{R}^2 & \to & \mathbb{R} \\ (x,y) & \mapsto & xy \end{array} \right. .$$
Montrer que g est surjective et que f ne l'est pas.

Proposition 16.

La composée de deux applications surjectives est surjective.

Proposition 17 (Une réciproque partielle).

Soient deux applications $f : E \to F$ et $g : F \to G$.

$$g \circ f \text{ est surjective} \implies g \text{ est surjective.}$$

2.3 Bijectivité et application réciproque.

Définition 18.

Soit une application $f : E \to F$. Elle est dite **bijective** si elle est à la fois injective et surjective, c'est-à-dire si tout élément de F possède un unique antécédent dans E, ce qui s'écrit

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

D'une application $f : E \to F$ bijective, on peut dire aussi que c'est une **bijection** de E vers F.

Définition 19.

Soit une application bijective $f : E \to F$. Tout élément $y \in F$ possède un unique antécédent dans E par f ; notons-le $f^{-1}(y)$. Ceci définit la fonction **réciproque** de f.

$$f^{-1} : \left\{ \begin{array}{ccc} F & \to & E \\ y & \mapsto & f^{-1}(y) \end{array} \right. .$$

Proposition 20 (La réciproque est un inverse pour la composition).

Soit $f : E \to F$ une bijection et $f^{-1} : F \to E$ sa réciproque. On a

$$f^{-1} \circ f = \mathrm{id}_E, \qquad \text{et} \qquad f \circ f^{-1} = \mathrm{id}_F.$$

Méthode (Calcul de la réciproque d'une fonction).

Soit $f : E \to F$ une fonction bijective et $y \in F$. S'il est possible de résoudre l'équation

$$y = f(x),$$

c'est-à-dire d'exprimer x en fonction de y, on a une expression de $f^{-1}(y)$.

Si, pour tout élément $y \in F$, on sait prouver l'existence et l'unicité d'un antécédent dans E (une solution de l'équation $y = f(x)$), on a prouvé la bijectivité de f.

Exemple 21.

Justifier que ch réalise une bijection de $[0, +\infty[$ dans $[1, +\infty[$ et expliciter sa réciproque.

Théorème 22 (Caract. de la bijectivité par l'existence d'un *inverse* pour la composition).

Soit $f \in \mathcal{F}(E, F)$ une application. Alors,

$$f \text{ est bijective} \iff \left(\exists g \in \mathcal{F}(F, E) \ : \ g \circ f = \mathrm{id}_E \ \text{ et } f \circ g = \mathrm{id}_F\right)$$

Autrement dit, f est bijective si et seulement si elle admet un (même) « inverse » à gauche et à droite pour la composition. De plus, lorsque cet inverse g existe, $g = f^{-1}$.

Proposition 23 (Bijectivité de la réciproque).

Si $f : E \to F$ est une bijection, alors $f^{-1} : E \to F$ est une bijection et

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

Proposition 24 (Composée de bijections).

Si $f : E \to F$ et $g : F \to G$ sont deux bijections, alors $g \circ f$ est une bijection de E vers G et

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

Exercices

Images directes, images réciproques.

$\boxed{14.1}$ **[♦◇◇]** Soit $f : E \to F$ une application. Soient deux parties $A \subset E$ et $B \subset F$. Montrer l'égalité

$$f(A) \cap B = f\left(A \cap f^{-1}(B)\right).$$

$\boxed{14.2}$ **[♦♦◇]** Soit $f : E \to F$ une application. Soit A une partie de E et B une partie de F.

1. (a) Montrer que $A \subset f^{-1}(f(A))$.
   (b) Démontrer que si f est injective, l'inclusion réciproque est vraie.
2. Soit B une partie de F.
   (a) Montrer que $f\left(f^{-1}(B)\right) \subset B$.
   (b) Démontrer que si f est surjective, l'inclusion réciproque est vraie.
3. Montrer que $f(f^{-1}(f(A))) = f(A)$.
4. Montrer que $f^{-1}(f(f^{-1}(B))) = f^{-1}(B)$.

$\boxed{14.3}$ **[♦♦♦]** Soit $f : E \to F$ une application. Montrer que

$$f \text{ est injective} \iff [\forall A, B \in \mathcal{P}(E) \quad f(A \cap B) = f(A) \cap f(B)].$$

Applications injectives, surjectives.

$\boxed{14.4}$ **[♦◇◇]** Soient

$$f : \left\{ \begin{array}{ccc} \mathbb{N}^2 & \to & \mathbb{Z} \\ (n,p) & \mapsto & (-1)^n p \end{array} \right. \qquad \text{et} \qquad g : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{C} \\ x & \mapsto & \frac{1+ix}{1-ix} \end{array} \right. .$$

Ces fonctions sont-elles injectives ? surjectives ?

$\boxed{14.5}$ **[♦◇◇]** Dans cet exercice, on admet que π est irrationnel.
Démontrer que $\cos_{|\mathbb{Q}}$ n'est pas injective et que $\sin_{|\mathbb{Q}}$ l'est.

$\boxed{14.6}$ **[♦♦◇]** Soit l'application $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = \left\{ \begin{array}{ll} x^2 & \text{si } x \geq 0 \\ 2x^2 & \text{si } x < 0. \end{array} \right.$

1. Montrer que f n'est pas injective.
2. Montrer que $f_{|\mathbb{Q}}$ (restriction de f à $\mathbb{Q}$) est injective.

$\boxed{14.7}$ **[♦◇◇]** Soit $f : E \to E$. Montrer que

1. f est injective si et seulement si $f \circ f$ est injective.
2. f est surjective si et seulement si $f \circ f$ est surjective.

$\boxed{14.8}$ **[♦♦◇]** Soit E un ensemble et $f : E \to E$ une application.
On suppose que $f \circ f = f$ et que f est injective ou surjective. Montrer que $f = \mathrm{id}_E$.

$\boxed{\textbf{14.9}}$ **[♦♦◇]** Soit E un ensemble e et $f : E \to E$ une application telle que $f \circ f \circ f = f$.
Montrer que

$$f \text{ est surjective} \iff f \text{ est injective.}$$

$\boxed{\textbf{14.10}}$ **[♦◇◇]** Soit $f : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & n + (-1)^n \end{array} \right.$.
Démontrer que f est une bijection de $\mathbb{N}$ dans lui-même et donner sa réciproque.

$\boxed{\textbf{14.11}}$ **[♦♦◇]** Définir une bijection de $\mathbb{N}$ dans $\mathbb{Z}$.

$\boxed{\textbf{14.12}}$ **[♦♦◇]** Soient $f : E \to F$ et $g : F \to E$ deux applications.
On suppose $f \circ g \circ f$ bijective. Montrer que f et g le sont aussi.

$\boxed{\textbf{14.13}}$ **[♦♦◇]** Soit l'application

$$\Phi : \left\{ \begin{array}{ccc} \mathcal{C}^1(\mathbb{R}, \mathbb{R}) & \to & \mathcal{C}^0(\mathbb{R}, \mathbb{R}) \times \mathbb{R} \\ f & \mapsto & (f', f(1)) \end{array} \right. .$$

1. Prouver que Φ est injective.
2. Prouver que Φ est surjective.
3. Donner une expression explicite de Φ^{-1}.

$\boxed{\textbf{14.14}}$ **[♦♦♦]** Soient E un ensemble et $(A, B) \in \mathcal{P}(E)^2$. On définit

$$\Phi : \left\{ \begin{array}{ccc} \mathcal{P}(E) & \to & \mathcal{P}(A) \times \mathcal{P}(B) \\ X & \mapsto & (X \cap A, X \cap B). \end{array} \right.$$

1. Calculer $\Phi(\emptyset)$ et $\Phi\big(E \setminus (A \cup B)\big)$. Que dire de A et B si $(A, \emptyset)$ admet un antécédent par Φ ?
2. Montrer que : Φ injective $\iff A \cup B = E$.
3. Montrer que : Φ surjective $\iff A \cap B = \emptyset$.

$\boxed{\textbf{14.15}}$ **[♦♦♦]**
On souhaite que cet exercice éclaire la caractérisation de la bijectivité par existence d'un inverse

Soit $f \in \mathcal{F}(E, F)$.

1. Démontrer que f est injective si et seulement si elle est inversible à gauche.
   Plus précisément, prouver l'assertion

$$f \text{ est injective} \iff \exists g \in \mathcal{F}(F, E) \quad g \circ f = \mathrm{id}_E.$$

2. Démontrer que f est surjective si et seulement si elle est inversible à gauche.
   Plus précisément, prouver l'assertion

$$f \text{ est injective} \iff \exists g \in \mathcal{F}(F, E) \quad f \circ g = \mathrm{id}_F.$$

$\boxed{\textbf{14.16}}$ **[♦♦♦]** [Théorème de Cantor]
Soit $f \in \mathcal{F}(E, \mathcal{P}(E))$. Montrer que f n'est pas surjective.
Indication : on pourra considérer $A = \{x \in E \mid x \notin f(x)\}$.

---

15 Relations binaires

1 Relations binaires et leurs éventuelles propriétés.

Soit E un ensemble.

Définition 1.

On appelle **relation binaire** sur E un prédicat $\mathscr{R}(x, y)$ sur $E \times E$, c'est-à-dire une propriété dépendant de $(x, y) \in E \times E$ et pouvant être vérifiée ou pas par chaque couple (x, y) de $E \times E$.

Soit $(x, y) \in E^2$. Si la propriété $\mathscr{R}(x, y)$ est vérifiée, on dit que x et y sont **en relation**, et on note

$$x \mathscr{R} y.$$

Remarque. On peut aussi définir plus rigoureusement (mais moins clairement) une relation binaire $\mathscr{R}$ comme une partie de $E \times E$. Pour $(x, y) \in E \times E$, on dit alors que x est en relation avec y si $(x, y) \in \mathscr{R}$.

Définition 2 (Propriétés que possède *éventuellement* une relation binaire)**.**

On dit qu'une relation binaire $\mathscr{R}$ sur E est

- **réflexive** si
$$\forall x \in E \quad x \mathscr{R} x,$$
- **symétrique** si
$$\forall (x, y) \in E^2 \quad x \mathscr{R} y \Longrightarrow y \mathscr{R} x,$$
- **antisymétrique** si
$$\forall (x, y) \in E^2 \quad (x \mathscr{R} y \;\text{ et }\; y \mathscr{R} x) \Longrightarrow x = y,$$
- **transitive** si
$$\forall (x, y, z) \in E^3 \quad (x \mathscr{R} y \;\text{ et }\; y \mathscr{R} z) \Longrightarrow x \mathscr{R} z.$$

Exemples 3.

Soit $\mathcal{D}$ l'ensemble des droites du plan, et E un ensemble quelconque.

Relation	réflexive ?	symétrique ?	antisymétrique ?	transitive ?
$=$ sur E				
$<$ sur $\mathbb{R}$				
$\perp$ sur $\mathcal{D}$				
$\parallel$ sur $\mathcal{D}$				

2 Relations d'équivalence.

Définition 4.

Sur un ensemble E, une **relation d'équivalence** est une relation binaire $\sim$ qui est réflexive, symétrique et transitive.

Deux éléments x et y qui sont en relation (i.e. tels que $x \sim y$) sont dits **équivalents**.

Pour $x \in E$, on appelle **classe d'équivalence de** x l'ensemble des éléments qui sont équivalents à x ; on notera ici cet ensemble $[x]$:

$$[x] := \{y \in E \mid y \sim x\}.$$

Exemple Sur E, l'égalité est une relation d'équivalence (triviale). Que dire des classes d'équivalence ?

Exemple 5 (Relation d'équivalence associée à une fonction)**.**

Soit $f : E \to F$ une application. Pour $x, y \in E$, on pose $x \sim y$ si $f(x) = f(y)$.
La relation $\sim$ est une relation d'équivalence sur E. Décrire les classes d'équivalence.

Définition 6.

1. Soit $\alpha \in \mathbb{R}$. Sur $\mathbb{R}$, la relation de **congruence** modulo α est définie par

$$\forall (x, y) \in \mathbb{R}^2 \quad x \equiv y[\alpha] \iff \exists k \in \mathbb{Z}\ x = y + k\alpha.$$

2. Soit $n \in \mathbb{Z}$. Sur $\mathbb{Z}$, la relation de **congruence** modulo n est définie par

$$\forall (p, q) \in \mathbb{Z}^2 \quad p \equiv q[n] \iff \exists k \in \mathbb{Z}\ p = q + kn.$$

Proposition 7.

Les relations de congruence sont des relations d'équivalence.

Proposition 8.

Soit E un ensemble et $\sim$ une relation d'équivalence sur E. Pour $x, x' \in E$,

$$x \sim x' \iff x' \in [x] \iff [x] = [x'].$$

Théorème 9.

Les classes d'équivalence pour une relation d'équivalence sur un ensemble E forment une partition de cet ensemble.

3 Relations d'ordre.

Définition 10.

Sur un ensemble E, une **relation d'ordre** est une relation binaire $\preceq$ qui est réflexive, antisymétrique et transitive. Au sujet du couple $(E, \preceq)$, on peut alors parler d'*ensemble ordonné*.

Définition 11.

Une relation d'ordre sur un ensemble E est dite **totale** si on peut toujours comparer deux éléments de E, c'est-à-dire que

$$\forall (x, y) \in E^2 \quad x \preceq y \ \text{ ou } \ y \preceq x.$$

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

Remarque. Logique : prouver qu'un ordre $\preceq$ n'est pas total sur un ensemble E, c'est être en mesure d'exhiber deux éléments x et y de E pour lesquels les assertions $(x \preceq y)$ et $(y \preceq x)$ sont fausses.

Exemple 12 (Inégalités dans $\mathbb{R}$)**.**

La relation $\leq$ est une relation d'ordre sur $\mathbb{R}$. Il s'agit d'un ordre total.
Cette relation d'ordre est celle que nous connaissons le mieux : elle sera privilégiée pour les exemples élémentaires.

La relation $<$ n'est pas une relation d'ordre sur $\mathbb{R}$ (elle n'est pas réflexive).

Exemple 13 (Inclusion)**.**

Soit E un ensemble. La relation d'inclusion $\subset$ est une relation d'ordre sur $\mathcal{P}(E)$.
Dès que E possède plus de deux éléments, il s'agit d'un ordre partiel.

Exemple 14 (Divisibilité sur les entiers positifs)**.**

Soient p et q deux entiers naturels. On dit que p divise q si il existe un entier $k \in \mathbb{N}$ tel que $q = kp$; on note alors $p \mid q$. La relation $\mid$ est une relation d'ordre (partielle) sur $\mathbb{N}$.

Exemple 15 (L'ordre du dictionnaire)**.**

Soit $p \in \mathbb{N}^*$. L'ordre lexicographique est une relation d'ordre totale sur $\mathbb{N}^p$ ou bien $\mathbb{R}^p$.
Deux p-uplets $(x_1, \dots, x_p)$ et $(y_1, \dots, y_p)$ sont comparés d'abord selon leur première coordonnée, puis selon la deuxième en cas d'égalité, etc...
Les p-uplets sont alors ordonnés comme dans un dictionnaire.
Pour cet ordre sur $\mathbb{N}^3$, $(1, 2, 4)$ est plus petit que $(1, 3, 2)$, qui est lui-même plus petit que $(1, 3, 4)$.

Définition 16.

Considérons deux ensembles, chacun muni d'une relation d'ordre : $(E, \underset{E}{\preceq})$ et $(F, \underset{F}{\preceq})$.
D'une application $f : E \to F$, on dit qu'elle est

- **croissante** si
$$\forall (x, x') \in E^2 \quad x \underset{E}{\preceq} x' \implies f(x) \underset{F}{\preceq} f(x').$$
- **décroissante** si
$$\forall (x, x') \in E^2 \quad x \underset{E}{\preceq} x' \implies f(x') \underset{F}{\preceq} f(x).$$
- **monotone** si elle est croissante ou décroissante.

Exemple 17.

Connaissons-nous des fonctions monotones (au sens de l'inclusion) de $\mathcal{P}(E)$ dans lui-même ?

Définition 18 (Majorant, minorant)**.**

Soit $(E, \preceq)$ un ensemble ordonné et A une partie de E.

- On dit que A est **majorée** dans E si il existe un élément M de E tel que
$$\forall x \in A \quad x \preceq M.$$
Dans ce contexte, M est appelé un **majorant** de A.
- On dit que A est **minorée** dans E si il existe un élément m de E tel que
$$\forall x \in A \quad m \preceq x.$$
Dans ce contexte, m est appelé un **minorant** de A.
- On dit que A est **bornée** si elle est majorée et minorée.

Exemple 19 (Dans $(\mathbb{R}, \leq)$)**.**

Soit $A =]-\infty, 1[$.
La partie A est elle majorée, minorée ? Justifier.

Remarques. Comme on vient de le comprendre,

1. l'existence d'un majorant ou d'un minorant pour une partie A d'un ensemble E n'est pas garantie,
2. un majorant ou un minorant de A n'appartient pas nécessairement à A ;
3. un majorant ou un minorant n'est pas nécessairement unique.

Proposition-Définition 20 (Maximum, minimum)**.**

Soit $(E, \preceq)$ un ensemble ordonné et A une partie de E.

- S'il existe un majorant de A qui appartient à A, alors cet élément est unique.
  Il est appelé plus grand élément de A ou encore **maximum** de A et noté $\max(A)$.

- S'il existe un minorant de A qui appartient à A, alors cet élément est unique.
  Il est appelé plus petit élément de A ou encore **minimum** de A et noté $\min(A)$.

Exemple 21.

Soit $B = [-1, 1[$.
Démontrer que B possède un minimum et ne possède pas de maximum.

Remarques.

1. On vient de le voir, l'existence d'un maximum ou d'un minimum n'est pas garantie.
2. Insistons sur le fait que par définition, un maximum ou un minimum appartient nécessairement à A.

Exemple 22.

Soit E un ensemble. Alors $(\mathcal{P}(E), \subset)$ est un ensemble ordonné.
$\mathcal{P}(E)$ possède-t-il un plus petit élément ? Un plus grand élément ?
Proposez une partie de $\mathcal{P}(\mathbb{R})$ n'ayant pas de plus grand élément.

Définition 23 (Borne supérieure, inférieure)**.**

Soit $(E, \preceq)$ un ensemble ordonné et A une partie de E.

- Si l'ensemble des majorants de A admet un plus petit élément, alors cet élément est unique.
  Il est appelé **borne supérieure** de A et noté $\sup(A)$.

- Si l'ensemble des minorants de A admet un plus grand élément, alors cet élément est unique.
  Il est appelé **borne inférieure** de A et noté $\inf(A)$.

Remarque. Comme pour le maximum, l'existence d'une borne supérieure dans E n'est pas garantie.

Exemple 24 ((*) laissé en exercice, une fois apprivoisée la notion pour les parties de $\mathbb{R}$)**.**

Soit E un ensemble. Dans l'ensemble ordonné $(\mathcal{P}(E), \subset)$, toute partie $\mathcal{A}$ de $\mathcal{P}(E)$ possède une borne supérieure ainsi qu'une borne inférieure : on a

$$\sup(\mathcal{A}) = \bigcup_{X \in \mathcal{A}} X \quad \text{et} \quad \inf(\mathcal{A}) = \bigcap_{X \in \mathcal{A}} X.$$

Exercices

$\boxed{\textbf{15.1}}$ **[♦♦♢]** Soit $\mathscr{R}$ la relation définie sur $\mathbb{R}$ par :

$$x \mathscr{R} y \iff xe^y = ye^x.$$

1. Montrer que $\mathscr{R}$ est une relation d'équivalence sur $\mathbb{R}$.
2. Préciser le cardinal de la classe d'équivalence d'un réel x.

$\boxed{\textbf{15.2}}$ **[♦♦♢]** On considère la relation $\mathscr{R}$ définie sur $\mathbb{N}^*$ par

$$p \mathscr{R} q \iff \exists n \in \mathbb{N}^* : p^n = q.$$

Montrer que $\mathscr{R}$ est une relation d'ordre partiel sur $\mathbb{N}^*$.

$\boxed{\textbf{15.3}}$ **[♦♦♢]** Soient $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ et $y = (y_1, \dots y_n) \in \mathbb{R}^n$. On note $x \preceq y$ si

$$\forall k \in [\![1, n]\!] \quad : \quad \sum_{i=1}^{k} x_i \leq \sum_{i=1}^{k} y_i.$$

1. Montrer que $\preceq$ est une relation d'ordre sur $\mathbb{R}^n$.
2. Si $n \geq 2$, montrer qu'il s'agit d'un ordre partiel.

$\boxed{\textbf{15.4}}$ **[♦♦♢]** Sur $\mathbb{R}_+^*$, on définit une relation binaire en posant que deux réels strictement positifs sont en relation, ce qu'on note $x\mathcal{R}y$ si et seulement si

$$\exists (p, q) \in (\mathbb{N}^*)^2 \quad px = qy.$$

1. Démontrer que $\mathcal{R}$ est une relation d'équivalence.
2. Démontrer que pour cette relation, deux classes d'équivalences sont nécessairement en bijection.

$\boxed{\textbf{15.5}}$ **[♦♦♢]** Sur $\mathbb{R}$, on définit la relation $\mathcal{R}$ par

$$x\mathcal{R}y \iff x^2 + 2y = y^2 + 2x.$$

1. Montrer que $\mathcal{R}$ est une relation d'équivalence sur $\mathbb{R}$.
2. Déterminer la classe d'équivalence d'un réel a.

$\boxed{\textbf{15.6}}$ **[♦♦♢]** Soit $\mathcal{R}$ une relation sur un ensemble E.
Pour $(x, y) \in E$, on note $x \sim y$ s'il existe $n \in \mathbb{N}^*$ et $x_0, \dots, x_n \in E$ tels que

$$x_0 = x, \quad x_0\mathcal{R}x_1, \quad x_1\mathcal{R}x_2, \quad x_{n-1}\mathcal{R}x_n, \quad x_n = y.$$

1. Montrer que $\sim$ est une relation transitive sur E.
2. On suppose que $\mathcal{R}$ est réflexive et symétrique. Montrer que $\sim$ est une relation d'équivalence sur E.

$\boxed{\textbf{15.7}}$ **[♦♦♦]** Soit E un ensemble et A une partie de E. Pour deux parties X et Y de E, on note $X \sim Y$ lorsque $X \cap A = Y \cap A$, ce qui définit sur $\mathcal{P}(E)$ une relation binaire.

1. Montrer que $\sim$ est une relation d'équivalence.
2. On note $\mathcal{P}(E)/\sim$ l'ensemble des classes d'équivalences pour $\sim$.
   Démontrer qu'il existe une bijection de $\mathcal{P}(A)$ dans $\mathcal{P}(E)/\sim$.

Nombres réels

1 Ensembles de nombres inclus dans $\mathbb{R}$.

1.1 Nombres entiers.

Définition 1.

On note $\mathbb{N}$ l'ensemble des entiers naturels $\mathbb{N} = \{0, 1, 2, \dots\}$ et $\mathbb{Z} = \{0, 1, 2, \dots\} \cup \{-1, -2, \dots\}$ l'ensemble des entiers relatifs.

On admet les deux propositions suivantes :

Proposition 2.

L'ensemble des entiers relatifs est stable par somme, différence, et produit.

Proposition 3.

Toute partie non vide et majorée de $\mathbb{N}$ ou de $\mathbb{Z}$ admet un plus grand élément.
Toute partie non vide et minorée de $\mathbb{Z}$ admet un plus petit élément.
En particulier, toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Définition 4.

Pour tout nombre réel x, on appelle **partie entière** de x, et on note $\lfloor x \rfloor$ le plus grand entier relatif inférieur à x :

$$\lfloor x \rfloor = \max \{k \in \mathbb{Z} \ | \ k \leq x\}.$$

Proposition 5.

Pour tout nombre réel x,
$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1.$$
En « croisant » les inégalités, ceci implique notamment que pour tout $x \in \mathbb{R}$,
$$x - 1 < \lfloor x \rfloor \leq x.$$

On connaît le graphe de la fonction $x \mapsto \lfloor x \rfloor$. On avait démontré dans le cours sur les fonctions de la variable réelle que cette fonction est croissante (bon exercice).

Corollaire 6.

L'ensemble $\mathbb{R}$ possède la propriété dite d'Archimède : pour tout nombre réel $x \in \mathbb{R}_+^*$, pour tout réel positif $\varepsilon > 0$, il existe $n \in \mathbb{N}$ tel que $n\varepsilon > x$.

1.2 Nombres décimaux.

Définition 7.

On appelle **nombre décimal** un nombre réel qui s'écrit sous la forme $\dfrac{p}{10^k}$, où $p \in \mathbb{Z}$ et $k \in \mathbb{N}$.
L'ensemble des nombres décimaux, est noté $\mathbb{D}$.

Définition 8 (généralisation)**.**

Soit p un entier naturel supérieur ou égal à 2.
On appelle **fraction p-adique** un nombre réel qui s'écrit sous la forme $\dfrac{q}{p^k}$ où $q \in \mathbb{Z}$ et $k \in \mathbb{N}$.

Les fractions 2-adiques sont dites dyadiques. Les nombres "flottants" en info sont des dyadiques.

L'encadrement donné par la partie entière est à la précision 1. Ce qui suit généralise le principe et permet d'obtenir une précision arbitraire.

Proposition 9.

Soit $x \in \mathbb{R}$ et $n \in \mathbb{N}$. Le nombre $d_n(x) := \frac{\lfloor 10^n x \rfloor}{10^n}$ satisfait l'encadrement
$$d_n(x) \leq x < d_n(x) + 10^{-n}.$$
Les nombres $d_n(x)$ et $d_n(x) + 10^{-n}$ sont appelés respectivement **valeur décimale** par défaut (resp. par excès) de x à la précision 10^{-n}.

Exemple. Voici les valeurs décimales par défaut et par excès à la précision 10^{-3} de certaines constantes.

	1	$\sqrt{2}$	$\sqrt{3}$	π	e	$\ln(2)$
par défaut à 10^{-3} près	$1,000$	$1,414$	$1,732$	$3,141$	$2,718$	0.693
par excès à 10^{-3} près	$1,001$	$1,415$	$1,733$	$3,142$	$2,719$	0.694

Corollaire 10 ($\mathbb{D}$ est *dense* dans $\mathbb{R}$)**.**

Entre deux réels distincts, il existe toujours un nombre décimal :

$$\forall a < b \in \mathbb{R} \quad \mathbb{D} \cap]a, b[\neq \emptyset.$$

1.3 Nombres rationnels.

Définition 11.

Un nombre **rationnel** est un nombre réel qui s'écrit sous la forme d'un quotient d'entiers $\frac{p}{q}$, où $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$. On note $\mathbb{Q}$ l'ensemble des nombres rationnels.
On dit d'un nombre de $\mathbb{R} \setminus \mathbb{Q}$ qu'il est **irrationnel**.

Les nombres décimaux sont des nombres rationnels, et on peut écrire les inclusions

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

La dernière inclusion est stricte car il existe des nombres irrationnels. On a prouvé que $\sqrt{2}$ est irrationnel. Les nombres e et π sont aussi irrationnels (ce sera prouvé dans des exercices). On pense que la constante d'Euler γ est irrationnelle mais il s'agit toujours d'une conjecture.

Proposition 12.

L'ensemble des rationnels est stable par somme, produit, et passage à l'inverse.

Exemple 13.

Justifier que $\mathbb{R} \setminus \mathbb{Q}$ n'est PAS stable par somme, ni par produit.

Théorème 14 ($\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$ sont *denses* dans $\mathbb{R}$)**.**

Entre deux réels distincts, il existe toujours un nombre rationnel et un irrationnel.
Autrement dit, pour tous a, b réels avec $a < b$,

$$]a, b[\cap \mathbb{Q} \neq \emptyset \quad \text{et} \quad]a, b[\cap (\mathbb{R} \setminus \mathbb{Q}) \neq \emptyset.$$

Autrement dit, tout intervalle ouvert non vide rencontre $\mathbb{Q}$:

2 Bornes d'une partie de $\mathbb{R}$.

2.1 Majorants, minorant, maximum, minimum.

Les quatre notions figurant dans le titre du paragraphe ont été définies pour une relation d'ordre quelconque.

On rappelle que si A est une partie de $\mathbb{R}$, un réel M est un **majorant** de A si tous les éléments de A sont inférieurs à M. Lorsqu'un tel réel existe, la partie A est dite **majorée**. Il n'y a pas unicité du majorant, bien sûr : si M est un majorant de A, alors M' en est un autre dès que $M \leq M'$.

Si A est un ensemble de réels, on parle de **maximum** de A au sujet d'un majorant qui appartient à A.
On sait que le maximum est unique lorsqu'il existe, mais certaines parties majorées n'ont pas de maximum.

Proposition 15 (Caractérisation des parties bornées de $\mathbb{R}$)**.**

Soit A une partie de $\mathbb{R}$.

$$A \text{ est bornée} \quad \Longleftrightarrow \quad \exists \mu \in \mathbb{R}_+ \ \forall x \in A \quad |x| \leq \mu.$$

2.2 Borne supérieure, borne inférieure.

Définition 16.

Soit A une partie de $\mathbb{R}$.
- On appelle **borne supérieure** de A et on note $\sup A$, le plus petit des majorants de A, lorsque ce nombre existe.
- On appelle **borne inférieure** de A et on note $\inf A$, le plus grand des minorants de A, lorsque ce nombre existe.

Implicite dans cette définition : l'*unicité* de la borne supérieure. On peut la montrer comme on avait prouvé celle d'un maximum. Pour ce qui concerne l'*existence*, commençons par examiner un cas simple.

Proposition 17.

Si une partie de $\mathbb{R}$ possède un maximum M, alors elle a une borne supérieure, qui vaut M.

Le théorème ci-dessous, admis, est une propriété fondamentale de $\mathbb{R}$.

Théorème 18 (Propriété de la borne supérieure/inférieure)**.**

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

Remplacez $\mathbb{R}$ par $\mathbb{Q}$ dans les phrases précédentes et elles deviennent fausses : voir l'exercice 7

Proposition 19 (Caractérisation de la borne supérieure.).

Soit A une partie de $\mathbb{R}$ non vide et majorée et $\alpha \in \mathbb{R}$. On a l'équivalence

$$\sup A = M \quad \Longleftrightarrow \quad \left\{ \begin{array}{l} M \text{ est un majorant de } A \\ \forall \varepsilon > 0, \exists x \in A : M - \varepsilon < x \leq M \end{array} \right.$$

Interprétons l'assertion commençant par $\forall \varepsilon \ \exists x \in A : M - \varepsilon < x \leq M$ dans ce qui précède : il est dit que l'on peut trouver un élément de A *aussi proche que l'on veut* de M.

Si on a compris pour la borne supérieure, on sait adapter pour la borne inférieure : pour A une partie non vide et minorée et α un réel,

$$\inf A = m \quad \Longleftrightarrow \quad \left\{ \begin{array}{l} m \text{ est un minorant de } A \\ \ldots \end{array} \right.$$

Exemple 20.

Soit $A = [0, 1[$. Justifier l'existence de $\sup A$ puis la calculer.

Soit $B = \left\{ r \in \mathbb{Q} : r < \sqrt{2} \right\}$. Justifier l'existence de $\sup B$ puis la calculer.

Soit $C = \{1/n - 1/p,\ n, p \in \mathbb{N}^*\}$. Calculer $\sup C$ et $\inf C$, après avoir justifié qu'elles existent.

Méthode (Majorer une borne supérieure/"Passage au sup").

Soient M un réel et A une partie de $\mathbb{R}$ possédant une borne supérieure. Pour démontrer l'inégalité

$$\sup A \leq M,$$

il suffira de montrer que M est un majorant de A ($\sup A$ étant le *plus petit* des majorants de A).

Exemple 21 (Calculs de bornes supérieures).

Soient A et B deux parties non vides et majorées de $\mathbb{R}$ telles que $A \subset B$.
Justifier que $\sup A \leq \sup B$.

Remarque : Pour montrer que deux bornes supérieures sont égales, on pourra utiliser l'équivalence

$$\sup A = \sup B \quad \Longleftrightarrow \quad \sup A \leq \sup B \quad \text{et} \quad \sup B \leq \sup A.$$

Exemple 22 (Homogénéité du sup).

Soit A une partie de $\mathbb{R}$ non vide et majorée et $\lambda \in \mathbb{R}_+$. On définit la partie $\lambda A := \{\lambda x \mid x \in A\}$.
Montrer l'égalité

$$\sup(\lambda A) = \lambda \sup(A).$$

2.3 Retour sur la notion d'intervalle.

Définition 23.

On dit qu'une partie A de $\mathbb{R}$ est **convexe** si pour tout $a, b \in A$ avec $a < b$, on a $[a, b] \subset A$.

Proposition 24 (Caractérisation des intervalles)**.**

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

Preuve. Soit X une partie de $\mathbb{R}$.

• Supposons que X est un intervalle. Il est donc de l'un des trois types suivants.
- un segment $[g, d] = \{x \in \mathbb{R} : g \leq x \text{ et } x \leq d\}$ où $g, d \in \mathbb{R}$.
- un intervalle ouvert $]g, d[= \{x \in \mathbb{R} : g < x \text{ et } x < d\}$ où $g \in \mathbb{R} \cup \{-\infty\}, d \in \mathbb{R} \cup \{+\infty\}$,
- un intervalle semi-ouvert, par exemple du type $]g, d] = \{x \in \mathbb{R} : g < x \text{ et } x \leq d\}$ où $g \in \mathbb{R} \cup \{-\infty\}, d \in \mathbb{R}$

Dans les trois cas, on peut vérifier facilement que ces parties sont convexes.

• Supposons que X est convexe, c'est-à-dire satisfait : $\forall a, b \in X \quad [a, b] \subset X$.

⋆ Cas où X est vide. Alors X est un intervalle : l'intervalle $[0, -5]$ par exemple !

⋆ Cas où X est non vide, majorée et minorée. La partie X admet alors une borne supérieure, que l'on note d et une borne inférieure, que l'on note g. Ce sont respectivement un majorant, et un minorant de X, de sorte que

$$X \subset [g, d].$$

Soit $\varepsilon > 0$. D'après la caractérisation de la borne supérieure (et inférieure), il existe $\alpha \in X$ tel que $g \leq \alpha < g + \varepsilon$. Il existe $\beta \in X$ tel que $d - \varepsilon < \beta \leq d$. Si on a supposé de surcroît que $\varepsilon < \frac{d-g}{2}$, on a

$$g \leq \alpha < g + \varepsilon < d - \varepsilon < \beta \leq d.$$

Or, d'après l'hypothèse, le segment $[\alpha, \beta]$ est tout entier inclus dans X. Puisqu'il contient $[g + \varepsilon, d - \varepsilon]$, on a

$$[g + \varepsilon, d - \varepsilon] \subset X \subset [g, d].$$

Dans ce qui précède, le nombre ε, peut être pris arbitrairement petit, ce qui conduit à

$$]g, d[\subset X \subset [g, d],$$

$$\text{et donc} \qquad X =]g, d[\quad \text{ou} \quad X = [g, d[\quad \text{ou} \quad X =]g, d] \quad \text{ou} \quad X = [g, d].$$

On a bien montré que X est un intervalle.

⋆ Cas où X est non vide, majorée et non minorée. En adaptant les idées ci-dessus, le lecteur montrera que qu'il existe $d \in \mathbb{R}$ tel que

$$X =]-\infty, d[\quad \text{ou} \quad X =]-\infty, d].$$

⋆ Cas où X est non vide, non majorée, et minorée. En adaptant les idées ci-dessus, le lecteur montrera que qu'il existe $g \in \mathbb{R}$ tel que

$$X =]g, +\infty[\quad \text{ou} \quad X = [g, +\infty[.$$

⋆ Cas où X est non vide, non majorée et non minorée. On peut alors montrer que $X =]-\infty, +\infty[= \mathbb{R}$.

□

Exemple 25.

Démontrer qu'une intersection d'intervalles est un intervalle.

Exercices

$\boxed{\textbf{16.1}}$ **[♦◇◇]** Prouver que $\dfrac{\ln(2)}{\ln(3)}$ est un nombre irrationnel.

$\boxed{\textbf{16.2}}$ **[♦♦◇]** Soient x et y deux rationnels positifs tels que que $\sqrt{x}$ et $\sqrt{y}$ sont irrationnels.
Montrer que $\sqrt{x} + \sqrt{y}$ est irrationnel.

$\boxed{\textbf{16.3}}$ **[♦◇◇]**

1. Montrer que
$$\forall (a,b) \in (\mathbb{R}_+^*)^2 \quad : \quad \frac{a^2}{a+b} \geq \frac{3a-b}{4}.$$
Étudier le cas d'égalité.
2. En déduire que l'ensemble
$$E = \left\{ \frac{a^2}{a+b} + \frac{b^2}{b+c} + \frac{c^2}{c+a} \mid (a,b,c) \in (\mathbb{R}_+^*)^3 \text{ et } a+b+c \geq 2 \right\}$$
admet un minimum et le calculer.

$\boxed{\textbf{16.4}}$ **[♦♦◇]** Calculer les bornes supérieures et inférieures des parties, après en avoir prouvé l'existence.

$$A = \left\{ \frac{1}{n} + (-1)^n \mid n \in \mathbb{N}^* \right\}, \quad B = \left\{ \frac{m}{nm+1} \mid m \in \mathbb{N}^*, n \in \mathbb{N}^* \right\}, \quad C = \left\{ x^2 + y^2 \mid (x,y) \in \mathbb{R}^2 \text{ et } xy = 1 \right\}.$$

$\boxed{\textbf{16.5}}$ **[♦♦◇]** Soit u une suite bornée et v la suite définie par
$$\forall n \in \mathbb{N} \quad v_n = \sup \{u_k \mid k \in [\![n, +\infty [\![\}.$$
Justifier que v est bien définie et qu'elle est convergente.

$\boxed{\textbf{16.6}}$ **[♦♦♦]** Soient A et B deux parties non vides et majorées de $\mathbb{R}$. On note $A+B := \{x+y \mid x \in A, y \in B\}$.
Prouver l'égalité :
$$\sup(A+B) = \sup(A) + \sup(B)$$

$\boxed{\textbf{16.7}}$ **[♦♦♦]** [$\mathbb{Q}$ ne possède pas la propriété de la borne supérieure]
Justifier que $\{r \in \mathbb{Q} \mid r < \sqrt{2}\}$ est une partie non vide et majorée de $\mathbb{Q}$.
Démontrer qu'elle n'a pas de plus petit majorant dans $\mathbb{Q}$

$\boxed{\textbf{16.8}}$ **[♦♦♦]** Soit $f : [0,1] \longrightarrow [0,1]$ une application croissante. On pose
$$E = \{x \in [0,1] / f(x) \geq x\}$$

1. Montrer que E admet une borne supérieure notée a.
2. Montrer que E est stable par f.
3. Montrer que $f(a) = a$.

---

17 Suites : la théorie

1 Limite d'une suite.

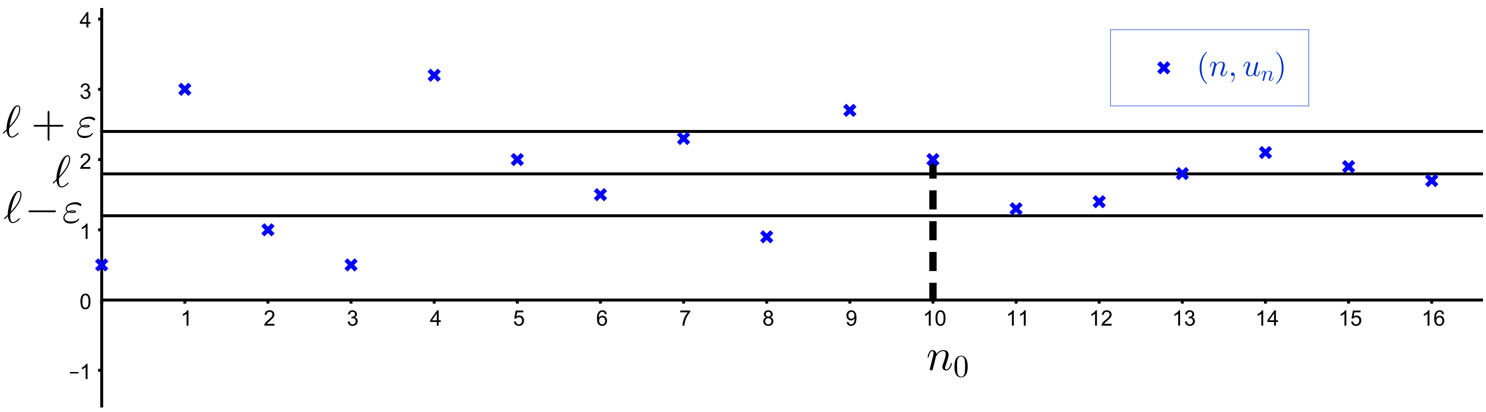
Définition 1 (Convergence vers $\ell \in \mathbb{R}$).

Soit $(u_n)_{n\geq 0}$ une suite réelle et $\ell \in \mathbb{R}$. On dit que (u_n) **converge** vers ℓ (ou qu'elle **tend** vers ℓ), et on note $u_n \to \ell$ si

$$\forall \varepsilon > 0 \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad |u_n - \ell| \leq \varepsilon.$$

Une autre écriture de « $u_n \to \ell$ », avec une utilisation plus rigoureuse du quantificateur $\forall$:

$$\forall \varepsilon > 0 \quad \exists n_0 \in \mathbb{N} \quad \forall n \in \mathbb{N} \quad n \geq n_0 \implies |u_n - \ell| \leq \varepsilon.$$



Cette définition est écrite sous cette forme par Cauchy en 1821. Elle avait été donnée par d'Alembert dans l'Encyclopédie (1767) : « *On dit qu'une grandeur est la limite d'une autre grandeur quand la seconde peut approcher de la première plus près que d'une grandeur donnée si petite qu'on la puisse supposer...* »

Proposition 2.

Soit $(u_n)_{n\in\mathbb{N}}$ et $\ell \in \mathbb{R}$. On a

$$u_n \longrightarrow \ell \quad \Longleftrightarrow \quad |u_n - \ell| \longrightarrow 0.$$

Méthode (la théorie et la pratique)**.**

Prouver une convergence du type $u_n \to \ell$, c'est montrer que la **distance** $|u_n - \ell|$ peut être rendue « aussi petite que l'on veut ». On cherchera donc

- dans un contexte théorique, à majorer $|u_n - \ell|$ par un réel ε quelconque *à partir d'un certain rang* n_0 qui dépend de ε. C'est ce que nous ferons dans les preuves de ce cours mais dans les exercices, on dégainera rarement ε !
- dans un contexte pratique, à majorer $|u_n - \ell|$ par une suite convergeant notoirement vers 0. On pourra alors conclure grâce au théorème d'encadrement.

Exemple 3.

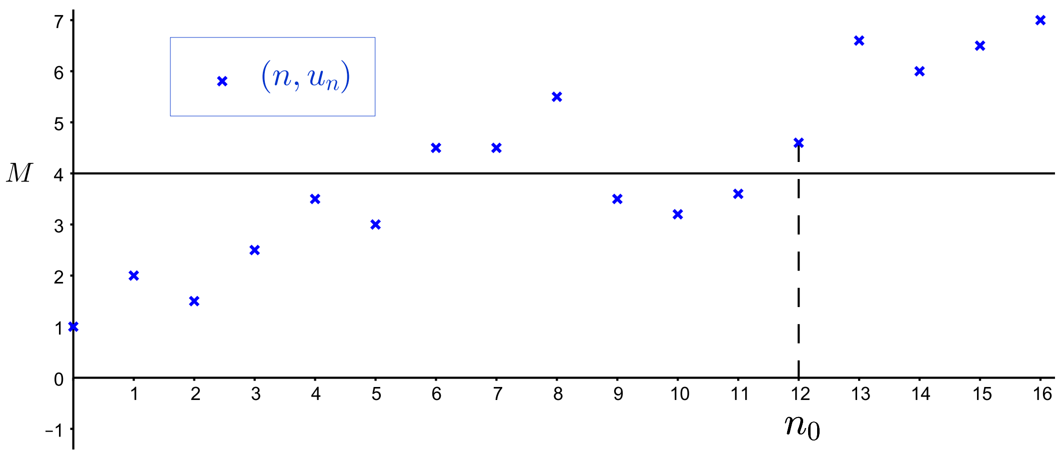
• Soit (u_n) une suite constante égale à $a \in \mathbb{R}$. Démontrer en revenant à la définition que $u_n \to a$.

• Soit la suite (u_n) de terme général $u_n = \frac{n+1}{n}$.
Démontrer en revenant à la définition que $u_n \to \ell$ où ℓ est un réel à deviner.

Définition 4 (Tendre vers $+\infty$)**.**

Soit (u_n) une suite réelle. On dit qu'elle **tend vers** $+\infty$ et on note $u_n \to +\infty$ si

$$\forall M > 0 \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad u_n \geq M.$$



Exemple 5.

Pour $n \geq 2$, posons $u_n = \ln(\ln(n))$. En revenant à la définition, démontrer que $u_n \to +\infty$.

Proposition-Définition 6 (Tendre vers $-\infty$)**.**

Soit (u_n) une suite réelle. On dit qu'elle **tend vers** $-\infty$ et on note $u_n \to -\infty$ si

$$\forall M < 0 \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad u_n \leq M.$$

On a l'équivalence

$$u_n \to -\infty \quad \Longleftrightarrow \quad -u_n \to +\infty.$$

Proposition-Définition 7 (Unicité de la limite)**.**

Soit (u_n) une suite réelle et $L, L' \in \overline{\mathbb{R}}$. Si $u_n \to L$ et $u_n \to L'$, alors $L = L'$.

Le nombre L est alors appelé **limite** de la suite (u_n) et noté $\lim u_n$.

Définition 8.

On dit d'une suite (u_n) qu'elle est **convergente** si elle converge vers une limite finie.

Si une suite n'est pas convergente, elle est dite **divergente**.

Ainsi, on pourra dire d'une suite qui tend vers $+\infty$ qu'elle *diverge vers* $+\infty$.

Exemple 9.

On démontre (par l'absurde) que la suite de terme général $(-1)^n$ est divergente.

Proposition 10.

Toute suite convergente est bornée.

La réciproque est fausse : la suite de terme général $(-1)^n$ est bornée et divergente.

2 Limites et opérations : preuves des résultats.

On démontre ici une partie seulement de tous les résultats ayant donnés sous forme de tableaux de cas dans le cours Suites réelles : la pratique.

Proposition 11 (Somme de deux suites ayant une limite)**.**

Soient (u_n) et (v_n) deux suites réelles, et ℓ, ℓ' deux nombres réels.

$$\text{Si } u_n \to \ell \text{ et } v_n \to \ell', \qquad \text{alors } u_n + v_n \to \ell + \ell'$$

$$\text{Si } u_n \to \ell \text{ et } v_n \to +\infty, \qquad \text{alors } u_n + v_n \to +\infty$$

Lemme 12.

Le produit d'une suite bornée et d'une suite de limite nulle est une suite de limite nulle.

Lemme 13.

Si (u_n) converge vers ℓ et $\ell > a$, alors alors $u_n > a$ à partir d'un certain rang.

Proposition 14 (Produit de deux suites ayant une limite)**.**

Soient (u_n) et (v_n) deux suites réelles, et ℓ, ℓ' deux nombres réels.

$$\text{Si } u_n \to \ell \text{ et } v_n \to \ell', \qquad \text{alors } u_n v_n \to \ell\ell'$$

$\underline{\text{Supposons } \ell > 0}$ $\qquad$ Si $u_n \to \ell$ et $v_n \to +\infty$, $\quad$ alors $u_n v_n \to +\infty$

Proposition 15 (Inverse, quotient de deux suites ayant une limite)**.**

Soient (u_n) et (v_n) deux suites réelles, et ℓ, ℓ' deux nombres réels, avec $\ell' \neq 0$.

$$\text{Si } u_n \to 0+ \text{ alors } \frac{1}{u_n} \to +\infty. \qquad\qquad \text{Si } u_n \to \ell \text{ et } v_n \to \ell', \quad \text{alors } \frac{u_n}{v_n} \to \frac{\ell}{\ell'}$$

Proposition 16 (Lemme de Cesàro (hors-programme mais très classique))**.**

Soit $(u_n)_{n\geq 1}$ une suite réelle et $\ell \in \mathbb{R}$.

Pour $n \in \mathbb{N}^*$, on note c_n la moyenne arithmétique des n premiers termes de u : $c_n = \frac{1}{n}\sum_{k=1}^{n} u_k$.

$$\text{Si } u_n \to \ell \qquad \text{alors } c_n \to \ell.$$

Quel contre exemple permet de voir que la réciproque de l'implication ci-dessus est fausse ?

3 Existence d'une limite : preuves des théorèmes.

On se concentre ici sur les preuves de résultats qui ont été abondamment utilisés dans le cours **Suites réelles : la pratique**. On y renvoie le lecteur pour les illustrations, les exemples, les corollaires...

On rappelle qu'établir un encadrement ou exploiter une monotonie sont les deux stratégies principales face à un problème de convergence de suites.

Encadrement

Théorème 17 (d'encadrement, ou des gendarmes)**.**

Soient trois suites réelles (g_n), (u_n), (d_n) telles que $\forall n \in \mathbb{N} \quad g_n \leq u_n \leq d_n$.
Si de surcroît, (g_n) et (d_n) convergent vers la même limite $\ell \in \mathbb{R}$, alors

$$(u_n) \text{ est convergente} \quad \text{et} \quad \lim u_n = \ell.$$

Proposition 18 (de minoration, de majoration)**.**

Soient (u_n) et (v_n) deux suites réelles.

- Si $\forall n \in \mathbb{N}\ u_n \leq v_n$ et $u_n \to +\infty$, alors $v_n \to +\infty$.
- Si $\forall n \in \mathbb{N}\ u_n \leq v_n$ et $v_n \to -\infty$, alors $u_n \to -\infty$.

Monotonie

Théorème 19 (de la limite monotone)**.**

Toute suite croissante et majorée converge vers une limite finie.
Toute suite croissante et non majorée diverge vers $+\infty$.

Remarque. Le théorème de la limite monotone établit ainsi une dichotomie qui n'existe pas pour les suites quelconques : une suite croissante a toujours une limite, finie ou infinie selon que la suite est majorée ou pas.

On rappelle que deux suites (u_n) et (v_n) sont dites **adjacentes** lorsqu'elles sont monotones, de monotonie contraire, et que leur différence tend vers 0.

Théorème 20 (Convergence des suites adjacentes)**.**

Deux suites adjacentes convergent vers une même limite finie.

Plus précisément, si (u_n) et (v_n) sont deux suites adjacentes (u croissante et v décroissante), alors elles convergent vers une même limite finie $\ell \in \mathbb{R}$ telle que $\forall n \in \mathbb{N}\ u_n \leq \ell \leq v_n$.

4 Passer à la limite ?

Proposition 21 (Passage à la limite d'une inégalité large)**.**

Soient u et v deux suites réelles convergentes, de limites respectives ℓ et ℓ'.

$$\text{Si } u_n \leq v_n \text{ àpdcr} \quad \text{alors } \ell \leq \ell'.$$

En particulier,
- si une suite u convergente est majorée par un réel M, alors $\lim u_n \leq M$.
- si une suite u convergente est minorée par un réel m, alors $\lim u_n \geq m$.

⚠ Les inégalités strictes ne sont **pas** conservées : $\forall n \in \mathbb{N}^* \ \frac{1}{n} > 0$ et $\lim \frac{1}{n} = 0$.

Proposition 22 (La limite comme point fixe)**.**

Soit $X \in \mathcal{P}(\mathbb{R})$, $f : X \to X$ et u une suite satisfaisant $u_0 \in X$ et $\forall n \in \mathbb{N} \ u_{n+1} = f(u_n)$.
Si (u_n) converge vers une limite ℓ, que $\ell \in X$ et que f est continue en ℓ, alors $\boxed{f(\ell) = \ell}$

Exemple 23.

Soit (u_n) la suite définie par : $\begin{cases} u_0 \in \mathbb{R} \\ \forall n \in \mathbb{N} \quad u_{n+1} = u_n - u_n^2. \end{cases}$

1. Que dire de la monotonie de u ?
2. Supposons que $u_0 \in [0, 1]$. Montrer que (u_n) est convergente déterminer $\lim u_n$.
3. Supposons que $u_0 < 0$. Montrer que $u_n \to -\infty$. Que dire si $u_0 > 1$?

Exemple 24.

Soit (u_n) une suite réelle telle que $\forall n \in \mathbb{N} \ u_{n+1} = \mathrm{ch}(u_n)$. Démontrer que (u_n) diverge.

Exemple 25.

Pour bien insister sur l'importance de l'hypothèse de **continuité** dans la proposition 22, exhiber un triplet (u, ℓ, f) tel que

$$u_n \to \ell \qquad \text{et} \qquad f(u_n) \not\longrightarrow f(\ell).$$

Exemple 26.

Écrire une fausse preuve du théorème des gendarmes en utilisant le passage à la limite.

5 Suites extraites.

Définition 27.

Soit (u_n) une suite. Une **suite extraite** de (u_n) est une suite (v_n) dont le terme général est de la forme
$$v_n = u_{\varphi(n)},$$
où $\varphi : \mathbb{N} \to \mathbb{N}$ est une application strictement croissante.

Exemple. Soit (u_n) une suite réelle.

- Les suites (u_{2n}) et (u_{2n+1}) sont des suites extraites de (u_n).
- D'autres exemples : (u_{n+1}), (u_{n^2}), (u_{2^n})...

Lemme 28.

Si φ est une application strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$ alors, $\forall n \in \mathbb{N}$ $\varphi(n) \geq n$.

Proposition 29.

Soit (u_n) une suite convergente.
Toute suite extraite de (u_n) converge vers la limite de (u_n).

Méthode (Prouver la divergence d'une suite avec deux suites extraites)**.**

Si une suite a deux suites extraites ne convergeant pas vers la même limite, alors elle diverge.

Exemple 30.

Montrer (à nouveau) que la suite de terme général $(-1)^n$ diverge.

Proposition 31.

Soit $(u_n)_{n\geq 0}$ une suite réelle et $\ell \in \mathbb{R}$

$$\text{Si } u_{2n} \to \ell \text{ et } u_{2n+1} \to \ell, \text{ alors } u_n \to \ell.$$

Théorème 32 (de Bolzano-Weierstrass)**.**

Toute suite bornée possède une suite extraite convergente.

6 Traduction séquentielle de certaines propriétés.

Définition 33.

Soit X une partie de $\mathbb{R}$. On dit que X est **dense** dans $\mathbb{R}$ si elle rencontre tout intervalle ouvert de $\mathbb{R}$. Plus précisément, si

$$\forall a < b \in \mathbb{R} \quad X \cap]a, b[\neq \emptyset.$$

Exemple. Dans le cours Nombres réels, on a démontré que $\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$ sont denses dans $\mathbb{R}$.
Expérience de pensée : sur le segment $[0, 1]$, mettons une goutte d'encre bleue sur les rationnels et une goutte d'encre jaune sur les irrationnels. Que se passe-t-il ?

Proposition 34 (Caractérisation séquentielle de la densité)**.**

Soit X une partie de $\mathbb{R}$. Il y a équivalence entre les assertions

1. X est dense dans $\mathbb{R}$.
2. Pour tout réel α, il existe une suite d'éléments de X qui tend vers α.

Preuve. Au tableau, comme d'habitude. On retiendra l'idée de travailler avec « $\varepsilon = \frac{1}{n}$ » pour créer une suite dans le sens direct. □

Corollaire 35.

Tout réel est la limite d'une suite de nombres rationnels.

Retour sur la notion de borne supérieure.

Proposition 36 (Caractérisation séquentielle de la borne supérieure)**.**

Soit A est une partie de $\mathbb{R}$ non vide et majorée et $M \in \mathbb{R}$. On a l'équivalence

$$\sup A = M \quad \Longleftrightarrow \quad \begin{cases} M \text{ est un majorant de } A \\ \exists (a_n) \in A^{\mathbb{N}} \quad a_n \to M \end{cases}$$

Preuve. Celle-ci est laissée au lecteur : on s'appuiera sur la caractérisation séquentielle de la borne supérieure, avec « $\varepsilon = \frac{1}{n}$ » pour créer une suite dans le sens direct. □

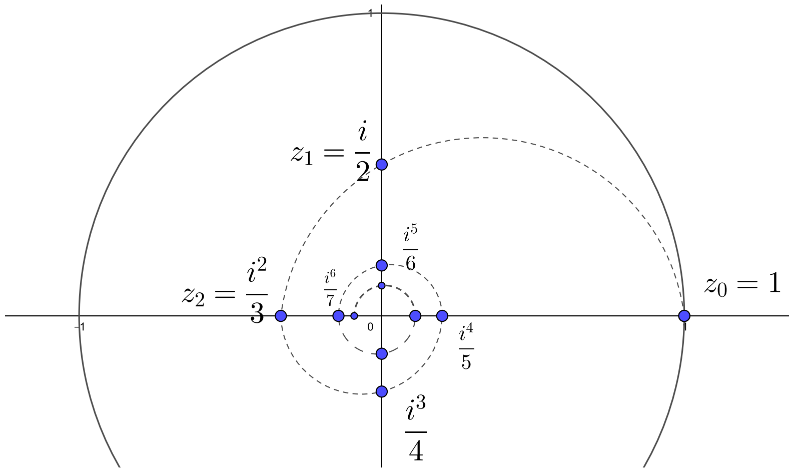
Proposition 37 (Caractérisation séquentielle des parties non majorées)**.**

Soit A est une partie de $\mathbb{R}$. On a l'équivalence

$$A \text{ est non majorée} \quad \text{ssi} \quad \exists (a_n) \in A^{\mathbb{N}} \;\; a_n \to +\infty.$$

7 Suites complexes.

Une suite complexe est une application de $\mathbb{N}$ dans $\mathbb{C}$. Ci-dessous, en confondant un point du plan et son affixe, une représentation de $z : n \mapsto \frac{i^n}{n+1}$. La spirale, décorative, permet de mieux percevoir la dynamique, le temps discret n étant "caché" dans cette représentation.



Définition 38 (Le module remplace la valeur absolue)**.**

Soit $(u_n)_{n\geq 0} \in \mathbb{C}^{\mathbb{N}}$ et $\ell \in \mathbb{C}$. On dit que (u_n) **converge** vers ℓ et on note $u_n \to \ell$ si

$$\forall \varepsilon > 0 \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad |u_n - \ell| \leq \varepsilon.$$

Rappelons que la distance entre deux nombres complexes est donnée par le module de leur différence. Ainsi, pour $z, \ell \in \mathbb{C}$ et $\varepsilon > 0$, on rappelle qu'écrire $|z - \ell| \leq \varepsilon$ équivaut à écrire que z appartient au *disque* de centre ℓ et de rayon ε.

Proposition 39.

$$\forall u \in \mathbb{C}^{\mathbb{N}} \quad \forall \ell \in \mathbb{C} \qquad u_n \to \ell \iff \begin{cases} \mathrm{Re}(u_n) \to \mathrm{Re}(\ell) \\ \mathrm{Im}(u_n) \to \mathrm{Im}(\ell) \end{cases}$$

Reste vrai avec des suites à valeurs complexes :

- Les résultats sur la limite d'une somme, d'un produit.
- Une limite usuelle : si $z \in \mathbb{C}$ est tel que $|z| < 1$, alors $z^n \to 0$.
- L'idée que pour prouver qu'une suite de nombres complexes tend vers 0, on peut écraser son module par une suite qui tend vers 0.
- Toute suite de nombres complexes qui converge vers une limite finie est bornée (c'est-à-dire que la suite des modules est majorée).
- Bolzano-Weierstrass : de toute suite de nombres complexes bornée (majorée en valeur absolue), on peut extraire une suite convergente (preuve instructive : « double-extraction »).

À oublier en revanche : tous les arguments à base d'encadrement ou de monotonie : on rappelle que dans $\mathbb{C}$, on ne dispose pas d'une relation d'ordre.

Preuves

Preuve de la proposition 16. Soit $n \in \mathbb{N}^*$. Commençons par écrire ℓ comme une moyenne : $\ell = \frac{1}{n} \sum_{k=1}^{n} \ell$.
On a alors,

$$c_n - \ell = \frac{1}{n} \sum_{k=1}^{n} u_k - \frac{1}{n} \sum_{k=1}^{n} \ell = \frac{1}{n} \sum_{k=1}^{n} (u_k - \ell).$$

Prenons la valeur absolue :

$$|c_n - \ell| = \frac{1}{n} \left| \sum_{k=1}^{n} (u_k - \ell) \right| \leq \frac{1}{n} \sum_{k=1}^{n} |u_k - \ell| \qquad \text{(inégalité triangulaire)}$$

Puisque $u_n \to \ell$ et que $\frac{\varepsilon}{2} > 0$, la définition de la convergence de la suite u donne l'existence de $n_0 \in \mathbb{N}^*$ tel que

$$\forall k \geq n_0 \quad |u_k - \ell| \leq \frac{\varepsilon}{2}.$$

Reprenons la majoration ci-dessus avec en supposant que $n \geq n_0$. La relation de Chasles donne

$$|c_n - \ell| \leq \frac{1}{n} \sum_{k=1}^{n_0 - 1} |u_k - \ell| + \frac{1}{n} \sum_{k=n_0}^{n} |u_k - \ell|.$$

On sait que pour tout $k \geq n_0$, $|u_k - \ell| \leq \frac{\varepsilon}{2}$. Sommons ces inégalités :

$$\frac{1}{n} \sum_{k=n_0}^{n} |u_k - \ell| \leq \frac{1}{n} \sum_{k=n_0}^{n} \frac{\varepsilon}{2} = (n - n_0 + 1) \cdot \frac{\varepsilon}{2}.$$

On obtient bien

$$|c_n - \ell| \leq \frac{1}{n} \sum_{k=1}^{n_0 - 1} |u_k - \ell| + \frac{n - n_0 + 1}{n} \cdot \frac{\varepsilon}{2}.$$

La somme $\sum_{k=1}^{n_0-1} |u_k - \ell|$ est une *constante* indépendante de n, qu'on peut noter C.
Remarquons aussi que pour tout $n \in \mathbb{N}^*$, $\frac{n - n_0 + 1}{n} \leq 1$. On obtient donc que pour tout $n \geq n_0$, $|c_n - \ell| \leq \frac{C}{n} + \frac{\varepsilon}{2}$.
Puisque $\frac{C}{n} \to 0$, il existe $n_1 \in \mathbb{N}^*$ tel que $\frac{C}{n} \leq \frac{\varepsilon}{2}$. Posons alors $N = \max(n_0, n_1)$. On a

$$\forall n \geq N \quad |c_n - \ell| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Ceci achève de prouver que $c_n \longrightarrow \ell$. $\square$

Proposition 40 (des segments emboîtés, bonus hors-programme)**.**

Soit $(I_n)_{n\geq 1}$ une suite de segments de $\mathbb{R}$. On note, pour tout $n \in \mathbb{N}$ $I_n = [a_n, b_n]$.
On suppose que ces segments sont <u>emboités</u>, c'est-à-dire que pour tout entier $n \geq 1$, $I_{n+1} \subset I_n$.
Alors il existe au moins un réel qui appartient à tous les segments :

$$\bigcap_{n\geq 1} I_n \neq \emptyset.$$

De plus, si la suite $(b_n - a_n)$ tend vers 0, l'intersection $\bigcap_{n\geq 1} I_n$ est un singleton.

Preuve de la proposition 40.
• Soit (I_n) une suite de segments emboîtés, et les suites (a_n) et (b_n) telles que $\forall n \in \mathbb{N}$ $I_n = [a_n, b_n]$. Pour $n \in \mathbb{N}$, l'inclusion $I_{n+1} \subset I_n$ amène $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$. La suite (a_n) est croissante, majorée par b_0 donc converge vers un réel α. La suite (b_n) est décroissante, minorée par a_0 donc converge vers un réel β. *[On retrouve les arguments utilisés dans la preuve du théorème de convergence des suites adjacentes. C'est encore plus facile ici puisque le fait que (a_n) reste inférieure à (b_n) nous est donné par l'énoncé.]* Par stabilité des inégalités larges, $\alpha \leq \beta$ et même, $\forall n \in \mathbb{N}$ $a_n \leq \alpha \leq \beta \leq b_n$ d'où $[\alpha, \beta] \subset I_n$. Puisque $[\alpha, \beta]$ est inclus dans tous les I_n, il est inclus dans leur intersection (la convexité est une propriété stable par intersection)

$$[\alpha, \beta] \subset \bigcap_{n=0}^{+\infty} I_n.$$

Ainsi, l'intersection est bien non vide.

• Supposons maintenant que $(b_n - a_n)$ tend vers 0. Par unicité de la limite, $\beta - \alpha = 0$. Notons x la valeur commune de α et β. On sait déjà que $x \in \bigcap_{n=1}^{+\infty} I_n$. Soit réciproquement un élément y dans $\bigcap_{n=1}^{+\infty} I_n$. Pour tout $n \in \mathbb{N}$, $y \in I_n$ donc $a_n \leq y \leq b_n$. En passant à la limite, $x \leq y \leq x$ d'où $y = x$. On vient bien de montrer que l'intersection des segments I_n était réduite à $\{x\}$. □

Proposition 41 (bonus hors-programme)**.**

$\mathbb{R}$ n'est pas dénombrable.

Plus précisément, $\mathbb{R}$ ne saurait s'écrire comme l'ensemble des termes d'une suite réelle.

Preuve de la proposition 41. La preuve classique par procédé diagonal de Cantor repose sur l'existence d'un développement décimal pour tout réel (fin d'année : cours sur les séries). La preuve suivante s'appuie sur le théorème des segments emboîtés.
Raisonnons par l'absurde et supposons que $\mathbb{R}$ peut s'écrire comme l'ensemble des termes d'une suite (x_n) :

$$\mathbb{R} = \{x_0, x_1, x_2 \dots\}.$$

Considérons le segment $[0, 1]$ que l'on découpe en trois sous-segments $[0, \frac{1}{3}]$, $[\frac{1}{3}, \frac{2}{3}]$ et $[\frac{2}{3}, 1]$. Prenons x_0 : il ne peut pas se trouver dans les trois segments à la fois *[Si on avait coupé en deux seulement, il pouvait encore se trouver dans les deux à la fois... au milieu !]* L'un des trois segments (au moins) ne contient x_0 ; notons I_0 un tel segment. Coupons-le en trois : l'une des trois parties ne contient pas x_1 : notons I_1 une telle partie. On a donc $I_1 \subset I_0$ et I_1 ne contient ni x_0, ni x_1. En itérant le procédé, on construit une suite de segments emboîtés (I_n) tels que pour n fixé, I_n ne contient aucun des nombres. $x_0, x_1, \dots, x_n$. Pour n donné, $x_n \notin I_n$ donc $x_n \notin \bigcap_{n\geq 1} I_n$. Ainsi, $\bigcap_{n\geq 1} I_n$ ne contient aucun des x_n donc par hypothèse ne contient aucun nombre réel : l'intersection de nos segments emboîtés est vide ! Ceci est en contradiction avec le théorème des segments emboîtés : on tient notre absurdité. □

Exercices

On rappelle que de nombreux exercices ont été proposés dans le chapitre *Suites, la pratique.*

Encadrement et monotonie : deux exercices de plus

$\boxed{\textbf{17.1}}$ **[♦♦◊]** Soit (u_n) une suite de réels non nuls telle que $\dfrac{u_{n+1}}{u_n} \to 0$.
Montrer que (u_n) converge et préciser sa limite.

$\boxed{\textbf{17.2}}$ **[♦♦◊]** Soient (u_n) et (v_n) deux suites définies par $u_0 > v_0 > 0$ et

$$u_{n+1} = \frac{u_n + v_n}{2}; \quad v_{n+1} = \frac{2u_n v_n}{u_n + v_n}.$$

Montrer que ces deux suites convergent vers une limite commune.
En examinant la suite $(u_n v_n)$, exprimer cette limite en fonction de u_0 et v_0.

Exercices *avec epsilon.*

$\boxed{\textbf{17.3}}$ **[♦◊◊]** Montrer qu'une suite d'entiers qui converge est stationnaire.

$\boxed{\textbf{17.4}}$ **[♦♦◊]** Soit (u_n) une suite réelle. Prouver l'équivalence

$$u_n \to 0 \iff \frac{u_n}{1+|u_n|} \to 0.$$

$\boxed{\textbf{17.5}}$ **[♦♦♦]** <u>Cesáro généralisé</u>
Soit $(u_n)_{n\in\mathbb{N}^*}$ une suite de nombres réels et $\ell \in \mathbb{R}$.

Soit $(a_n)_{n\in\mathbb{N}^*}$ une suite de nombres réels strictement positifs telle que $\sum\limits_{k=1}^{n} a_k \underset{n\to+\infty}{\longrightarrow} +\infty$. Montrer que

$$\text{Si } u_n \underset{n\to+\infty}{\longrightarrow} \ell \qquad \text{alors } \frac{\sum\limits_{k=1}^{n} a_k u_k}{\sum\limits_{k=1}^{n} a_k} \underset{n\to+\infty}{\longrightarrow} \ell.$$

Suites extraites.

$\boxed{\textbf{17.6}}$ **[♦♦◊]** Soit $u \in \mathbb{R}^{\mathbb{N}}$.
Montrer que $(|u_n|)$ ne tend pas vers $+\infty$ si et seulement si u admet une suite extraite convergente.

$\boxed{\textbf{17.7}}$ **[♦♦◊]** Soit (u_n) une suite telle que (u_{2n}), (u_{2n+1}) et (u_{3n}) sont convergentes.
Montrer que (u_n) est convergente.

$\boxed{\textbf{17.8}}$ **[♦♦♦]** Soient $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ deux suites d'entiers telles que

$$\forall n \in \mathbb{N}\ b_n > 0 \qquad \frac{a_n}{b_n} \to \ell \quad \text{et} \quad \ell \notin \mathbb{Q}.$$

Montrer que $b_n \to +\infty$.

$\boxed{\textbf{17.9}}$ **[♦♦♦]** On veut montrer que la suite de terme général $\sin(n)$ diverge.
On note $u_n = \sin(n)$. On raisonne par l'absurde en supposant que (u_n) est convergente, de limite ℓ.

1. En considérant $\sin(n+1) - \sin(n-1)$, montrer que $(\cos n)_{n\in\mathbb{N}}$ tend vers 0.
2. En déduire une contradiction.

$\boxed{\textbf{17.10}}$ **[♦♦♦]** Démontrer la divergence de la suite de terme général $\sin(\ln(n))$.

Arithmétique dans $\mathbb{Z}$

1 Divisibilité dans $\mathbb{Z}$.

1.1 Diviseurs et multiples.

Définition 1.

Soit $(a, b) \in \mathbb{Z}^2$. On dit que b **divise** a (on note $b \mid a$) s'il existe un entier $k \in \mathbb{Z}$ tel que $a = kb$.
Si b divise a, on dit encore que b est un **diviseur** de a ou encore que a est un **multiple** de b.

Proposition 2 (Faits immédiats)**.**

Tous les entiers divisent 0 et 1 divise tous les entiers. Ajoutons que pour $(a, b, c) \in \mathbb{Z}^3$,

1. Si b est un diviseur de a et si $a \neq 0$, alors $|b| \leq |a|$.
2. Si $c \mid a$ et $c \mid b$, alors $c \mid au + bv$, pour tous u et v dans $\mathbb{Z}$.
   En particulier, si c divise a et b, il divise aussi $a + b$ et $a - b$.

Notation (locale).

L'ensemble des diviseurs *positifs* de a sera noté dans ce cours

$$\mathcal{D}(a) = \{b \in \mathbb{N} : b \mid a\}$$

Par exemple, on a $\mathcal{D}(12) = \{1, 2, 3, 4, 6, 12\}$. Pour $a \in \mathbb{Z}$, il est clair que $\mathcal{D}(-a) = \mathcal{D}(a)$.

Proposition 3.

1. Si a est un entier relatif non nul, alors $\mathcal{D}(a)$ est un ensemble fini et son maximum est $|a|$.
2. $\mathcal{D}(0) = \mathbb{N}$.

Notation.

L'ensemble des multiples de a dans $\mathbb{Z}$ est noté

$$a\mathbb{Z} = \{ak, k \in \mathbb{Z}\}.$$

On peut écrire une relation de divisibilité à l'aide des ensembles de multiples :

$$b \mid a \iff a\mathbb{Z} \subset b\mathbb{Z}.$$

On se souvient que, définie sur $\mathbb{N}$, divise était une relation d'ordre. Ce n'est plus le cas dans $\mathbb{Z}$.

Proposition 4.

Sur $\mathbb{Z}$, la relation *divise* est réflexive, transitive, mais pas antisymétrique. On a

$$\forall (a, b) \in \mathbb{Z}^2 \qquad (a \mid b \text{ et } b \mid a) \iff (a = b \ \text{ ou } \ a = -b).$$

Dans ce cas où ($a \mid b$ et $b \mid a$) on dit que a et b sont **associés**. On a facilement que

$$(a = \pm b) \iff \mathcal{D}(a) = \mathcal{D}(b) \iff a\mathbb{Z} = b\mathbb{Z}.$$

1.2 Division euclidienne.

Théorème 5.

Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

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

Proposition 6.

Soit a et b deux entiers relatifs (b non nul).
L'entier b divise a si et seulement le reste dans la division euclidienne de a par $|b|$ est nul.

1.3 Congruences.

Définition 7.

Soit $n \in \mathbb{Z}$. On dit que deux entiers relatifs sont **congrus modulo** n, ce que l'on note $a \equiv b$ $[n]$ s'il existe un entier relatif k tel que $a = b + kn$.

Proposition 8 (Propriétés des relations de congruence dans $\mathbb{Z}$)**.**

Soit $n \in \mathbb{Z}$.

1. La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$ (*réflexive, symétrique et transitive*).
2. $\forall a \in \mathbb{Z} \quad n \mid a \iff a \equiv 0$ $[n]$. En particulier, $n \equiv 0$ $[n]$.
3. Compatibilité avec les sommes et produits

$$\forall (a, b, a', b') \in \mathbb{Z}^4 \quad \begin{cases} a \equiv b & [n] \\ a' \equiv b' & [n] \end{cases} \implies \begin{cases} a + a' \equiv b + b' & [n] \\ a \times a' \equiv b \times b' & [n]. \end{cases}$$

La compatibilité avec le produit amène, par simple récurrence,

$$\forall (a, b) \in \mathbb{Z}^2 \quad \forall \ell \in \mathbb{N} \qquad a \equiv b\ [n] \implies a^\ell \equiv b^\ell\ [n].$$

Proposition 9 (Classes de congruence)**.**

Soit $n \in \mathbb{N}^*$.

1. Pour tout $a \in \mathbb{Z}$, il existe un unique $r \in [\![0, n-1]\!]$ tel que $a \equiv r$ $[n]$.
   L'entier r est le reste de la division euclidienne de a par n.
2. Il y a exactement n classes d'équivalences pour la relation de congruence modulo n.
   Ce sont les classes de $0, 1, \ldots n-1$.

Exemple 10 (Multiples de 3)**.**

— Déterminer les entiers naturels n tels que 3 divise $2^n + 1$.
— Démontrer qu'un entier naturel est un multiple de 3 si et seulement si la somme de ses chiffres (en écriture décimale) est un multiple de 3. Idem en remplaçant 3 par 9.

1.4 Nombres premiers.

Définition 11.

Un entier $p \in \mathbb{N} \setminus \{0, 1\}$ est dit **premier** si ses seuls diviseurs positifs sont 1 et p.

Exemples. 2, 3, 5, 7, 11, 13...

Exemple 12 (*Two is the oddest prime*)**.**

Le nombre 2 est le seul entier premier et pair.

Proposition 13.

Tout entier naturel supérieur ou égal à 2 admet un diviseur premier.

Puisque tout nombre non premier possède un diviseur premier, on comprend vite que tout entier s'écrit comme un produit de nombres premiers. Ainsi, les nombres premiers sont comme les atomes de l'arithmétique : insécables, et briques élémentaires pour construire les autres nombres. Cette intuition deviendra un théorème dans la partie 4 de ce cours.

On peut affiner « quantitativement » le résultat précédent.

Proposition 14.

Pour tout entier naturel n non premier et supérieur à 2 admet un diviseur premier inférieur à $\sqrt{n}$.

Application : crible d'Eratosthène. Un nombre *non* premier inférieur à 100 a d'après ce qui précède un diviseur premier inférieur à 10. Ainsi, une fois éliminés de la grille ci-dessous tous les multiples (non triviaux) de 2, 3, 5 et 7, il ne restera que les entiers premiers inférieurs à 100.

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

Théorème 15 (d'Euclide)**.**

Il existe une infinité de nombres premiers.

2 PGCD et PPCM.

2.1 PGCD de deux entiers.

Soient a et b deux entiers relatifs. L'ensemble $\mathcal{D}(a) \cap \mathcal{D}(b)$ est celui de leurs diviseurs communs.
Si l'un des deux entiers a et b est non nuls, l'un des deux ensembles $\mathcal{D}(a)$ ou $\mathcal{D}(b)$ est fini, et $\mathcal{D}(a) \cap \mathcal{D}(b)$ est une partie de $\mathbb{Z}$ majorée par $\max(|a|, |b|)$.

Définition 16 (Le PGCD : un maximum pour $\leq$)**.**

Soient a et b deux entiers relatifs.

- Si $(a, b) \neq (0, 0)$, on appelle **Plus Grand Commun Diviseur** de a et b, et on note $a \wedge b$ ou encore $\mathrm{PGCD}(a, b)$ le plus grand entier qui divise a et b.
- Si $a = b = 0$, on pose $a \wedge b = 0$.

Remarque. Par définition, pour $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$, on a

$$a \wedge b = \max\left(\mathcal{D}(a) \cap \mathcal{D}(b)\right),$$

où le max est compris pour l'ordre naturel $\leq$ sur les entiers relatifs.

Exemple.
Calculer $\mathrm{PGCD}(12, 28)$ en écrivant les ensembles de diviseurs (*il faudra proposer une méthode plus efficace !*)

Proposition 17 (Propriétés élémentaires du PGCD)**.**

Soient a et b deux entiers relatifs.

1. Le PGCD de a et b est un entier naturel.
2. $a \wedge b = b \wedge a = (-a) \wedge b = a \wedge (-b) = (-a) \wedge (-b)$.
3. Si b divise a et $a \in \mathbb{N}^*$ alors $a \wedge b = a$.
4. *Le cas de zéro.* Si $a \in \mathbb{N}$, alors $a \wedge 0 = a$.

Théorème 18 (Caractérisation du PGCD par une relation de Bézout)**.**

Soient a et b deux entiers relatifs dont l'un au moins est non nul.

$$\exists (u, v) \in \mathbb{Z}^2 \quad au + bv = a \wedge b.$$

L'égalité ci-dessus est appelée une **relation de Bézout**.
Le couple (u, v) peut-être désigné comme un couple de *coefficients de Bézout*, il n'est pas unique.

$\boxed{a \wedge b \text{ est le plus petit entier naturel non nul qui s'écrit sous la forme } au + bv, \text{ avec } (u, v) \in \mathbb{Z}^2.}$

Remarque. Lorsque $a = b = 0$, on peut aussi écrire une relation de Bézout (tout couple (u, v) convient !) mais le PGCD vaut alors 0 et l'assertion encadrée devient fausse.

Proposition 19 (Les diviser tous les deux, c'est diviser leur PGCD)**.**

Soit $(a,b) \in \mathbb{Z}^2$. Alors
$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b).$$
En français : les diviseurs communs de a et b sont exactement les diviseurs de leur PGCD.

Corollaire 20 (Le PGCD : un maximum pour la relation $|$)**.**

Le PGCD de deux entiers naturels a et b est le *plus grand* diviseur commun de a et b pour divise, relation d'ordre sur $\mathbb{N}$.

Plus précisément, pour a et b deux entiers naturels, on a

1. $a \wedge b \in \mathcal{D}(a) \cap \mathcal{D}(b)$
   i.e. $a \wedge b$ *est un diviseur commun de* a *et* b.
2. $\forall \delta \in \mathcal{D}(a) \cap \mathcal{D}(b) \quad \delta \in \mathcal{D}(a \wedge b)$
   i.e. $a \wedge b$ *est le plus grand des diviseurs communs positifs* *<u>au sens de la relation d'ordre divise</u>*.

Proposition 21.

$$\forall (a,b) \in \mathbb{Z}^2, \quad \forall k \in \mathbb{Z}, \quad \mathrm{PGCD}\,(ka, kb) = |k| \cdot \mathrm{PGCD}(a,b).$$

2.2 Calculs effectifs : l'algorithme d'Euclide.

Proposition 22 (Réduction du problème)**.**

Soit $(a,b,c,q) \in \mathbb{Z}^4$ tel que $a = bq + c$.
Alors $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(b) \cap \mathcal{D}(c)$. En particulier, $a \wedge b = b \wedge c$.

On rappelle que si $(a,b) \in \mathbb{Z}^2$, on a $a \wedge b = |a| \wedge |b|$. C'est donc sans perte de généralité qu'on présente ci-dessous l'algorithme d'Euclide pour des entiers naturels.

Théorème 23 (Algorithme d'Euclide)**.**

Soit $(a,b) \in \mathbb{N}^2$, $b \neq 0$.

- On note $r_0 = a$ et $r_1 = b$.
- Tant qu'il existe $i \in \mathbb{N}^*$ tel que r_i est non nul, on définit r_{i+1} comme le reste dans la division euclidienne de r_{i-1} par r_i.

Cet algorithme termine : il existe $p \in \mathbb{N}^*$ tel que $r_1, \ldots, r_p$ sont non nuls et $r_{p+1} = 0$. Alors,
$$\boxed{a \wedge b = r_p}.$$

Une exécution ressemble à ça :

$$\begin{aligned}
\overbrace{r_0}^{=a} &= \overbrace{r_1}^{=b} q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
&\dots \\
r_{p-2} &= r_{p-1} q_p + \boxed{r_p} \longleftarrow a \wedge b \\
r_{p-1} &= r_p q_{p+1} + 0
\end{aligned}$$

Algorithme 24 (Algorithme d'Euclide)**.**

En Python :

```
def PGCD(a,b):
     while b!=0:
          a,b=b,a%b    # a%b : reste dans la div.eucl. de a par b
     return a
```

En OCaml :

```
let rec pgcd a b =
    if b = 0 then a
    else pgcd b (a mod b)    (* (a mod b) : reste dans la div.eucl. de a par b *)
```

Exemple 25 (Éxécution de l'algorithme d'Euclide)**.**

Calculer le PGCD de 342 et 95 puis donner $\mathcal{D}(342) \cap \mathcal{D}(95)$.

Méthode (Algorithme d'Euclide étendu)**.**

Pour $a, b \in \mathbb{N}$ avec $b \neq 0$, on note $r_0, \dots, r_p$ la suite des restes écrits en exécutant l'algorithme d'Euclide, avec $p \in \mathbb{N}^*$ le rang du dernier reste non nul. On rappelle : $r_0 = a$, $r_1 = b$ et $r_p = a \wedge b$.

Pour tout $i \in [\![1, p]\!]$

$$\exists (u_i, v_i) \in \mathbb{Z}^2 \quad au_i + bv_i = r_i.$$

C'est vrai en particulier pour $i = p$: (u_p, v_p) est un couple de coefficients de Bézout pour r_p, le PGCD de a et b.

Les coefficients (u_i, v_i) se calculent de proche en proche, en *remontant* l'algorithme de Bézout (voir exemple ci-après).

Exemple 26 (Éxécution de l'algorithme d'Euclide étendu)**.**

Calculer $118 \wedge 24$ et donner une relation de Bézout pour ce PGCD.

2.3 PPCM de deux entiers.

Soient a et b deux entiers relatifs. L'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ est celui de leurs multiples communs.
Si a et b sont non nuls, son intersection avec $\mathbb{N}^*$ est non vide puisqu'elle contient au moins $|a| \cdot |b|$.

Définition 27 (Le PPCM : un minimum pour $\leq$).

Soient a et b deux entiers relatifs.

- Si a et b sont non nuls, on appelle **Plus Petit Commun Multiple** de a et b, noté $a \vee b$, ou encore $\text{PPCM}(a, b)$, le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$.
- Si a ou b vaut 0, on pose $a \vee b = 0$.

Par exemple, le PPCM de 12 et 16 vaut 48. Si $a \in \mathbb{Z}$, alors $a \wedge 1 = |a|$.

Proposition 28.

Pour tout couple d'entiers relatifs $(a, b) \in \mathbb{Z}^2$,

$$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}.$$

Corollaire 29 (Le PPCM : un minimum pour la relation $|$).

Pour deux entiers naturels a et b non nuls, le PPCM est le *plus petit* diviseur commun de a et b pour divise, relation d'ordre sur $\mathbb{N}$.

Plus précisément, pour a et b deux entiers naturels non nuls, on a

1. $a \mid a \vee b$ et $b \mid a \vee b$, *(le PPCM est un multiple commun)*
2. $\forall \mu \in \mathbb{Z} \quad (a \mid \mu \text{ et } b \mid \mu) \Longrightarrow a \vee b \mid \mu$, *(tout multiple commun est multiple du PPCM).*

Proposition 30.

$$\forall (a, b) \in \mathbb{Z}^2 \quad \text{PGCD}(a, b) \times \text{PPCM}(a, b) = |a \times b|.$$

2.4 Extension à un nombre fini d'entiers.

Définition 31.

Soit $n \in \mathbb{N}^*$ et $(a_1, \ldots, a_n) \in \mathbb{Z}^n \setminus \{(0, \ldots, 0)\}$.
Le plus grand diviseur positif commun à $a_1, \ldots, a_n$ est appelé leur **PGCD** et noté

$$a_1 \wedge \cdots \wedge a_n.$$

On convient que le PGCD de n entiers nuls vaut 0.

Les deux propositions ci-après se démontrent comme dans le cas $n = 2$ traité plus haut.

Proposition 32 (Relation de Bézout)**.**

Soit $n \in \mathbb{N}^*$ et $(a_1, \dots, a_n) \in \mathbb{Z}^n \setminus \{(0, \dots, 0)\}$.

$$\exists (u_1, \dots, u_n) \in \mathbb{Z}^n \quad a_1 \wedge \dots \wedge a_n = a_1 u_1 + \dots + a_n u_n.$$

Une telle égalité est appelée **relation de Bézout**.

$a_1 \wedge \dots \wedge a_n$ est le plus petit entier strictement positif s'écrivant comme une combinaisons linéaire de Bézout des entiers $a_1, \dots, a_n$.

Proposition 33 (Les diviser tous, c'est diviser leur PGCD)**.**

Soit $n \in \mathbb{N}^*$ et $(a_1, \dots, a_n) \in \mathbb{Z}^n$. On a

$$\bigcap_{k=1}^{n} \mathcal{D}(a_k) = \mathcal{D}(a_1 \wedge \dots \wedge a_n).$$

Lemme 34 (Associativité du PGCD)**.**

Soit $n \in \mathbb{N}^*$ et $a_1, \dots, a_{n+1}$ des entiers relatifs. Alors,

$$a_1 \wedge \dots \wedge a_n \wedge a_{n+1} = (a_1 \wedge \dots \wedge a_n) \wedge a_{n+1}.$$

Preuve. Notons

$$d_n = a_1 \wedge \dots \wedge a_n, \qquad d_{n+1} = a_1 \wedge \dots \wedge a_n \wedge a_{n+1} \quad \text{et} \quad d'_{n+1} = d_n \wedge a_{n+1}.$$

D'une part, d'_{n+1} divise d_n donc divise $a_1, \dots, a_n$. Comme il divise aussi a_{n+1}, c'est un diviseur commun à $a_1, \dots, a_{n+1}$: d'_{n+1} divise leur PGCD d_{n+1}.

D'autre part, d_{n+1} divise $a_1, \dots, a_n$ donc divise leur PGCD d_n. Il divise aussi a_{n+1} donc divise $d_n \wedge a_{n+1}$, c'est-à-dire divise d'_{n+1}.

Ceci amène que d_{n+1} et d'_{n+1} sont associés, et donc égaux car positifs.

□

Proposition 35.

$$\forall (a_1, \dots, a_n) \in \mathbb{Z}^n, \quad \forall k \in \mathbb{Z}, \quad \mathrm{PGCD}\,(ka_1, \dots, ka_n) = |k| \cdot \mathrm{PGCD}(a_1 \dots, a_n).$$

Preuve. Récurrence sur n en utilisant l'associativité du PGCD. □

3 Entiers premiers entre eux.

3.1 Couples d'entiers premiers entre eux.

Définition 36.

On dit que deux entiers sont **premiers entre eux** si leur PGCD est égal à 1.

Ainsi, deux entiers sont premiers entre eux si et seulement leurs seuls diviseurs communs sont 1 et -1.
Si deux entiers sont premiers entre eux, au moins l'un d'entre eux est non nul.

On remarquera que la notion d'entiers *premiers entre eux* est définie sans recours aux *nombres premiers*.

Exemple. Deux entiers consécutifs sont toujours premiers entre eux.

Proposition 37.

Deux entiers naturels non nuls a et b sont premiers entre eux si et seulement si $a \vee b = |ab|$.

Proposition 38 (se ramener à deux entiers premiers entre eux)**.**

Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ et $d = a \wedge b$.
Si a' et b' sont les deux entiers relatifs tels que $a = da'$ et $b = db'$, alors $a' \wedge b' = 1$.

Soit $(p, q) \in \mathbb{Z} \times \mathbb{Z}^*$. Notons $d = p \wedge q$. Il existe $(p', q') \in \mathbb{Z} \times \mathbb{Z}^*$ tels que $p = dp'$, $q = dq'$ et $p' \wedge q' = 1$. On a

$$\frac{p}{q} = \frac{dp'}{dq'} = \frac{p'}{q'}.$$

Puisque p' et q' sont sans facteur commun non trivial, on dit que l'écriture $\frac{p'}{q'}$ est **irréductible**.

Théorème 39 (de Bézout)**.**

$$\forall (a, b) \in \mathbb{Z}^2 \qquad a \wedge b = 1 \iff \exists (u, v) \in \mathbb{Z}^2 \;\; au + bv = 1.$$

Corollaire 40.

Soit $(a, b, c) \in \mathbb{Z}^3$.

1. Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge (bc) = 1$.
2. Plus généralement, si a est premier avec chacun des m entiers $b_1, \ldots, b_m$, où $m \in \mathbb{N}^*$, alors il est premier avec leur produit $b_1 \cdots b_m$.
3. Si $a \wedge b = 1$, alors pour tout $(n, p) \in \mathbb{N}^2$, $a^n \wedge b^p = 1$.

3.2 Produit de diviseurs, diviseurs d'un produit.

Remarque naïve : 4 et 6 divisent 12 mais 4×6 ne divise pas 12.

Proposition 41 (Produit de diviseurs premiers entre eux).

$$\forall (a_1, a_2, b) \in \mathbb{Z}^3 \qquad \begin{cases} a_1 \mid b \ \text{ et } \ a_2 \mid b \\ a_1 \wedge a_2 = 1 \end{cases} \implies \quad a_1 a_2 \mid b.$$

Remarque naïve : 4 divise 2×6 mais 4 ne divise ni 2, ni 6...

Théorème 42 (Lemme de Gauss).

$$\forall (a, b, c) \in \mathbb{Z}^3 \qquad \begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \implies \quad a \mid c.$$

3.3 Le cas des diviseurs premiers.

Proposition 43.

Deux entiers relatifs sont premiers entre eux si et seulement si ils n'admettent aucun nombre premier comme diviseur commun.

Proposition 44 (Deux entiers, dont l'un est premier).

Si a est un entier et p un nombre premier, alors p divise a ou p est premier avec a.

Proposition 45 (quand un nombre premier divise un produit).

Soit $(a, b) \in \mathbb{Z}^2$ et p un nombre premier.

1. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$ (lemme d'Euclide).
2. Plus généralement, si p divise un produit d'entiers, alors p divise un des facteurs.

3.4 Famille d'entiers premiers entre eux.

Dans ce paragraphe, n est un entier naturel supérieur à 2.

Définition 46.

Des entiers relatifs $a_1, \ldots, a_n$ sont dits **premiers entre eux dans leur ensemble** si leur PGCD est égal à 1, ou de manière équivalente si 1 et -1 sont les seuls diviseurs communs.

Les entiers $a_1, \dots, a_n$ sont **deux à deux premiers entre eux** si

$$\forall (i,j) \in [\![1,n]\!]^2 \quad i \neq j \implies a_i \wedge a_j = 1.$$

Exemple 47 (*dans leur ensemble* VS *deux à deux*)**.**

Justifier que si n entiers sont premiers entre eux deux à deux, ils le sont dans leur ensemble.
Justifier que la réciproque est fausse en général.

Proposition 48 (Théorème de Bezout généralisé)**.**

Soit $(a_1, \dots, a_n) \in \mathbb{Z}^n$

$a_1, \dots, a_n$ sont premiers entre eux dans leur ensemble $\iff \exists (u_1, \dots, u_n) \in \mathbb{Z}^n \quad \sum_{i=1}^{n} a_i u_i = 1.$

Proposition 49 (Produit de diviseurs deux à deux premiers entre eux)**.**

Soient n entiers relatifs $a_1, a_2, \dots, a_n$ et un entier b.

Si tous les a_i divisent b et si les a_i sont deux à deux premiers entre eux,
alors le produit $a_1 \cdots a_n$ divise b.

3.5 Inversibilité modulo n.

Proposition 50 (Inversibilité modulo n)**.**

Soit $n \in \mathbb{N}^*$, et a un entier relatif premier avec n.
Il existe un entier relatif b tel que $ab \equiv 1\ [n]$ (la réciproque étant vraie).
Pour tous entiers x et y, on a

$$ax \equiv y\ [n] \iff x \equiv by\ [n].$$

Preuve. Supposons que a et n sont premiers entre eux. Le théorème de Bézout donne alors l'existence d'un couple (u,v) d'entiers relatifs tels que $au + nv = 1$. Posons $\boxed{b = u}$ et passons modulo n : on obtient

$$ab + 0v \equiv 1\ [n] \quad \text{i.e.} \quad ab \equiv 1\ [n]$$

ce qui montre que b est un *inverse* de a modulo n. Pour x et y dans $\mathbb{Z}$, on a

$$ax \equiv y\ [n] \iff abx \equiv by\ [n]$$

(on multiplie par b dans le sens direct, et par a dans l'autre sens). Puisque $ab \equiv 1[n]$, on a bien le résultat. □

Exemple 51.

Résoudre l'équation $7x \equiv 11\ [31]$.

Corollaire 52.

Soit $n \in \mathbb{N}^*$, ainsi que deux entiers relatifs a et y.
L'équation $ax \equiv y\ [n]$ possède une solution dans $\mathbb{Z}$ si et seulement si $a \wedge n$ divise y.
Dans le cas où une solution existe, elle est unique modulo $\frac{n}{a \wedge n}$.

Preuve. Les entiers relatifs a et y sont fixés ainsi que $n \in \mathbb{N}^*$.
• Supposons qu'il existe $x \in \mathbb{Z}$ tel que $ax \equiv y[n]$. Alors, il existe $k \in \mathbb{Z}$ tel que $y = ax + kn$.
Puisque $a \wedge n$ divise a et n, il divise y.
• Supposons réciproquement que $a \wedge n$ divise y. Notons alors $d = a \wedge n$; il existe a' et n' premiers entre eux tels que $a = da'$, $n = dn'$ et $y = dy'$. Pour $x \in \mathbb{Z}$, on a

$$ax \equiv y[n] \iff da'x \equiv dy'[dn'] \iff a'x \equiv y'[n']$$

On a pu simplifier par d : puisque n n'est pas nul, d ne l'est pas non plus.
Or, a' et n' sont premiers entre eux : il existe b' tel que $a'b' \equiv 1[n']$ et l'équation $a'x \equiv y'[n']$ possède by' comme unique solution modulo n', c'est-à-dire modulo $\frac{n}{a \wedge n}$. □

3.6 Petit théorème de Fermat.

Proposition 53.

Soit p un nombre premier.

1. Pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$.
2. $\forall (a, b) \in \mathbb{Z}^2 \quad (a+b)^p \equiv a^p + b^p\ [p]$.

Théorème 54 (Petit théorème de Fermat)**.**

Soit n un entier relatif et p un nombre premier. On a $\boxed{n^p \equiv n\ [p]}$.

Si de surcroît n n'est pas un multiple de p, alors $n^{p-1} \equiv 1\ [p]$.

Exemple 55 (Plus petit nombre de Carmichael)**.**

1. Vérifier que
$$561 \equiv 1\ [2], \qquad 561 \equiv 1\ [10], \qquad 561 \equiv 1\ [16].$$
2. Démontrer que pour tout entier n,
$$n^{561} \equiv n\ [3], \qquad n^{561} \equiv n\ [11], \qquad n^{561} \equiv n\ [17].$$
3. Démontrer que pour tout entier relatif n, on a $n^{561} \equiv n\ [561]$.
4. *Le petit théorème de Fermat n'est pas un critère de primalité.* Expliquer.

4 Théorème fondamental de l'arithmétique et applications.

4.1 Le TFAr.

Théorème 56 (Théorème fondamental de l'arithmétique)**.**

Soit n est un entier supérieur à 2. Il existe un entier naturel r non nul et r nombres premiers $p_1 < p_2 < \cdots < p_r$, ainsi que des entiers naturels non nuls $\alpha_1, \ldots, \alpha_r$ tels que

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

Cette décomposition de n en facteurs premiers (ou décomposition *primaire*) est unique.

Exemple. La décomposition primaire de trente six milliards (36×10^9) est $2^{11}\ 3^2\ 5^9$.

Remarques. Assouplissement des notations.

1. Soit $\{p_1, \ldots, p_r\}$ les nombres premiers intervenant dans la décomposition en facteurs premiers d'un entier n. Considérons $\{q_1, \ldots, q_s\}$ une famille de nombres premiers qui contient tous les p_i. Alors, on peut écrire n sous la forme
$$n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}.$$
Il suffit en effet d'autoriser les β_i à valoir 0 quand q_i ne figure pas dans la décomposition primaire de n.
2. Si a et b sont deux entiers et $\{p_1, \ldots, p_r\}$ la famille des nombres premiers intervenant dans la décomposition primaire de a *ou* dans celle de b. On peut décomposer a et b sur cette famille *commune* :
$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \quad \text{et} \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r},$$
avec $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r$ des entiers naturels *éventuellement nuls*.
3. La même idée permet de décomposer 1 sur n'importe quelle famille de nombres premiers $\{p_1, \ldots, p_r\}$:
$$1 = p_1^0 p_2^0 \cdots p_r^0.$$

4.2 Valuations p-adiques.

Définition 57.

Soit p un nombre premier et n un entier naturel non nul.
On appelle **valuation p-adique** de n, notée $v_p(n)$ l'exposant de p dans la décomposition de n en facteurs premiers (cet exposant valant 0 si p ne figure pas dans la décomposition).

Par exemple, si $n = 3^{15} \cdot 7^3 \cdot 11$, alors $v_3(n) = 15$, $v_7(n) = 3$ et $v_{11}(n) = 1$.
De plus, pour tout nombre premier $p \notin \{3, 7, 11\}$, $v_p(n) = 0$.

Proposition 58.

Soit p un nombre premier.

1. $\forall (m, n) \in (\mathbb{N}^*)^2 \quad v_p(mn) = v_p(m) + v_p(n)$.
2. $\forall n \in \mathbb{N}^*\ \forall k \in \mathbb{N} \quad v_p(n^k) = k v_p(n)$.

Exemple 59.

Soit n un entier supérieur à 2. Montrer que $\sqrt{n} \in \mathbb{Q}$ si et seulement si n est le carré d'un entier.

Proposition 60.

Soient m et n deux entiers naturels non nuls,

$$m \text{ divise } n \quad \text{si et seulement si} \quad \text{pour tout nombre premier } p,\ v_p(m) \leq v_p(n).$$

Théorème 61 (Description des diviseurs d'un entier)**.**

Soit n un entier naturel supérieur ou égal à 2, s'écrivant

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

Ses diviseurs positifs sont exactement les entiers de la forme

$$p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}, \qquad \text{avec } \forall i \in [\![1, r]\!]\ 0 \leq \beta_i \leq \alpha_i.$$

Exemple 62 (Un cas particulier important)**.**

Soit p un nombre premier et α un entier naturel non nul. Quels sont les diviseurs de p^α ?

Exemple 63.

Combien de diviseurs possède le nombre trente six milliards ?

Proposition 64 (Décomposition primaire du PGCD, du PPCM)**.**

Soient a et b deux entiers naturels non nuls, dont une décomposition sur une même famille de nombres premiers $p_1 < \cdots < p_r$ est

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \quad \text{et} \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r},$$

où les α_i et β_i sont des entiers naturels éventuellement nuls. On a alors

$$a \wedge b = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)}, \quad \text{et} \quad a \vee b = \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}.$$

De manière équivalente, pour tout nombre premier p,

$$v_p(a \wedge b) = \min\left(v_p(a), v_p(b)\right), \quad \text{et} \quad v_p(a \vee b) = \max\left(v_p(a), v_p(b)\right).$$

Exercices

Divisibilité

$\boxed{\textbf{18.1}}$ **[♦◇◇]** Soit $n \in \mathbb{N}^*$. Déterminer le reste dans la division euclidienne de $\sum_{k=1}^{n} k$ par n.

$\boxed{\textbf{18.2}}$ **[♦◇◇]** Soit $n \in \mathbb{N}$. Que vaut le PGCD de $3n+1$ et de $2n$?

$\boxed{\textbf{18.3}}$ **[♦♦◇]** Soient deux entiers relatifs a et b tels que $a^2 \mid b^2$. Montrer que $a \mid b$.

$\boxed{\textbf{18.4}}$ **[♦◇◇]** Soient a et b deux entiers strictement positifs et premiers entre eux.
Montrer que $\dfrac{\ln(a)}{\ln(b)}$ est irrationnel.

$\boxed{\textbf{18.5}}$ **[♦♦◇]** Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$.

1. Montrer que a et b sont premiers entre eux si et seulement si $a+b$ et ab sont premiers entre eux.
2. Simplifier $(a+b) \wedge (a \vee b)$.

$\boxed{\textbf{18.6}}$ **[♦♦♦]** Soient $(n, p, q) \in (\mathbb{N}^*)^3$ tel que $n \geq 2$.

1. On note r le reste de la division euclidienne de p par q.
   Montrer que $n^r - 1$ est le reste de la division euclidienne de $n^p - 1$ par $n^q - 1$.
2. En déduire que
$$(n^p - 1) \wedge (n^q - 1) = n^{p \wedge q} - 1.$$

$\boxed{\textbf{18.7}}$ **[♦♦◇]** Soit $(q_1, q_2) \in \mathbb{Q}^2$.
Démontrer qu'il existe trois entiers relatifs a, b, c premiers entre eux dans leur ensemble tels que
$$q_1 = \frac{a}{c} \quad \text{et} \quad q_2 = \frac{b}{c}.$$

Nombres premiers et théorème fondamental.

$\boxed{\textbf{18.8}}$ **[♦◇◇]** Trouver un entier dont le produit des diviseurs vaut $2^{60}3^{75}$.

$\boxed{\textbf{18.9}}$ **[♦♦◇]** Soit $n \geq 1$ un entier et p un nombre premier. Soit N tel que $p^N \geq n$.

1. Soit $q \in \mathbb{N}^*$. Combien y-a-t-il de multiples de q dans $[\![1, n]\!]$?
2. Soit $k \in \mathbb{N}^*$ et $A_k = \{m \in [\![1, n]\!] \mid v_p(m) = k\}$. Calculer le cardinal de A_k.
3. En déduire que
$$v_p(n!) = \sum_{k=1}^{N} \left\lfloor \frac{n}{p^k} \right\rfloor.$$
4. Déterminer par combien de zéros se termine l'écriture décimale de 1000!.

$\boxed{\textbf{18.10}}$ **[♦♦◊]** [Nombres de Fermat]

1. Soit $(a, m) \in \mathbb{N}^2$. On suppose que $a^m + 1$ est premier et que $a \geq 2$ et $m \neq 0$.
   Montrer que a est pair et que m est une puissance de 2.
2. Pour $n \in \mathbb{N}$, on note $F_n = 2^{2^n} + 1$.
   Culture : pour tout $i \in [\![0, 4]\!]$, les nombres F_i sont premiers.
   Ceci a fait conjecturer à Fermat que tous les F_n le sont. C'est faux : F_5 est composé.
   (a) Montrer que pour tout $n \in \mathbb{N}^*$, $F_n = 2 + \prod_{k=0}^{n-1} F_k$
   (b) En déduire que si n et m sont deux entiers naturels distincts, F_n et F_m sont premiers entre eux.
   (c) Déduire de la question précédente que l'ensemble des nombres premiers est infini.

Congruences.

$\boxed{\textbf{18.11}}$ **[♦◊◊]** Soit $n \in \mathbb{N}^*$ et a, b deux entiers relatifs tels que $a \equiv b\ [n]$. Démontrer que

$$a^n \equiv b^n\ [n^2].$$

$\boxed{\textbf{18.12}}$ **[♦♦◊]** Un nombre palindrome est un nombre qui se lit indifféremment de gauche à droite ou de droite à gauche. Par exemple, 2002 et 12321 sont des nombres palindromes. Prouver qu'un nombre palindrome ayant un nombre pair de chiffres est divisible par 11

$\boxed{\textbf{18.13}}$ **[♦♦◊]** Déterminer les entiers relatifs n tels que $n^{13} \equiv n[42]$.

$\boxed{\textbf{18.14}}$ **[♦♦◊]** [Banque oraux CCINP (numéro 94)]

On considère le système (S) : $\left\{\begin{array}{lll} x & \equiv & 6 \quad [17] \\ x & \equiv & 4 \quad [15] \end{array}\right.$ dans lequel l'inconnue x appartient à $\mathbb{Z}$.

1. Déterminer une solution particulière x_0 de (S) dans $\mathbb{Z}$.
2. Résoudre alors dans $\mathbb{Z}$ le système (S).

$\boxed{\textbf{18.15}}$ **[♦♦♦]** [Progression arithmétique]

1. Montrer que tout entier naturel congru à 3 modulo 4 admet un diviseur premier congru à 3 modulo 4.
2. Démontrer qu'il existe une infinité de nombres premiers de la forme $4n + 3$ avec $n \in \mathbb{N}$.

Le théorème de la progression arithmétique (Dirichlet, 1838) énonce que si a et b sont deux entiers naturels premiers entre eux, il existe une infinité de nombres premiers de la forme $an + b$ avec n entier.

19

Structures algébriques

1 Loi de composition interne sur un ensemble.

1.1 Définitions et propriétés.

Définition 1.

On appelle **loi de composition interne** sur un ensemble E (on écrira l.c.i.) une application

$$\star : \left\{ \begin{array}{ccc} E \times E & \to & E \\ (x, y) & \mapsto & x \star y \end{array} \right. .$$

On notera que l'image de (x, y) par $\star$ est notée $x \star y$ plutôt que $\star(x, y)$.

Soit E un ensemble et $\star$ une loi de composition interne sur E.

- La loi $\star$ est dite **associative** si

$$\forall (x, y, z) \in E^3 \quad (x \star y) \star z = x \star (y \star z).$$

- De deux éléments x et y de E, on dit qu'ils **commutent** pour $\star$ lorsque $x \star y = y \star x$.
On dit que la loi $\star$ est **commutative** si deux éléments de E quelconques commutent, c'est-à-dire si

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

- On appelle **élément neutre** pour la loi $\star$ tout élément $e \in E$ tel que

$$\forall x \in E \quad x \star e = x \text{ et } e \star x = x.$$

Pourquoi *loi de composition interne* ? Grâce à $\star$, à partir d'un couple (x, y) d'éléments de E, on obtient le composé $x \star y$ qui est un élément de E : la composition s'est faite à l'intérieur de E.

Définition 2 (un peu de vocabulaire qui n'est pas dans le programme)**.**

Un couple $(E, \star)$, où E est un ensemble et $\star$ une l.c.i. sur E est appelé un **magma**.

On dit que ce magma est associatif si $\star$ est associative, commutatif si $\star$ est commutative, et **unifère** s'il existe dans E un élément neutre pour $\star$.

Si $(E, \star)$ est un magma associatif et x, y, z trois éléments de E, la définition de l'associativité donne que l'écriture $x \star y \star z$ n'est pas ambiguë. De la même manière, si t est un quatrième élément de E, on a les égalités

$$(x \star y) \star (z \star t) = ((x \star y) \star z) \star t = x \star ((y \star z) \star t) = x \star (y \star (z \star t)) = (x \star (y \star z)) \star t,$$

de sorte qu'on pourra écrire $x \star y \star z \star t$ sans ambiguïté.

Proposition 3.

Dans un magma unifère, il y a unicité de l'élément neutre.

Définition 4.

Soit $(E,\star)$ un magma. Une partie A de E est dite **stable** par $\star$ si

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

Définition 5.

Soit $(E,\star)$ un magma et A une partie de E stable par $\star$. La restriction de $\star$ à A^2 :

$$\star : \left\{ \begin{array}{ccc} A\times A & \to & A \\ (x,y) & \mapsto & x\star y \end{array} \right.$$

est une loi de composition interne sur A : on l'appelle **loi induite** par $\star$ sur A.

Exemple 6 (Ensembles de nombres)**.**

- L'addition $+$ est une loi de composition interne sur chacun des ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. Elle est associative, commutative et admet 0 pour élément neutre.
  Les parties $[0,+\infty[$ et $]-\infty,0[$ de $\mathbb{R}$ sont stables par $+$.
- La multiplication $\times$ est une l.c.i sur chacun des ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. Elle est associative, commutative et admet 1 pour élément neutre.
  Les parties $[0,+\infty[$ et $\mathbb{R}^*$ de $\mathbb{R}$ sont stables par $\times$.
- La soustraction $-$ est une loi de composition interne sur $\mathbb{Z}$ qui n'est ni associative, ni commutative et n'admet pas d'élément neutre.
  $\mathbb{N}$ est une partie de $\mathbb{Z}$ qui n'est pas stable par $-$.

Exemple 7 (Ensemble des parties)**.**

Soit E un ensemble. L'intersection $\cap$ et la réunion $\cup$ définissent des l.c.i. sur $\mathcal{P}(E)$.

- Le magma $(\mathcal{P}(E),\cap)$ est associatif, commutatif et unifère, avec E pour élément neutre.
- Le magma $(\mathcal{P}(E),\cup)$ est associatif, commutatif et unifère, avec $\emptyset$ pour élément neutre.

Exemple 8 (Ensemble de fonctions et composition)**.**

Soit E un ensemble. La composition $\circ$ est une loi de composition interne sur E^E, l'ensemble des fonctions définies sur E et à valeurs dans E.

Le magma $(E^E,\circ)$ est associatif et unifère : il admet Id_E pour élément neutre.
Si E admet au moins deux éléments, $\circ$ n'est pas commutative.

L'ensemble des fonctions injectives est une partie de E^E stable par $\circ$.
C'est aussi le cas pour l'ensemble des fonctions surjectives et pour celui des fonctions bijectives.

Définition 9 (Distributivité d'une loi par rapport à une autre)**.**

Soit E un ensemble muni de deux lois de composition internes $\oplus$ et $\otimes$.
On dit que $\otimes$ est **distributive par rapport à** $\oplus$ si

$$\forall (x,y,z) \in E^3 \quad : \quad \begin{cases} x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z) \\ (y \oplus z) \otimes x = (y \otimes x) \oplus (z \otimes x). \end{cases}$$

(Si la loi $\otimes$ n'est pas commutative, il est primordial de vérifier les deux égalités.)

Exemple 10.

- Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, la multiplication $\times$ est distributive par rapport à l'addition $+$.
- Dans $\mathcal{P}(E)$, $\cap$ est distributive par rapport à $\cup$.
- Dans $\mathcal{P}(E)$, $\cup$ est distributive par rapport à $\cap$.

1.2 Éléments symétrisables.

Définition 11.

Soit $(E, \star)$ un magma unifère d'élément neutre e, et x un élément de E.
On dit que x est **symétrisable** (ou **inversible**) s'il existe un élément x' dans E tel que

$$x \star x' = e \quad \text{et} \quad x' \star x = e.$$

Proposition-Définition 12.

Soit $(E, \star)$ un magma <u>associatif</u> et unifère d'élément neutre e.
Si x est un élément de E symétrisable, il existe un unique x' dans E tel que $x \star x' = x' \star x = e$.
On appelle cet élément le **symétrique** de x (ou son inverse), et on le note x^{-1}.

Exemples 13.

- Les inversibles du magma $(\mathbb{Z}, \times)$ sont -1 et 1.
- Les inversibles du magma $(\mathbb{R}, \times)$ sont les réels non nuls ; on a admis en effet que pour tout $x \in \mathbb{R}^*$, il existe un réel x^{-1} tel que $x \times x^{-1} = x^{-1} \times x = 1$.

Exemple 14.

Les inversibles du magma $(E^E, \circ)$ sont les bijections $f : E \to E$.
Si $f : E \to E$ est une bijection, son inverse f^{-1} est sa réciproque.

Proposition 15.

Soit $(E, \star)$ un magma associatif et unifère, et x et y deux éléments de E.

1. Si x est symétrisable, x^{-1} l'est aussi et $(x^{-1})^{-1} = x$.
2. Si x et y sont symétrisables, $x \star y$ l'est aussi et
$$(x \star y)^{-1} = y^{-1} \star x^{-1}.$$

1.3 Itérés.

On fixe pour tout ce paragraphe un magma $(E, \star)$ associatif et unifère, dont l'élément neutre est noté e.

Définition 16 (Itérés d'un élément).

Soit $x \in E$.

1. Pour $n \in \mathbb{N}$, on définit x^n par récurrence sur $n \in \mathbb{N}$.
   — On pose $x^0 = e$.
   — Pour tout $n \in \mathbb{N}$: $x^{n+1} = x^n \star x$.
2. Si x est inversible et $n \in \mathbb{N}^*$, on pose
$$x^{-n} = \left(x^{-1}\right)^n.$$

Remarque. Si $n \in \mathbb{N}^*$, x^n est donc égal à $x^n = \underbrace{x \star \ldots \star x}_{n \text{ facteurs}}$, écriture non ambiguë par associativité.

Proposition 17 (Propriétés des itérés).

$$\forall x \in E \quad \forall (m,n) \in \mathbb{N}^2 \qquad x^m \star x^n = x^{m+n} \quad \text{ et } \quad (x^m)^n = x^{mn}.$$

Si x est inversible, les identités ci-dessus sont vraies pour $(m,n) \in \mathbb{Z}^2$. En particulier,

Si x est inversible, pour $n \in \mathbb{N}$, x^n est inversible d'inverse x^{-n}.

Proposition 18 (Itérés d'éléments qui *commutent*).

Soient x et y deux éléments de E qui commutent (c'est-à-dire que $x \star y = y \star x$). Alors
$$\forall (m,n) \in \mathbb{N}^2 \quad x^m \star y^n = y^n \star x^m,$$
$$\forall n \in \mathbb{N} \quad (x \star y)^n = x^n \star y^n.$$

⚠ Les identités ci-dessus sont FAUSSES en général lorsque x et y ne commutent pas.

1.4 Notations multiplicatives et additives.

Utiliser la **notation multiplicative**, lorsqu'on travaille avec un magma $(E, \star)$ consiste à ne pas écrire $\star$ lorsqu'on calcule l'image d'un couple $(x, y) \in E^2$. Concrètement, on note alors xy à la place de $x \star y$.

Lorsqu'on travaille avec un magma associatif, commutatif et unifère, on pourra utiliser la notation $+$ pour la loi de composition interne. Le vocabulaire et les notations introduits plus haut sont alors adaptés à cette **notation additive**, comme explicité dans le tableau ci-dessous.

notation l.c.i	$\star$	$\cdot$	$+$
image de (x, y)	$x \star y$	xy	$x + y$
notation neutre	e	e	0
on dit	symétrisable	inversible	symétrisable
on dit	symétrique	inverse	opposé
notation symétrique	x^{-1}	x^{-1}	$-x$
notation itéré	x^n	x^n	nx

2 Structure de groupe.

2.1 Définition et exemples.

Définition 19.

On appelle **groupe** un magma associatif et unifère dans lequel tout élément est symétrisable.

Plus précisément, un groupe est la donnée d'un couple $(G, \star)$, où G est un ensemble et $\star$ une loi de composition interne sur G tels que

1. $\star$ est associative : $\forall (x, y, z) \in G^3 \quad (x \star y) \star z = x \star (y \star z)$.
2. il existe dans G un élément e neutre pour la loi $\star$: $\forall x \in G \quad x \star e = e \star x = x$.
3. tout élément de G est symétrisable : $\forall x \in G \quad \exists x' \in G \quad x \star x' = x' \star x = e$.

Si de surcroît $\star$ est commutative, alors le groupe $(G, \star)$ est dit **abélien** (ou commutatif).

Remarques. Soit $(G, \star)$ un groupe.

1. S'il n'y a pas d'ambiguïté sur la loi de composition interne $\star$ dont on parle, on pourra écrire avec un léger abus que « G est un groupe ».
2. Un groupe n'est jamais vide car il contient au moins son élément neutre.

Proposition 20 (Ensembles de nombres)**.**

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes abéliens.
2. $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes abéliens.

Exemple 21 (Ce ne sont pas des groupes).

1. $(\mathbb{N}, +)$ n'est pas un groupe car 1 n'est pas symétrisable : il n'a pas d'opposé dans $\mathbb{N}$.
2. $(\mathbb{Z}^*, \times)$ n'est pas un groupe car 2 n'est pas inversible dans $\mathbb{Z}^*$.
3. $(\mathbb{C}, \times)$ n'est pas un groupe car 0 n'a pas d'inverse dans $\mathbb{C}$.

Exemple 22 (Vérifier les axiomes de groupe sur une loi artificielle).

On pose $G = \mathbb{R}^* \times \mathbb{R}$. Pour $(a, b) \in G$ et $(a', b') \in G$ on définit

$$(a, b) \star (a', b') = (aa', ab' + b).$$

Montrer que $(G, \star)$ est un groupe

Définition 23.

Soit E un ensemble non vide. On appelle **permutation** de E une bijection $\sigma : E \to E$.
On note S_E l'ensemble des permutations de E.

Proposition-Définition 24.

$(S_E, \circ)$ est un groupe, appelé **groupe des permutations** de E, ou encore *groupe symétrique* de E.
Dès que E contient au moins 3 éléments, le groupe S_E n'est pas abélien.

Proposition 25 (Produit de deux groupes).

Soient $(G, \star)$ et $(G', \top)$ deux groupes. On note e le neutre de G et e' celui de G'.
Pour (x, x') et (y, y') deux éléments de $G \times G'$, on pose

$$(x, x') \heartsuit (y, y') := (x \star y, x' \top y').$$

Muni de la l.c.i. $\heartsuit$, le produit cartésien $G \times G'$ est un groupe, d'élément neutre (e, e').

Proposition 26 (Produit de n groupes).

Soient $G_1, \ldots, G_n$ n groupes (les l.c.i. étant sous-jacentes et notées multiplicativement).
Pour $(x_1, \ldots, x_n)$ et $(y_1, \ldots, y_n)$ deux éléments de $G_1 \times \cdots \times G_n$, on pose

$$(x_1, \ldots, x_n) \heartsuit (y_1, \ldots, y_n) = (x_1 y_1, \cdots, x_n y_n).$$

Muni de la l.c.i. $\heartsuit$, le produit cartésien $G_1 \times \cdots \times G_n$ est un groupe.
Son neutre est le n-uplet $(e_1, \ldots, e_n)$ où pour tout $k \in [\![1, n]\!]$, e_k est le neutre du groupe G_k.

Application : définition du groupe additif $(\mathbb{R}^n, +)$, dont le neutre est le n-uplet $(0, \cdots, 0)$.

2.2 Sous-groupes.

Définition 27.

Soit $(G, \star)$ un groupe et H une partie de G.
On dit que H est un **sous-groupe** de G si H est stable par $\star$ et si $(H, \star)$ est un groupe.

Remarque. Ci-dessus, lorsqu'on écrit $(H, \star)$, il faut comprendre que $\star$ est la *loi induite* sur H par la loi $\star$ définie sur G. Cette loi induite est bien définie car H est supposé stable par $\star$.

Exemples. Si $(G, \star)$ est un groupe, de neutre e, alors $\{e\}$ et G sont des sous-groupes de G. On pourra parler à leur sujet de *sous-groupes triviaux*.

Proposition 28 (Élément neutre et inverses dans un sous-groupe)**.**

Soit $(G, \star)$ un groupe et H un sous-groupe de G .

1. L'élément neutre du groupe H n'est autre que celui de G.
2. Soit $x \in H$. L'inverse de x dans le groupe $(H, \star)$ et celui dans le groupe $(G, \star)$ sont égaux.

Théorème 29 (Caractérisation des sous-groupes)**.**

Soit $(G, \star)$ un groupe dont l'élément neutre est noté e, et H une partie de G.
Les trois assertions suivantes sont équivalentes.

1. H est un sous-groupe de $(G, \star)$.
2. $\begin{cases} \bullet\ e \in H \\ \bullet\ \forall (x, y) \in H^2 \quad x \star y^{-1} \in H. \end{cases}$
3. $\begin{cases} \bullet\ e \in H \\ \bullet\ \forall (x, y) \in H^2 \quad x \star y \in H \\ \bullet\ \forall x \in H \quad x^{-1} \in H. \end{cases}$

Remarque. Récrivons une des équivalences ci-dessus dans le contexte où on utilise la <u>notation additive</u>. Soit $(G, +)$ un groupe dont l'élément neutre est noté 0 et H une partie de G. On a

$$H \text{ est un sous-groupe de } (G, +) \iff \begin{cases} 0 \in H \\ \forall (x, y) \in H^2 \quad x - y \in H. \end{cases}$$

Lemme 30 (Les sous-groupes sont stables par itération)**.**

Soit H un sous-groupe d'un groupe G et x un élément de H. Alors,

$$\forall p \in \mathbb{Z} \quad x^p \in H.$$

Proposition 31 (Ensembles de nombres).

1. $(\mathbb{Q},+)$ est un sous-groupe de $(\mathbb{R},+)$, qui est lui-même un sous-groupe de $(\mathbb{C},+)$.
2. $\mathbb{R}_+^*$ est un sous-groupe de $(\mathbb{R}^*,\times)$.
3. $\mathbb{U}$ et $\mathbb{U}_n$ sont des sous-groupes de $(\mathbb{C}^\star,\times)$.

Exemple 32 (Centre d'un groupe).

Soit $(G,\star)$ un groupe. On note

$$Z(G)=\{x\in G \mid \forall a\in G \quad x\star a=a\star x\}\,.$$

Montrer que $Z(G)$ est un sous-groupe de G.

Proposition 33 (Une intersection de sous-groupes est un sous-groupe).

Soient H et H' deux sous-groupes d'un groupe $(G,\star)$.
Leur intersection $H\cap H'$ est un sous-groupe de G.

Plus généralement, si $(H_i)_{i\in I}$ est une famille de sous-groupes d'un même groupe G, alors $\bigcap\limits_{i\in I} H_i$ est un sous-groupe de G.

Exemple 34 (Une union de sous-groupes n'est pas (toujours) un sous-groupe).

Montrer que $\mathbb{U}_2\cup\mathbb{U}_3$ n'est <u>pas</u> un sous-groupe de $(\mathbb{C}^*,\times)$ puis que $\bigcup\limits_{n\in\mathbb{N}^\star}\mathbb{U}_n$ en est un.

Proposition 35 (Sous-groupes de $(\mathbb{Z},+)$ (programme spé)).

Pour $n\in\mathbb{N}$, on note

$$n\mathbb{Z}=\{nk \mid k\in\mathbb{Z}\}\,.$$

Les sous-groupes de $(\mathbb{Z},+)$ sont exactement les $n\mathbb{Z}$, avec $n\in\mathbb{N}$.

Plus précisément,

1. Pour tout $n\in\mathbb{N}$, $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$.
2. Si H est un sous-groupe de $(\mathbb{Z},+)$ alors $\exists! n\in\mathbb{N} \;\; H=n\mathbb{Z}$.

Remarque. On a croisé des sous-groupes de $\mathbb{Z}$ dans le cours d'arithmétique. Si a et b sont deux entiers relatifs, on a

$$a\mathbb{Z}\cap b\mathbb{Z}=(a\vee b)\mathbb{Z} \qquad \text{et} \qquad a\mathbb{Z}+b\mathbb{Z}=(a\wedge b)\mathbb{Z},$$

où on note $a\mathbb{Z}+b\mathbb{Z}=\{au+bv \mid (u,v)\in\mathbb{Z}^2\}$ l'ensemble des combinaisons de Bézout de a et b.

2.3 Morphismes de groupes.

Définition 36.

Soient $(G, \star)$ et $(G', \top)$ deux groupes.

On appelle **morphisme de groupe** de G dans G' toute application $f : G \to G'$ telle que

$$\forall (x, y) \in G^2 \quad f(x \star y) = f(x) \top f(y).$$

Si de surcroît f est bijective, on dit qu'une telle application f est un **isomorphisme** de groupes.
Un morphisme d'un groupe G vers lui même est appelé **endomorphisme** de G.
Si un tel endomorphisme est bijectif, on parle d'**automorphisme** de G.

Définition 37.

On dit que deux groupes sont **isomorphes** s'il existe un isomorphisme du premier vers le deuxième.

Exemple 38.

- L'exponentielle réelle est un isomorphisme de groupes de $(\mathbb{R}, +)$ dans $(]0, +\infty[, \times)$.
- L'exponentielle complexe est un morphisme de groupes de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$.
- $t \mapsto e^{it}$ est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{U}, \times)$.
- Le logarithme népérien est un isomorphisme de groupes de $(]0, +\infty[, \times)$ dans $(\mathbb{R}, +)$.

Exemple 39.

Justifier que les groupes $(\mathbb{R}^2, +)$ et $(\mathbb{C}, +)$ sont isomorphes.

Proposition 40.

Soient G et G' deux groupes de neutres respectifs e et e', et $f : G \to G'$ un morphisme de groupes.

1. $f(e) = e'$.
2. $\forall x \in G \quad f(x^{-1}) = (f(x))^{-1}$.
3. $\forall x \in G \quad \forall p \in \mathbb{Z} \quad f(x^p) = (f(x))^p$.
4. Si H est un sous-groupe de G alors $f(H)$ est un sous-groupe de G'.
5. Si H' est un sous-groupe de G', alors $f^{-1}(H')$ est un sous-groupe de G.
6. Si f est un isomorphisme de G vers G', alors f^{-1} est un isomorphisme de G' vers G.

1. En notation additive, le point 2 s'écrit $\forall x \in G \quad f(-x) = -f(x)$.
2. En notation additive, le point 3 s'écrit $\forall x \in G \quad \forall p \in \mathbb{Z} \quad f(px) = pf(x)$.

Définition 41.

Soient G et G' deux groupes de neutres respectifs e et e', et $f : G \to G'$ un morphisme de groupes.

1. On appelle **noyau** de f et on note $\mathrm{Ker} f$ l'ensemble
$$\mathrm{Ker} f = \{x \in G \mid f(x) = e'\}.$$
2. On appelle **image** de f et on note $\mathrm{Im} f$ l'ensemble
$$\mathrm{Im} f = \{y \in G' \mid \exists x \in G : y = f(x)\}.$$

Proposition 42.

Soient G et G' deux groupes de neutres respectifs e et e', et $f : G \to G'$ un morphisme de groupes.

1. $\mathrm{Ker} f$ est un sous-groupe de G et
$$f \text{ est injective} \iff \mathrm{Ker} f = \{e\}.$$
2. $\mathrm{Im} f$ est un sous-groupe de G' et
$$f \text{ est surjective} \iff \mathrm{Im} f = G'.$$

3 Structure d'anneau.

3.1 Définitions et règles de calcul.

Définition 43.

On appelle **anneau** tout triplet $(A, +, \times)$, où A est un ensemble et $+$ et $\times$ des l.c.i. tels que

- $(A, +)$ est un groupe abélien, de neutre 0_A.
- $(A, \times)$ est un magma associatif et unifère, de neutre 1_A,
- $\times$ est distributive par rapport à $+$.

Les lois $+$ et $\times$ sont appelées respectivement **addition** et **multiplication** de l'anneau A.

Si de surcroît $\times$ est commutative, on dit que l'anneau A est commutatif.

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

1. Par définition des éléments neutres, $\forall a \in A \quad a + 0_A = 0_A + a = a$ et $1_A \times a = a \times 1_A = a$.
2. $(A, +)$ étant un groupe, tout élément a de A est symétrisable pour $+$, c'est-à-dire admet un opposé $-a$ tel que $a + (-a) = 0_A = (-a) + a$.
3. En revanche, tout élément de A n'est pas nécessairement symétrisable (inversible) dans $(A, \times)$ et c'est d'ailleurs ce qui empêche $(A, \times)$ d'être un groupe.
4. Généralement, A possède plus de deux éléments, sauf si $0_A = 1_A$ (A est alors réduit à $\{0_A\}$).

Exemples 44 (Ensembles de nombres).

$(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des anneaux commutatifs.

Exemple 45 (Anneau de fonctions).

On rappelle que, pour X une partie de $\mathbb{R}$, $\mathcal{F}(X,\mathbb{R})$, ensemble des fonctions définies sur X et à valeurs réelles a été muni d'une addition et d'une multiplication $+$ et $\times$ de la manière suivante :

$$\forall f,g \in \mathcal{F}(X,\mathbb{R}) \quad f+g : \left\{ \begin{array}{ccc} X & \to & \mathbb{R} \\ x & \mapsto & f(x)+g(x) \end{array} \right. \quad \text{et} \quad f \times g : \left\{ \begin{array}{ccc} X & \to & \mathbb{R} \\ x & \mapsto & f(x)g(x) \end{array} \right. .$$

Le triplet $(\mathcal{F}(X,\mathbb{R}),+,\times)$ est un anneau commutatif.
L'élément neutre pour $+$ est la fonction nulle sur X.
L'élément neutre pour $\times$ est la fonction constante sur X égale à 1.

En particulier $(\mathbb{R}^{\mathbb{N}},+,\times)$ est un anneau commutatif : celui des suites réelles.

Exemples 46 (Pas des anneaux).

- $(2\mathbb{Z},+,\times)$ n'est pas un anneau car...
- $(\mathcal{F}(\mathbb{R},\mathbb{R}),+,\circ)$ n'est pas un anneau car...

Règles de calcul. Soit $(A,+,\times)$ un anneau.

On rappelle les faits ci-dessous concernant les itérés d'un élément pour l'addition et la multiplication.

1. $(A,+)$ étant un groupe, le $n$ème itéré d'un élément a, noté na, est défini par

$$na = \underbrace{a+\ldots+a}_{n \text{ termes}} \quad \text{si } n \geq 1 \qquad na = \underbrace{(-a)+\ldots+(-a)}_{(-n) \text{ termes}} \quad \text{si } n \leq -1 \qquad \text{et} \qquad 0a = 0_A.$$

   On a aussi, pour tous $(a,b) \in A^2$ et $(p,q) \in \mathbb{Z}^2$,

$$pa+qa = (p+q)a, \qquad p(qa) = (pq)a \qquad pa+pb = p(a+b),$$

   la dernière égalité étant vraie par commutativité de $+$.

2. $(A,\times)$ étant un magma associatif, le $n$ème itéré d'un élément x, noté a^n, est défini par

$$a^n = \underbrace{a\times\ldots\times a}_{n \text{ facteurs}} \quad \text{si } n \geq 1 \qquad \text{et} \qquad a^0 = 1_A.$$

   On a aussi, pour tous $(a,b) \in A^2$ et $(m,n) \in \mathbb{N}^2$,

$$a^m \times a^n = a^{m+n}, \qquad (a^m)^n = a^{mn},$$

   ⚠ mais attention ! l'égalité $(ab)^n = a^n b^n$ est FAUSSE en général si $\times$ n'est pas commutative.

3. Si a est un élément inversible dans A, on peut alors définir la puissance $n$ème de a pour n strictement négatif par $a^n = (a^{-1})^{-n}$. Les identités de (2) sont alors vraies pour $(m,n) \in \mathbb{Z}^2$.

Proposition 47.

Soit $(A,+,\times)$ un anneau. En utilisant la notation multiplicative pour la loi $\times$,

1. $\forall a \in A \quad 0_A \times a = a \times 0_A = 0_A$.
2. $\forall (a,b) \in A^2 \quad a(-b) = (-a)b = -(ab)$.
3. $\forall (a,b) \in A^2 \quad (-a)(-b) = ab$.
4. $\forall (a,b) \in A^2 \quad \forall n \in \mathbb{Z} \quad a(nb) = (na)b = n(ab)$.

Proposition 48 (Identités remarquables : si ça commute, d'accord)**.**

Soit $(A,+,\times)$ un anneau et $(a,b) \in A^2$.

1. Si $\boldsymbol{ab = ba}$, alors $\forall n \in \mathbb{N} \quad (a+b)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.
2. Si $\boldsymbol{ab = ba}$, alors $\forall n \in \mathbb{N}^* \quad a^n - b^n = (a-b) \displaystyle\sum_{k=0}^{n-1} a^k b^{n-1-k}$.

   En particulier : $\forall n \in \mathbb{N}^* \quad 1_A - a^n = (1_A - a) \displaystyle\sum_{k=0}^{n-1} a^k$.

3.2 Groupe des inversibles dans un anneau.

Définition 49.

Dans un anneau $(A,+,\times)$, les **inversibles** sont les éléments de A inversibles pour la loi $\times$.

L'ensemble des éléments de A qui sont inversibles sera noté $U(A)$, ou encore $A^\times$.

Exemples 50.

- $U(\mathbb{Z}) = \{-1, 1\}$.
- $U(\mathbb{R}) = \mathbb{R}^*$.
- Pour X une partie de $\mathbb{R}$, $U(\mathcal{F}(X,\mathbb{R}))$ est l'ensemble des fonctions *ne s'annulant pas* sur X.

Proposition 51.

Si $(A,+,\times)$ est un anneau, $(U(A),\times)$ est un groupe. On l'appelle **groupe des inversibles**. On a notamment

$$\forall (a,b) \in (U(A))^2 \quad ab \text{ est inversible} \quad \text{et} \quad (ab)^{-1} = b^{-1}a^{-1},$$

3.3 Nilpotents dans un anneau.

Définition 52.

Dans un anneau $(A,+,\times)$ on dit d'un élément $a \in A$ qu'il est **nilpotent** s'il possède une puissance nulle, c'est-à-dire
$$\exists p \in \mathbb{N}^* \quad a^p = 0_A.$$

Exemple 53.

Soit $(A,+,\times)$ un anneau et $(a,b) \in A^2$.

1. Montrer que si a est nilpotent et si b commute avec a, alors ab est nilpotent.
2. Montrer que si ab est nilpotent, alors ba est nilpotent.

Exemple 54.

Soit $(A,+,\times)$ un anneau non réduit à $\{0_A\}$ et $a \in A$ un élément nilpotent.

1. Montrer que a n'est pas inversible.
2. Montrer $1_A - a$ est inversible et exprimer son inverse.

3.4 Sous-anneaux, morphismes d'anneaux.

Proposition-Définition 55.

Soit $(A,+,\times)$ un anneau et B une partie de A. On dit que B est un **sous-anneau** de A si

- $\forall (a,b) \in B^2 \quad a-b \in B$,
- $\forall (a,b) \in B^2 \quad ab \in B$,
- $1_A \in B$.

Muni des lois induites par $+$ et $\times$, B est un anneau.

Exemples 56.

- A est un sous-anneau de A. Si $0_A \neq 1_A$, alors $\{0_A\}$ n'est pas un sous-anneau de A
- Montrer que $\mathbb{Z}$ est le seul sous-anneau de $\mathbb{Z}$.

Exemple 57 (Anneau de Gauss)**.**

Soit l'ensemble
$$\mathbb{Z}[i] = \left\{a+ib \mid (a,b) \in \mathbb{Z}^2\right\}.$$
Montrer que $(\mathbb{Z}[i],+,\times)$ est un anneau commutatif et déterminer ses éléments inversibles.

Définition 58.

Soient $(A, +, \times)$ et $(A', +, \times)$ deux anneaux.
On appelle **morphisme d'anneaux** de A dans A' toute application $f : A \to A'$ telle que

- $\forall (a, b) \in A^2 \quad f(a + b) = f(a) + f(b)$,
- $\forall (a, b) \in A^2 \quad f(ab) = f(a)f(b)$,
- $f(1_A) = 1_{A'}$.

Si de surcroît f est bijective, on dit qu'une telle application f est un **isomorphisme** d'anneaux.

Exemple 59.

La conjugaison

$$\text{conj} : \begin{cases} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & \overline{z} \end{cases}$$

est un isomorphisme de l'anneau $(\mathbb{C}, +, \times)$ dans lui-même.

3.5 Anneaux intègres.

Définition 60.

Soit $(A, +, \times)$ un anneau. On dit d'un élément a de A qu'il est un **diviseur de zéro** si $a \neq 0_A$ et s'il existe un élément b dans $A \setminus \{0_A\}$ tel que $ab = ba = 0_A$.

Exemples 61.

- Dans l'anneau $(\mathbb{Z}, +, \times)$, il n'y a pas de diviseurs de zéro.
- Dans l'anneau $(\mathbb{R}^{\mathbb{R}}, +, \times)$, il existe des diviseurs de zéro. En exhiber un.

Définition 62.

On appelle anneau **intègre** tout anneau commutatif sans diviseurs de 0. Dans un tel anneau,

$$\forall (a, b) \in A^2 \qquad (ab = 0_A) \Longrightarrow (a = 0_A \;\text{ ou } b = 0_A)\,.$$

Exemples 63.

$\mathbb{Z}$ est un anneau intègre.

Dans les chapitres suivants, nous définirons deux anneaux importants :
— l'anneau des polynômes, $\mathbb{K}[X]$, qui sera un anneau intègre,
— pour $n \geq 2$, l'anneau de matrices $M_n(\mathbb{K})$, qui ne sera *pas* intègre.

4 Structure de corps.

4.1 Définitions et exemples.

Définition 64.

On appelle **corps** tout anneau commutatif $(K,+,\times)$, non réduit à $\{0_K\}$, dans lequel tout élément non nul est inversible.

Par définition, si K est un corps, $U(K) = K \setminus \{0_K\}$. Ce groupe commutatif pourra être noté K^*.

Exemples. $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des corps.

Proposition 65.

Tout corps est un anneau intègre. La réciproque est fausse.

Exemple 66.

Soit
$$\mathbb{Q}[\sqrt{2}] = \left\{x \in \mathbb{R} \mid \exists (a,b) \in \mathbb{Q}^2, x = a + b\sqrt{2}\right\}.$$
Montrer que $\mathbb{Q}[\sqrt{2}]$ est un corps.

4.2 Notation fractionnaire dans un corps.

Soit $(K,+,\times)$ un corps.
Soient $a \in K$ et $b \in K^*$. b est inversible donc b^{-1} existe. K étant commutatif, on a $ab^{-1} = b^{-1}a$.

$$\boxed{\text{L'élément } ab^{-1} \text{ est noté } \frac{a}{b}}.$$

Pour $(a,c) \in K^2$ et $(b,d) \in (K^*)^2$, on peut vérifier que

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd} \qquad \frac{a}{b} = \frac{c}{d} \iff ad = bc \qquad \frac{1}{a} = a^{-1}.$$

4.3 Corps des fractions d'un anneau intègre.

Théorème 67.

Pour tout anneau intègre A, il existe un unique corps commutatif K contenant A et vérifiant

$$\forall x \in K \quad \exists a \in A \ \exists b \in A \setminus \{0_A\} \ x = \frac{a}{b}.$$

Le corps K est appelé **corps des fractions** de l'anneau A.

Exemple. Le corps des fractions de $\mathbb{Z}$ n'est autre que $\mathbb{Q}$.

Exercices

On rappelle que les exemples du cours (et ils sont nombreux dans celui-ci) sont autant d'exercices classiques (et corrigés) : n'hésitez pas à les refaire !

Groupes, sous-groupes, morphismes de groupes.

19.1 **[♦◇◇]** Soit $(G, \star)$ $p \in \mathbb{N}^*$ et $a_1, \ldots, a_p$ des éléments de G. Quel est le symétrique de

$$a_1 \star a_2 \star \cdots \star a_p?$$

19.2 **[♦◇◇]** Soit $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$. Posons

$$H = \{x \in \mathbb{R} \mid \cos(a_n x) \to 1\}\,.$$

Montrer que H est un sous-groupe de $(\mathbb{R}, +)$.

19.3 **[♦◇◇]** Soient $(G, \star)$ un groupe et H un sous-groupe de G. Pour $a \in G$, on pose

$$aHa^{-1} = \left\{a \star h \star a^{-1} \mid h \in H\right\}.$$

Montrer que aHa^{-1} est un sous-groupe de G.

19.4 **[♦◇◇]** Soit $(G, \star)$ un groupe et f la fonction $x \mapsto x^{-1}$, application de G dans lui-même. Démontrer que f est un morphisme de groupes si et seulement si G est abélien.

19.5 **[♦♦◇]** Soit l'ensemble d'applications $G = \{x \mapsto ax + b \ \mid\ a \in \mathbb{R}^*, b \in \mathbb{R}\}$.
En vous appuyant sur un groupe connu, montrer que $(G, \circ)$ est un groupe.

19.6 **[♦♦◇]** Soit G un groupe noté multiplicativement, et H et K deux sous-groupes de G. On définit

$$HK = \{x \in G \mid \exists h \in H\ \exists k \in K, x = hk\} \quad \text{et} \quad KH = \{x \in G \mid \exists k \in K\ \exists h \in H, x = kh\}\,.$$

Démontrer l'équivalence entre

1. HK et KH sont des sous-groupes de G.
2. $HK = KH$.

19.7 **[♦♦♦]** [Sous-groupes de $(\mathbb{R}, +)$]
Montrer que si H est un sous-groupe de $(\mathbb{R}, +)$, alors
— ou bien il existe un réel a positif tel que $H = a\mathbb{Z}$, en notant $a\mathbb{Z} = \{ak \mid k \in \mathbb{Z}\}$,
— ou bien H est dense dans $\mathbb{R}$.

19.8 **[♦♦◇]** Pour x et y dans $]-1, 1[$, on pose $x \star y = \frac{x+y}{1+xy}$. Montrer que $(]-1, 1[, \star)$ est un groupe abélien.

19.9 **[♦♦◇]** Soit G un groupe noté multiplicativement. Pour $a \in G$, on pose $\tau_a : x \mapsto ax$.

1. Pour tout $a \in G$, montrer que $\tau_a \in S_G$.
2. Montrer que $a \mapsto \tau_a$ est un morphisme injectif de G dans S_G.

19.10 **[♦♦◇]** Démontrer que $(\mathbb{C}^*, \times)$ est isomorphe à $(\mathbb{R}_+^* \times \mathbb{U}, \times)$.

19.11 **[♦♦♦]** Soit G un groupe. Montrer qu'une partie H finie, non vide et stable par la loi de G est nécessairement un sous-groupe de G.

19.12 **[♦♦◇]** Soit $(G, \cdot)$ un groupe. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.
Pour $g \in G$, on note σ_g l'application $x \mapsto gxg^{-1}$.

1. Démontrer que $(\mathrm{Aut}(G), \circ)$ est un groupe.
2. Montrer que pour tout $g \in G$, $\sigma_g \in \mathrm{Aut}(G)$.
3. Démontrer que l'application $\sigma : g \mapsto \sigma_g$ est un morphisme de groupes de G dans $\mathrm{Aut}(G)$.
4. Montrer que $\mathrm{Ker}(\sigma) = Z(G)$, où G est le centre de G.

19.13 **[♦♦♦]** Soit $(G, \cdot)$ un groupe fini et χ un morphisme de groupes de $(G, \cdot)$ dans $(\mathbb{C}^*, \times)$. Calculer

$$S = \sum_{x \in G} \chi(x).$$

19.14 **[♦♦◇]** Soit $(G, \star)$ un groupe et x un élément de G.
On note $\langle x \rangle$ l'ensemble des itérés de x :

$$\langle x \rangle = \{x^p \mid p \in \mathbb{Z}\}.$$

1. Montrer que $\langle x \rangle$ est un sous-groupe de G. *On l'appelle sous-groupe engendré par x.*
2. Prouver que c'est le plus petit sous-groupe de G contenant x.

19.15 **[♦♦♦]** Soit $(E, \star)$ un magma associatif fini.
Démontrer qu'il existe dans E un élément idempotent, c'est-à-dire un élément x tel que $x^2 = x$.

Anneaux, corps.

19.16 **[♦♦◇]**
Montrer que dans un anneau, la somme de deux éléments nilpotents qui commutent est nilpotent.

19.17 **[♦♦♦]** Soit $(A, +, \times)$ un anneau. On suppose qu'il existe deux éléments a, b de A tels que

$$ab + ba = 1_A \quad \text{et} \quad a^2b + ba^2 = a$$

1. Montrer que $a^2b = ba^2$ et $2aba = a$.
2. Montrer que a est inversible et que $a^{-1} = 2b$.

19.18 **[♦♦♦]** Soit E un ensemble. On définit sur E la différence symétrique

$$\Delta : \left\{ \begin{array}{rcl} E \times E & \to & E \\ (A, B) & \mapsto & A \Delta B = (A \cup B) \setminus (A \cap B) \end{array} \right. .$$

1. Montrer que $(\mathcal{P}(E), \Delta)$ est un groupe commutatif.
2. Montrer que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif.
3. Démontrer que si E possède au moins deux éléments, alors l'anneau $(\mathcal{P}(E), \Delta, \cap)$ n'est pas intègre.

19.19 **[♦♦♦]** Soit $(A, +, \times)$ un anneau commutatif fini.
Démontrer que A est un corps si et seulement si il possède exactement un élément nilpotent et exactement deux éléments idempotents (éléments x tels que $x^2 = x$).

Calcul matriciel

Dans tout ce qui suit, n et p et q désigneront des entiers naturels non nuls, et $\mathbb{K}$ le corps $\mathbb{R}$ ou $\mathbb{C}$.

1 Matrices rectangulaires et opérations.

1.1 Combinaisons linéaires de matrices de $M_{n,p}(\mathbb{K})$.

Définition 1.

- On appelle **matrice** de type (n, p) à coefficients dans $\mathbb{K}$ un tableau d'éléments de $\mathbb{K}$ ayant n lignes et p colonnes.
- L'ensemble des matrices à n lignes et p colonnes, à coefficients dans $\mathbb{K}$ est noté $M_{n,p}(\mathbb{K})$.
- L'ensemble $M_{n,n}(\mathbb{K})$ est noté $M_n(\mathbb{K})$. Les matrices de cet ensemble sont qualifiées de *carrées*.
- Soit $A \in M_{n,p}(\mathbb{K})$. Les **coefficients** de A sont écrits à l'aide d'un double indice : $a_{i,j}$ désigne le coefficient qui est sur la *ligne* i et sur la *colonne* j. Ainsi, on note

$$A = (a_{i,j})_{\substack{1\leq i\leq n \\ 1\leq j\leq p}}.$$

- La matrice A écrite ci-dessus se représente entre parenthèses.

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,p} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,p} \\ \vdots & \vdots & & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,p} \end{pmatrix}$$

Remarque. Ayant $\mathbb{R} \subset \mathbb{C}$, on a l'inclusion $M_{n,p}(\mathbb{R}) \subset M_{n,p}(\mathbb{C})$.

Définition 2.

Soient $A = (a_{i,j})_{\substack{1\leq i\leq n\\ 1\leq j\leq p}}$ et $B = (b_{i,j})_{\substack{1\leq i\leq n\\ 1\leq j\leq p}}$ deux matrices de même type.
On dit que A et B sont **égales** et on note $A = B$ si

$$\forall i \in [\![1,n]\!]\ \forall j \in [\![1,p]\!] \quad a_{i,j} = b_{i,j}.$$

On va munir $M_{n,p}(\mathbb{K})$ d'une structure de groupe additif.

Définition 3 (Somme de deux matrices)**.**

Soient $A = (a_{i,j})$ et $B = (b_{i,j})$ deux matrices de $M_{n,p}(\mathbb{K})$.
On appelle **somme** de A et B, et on note $A + B$ la matrice de $M_{n,p}(\mathbb{K})$

$$A + B = (c_{i,j})_{\substack{1\leq i\leq n\\ 1\leq j\leq p}} \quad \text{où} \quad \forall i \in [\![1,n]\!]\ \forall j \in [\![1,p]\!] \quad c_{i,j} = a_{i,j} + b_{i,j}.$$

Proposition 4.

Le couple $(M_{n,p}(\mathbb{K}), +)$ est un groupe abélien. Plus précisément,

1. $+$ est une loi de composition interne sur $M_{n,p}(\mathbb{K})$;
2. $+$ est associative ;
3. $+$ est commutative ;
4. il existe une matrice dans $M_{n,p}(\mathbb{K})$ qui est neutre pour l'addition : c'est la matrice nulle, dont tous les coefficients sont nuls et elle est notée $0_{n,p}$;
5. toute matrice A de $M_{n,p}(\mathbb{K})$ possède un symétrique $-A$ dans $M_{n,p}(\mathbb{K})$.
   Si $A = (a_{i,j})$, la matrice $-A$ est la matrice $(-a_{i,j})$ et on a $-A + A = A + (-A) = 0_{n,p}$.

Définition 5 (Multiplication par un scalaire)**.**

Soient $A = (a_{i,j})$ une matrice de $M_{n,p}(\mathbb{K})$ et λ un élément du corps $\mathbb{K}$. On appelle multiple de A par le *scalaire* λ, et on note $\lambda \cdot A$ ou plus simplement λA la matrice

$$\lambda A = (\lambda a_{i,j}).$$

Si A et B sont deux matrices de $M_{n,p}(\mathbb{K})$ et λ, μ deux éléments de $\mathbb{K}$, la matrice $\lambda A + \mu B$ est appelée une **combinaison linéaire** de A et B.

Remarque.
Ce qui précède définit une application $\cdot : \left\{ \begin{array}{ccc} M_{n,p}(\mathbb{K}) \times \mathbb{K} & \to & M_{n,p}(\mathbb{K}) \\ (A, \lambda) & \mapsto & \lambda \cdot A \end{array} \right.$, appelée loi de composition *externe* (on prend une matrice A et on va chercher un scalaire λ à l'extérieur de $M_{n,p}(\mathbb{K})$ pour construire λA).

Proposition 6 (Propriétés de la multiplication par un scalaire)**.**

- $\forall A \in M_{n,p}(\mathbb{K}) \quad 1_{\mathbb{K}} \cdot A = A$;
- $\cdot$ est distributive par rapport à l'addition dans $M_{n,p}(\mathbb{K})$:

$$\forall A, B \in M_{n,p}(\mathbb{K}) \quad \forall \lambda \in \mathbb{K} \quad \lambda \cdot (A + B) = \lambda \cdot A + \lambda \cdot B;$$

- $\cdot$ est distributive par rapport à l'addition dans $\mathbb{K}$:

$$\forall A \in M_{n,p}(\mathbb{K}) \quad \forall \lambda, \mu \in \mathbb{K} \quad (\lambda + \mu) \cdot A = \lambda \cdot A + \mu \cdot A;$$

- $\forall \lambda, \mu \in \mathbb{K} \quad \forall A \in M_{n,p}(\mathbb{K}) \quad \lambda \cdot (\mu \cdot A) = (\lambda\mu) \cdot A.$

Remarque. Le triplet $(M_{n,p}(\mathbb{K}), +, \cdot)$ a une structure de $\mathbb{K}$-**espace vectoriel** ($\to$ algèbre linéaire).

Proposition 7 (Autour du zéro et du symétrique)**.**

- $\forall A \in M_{n,p}(\mathbb{K}) \quad 0_{\mathbb{K}} \cdot A = 0_{n,p}$.
- $\forall \lambda \in \mathbb{K} \quad \lambda \cdot 0_{n,p} = 0_{n,p}$.
- $\forall A \in M_{n,p}(\mathbb{K}) \quad -A = (-1) \cdot A$.
- $\forall \lambda \in \mathbb{K} \quad \forall A \in M_{n,p}(\mathbb{K}) \quad \lambda \cdot A = 0_{n,p} \implies (\lambda = 0_{\mathbb{K}} \text{ ou } A = 0_{n,p})$.

Définition 8.

Dans $M_{n,p}(\mathbb{K})$, pour $i \in [\![1, n]\!]$, $j \in [\![1, p]\!]$, on note $E_{i,j}$ la matrice dont tous les coefficients sont nuls sauf celui à la position (i, j), qui vaut 1. Une telle matrice est parfois dite **élémentaire**.

$$E_{i,j} = \begin{array}{cc} \begin{pmatrix} & & & & \vdots & & \\ & & (0) & & \vdots & (0) & \\ \cdots & \cdots & \cdots & \cdots & 1 & \cdots & \cdots \\ & & & & \vdots & & \\ & & (0) & & \vdots & (0) & \\ & & & & \vdots & & \end{pmatrix} & \begin{matrix} \\ \\ \leftarrow i \\ \\ \\ \\ \end{matrix} \\ \begin{matrix} \uparrow \\ j \end{matrix} & \end{array}.$$

Proposition 9 (Décomposition sur la base canonique)**.**

Toute matrice de $M_{n,p}(\mathbb{K})$ s'écrit de manière unique comme une combinaison linéaire des matrices de la famille $(E_{i,j}, i \in [\![1, n]\!], j \in [\![1, p]\!])$, qui sera appelée **base canonique** de $M_{n,p}(\mathbb{K})$.
Plus précisément

$$\forall M = (m_{i,j}) \in M_{n,p}(\mathbb{K}) \quad M = \sum_{i=1}^{n} \sum_{j=1}^{p} m_{i,j} E_{i,j}.$$

1.2 Produit matriciel.

Définir le produit de deux matrices en multipliant coefficient par coefficient, n'a pas d'intérêt. Même si la définition qui suit peut sembler étrange au premier abord, nous verrons que le produit matriciel :

$\longrightarrow$ a un lien avec la résolution des systèmes linéaires (partie 3),

$\longrightarrow$ a un lien avec la composition des applications linéaires (second semestre).

Définition 10.

Soient deux matrices $A = (a_{i,j}) \in M_{n,p}(\mathbb{K})$ et $B = (b_{i,j}) \in M_{p,q}(\mathbb{K})$.
On appelle **produit** de A et B, et on note AB la matrice de $M_{n,q}(\mathbb{K})$ définie par

$$AB = (c_{i,j})_{\substack{1\le i\le n\\ 1\le j\le q}} \quad \text{où} \quad \forall i \in [\![1,n]\!]\ \forall j \in [\![1,q]\!] \quad c_{i,j} = \sum_{k=1}^{p} a_{i,k}b_{k,j}.$$

Exemples 11.

Soient $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$, $B = \begin{pmatrix} 3 & -1 \\ 5 & 0 \end{pmatrix}$, $C = \begin{pmatrix} 0 & x \\ y & 0 \\ z & 0 \end{pmatrix}$, avec x, y, z des réels.
Calculer AA, AB, AC, BA, BB, BC, CA, CB, CC, lorsque le produit a un sens.

Proposition 12 (Propriétés du produit matriciel)**.**

Soient A, B, C trois matrices à coefficients dans $\mathbb{K}$ et $\lambda \in \mathbb{K}$.
Lorsque les produits écrits ci-dessous ont un sens, ces égalités sont vraies :

1. $A(B + C) = AB + AC$ (distributivité du produit à gauche)
2. $(A + B)C = AC + BC$ (distributivité du produit à droite)
3. $(\lambda A)B = A(\lambda B) = \lambda(AB)$ et ainsi $(\lambda A)(\mu B) = (\lambda\mu)AB$ (la balade des scalaires)
4. $(AB)C = A(BC)$ (associativité du produit)

Proposition 13 (Produit par la matrice nulle)**.**

$$\forall A \in M_{n,p}(\mathbb{K}) \qquad A \cdot 0_{p,q} = 0_{n,q} \quad \text{et} \quad 0_{q,n} \cdot A = 0_{q,p}.$$

Exemple 14 (Deux propriétés que le produit matriciel NE possède PAS)**.**

Considérons $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. On a $AB = 0_{2,2}$ et $BA = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Ainsi,

1. Même lorsque les deux produits AB et BA ont un sens, et ont même type, l'égalité $AB = BA$ n'est pas toujours vraie : A et B ne commutent pas toujours.
2. Le produit AB peut être nul sans que ni A ni B ne soit la matrice nulle.

Définition 15.

On appelle matrice **diagonale** d'ordre n toute matrice $D = (d_{i,j}) \in M_n(\mathbb{K})$ telle que

$$\forall\ 1 \leq i, j \leq n \quad i \neq j \Longrightarrow d_{i,j} = 0.$$

Pas de contrainte sur les coefficients $d_{i,i}$ dits coefficients *diagonaux*.

On note parfois, pour $d_1, \ldots, d_n \in \mathbb{K}$,

$$\mathrm{Diag}(d_1, \ldots, d_n) := \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & d_n \end{pmatrix}.$$

Exemples. $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ est diagonale, $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 3 \end{pmatrix}$ aussi.

Proposition 16 (Effet de la multiplication par une matrice diagonale)**.**

Soit une matrice $M \in M_{n,p}(\mathbb{K})$ et deux matrices diagonales

$$D = \mathrm{Diag}(d_1, \ldots, d_n) \in M_n(\mathbb{K}) \quad \text{et} \quad D' = \mathrm{Diag}(d'_1, \ldots, d'_p) \in M_p(\mathbb{K}).$$

- Produit à gauche.
  La matrice DM s'obtient en multipliant la ligne i de M par d_i, et ce pour tout $i \in [\![1, n]\!]$.
- Produit à droite.
  La matrice MD' s'obtient en multipliant la colonne j de M par d'_j, et ce pour tout $j \in [\![1, p]\!]$.

Exemple.
Soient $M = \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix}$ et $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 3 \end{pmatrix}$. On a $DM = \begin{pmatrix} a & b & c \\ 0 & 0 & 0 \\ 3a'' & 3b'' & 3c'' \end{pmatrix}$ et $MD = \begin{pmatrix} a & 0 & 3c \\ a' & 0 & 3c' \\ a'' & 0 & 3c'' \end{pmatrix}$.

Définition 17.

Soit $n \in \mathbb{N}^*$. On appelle **matrice identité** d'ordre n, et on note I_n la matrice diagonale de $M_n(\mathbb{K})$ dont tous les coefficients diagonaux sont égaux à 1 :

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Proposition 18.

La matrice identité est neutre pour la multiplication matricielle :

$$\forall A \in M_{n,p}(\mathbb{K}) \quad I_n A = A \;\text{ et }\; A I_p = A.$$

En particulier pour les matrices carrées,

$$\forall M \in M_n(\mathbb{K}) \quad M I_n = I_n M = M.$$

On appelle parfois **matrice scalaire** une matrice de la forme λI_n, avec $\lambda \in \mathbb{K}$. Lorsqu'il a un sens, le produit d'une matrice M par λI_n donne λM.

1.3 Transposition

Définition 19.

Soit $A = (a_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} \in M_{n,p}(\mathbb{K})$.

On appelle **transposée** de la matrice A, et on note $A^\top$ (ancienne notation : ${}^t A$) la matrice de $M_{p,n}(\mathbb{K})$ définie par

$$A^\top = (a'_{i,j})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq n}} \quad \text{où} \quad \forall i \in [\![1, p]\!] \; \forall j \in [\![1, n]\!] \quad a'_{i,j} = a_{j,i}$$

Exemples.

- La transposée de la matrice $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ est $A^\top = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$.
- La transposée de la matrice $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est $B^\top = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$.
- Une matrice diagonale (donc carrée...) est sa propre transposée.
- Soit $(i, j) \in M_{n,p}(\mathbb{K})$.
  La transposée de la matrice élémentaire $E_{i,j}$ de $M_{n,p}(\mathbb{K})$ est la matrice élémentaire $E_{j,i}$ de $M_{p,n}(\mathbb{K})$.

Proposition 20 (Transposée de la transposée)**.**

$$\forall A \in M_{n,p}(\mathbb{K}) \qquad \left(A^\top\right)^\top = A.$$

Proposition 21 (Transposée d'une combinaison linéaire)**.**

$$\forall (A, B) \in (M_{n,p}(\mathbb{K}))^2 \quad \forall (\lambda, \mu) \in \mathbb{K}^2 \qquad (\lambda A + \mu B)^\top = \lambda A^\top + \mu B^\top.$$

Proposition 22 (Transposée d'un produit)**.**

$$\forall A \in M_{n,p}(\mathbb{K}) \quad \forall B \in M_{p,q}(\mathbb{K}) \qquad (AB)^\top = B^\top A^\top.$$

2 Matrices carrées.

On rappelle que $M_n(\mathbb{K})$ est l'ensemble des matrices carrées à n lignes et n colonnes.
Pour $A = (a_{i,j}) \in M_n(\mathbb{K})$, on appellera **coefficients diagonaux** les n coefficients $a_{i,i}$, avec $i \in [\![1, n]\!]$.

2.1 Structure d'anneau de $M_n(\mathbb{K})$.

Proposition 23.

$(M_n(\mathbb{K}), +, \times)$ est un anneau.
La matrice nulle 0_n est l'élément neutre du groupe additif et la matrice I_n le neutre pour la loi $\times$.
Dès que $n \geq 2$, $M_n(\mathbb{K})$ n'est pas commutatif et possède des diviseurs de zéro.

On appellera puissances d'une matrice ses itérés pour la loi produit. On redonne ci-dessous une définition.

Définition 24.

Soit $A \in M_n(\mathbb{K})$. La suite $(A^p)_{p\in\mathbb{N}}$ des **puissances** de A est définie par

$$A^0 = I_n \qquad \text{et} \qquad \forall p \in \mathbb{N} \quad A^{p+1} = A^p \cdot A.$$

Proposition 25.

$$\forall A \in M_n(\mathbb{K}) \quad \forall (p,q) \in \mathbb{N}^2 \quad \forall \lambda \in \mathbb{K} \quad A^pA^q = A^{p+q} = A^qA^p, \quad (A^p)^q = A^{pq}, \quad (\lambda A)^p = \lambda^p A^p.$$

Proposition 26.

$$\forall A \in M_n(\mathbb{K}) \quad \forall p \in \mathbb{N} \quad \left(A^\top\right)^p = (A^p)^\top.$$

Proposition 27 (si ça commute, d'accord).

Soient $A, B \in M_n(\mathbb{K})$ deux matrices $\boxed{\text{qui commutent}}$ (i.e. $AB = BA$). Alors,

1. $\forall (p,q) \in \mathbb{N} \quad A^pB^q = B^qA^p$,
2. $\forall p \in \mathbb{N} \quad (AB)^p = A^pB^p$,
3. $\forall p \in \mathbb{N} \quad A^p - B^p = (A-B)\sum_{k=0}^{p-1} A^kB^{p-1-k} \quad$ et $\quad (A+B)^p = \sum_{k=0}^{p} \binom{p}{k} A^kB^{p-k}$.

Exemple 28.

Calculer les puissances de la matrice $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$.

Exemple 29.

Soit $a \in \mathbb{K}$. On considère les matrices

$$N = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \text{et} \quad M_a = \begin{pmatrix} 1 & a & 0 & 0 \\ 0 & 1 & a & 0 \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Vérifier que N est nilpotente puis calculer les puissances de M_a.

Exemple 30 (Puissance de la *matrice Attila*)**.**

Soit J la matrice de $M_n(\mathbb{K})$ dont tous les coefficients sont égaux à 1. Déterminer ses puissances.

Proposition 31 (Produit de deux matrices élémentaires de $M_n(\mathbb{K})$)**.**

Soit $(E_{i,j}, 1 \leq i, j \leq n)$ la base canonique de $M_n(\mathbb{K})$. On a

$$\forall i, j, k, l \in [\![1, n]\!] \quad E_{i,j}E_{k,l} = \delta_{j,k}E_{i,l}.$$

où pour tout couple $(i, j) \in \mathbb{N}^2$, on définit le **symbole de Kronecker** par $\delta_{i,j} = \begin{cases} 1 & \text{si} \quad i = j \\ 0 & \text{si} \quad i \neq j \end{cases}$

Preuve. Considérons quatre entiers i, j, k, l entre 1 et n. Remarquons d'abord que le symbole de Kronecker permet d'exprimer les coefficients des matrices de la base canonique : pour r, s dans $[\![1, n]\!]$, on a par définition de la matrice $E_{i,j}$,

$$[E_{i,j}]_{r,s} = \begin{cases} 1 & \text{si } r = i \text{ et } s = j \\ 0 & \text{sinon.} \end{cases}$$

Un tel nombre peut être obtenu en multipliant deux coefficients de Kronecker : $\delta_{r,i}\delta_{s,j}$ vaut lui aussi 1 si $(r, s) = (i, j)$ et 0 sinon. On a donc

$$\forall r, s \in [\![1, n]\!] \quad [E_{i,j}]_{r,s} = \delta_{r,i}\delta_{s,j}.$$

Calculons le coefficient d'indice (r, s) du produit $E_{i,j}E_{k,l}$:

$$[E_{i,j}E_{k,l}]_{r,s} = \sum_{t=1}^{n} [E_{i,j}]_{r,t}[E_{k,l}]_{t,s} = \sum_{t=1}^{n} \delta_{r,i}\delta_{t,j}\delta_{t,k}\delta_{s,l} = \delta_{r,i}\delta_{s,l}\sum_{t=1}^{n} \delta_{t,j}\delta_{t,k}.$$

Pour t entre 1 et n, le produit $\delta_{t,j}\delta_{t,k}$ est nul, sauf si $t = j = k$, auquel cas il vaut 1. La somme $\sum_{t=1}^{n} \delta_{t,j}\delta_{t,k}$ est donc nulle si $j \neq k$. Si $j = k$, elle ne contient qu'un terme non nul qui vaut $\delta_{j,j}\delta_{k,k} = 1$. Ainsi, on a

$$\sum_{t=1}^{n} \delta_{t,j}\delta_{t,k} = \delta_{j,k},$$

d'où

$$[E_{i,j}E_{k,l}]_{r,s} = \delta_{j,k}(\delta_{r,i}\delta_{s,l}) = \delta_{j,k}[E_{i,l}]_{r,s}.$$

Ceci achève de prouver que les matrices $E_{i,j}E_{k,l}$ et $\delta_{j,k}E_{i,l}$ ont même coefficients. □

2.2 Trace d'une matrice carrée.

Définition 32.

Soit $A = (a_{i,j}) \in M_n(\mathbb{K})$. On appelle **trace** de la matrice A et on note $\mathrm{tr}(A)$ la somme de ses coefficients diagonaux :

$$\mathrm{tr}(A) = \sum_{i=1}^{n} a_{i,i}.$$

Proposition 33 (Trace et opérations)**.**

Pour toutes matrices A et B carrées d'ordre n, pour tous $\lambda, \mu \in \mathbb{K}$,

$$\mathrm{tr}(A^\top) = \mathrm{tr}(A), \qquad \mathrm{tr}\left(\lambda A + \mu B\right) = \lambda \mathrm{tr}(A) + \mu \mathrm{tr}(B), \qquad \boxed{\mathrm{tr}(AB) = \mathrm{tr}(BA)}.$$

2.3 Parties remarquables de $M_n(\mathbb{K})$.

• **Matrices diagonales**.

Proposition 34.

Notons ici $D_n(\mathbb{K})$ l'ensemble des matrices diagonales de taille n à coefficients dans $\mathbb{K}$.

1. $D_n(\mathbb{K})$ contient la matrice nulle et c'est un ensemble stable par combinaison linéaire.
2. $D_n(\mathbb{K})$ est stable par produit matriciel.

• **Matrices triangulaires**.

Définition 35.

Soit $T = (t_{i,j}) \in M_n(\mathbb{K})$. On dit qu'elle est **triangulaire supérieure** si tous ses coefficients sous la diagonale sont nuls, c'est-à-dire

$$\forall (i,j) \in [\![1,n]\!]^2 \quad i > j \Longrightarrow t_{i,j} = 0.$$

On dira que T est **triangulaire inférieure** si sa transposée est triangulaire supérieure.

Exemple. $T = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 5 \\ 0 & 0 & 2 \end{pmatrix}$ est triangulaire supérieure. $T' = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 0 & 0 \\ 3 & 0 & 3 \end{pmatrix}$ est triangulaire inférieure.

Proposition 36.

Notons ici $T_n^+(\mathbb{K})$ (resp. $T_n^-(\mathbb{K})$) l'ensemble des matrices triangulaires supérieures (resp. inférieures) de taille n, à coefficients dans $\mathbb{K}$.

1. $T_n^+(\mathbb{K})$ et $T_n^-(\mathbb{K})$ contiennent la matrice nulle et sont stables par combinaison linéaire.
2. $T_n^+(\mathbb{K})$ et $T_n^-(\mathbb{K})$ sont stables par produit matriciel.

- **Matrices symétriques, antisymétriques.**

Définition 37.

On dit d'une matrice carrée A qu'elle est **symétrique** si $A^\top = A$, **antisymétrique** si $A^\top = -A$.
L'ensemble des matrices symétriques de $M_n(\mathbb{K})$ est noté $S_n(\mathbb{K})$.
L'ensemble des matrices antisymétriques de $M_n(\mathbb{K})$ est noté $A_n(\mathbb{K})$.

Exemple. $S = \begin{pmatrix} 1 & 2 & 4 \\ 2 & 2 & 5 \\ 4 & 5 & 3 \end{pmatrix}$ est symétrique et $A = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & -\pi \\ 0 & \pi & 0 \end{pmatrix}$ est antisymétrique.

Exemple 38.

Montrer que $S_n(\mathbb{K})$ contient 0_n, est stable par combinaison linéaire, mais *pas* par produit.

Exemple 39.

Démontrer que toute matrice de $M_n(\mathbb{R})$ s'écrit de manière unique comme somme d'une matrice symétrique et d'une matrice antisymétrique.

2.4 Groupe des matrices inversibles.

Définition 40.

Le groupe des inversibles de l'anneau $(M_n(\mathbb{K}), +, \times)$ est appelé **groupe linéaire** et noté $GL_n(\mathbb{K})$.

Ainsi, une matrice $A \in M_n(\mathbb{K})$ est **inversible** (c'est-à-dire appartient à $GL_n(\mathbb{K})$) si

$$\exists B \in M_n(\mathbb{K}) \quad AB = I_n \quad \text{et} \quad BA = I_n.$$

Lorsque A est inversible, une telle matrice B est unique : on l'appelle **inverse** de A, notée A^{-1}.

Exemples élémentaires.
I_n et 0_n sont-elles inversibles ? Quid de $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ et de $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$?

Proposition 41 (Propriétés de groupe de $GL_n(\mathbb{K})$)**.**

1. $I_n \in GL_n(\mathbb{K})$,
2. $\forall (A,B) \in (GL_n(\mathbb{K}))^2 \quad AB \in GL_n(\mathbb{K})$ et $(AB)^{-1} = B^{-1}A^{-1}$.
3. $\forall A \in GL_n(\mathbb{K}) \quad A^{-1} \in GL_n(\mathbb{K})$ et $(A^{-1})^{-1} = A$.
4. $\forall A \in GL_n(\mathbb{K}) \quad \forall p \in \mathbb{N} \quad A^p \in GL_n(\mathbb{K})$ et $(A^p)^{-1} = (A^{-1})^p$.

Remarque. Il est tout à fait clair que $GL_n(\mathbb{K})$ n'est pas stable par somme : prenons l'exemple de I_n et $-I_n$, toutes deux inversibles ; leur somme vaut $0_{n,n}$ qui ne l'est pas.

Proposition 42 ($GL_n(\mathbb{K})$ est stable par transposition)**.**

Si $A \in M_n(\mathbb{K})$ est une matrice inversible, alors

$$A^T \text{ est inversible} \quad \text{et} \quad (A^T)^{-1} = (A^{-1})^T.$$

On va maintenant donner un critère d'inversibilité pour des matrices simples : les diagonales de taille quelconque, et les matrices quelconques de taille 2.

Proposition 43 (Inversibilité des matrices diagonales)**.**

Soit $D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$ une matrice diagonale de $M_n(\mathbb{K})$.

Elle est inversible si et seulement si ses coefficients diagonaux sont non nuls. Dans ce cas, on a

$$D^{-1} = \begin{pmatrix} d_1^{-1} & & \\ & \ddots & \\ & & d_n^{-1} \end{pmatrix}.$$

Proposition 44 (Inversibilité et inverse d'une matrice de taille 2)**.**

Soit $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in M_2(\mathbb{K})$. On appelle déterminant de A le réel $\det(A) = ad - bc$. On a

$$A^2 - \operatorname{tr}(A)A + \det(A)I_2 = 0.$$

La matrice A est inversible si et seulement si $\det(A) \neq 0$. Si c'est le cas, on a

$$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}.$$

Remarque. On définira la notion de déterminant d'une matrice carrée de taille quelconque en fin d'année, mais ce n'est pas une mince affaire...

Exemple 45 (Une diagonalisation)**.**

Soient

$$A = \begin{pmatrix} 0 & -2 \\ -1 & 1 \end{pmatrix} \quad \text{et} \quad P = \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$$

1. Montrer que P est inversible et calculer P^{-1}.
2. Il existe une matrice diagonale $D \in M_2(\mathbb{R})$ telle que $\underline{A = PDP^{-1}}$. Le prouver et expliciter D.
3. En utilisant la relation de la question 2, calculer les puissances de A.
4. En utilisant la relation de la question 2, prouver que A est inversible et calculer son inverse.

3 Systèmes linéaires et matrices.

3.1 Écriture matricielle des systèmes linéaires. Structure des ensembles de solutions.

Définition 46.

Soit $A = (a_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} \in M_{n,p}(\mathbb{K})$, $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$ et $B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$.

L'équation $AX = B$, d'inconnue $X \in M_{p,1}(\mathbb{K})$ est appelée **système linéaire** de n équations linéaires sur $\mathbb{K}^p$, de **second membre** B. Il s'écrit aussi

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,p} \\ \vdots & & & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,p} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \quad \text{i.e.} \left\{ \begin{array}{ccccccccc} a_{1,1}\, x_1 & + & a_{1,2}\, x_2 & + & \cdots & + & a_{1,p}\, x_p & = & b_1 \\ a_{2,1}\, x_1 & + & a_{2,2}\, x_2 & + & \cdots & + & a_{2,p}\, x_p & = & b_2 \\ \vdots & & & & & & & & \\ a_{n,1}\, x_1 & + & a_{n,2}\, x_2 & + & \cdots & + & a_{n,p}\, x_p & = & b_n \end{array} \right.$$

On appelle **solution** du système toute matrice colonne $X \in M_{p,1}(\mathbb{K})$ vérifiant $AX = B$, ou encore tout p-uplet $(x_1, \ldots, x_p) \in \mathbb{K}^p$ qui soit solution de chacune des n équations.

Ainsi, l'ensemble des solutions d'un système linéaire est une partie de $M_{p,1}(\mathbb{K})$ ou de $\mathbb{K}^p$, les notions de p-uplet et de matrice colonne à p lignes étant délibérément confondues.

Remarque. Insistons : même si, rigoureusement parlant, $M_{3,1}(\mathbb{R})$ et $\mathbb{R}^3$ ne sont pas le même ensemble, il sera très courant de confondre par exemple la matrice $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ et le triplet $(1, 2, 3)$.

Dans les énoncés ci-dessous, on fixe $A \in M_{n,p}(\mathbb{K})$ et $B \in M_{n,1}(\mathbb{K})$.

Proposition 47.

Un système linéaire de la forme $AX = 0_{n,1}$ est dit **homogène**.
L'ensemble S_0 de ses solutions contient le p-uplet nul et il est stable par combinaisons linéaires.

Définition 48.

Le système linéaire $AX = B$ est dit **compatible** s'il possède une solution.

Exemples.

- Le système $\left\{ \begin{array}{l} x + y = 0 \\ x - y = 2 \end{array} \right.$ est compatible. Il admet $(1, -1)$ comme unique solution.
- Le système $\left\{ \begin{array}{l} x + y = 0 \\ x + y = 2 \end{array} \right.$ est incompatible.
- Un système linéaire homogène sur $\mathbb{K}^p$ est toujours compatible : le p-uplet $(0, \ldots, 0)$ est solution.

Proposition 49.

Le système linéaire $AX = B$ est compatible s.s.i. B est une combinaison linéaire des colonnes de A.

Proposition 50.

Soit $AX = B$ un système linéaire compatible et $X_{pa} \in M_{p,1}(\mathbb{K})$ une solution particulière du système. L'ensemble des solutions S s'écrit

$$S = \{X_{pa} + Y,\ Y \in S_0\},$$

où S_0 est l'ensemble des solutions de $AX = 0_{n,1}$, système homogène associé.

3.2 Méthode du pivot et résolution des systèmes linéaires.

Exemple 51 (Révisons la méthode du pivot)**.**

On résout à l'aide de l'algorithme du pivot le système linéaire

$$\left\{\begin{array}{ccccccl} 3x & + & 4y & + & 9z & = 8 \\ 20x & + & 30y & + & 70z & = 60 \\ x & + & y & + & 2z & = 2 \end{array}\right.$$

Définition 52.

On appelle **opération élémentaire** sur les lignes d'un système ou d'une matrice l'une des opérations suivantes :

1. Échange des $i$èmes et $j$èmes lignes. On note $L_i \leftrightarrow L_j$.
2. Multiplication d'une ligne par un scalaire λ <u>non nul</u>. On note $L_i \leftarrow \lambda L_i$.
3. Ajout à la ligne L_i d'une ligne L_j $(i \neq j)$ multipliée par un scalaire μ. On note $L_i \leftarrow L_i + \mu L_j$.

Définition 53 (Un peu de vocabulaire sur les systèmes linéaires)**.**

Dans un système ou dans une matrice, on appelle **ligne nulle**, une ligne où tous les coefficients sont nuls ; elle correspond alors à l'équation linéaire $0 = 0$.
On appelle **pivot** d'une ligne non nulle le premier coefficient non nul.

On dit d'un système linéaire qu'il est **échelonné** s'il a une structure (strictement) *en escalier*. Plus précisément, si les lignes sous une ligne nulle sont toutes nulles et qu'à chaque ligne (non nulle), le pivot de la ligne se trouve strictement à droite du pivot de la ligne au-dessus.

Dans un système échelonné, on dit qu'une **inconnue** est **principale** si sur une des lignes du système, son coefficient est un pivot. Elle est dite **secondaire** sinon.

Exemple 54.

$$(\mathscr{S}_1)\left\{\begin{array}{rcrcrcl} \boxed{1}x & + & y & + & z & = 0 \\ & & \boxed{2}y & + & z & = 2 \\ & & \boxed{4}y & - & z & = -1 \\ & & & & 0 & = \boxed{5} \end{array}\right. \qquad (\mathscr{S}_2)\left\{\begin{array}{rcrcrcrl} \boxed{1}x & - & y & + & z & + & t & = 0 \\ & & & & \boxed{2}z & - & t & = 2 \\ & & & & & & 0 & = 0 \end{array}\right.$$

· Dans les systèmes linéaires ci-dessus, on a encadré les $\boxed{\text{pivots}}$.

· Le système $(\mathscr{S}_2)$ est échelonné, contrairement au système $(\mathscr{S}_1)$ qui ne l'est pas.

· Dans le système $(\mathscr{S}_2)$, x et z sont des inconnues principales, et y et t des inconnues secondaires.

Méthode (Écriture paramétrique de l'ensemble des solutions d'un système échelonné)**.**

Lorsqu'un système échelonné a des inconnues secondaires, on peut donner une représentation paramétrique de l'ensemble des solutions :

- en prenant les inconnues secondaires comme des paramètres prenant des valeurs quelconques dans $\mathbb{K}$,
- et en exprimant les inconnues principales en fonction des ces paramètres.

Proposition 55 (Existence et unicité de solutions pour un système échelonné)**.**

1. Un système linéaire échelonné est compatible si et seulement si il ne comporte pas de pivot sur la colonne des seconds membres.

2. Un système échelonné compatible a une unique solution si et seulement si il n'a que des inconnues principales, ce qui n'arrive que pour une matrice carrée.
   Son ensemble de solutions est alors un singleton.
   Un tel système est dit **de Cramer**.

3. Si le système échelonné possède au moins une inconnue secondaire, alors il possède une infinité de solutions. On sait donner une écriture paramétrique de cet ensemble de solutions.

Théorème 56 (admis)**.**

L' algorithme du pivot transforme un système linéaire quelconque en un système linéaire échelonné, ayant le même ensemble de solutions que le système de départ.

Remarque. Pour que ce *théorème* en fut vraiment un, il aurait fallu donner une présentation de l'algorithme du pivot plus formelle que celle que nous avons fournie.

Ainsi, pour résoudre un système linéaire, on l'échelonnera à l'aide de l'algorithme du pivot. Une fois échelonné, on applique la méthode ci-dessus pour écrire son ensemble de solutions.

3.3 Systèmes linéaires et inversibilité des matrices.

Théorème 57 (Caractérisation de l'inversibilité d'une matrice en termes de systèmes linéaires)**.**

Soit $A \in M_n(\mathbb{K})$. Les trois assertions ci-dessous sont équivalentes.

1. A est inversible.
2. Le système linéaire homogène $AX = 0_{n,1}$ a pour unique solution la colonne nulle $0_{n,1}$.
3. Pour tout $Y \in M_{n,1}(\mathbb{K})$, le système linéaire $AX = Y$, d'inconnue $X \in M_{n,1}(\mathbb{K})$, possède une unique solution.

Preuve. On va montrer la chaîne $1 \Longrightarrow 2 \Longrightarrow 3 \Longrightarrow 1$.

• Supposons 1. La colonne nulle $0_{n,1}$ est solution du système linéaire homogène. Montrons que c'est la seule.

Soit $X \in M_{n,1}(\mathbb{K})$ tel que $AX = 0$. Puisqu'on a supposé A inversible, on peut multiplier par A^{-1} à gauche et obtenir $X = 0$.

• Supposons 2. Soit $Y \in M_{n,1}(\mathbb{K})$. Posons le système linéaire $AX = Y$, d'inconnue $X \in M_{n,1}(\mathbb{K})$.

On échelonne le système linéaire : on obtient un système équivalent de la forme $TX = Y'$ où T est une matrice carrée échelonnée (donc triangulaire). Bien sûr, on aurait pu obtenir T en échelonnant le système homogène $AX = 0$. Comme on a supposé que ce système n'avait qu'une solution, on sait que $TX = 0$ (et donc $TX = Y'$!) n'a que des inconnues principales. Ainsi, le système $TX = Y'$, équivalent à $AX = Y$, possède une unique solution.

• Supposons 3, c'est-à-dire que pour tout Y, le système $AX = Y$ possède une unique solution.

Notons $C_1, \dots, C_n$ les n colonnes de la matrice I_n. Par hypothèse,

$$\forall j \in [\![1, n]\!] \quad \exists X_j \in M_{n,1}(\mathbb{K}) \quad AX_j = C_j.$$

Posons B la matrice dont les colonnes sont les X_j :

$$AB = (AX_1 \mid \cdots \mid AX_n) = (C_1 \mid \cdots \mid C_n) = I_n.$$

On a $AB = I_n$: on a trouvé un "inverse à droite" pour A. <u>A-t-on $BA = I_n$?</u> On a

$$A\,(BA - I_n) = \underbrace{(AB)}_{=I_n} A - A = I_n A - A = 0_n.$$

Si on note C'_j la $j$ème colonne de $BA - I_n$. Ce qui précède se récrit

$$A\left(C'_1 \mid \cdots \mid C'_n\right) = \left(AC'_1 \mid \cdots \mid AC'_n\right) = 0_n.$$

Ainsi

$$\forall j \in [\![1, n]\!] \quad AC'_j = 0_{n,1}.$$

Or, le système linéaire $AX = 0$ a par hypothèse pour seule solution $0_{n,1}$. Ceci donne que tous les C'_j sont nuls et donc que $BA - I_n$.

On dispose bel et bien d'une matrice B telle que $AB = BA = I_n$, donc A est inversible et $A^{-1} = B$.

□

Corollaire 58 (*un côté suffit*)**.**

Pour une matrice carrée, l'existence d'un inverse à gauche (resp. à droite) suffit pour que cette matrice soit inversible. Alors, son inverse n'est autre que l'inverse à gauche (resp. à droite).

Plus précisément, pour $A \in M_n(\mathbb{K})$,

$$(\exists B \in M_n(\mathbb{K}) \quad BA = I_n) \quad \Longrightarrow \quad \left(A \in GL_n(\mathbb{K}) \ \text{ et } \ A^{-1} = B\right).$$

$$(\exists B \in M_n(\mathbb{K}) \quad AB = I_n) \quad \Longrightarrow \quad \left(A \in GL_n(\mathbb{K}) \ \text{ et } \ A^{-1} = B\right).$$

Corollaire 59 (vers une méthode de calcul effectif de l'inverse)**.**

Soit $A \in M_n(\mathbb{K})$. S'il existe une matrice $B \in M_n(\mathbb{K})$ telle que

$$\forall (X, Y) \in M_{n,1}(\mathbb{K}) \quad AX = Y \Longleftrightarrow X = BY,$$

alors A est inversible et $A^{-1} = B$.

Méthode (calcul de l'inverse : en posant le système)**.**

Soit $A \in M_n(\mathbb{K})$. Pour calculer l'inverse de A (s'il existe) :

1. on pose le système linéaire $AX = Y$, avec $X, Y \in M_{n,1}(\mathbb{K})$;
2. on échelonne le système : s'il n'y a que des inconnues principales, le système est de Cramer (une unique solution) et la matrice A est <u>inversible</u> ;
3. on peut alors réaliser des opérations élémentaires supplémentaires sur les lignes, pour éliminer les coefficients au-dessus de la diagonale : on obtient une égalité du type $X = BY$ et

$$\boxed{A^{-1} = B}.$$

Exemple 60.

Inversibilité et inverse de $A = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$ et de $A' = \begin{pmatrix} 1 & 1 & 1 \\ -1 & 1 & 1 \\ -1 & -1 & 1 \end{pmatrix}$.

Proposition 61 (CNS d'inversibilité d'une matrice triangulaire)**.**

Une matrice triangulaire est inversible s.s.i. ses coefficients diagonaux sont tous non nuls.

Admis en attendant l'algèbre linéaire : (ou alors réfléchissez bien au pivot) :

$$\text{si } T \text{ est de la forme } T = \begin{pmatrix} d_1 & * & * \\ & \ddots & * \\ & & d_n \end{pmatrix} \text{ son inverse est de la forme } T^{-1} = \begin{pmatrix} d_1^{-1} & * & * \\ & \ddots & * \\ & & d_n^{-1} \end{pmatrix}.$$

3.4 Méthode du pivot et calcul de l'inverse.

Définition 62.

Dans $M_n(\mathbb{K})$, pour tout couple $(i,j) \in [\![1,n]\!]^2$, on appelle **matrice de transposition**, et on note $P_{i,j}$ la matrice $P_{i,j} = I_n + E_{i,j} + E_{j,i} - E_{i,i} - E_{j,j}$.

$$P_{i,j} = \begin{array}{cc} \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & \cdots & 1 & & \\ & & \vdots & & \vdots & & \\ & & 1 & \cdots & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} & \begin{array}{c} \\ \\ \leftarrow i \\ \\ \leftarrow j \\ \\ \\ \end{array} \\ \begin{array}{ccccccc} & & \uparrow & & \uparrow & & \\ & & i & & j & & \end{array} & \end{array}.$$

Proposition 63.

Soit $M \in M_{n,p}(\mathbb{K})$.
Soit $(i,j) \in [\![1,n]\!]^2$ et $P_{i,j} \in M_n(\mathbb{K})$ la matrice de transposition associée.
Soit $(k,l) \in [\![1,p]\!]^2$ et $P'_{k,l} \in M_p(\mathbb{K})$ la matrice de transposition associée.

- Faire l'opération $L_i \leftrightarrow L_j$ sur la matrice M revient à calculer le produit $P_{i,j}M$.
- Faire l'opération $C_k \leftrightarrow C_l$ sur la matrice M revient à calculer le produit $MP'_{k,l}$.
- La matrice $P_{i,j}$ est inversible et elle est son propre inverse.

Preuve. Soit $M \in M_{n,p}(\mathbb{K})$ et $(i,j) \in [\![1,n]\!]$.
On va calculer le coefficient $[P_{i,j}M]_{r,s}$, avec $1 \leq r \leq n$ et $1 \leq s \leq p$:

$$[P_{i,j}M]_{r,s} = \sum_{k=1}^{n} [P_{i,j}]_{r,k} M_{k,s}.$$

· Si $r \neq i$ et $r \neq j$, tout se passe comme si on multipliait à gauche par l'identité : $[P_{i,j}]_{r,k}$ est nul sauf pour $k = r$ où il vaut 1.

· Si $r = i$, on a $[P_{i,j}]_{i,k}$ est nul sauf pour $k = j$ où il vaut 1, d'où

$$[P_{i,j}M]_{i,s} = [P_{i,j}]_{i,j}[M]_{j,s} = [M]_{j,s}.$$

Sur la ligne i de $P_{i,j}M$, on retrouve la ligne j de M.

· De même, on a

$$[P_{i,j}M]_{j,s} = [M]_{i,s}.$$

Sur la ligne i de $P_{i,j}M$, on retrouve la ligne j de M.

D'après ce qui précède, calculer $P_{i,j}^2$, c'est échanger les lignes i et j de $P_{i,j}$: on a bien $P_{i,j}^2 = I_n$.

□

Définition 64.

Dans $M_n(\mathbb{K})$, pour tout $i \in [\![1, n]\!]$ et tout $\lambda \in \mathbb{K}^*$, on appelle **matrice de dilatation**, et on note $D_i(\lambda)$ la matrice $D_i(\lambda) = I_n + (\lambda - 1)E_{i,i}$.

$$D_i(\lambda) = \begin{array}{cc} \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \lambda & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} & \begin{array}{l} \\ \\ \\ \leftarrow i \\ \\ \\ \\ \end{array} \\ \begin{array}{ccccccc} & & & \uparrow & & & \\ & & & i & & & \end{array} & \end{array} .$$

Proposition 65.

Soit $M \in M_{n,p}(\mathbb{K})$.
Soit $i \in [\![1, n]\!]$, $\lambda \in \mathbb{K}^*$ et $D_i(\lambda) \in M_n(\mathbb{K})$ la matrice de dilatation associée dans $M_n(\mathbb{K})$.
Soit $j \in [\![1, p]\!]$, $\lambda \in \mathbb{K}^*$ et $D'_j(\lambda)$ la matrice de dilatation associée dans $M_p(\mathbb{K})$.

- Faire l'opération $L_i \leftarrow \lambda L_i$ sur la matrice M revient à calculer le produit $D_i(\lambda)M$.
- Faire l'opération $C_j \leftarrow \lambda C_j$ sur la matrice M revient à calculer le produit $MD'_j(\lambda)$.
- La matrice $D_i(\lambda)$ est inversible d'inverse $D_i\left(\frac{1}{\lambda}\right)$.

Définition 66.

Dans $M_n(\mathbb{K})$, pour tout couple $(i, j) \in [\![1, n]\!]^2$ avec $i \neq j$ et tout $\mu \in \mathbb{K}$, on appelle **matrice de transvection**, et on note $T_{i,j}(\mu)$ la matrice $T_{i,j}(\mu) = I_n + \mu E_{i,j}$.

$$T_{i,j}(\lambda) = \begin{array}{cc} \begin{pmatrix} 1 & & & & \vdots & & \\ & \ddots & & & \vdots & & \\ \cdots & \cdots & 1 & \cdots & \mu & \cdots & \cdots \\ & & & \ddots & \vdots & & \\ & & & & 1 & & \\ & & & & \vdots & \ddots & \\ & & & & & & 1 \end{pmatrix} & \begin{array}{l} \\ \\ \leftarrow i \\ \\ \\ \\ \\ \end{array} \\ \begin{array}{ccccccc} & & & & \uparrow & & \\ & & & & j & & \end{array} & \end{array} .$$

Proposition 67.

Soit $M \in M_{n,p}(\mathbb{K})$.
Soient $1 \leq i \neq j \leq n$, $\mu \in \mathbb{K}$ et $T_{i,j}(\mu)$ la matrice de transvection associée dans $M_n(\mathbb{K})$.
Soient $1 \leq i \neq j \leq n$ $\mu \in \mathbb{K}$ et $T'_{k,l}(\mu)$ la matrice de transvection associée dans $M_p(\mathbb{K})$.

- Faire l'opération $L_i \leftarrow L_i + \mu L_j$ sur la matrice M revient à calculer le produit $T_{i,j}(\mu)M$.
- Faire l'opération $C_k \leftarrow C_k + \mu C_l$ sur la matrice M revient à calculer le produit $MT'_{i,j}(\mu)$.
- La matrice $T_{i,j}(\mu)$ est inversible, d'inverse $T_{i,j}(-\mu)$.

Proposition 68.

Les opérations élémentaires préservent l'inversibilité.

Méthode (calcul de l'inverse : en opérant sur l'identité en parallèle)**.**

Soit $A \in M_n(\mathbb{K})$. On va travailler par opérations élémentaires sur la matrice $(A \mid I_n) \in M_{n,2n}(\mathbb{K})$.

- On échelonne A, en faisant les opérations élémentaires sur $(A \mid I_n)$.

$$\left(\begin{array}{c|c} A & I_n \end{array}\right) \underset{\text{pivot}}{\curvearrowright} \left(\begin{array}{c|c} T & * \end{array}\right).$$

  La matrice A est inversible si et seulement si la matrice T l'est, c'est-à-dire si cette dernière n'a que des coefficients diagonaux non nuls.

- Dans le dernier cas, à l'aide d'opérations élémentaires, on transforme T en la matrice I_n. La matrice à droite de la membrane n'est autre que A^{-1}

$$\left(\begin{array}{c|c} T & * \end{array}\right) \underset{\text{pivot}}{\curvearrowright} \left(\begin{array}{c|c} I_n & A^{-1} \end{array}\right).$$

Explications. Transformer A en I_n en faisant des opérations élémentaires sur les lignes revient à multiplier A à *gauche* par des matrices de permutation, de dilatation, ou de transvection $E_1, \dots, E_N$, où $N \in \mathbb{N}$. On a

$$E_N E_{N-1} \dots E_1 A = I_n.$$

La matrice $E_N E_{N-1} \dots E_1$ est un inverse à gauche (et donc l'inverse tout court) de A. En travaillant sur la "double-matrice" $(A \mid I_n)$, on calcule ce produit au fur et à mesure, en réalisant toutes les opérations faites sur A, simultanément sur la matrice à droite de la "membrane". Schématiquement, voici la matrice avant, et après les N opérations élémentaires.

$$\left(\begin{array}{c|c} A & I_n \end{array}\right) \underset{\text{pivot}}{\curvearrowright} \left(\begin{array}{c|c} E_N E_{N-1} \dots E_1 A & E_N E_{N-1} \dots E_1 I_n \end{array}\right) = \left(\begin{array}{c|c} I_n & A^{-1} \end{array}\right).$$

Exemple 69.

Inversibilité et inverse de $A = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ et de $A' = \begin{pmatrix} 1 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 1 \end{pmatrix}$.

Exemple 70.

Cet algorithme d'inversion d'une matrice de taille n a une complexité en $O(n^3)$.

Exercices

Combinaisons linéaires de matrices. Produit de matrices.

$\boxed{\textbf{20.1}}$ **[♦◇◇]** Soit θ un réel. Calculer les puissances des trois matrices définies ci-dessous :

$$A = \begin{pmatrix} 0 & 1 & -\sin\theta \\ -1 & 0 & \cos\theta \\ -\sin\theta & \cos\theta & 0. \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 1 & -\sin\theta \\ -1 & 1 & \cos\theta \\ -\sin\theta & \cos\theta & 1. \end{pmatrix}, \qquad C = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & -1. \end{pmatrix}.$$

$\boxed{\textbf{20.2}}$ **[♦♦◇]** Soient a, b deux scalaires de $\mathbb{K}$. Calculer les puissances de la matrice $\begin{pmatrix} a+b & 0 & a \\ 0 & b & 0 \\ a & 0 & a+b \end{pmatrix}$.

$\boxed{\textbf{20.3}}$ **[♦♦◇]** Soit $(a, b, c) \in \mathbb{K}^3$. On considère la matrice

$$A = \begin{pmatrix} a^2 & ab & ac \\ ab & b^2 & bc \\ ac & bc & c^2 \end{pmatrix}$$

1. Exprimer A à l'aide d'une matrice colonne et de sa transposée.
2. Calculer les puissances de A.

$\boxed{\textbf{20.4}}$ **[♦◇◇]** Soient A et B deux matrices symétriques. Démontrer que AB est symétrique ssi $AB = BA$.

$\boxed{\textbf{20.5}}$ **[♦◇◇]** Soit A une matrice carrée de $M_n(\mathbb{C})$ et $\sigma(A)$ la somme de ses coefficients.
Notons J la matrice de $M_n(\mathbb{C})$ dont tous les coefficients sont égaux à 1. Montrer que $JAJ = \sigma(A)J$.

$\boxed{\textbf{20.6}}$ **[♦♦◇]** Soit $A = (a_{i,j})$ une matrice carrée de $M_n(\mathbb{K})$. Elle est dite centro-symétrique si

$$\forall i, j \in [\![1, n]\!] \quad a_{n+1-i,n+1-j} = a_{i,j}.$$

On note $C_n(\mathbb{K})$ l'ensemble des matrices centro-symétriques de taille n.

1. Donner un exemple de matrice de $C_2(\mathbb{R})$ et de $C_3(\mathbb{R})$.
2. Montrer que $C_n(\mathbb{K})$ est stable par combinaison linéaire.
3. Montrer que $C_n(\mathbb{K})$ est stable par produit.

$\boxed{\textbf{20.7}}$ **[♦◇◇]** Soient A et B deux matrices de $M_n(\mathbb{K})$. Démontrer que $AB - BA \neq I_n$.

$\boxed{\textbf{20.8}}$ **[♦◇◇]** Soit $A = (a_{i,j}) \in M_n(\mathbb{R})$. Justifier l'équivalence $\mathrm{tr}(A^T A) = 0 \iff A = 0_{n,n}$.

$\boxed{\textbf{20.9}}$ **[♦♦♦]** Soit un couple de matrices $(A, B) \in M_n(\mathbb{K})$ tel que

$$\forall X \in M_n(\mathbb{K}) \qquad AXB = 0.$$

Montrer que $A = 0$ ou $B = 0$.

Matrices inversibles et leurs inverses.

$\boxed{\textbf{20.10}}$ **[♦◇◇]** Pour tout $\theta \in \mathbb{R}$, on note $A(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.

1. Pour $\theta, \theta' \in \mathbb{R}$, calculer $A(\theta)A(\theta')$.
2. Soit $\theta \in \mathbb{R}$. Justifier que $A(\theta)$ est inversible et calculer $A(\theta)^{-1}$.
3. Expliciter le morphisme de groupes qui a été croisé dans cet exercice.

$\boxed{\textbf{20.11}}$ **[♦♦◇]**

1. Soit N une matrice nilpotente, c'est à dire qu'il existe $p \in \mathbb{N}$ tel que $N^p = 0$.
   En considérant $I_n - N^p$, montrer que $I_n - N$ est inversible et exprimer son inverse en fonction de N.
2. En utilisant ce qui précède, calculer l'inverse de $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.
3. Vérifier en recalculant l'inverse à l'aide du pivot.

$\boxed{\textbf{20.12}}$ **[♦♦◇]** Soit $n \in \mathbb{N}^*$ et $\omega = e^{\frac{2i\pi}{n}}$.

On considère $M = (m_{i,j}) \in M_n(\mathbb{C})$, définie par :

$$\forall i, j \in [\![1, n]\!] \quad m_{i,j} = \omega^{(i-1)(j-1)}.$$

On pose $\overline{M} = (\overline{m_{i,j}})$.

1. Calculer $M\overline{M}$.
2. Justifier que M est inversible et donner M^{-1}.

$\boxed{\textbf{20.13}}$ **[♦♦◇]** Soit A une matrice inversible telle que la somme des coefficients de chaque ligne vaut s.
Démontrer que $s \neq 0$ puis que la somme des coefficients sur chaque ligne de A^{-1} vaut s^{-1}.

$\boxed{\textbf{20.14}}$ **[♦♦◇]** Dans tout l'exercice, n est un entier supérieur à 2.

1. Soit $M \in M_n(\mathbb{R})$. On suppose qu'il existe $a \in \mathbb{R}$ et $b \in \mathbb{R}^*$ tels que
   $$M^2 + aM + bI_n = 0.$$
   Montrer que M est inversible et exprimer son inverse en fonction de M.
2. Soit $J \in M_n(\mathbb{R})$ la matrice dont tous les coefficients sont égaux à 1.
   Calculer J^2. Montrer que $J - I_n$ est inversible et calculer son inverse.

$\boxed{\textbf{20.15}}$ **[♦♦♦]** Matrice à diagonale dominante.
Soit $A \in M_n(\mathbb{K})$ telle que

$$\forall i \in [\![1, n]\!] \qquad |a_{i,i}| > \sum_{i \neq j} |a_{i,j}| \qquad \text{(diagonale dominante).}$$

Montrer que A est inversible.

$\boxed{\textbf{20.16}}$ **[♦♦♦]** Soient A et B dans $M_n(\mathbb{R})$ telles que $AB = A + B$.
Montrer que A et B commutent.

Dénombrement

1 Cardinal d'un ensemble fini.

1.1 Cardinal d'un ensemble, d'une partie.

Définition 1 (point de vue naïf).

Soit E un ensemble non vide. Il est dit fini s'il a un nombre fini d'éléments.

Ce nombre est appelé **cardinal** de E et noté $|E|$, ou $\#E$, ou $\mathrm{Card}(E)$.

On pose que l'ensemble vide est fini et que son cardinal est 0.

Par exemple, $\mathrm{Card}\left(\{\bigstar, \blacktriangledown, \square\}\right) = 3$ et pour $n \in \mathbb{N}^*$, $|\mathbb{U}_n| = n$.

Si a et b sont deux entiers relatifs avec $a \leq b$, $\mathrm{Card}([\![a, b]\!]) =$.

Proposition 2 (La partie et le tout).

Soit E un ensemble fini et A une partie de E.

- Toute partie A de E est un ensemble fini et $|A| \leq |E|$.
- Si A et B sont des parties de E, alors

$$A = B \quad \Longleftrightarrow \quad \begin{cases} A \subset B \\ |A| = |B| \end{cases}$$

Ce résultat est admis, faute de définition suffisamment solide pour les ensembles finis et leurs cardinaux. Le slogan derrière l'implication $\Longleftarrow$: *si la partie est aussi grande que le tout, alors elle est égale au tout.*

1.2 Cardinal et réunion.

La proposition suivante est admise sans démonstration. Après, promis, on se met au travail.

Proposition 3 (Réunion de parties disjointes)**.**

Soit E un ensemble fini et A et B deux parties de E disjointes ($A \cap B = \emptyset$) ; alors la partie $A \cup B$ est finie et a pour cardinal

$$|A \cup B| = |A| + |B|.$$

Plus généralement, pour $n \in \mathbb{N}^*$, si $A_1, \dots A_n$ n parties d'un ensemble fini E, deux à deux disjointes, alors, leur réunion est un ensemble fini de cardinal

$$\left|\bigcup_{k=1}^{n} A_k\right| = \sum_{k=1}^{n} |A_k|.$$

Dans le cas où les ensembles ci-dessus sont de même cardinal, on reformule ainsi :

« Le cardinal de la réunion de n ensembles disjoints, tous de cardinal p, est de cardinal np. »

L'énoncé précédent est appelé *principe du berger* : dans un troupeau de n brebis, il y a $4n$ pattes de brebis.

Proposition 4 (Cardinal du complémentaire)**.**

Soit E un ensemble fini et soient A et B deux parties de E . Alors

$$|A \setminus B| = |A| - |A \cap B|.$$

Notamment, le complémentaire de A dans E a pour cardinal $\left|\overline{A}\right| = |E \setminus A| = |E| - |A|$.

Proposition 5 (Réunion de parties quelconques)**.**

Soit E un ensemble fini et A et B deux parties de E. La partie finie $A \cup B$ a pour cardinal

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Exemple 6.

Compter tous les couples d'entiers (i, j) de $[\![1, n]\!]^2$ tels que $i \geq j$.

Exemple 7 (Formule du crible pour trois parties)**.**

Soient A, B, C trois parties d'un ensemble fini. Justifier que

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

1.3 Cardinal et produit cartésien.

Rappel : si $A_1, \ldots, A_p$ sont p ensembles, leur *produit cartésien*, ensemble de p-**uplets**, est défini par

$$A_1 \times A_2 \times \ldots \times A_p = \{(a_1, \ldots, a_p), \quad a_1 \in A_1, \ldots, a_p \in A_p\}.$$

Proposition 8 (Cardinal d'un produit cartésien)**.**

• Soient A et B deux ensembles finis. Leur produit cartésien $A \times B = \{(x, y) \; x \in A, y \in B\}$ est un ensemble fini, de cardinal

$$|A \times B| = |A| \cdot |B|.$$

• Plus généralement, si $A_1, A_2, \ldots A_p$ sont p ensembles finis ($p \in \mathbb{N}^*$). Alors

$$|A_1 \times A_2 \times \ldots A_p| = \prod_{k=1}^{p} |A_k|.$$

1.4 Cardinal et applications entre ensembles finis.

Proposition 9.

Soient E et F deux ensembles finis et $f : E \to F$ une application. Alors,

1. Si f est injective, alors $|E| \leq |F|$.
2. Si f est surjective, alors $|E| \geq |F|$.

Corollaire 10 (Principe des tiroirs)**.**

Soient E et F deux ensembles finis. Si $|E| > |F|$, alors il n'existe pas d'injection de E vers F.

« Lorsqu'on range des chaussettes dans des tiroirs,
s'il y a (strictement) plus de chaussettes que de tiroirs,
alors au moins un tiroir contiendra plus de deux chaussettes. »

Proposition 11 (Caractérisation de la bijectivité à l'aide du cardinal)**.**

Soit E et F deux ensembles finis et une application $f : E \to F$. Alors

1) f est bijective $\iff \begin{cases} f \text{ est injective} \\ |E| = |F|. \end{cases}$ 2) f est bijective $\iff \begin{cases} f \text{ est surjective} \\ |E| = |F|. \end{cases}$

Proposition 12 (Compter les applications de E dans F)**.**

L'ensemble des applications de E vers F (finis), noté F^E est un ensemble fini et son cardinal est

$$\left|F^E\right| = |F|^{|E|}.$$

2 Listes et combinaisons.

Lorsqu'on voudra dénombrer (ou *compter*) des objets, on essaiera de modéliser la situation à l'aide d'objets mathématiques connus, appartenant à des ensembles dont on connaît le cardinal. Les objets qui seront utilisés sont essentiellement de deux types : les p-uplets, et les parties à p éléments. Avant de passer aux résultats de dénombrement proprement dit, on fait ci-dessous quelques rappels, et on introduit les mots *listes* et *combinaisons*, utilisés en combinatoire.

Définition 13 (*vocabulaire spécifique au dénombrement*).

Soit E un ensemble et p un entier naturel non nul.

Un élément de E^p, c-à-d un p-uplet $(x_1, \ldots, x_p)$ d'éléments de E peut être appelé **p-liste** de E.

Dans un p-uplet, $(x_1, \ldots, x_p)$ de E^p, certaines coordonnées peuvent être égales. De plus, l'ordre d'écriture des coordonnées est primordial. Ainsi,

$(1, 2, 3, 3, 2)$ est un 5-uplet de $\mathbb{N}$ (une *5-liste*), différent de $(1, 2, 2, 3, 3)$.

Définition 14 (*vocabulaire spécifique au dénombrement*).

Soit E un ensemble et p un entier naturel.

Une partie de E à p éléments $\{x_1, \ldots, x_p\}$ pourra être appelée **p-combinaison** de E.

L'ensemble $\{1, 2, 4, 4\}$ est égal à l'ensemble $\{1, 2, 4\}$. C'est donc une 3-combinaison de $\mathbb{N}$.

Lorsqu'on écrira que $\{x_1, \ldots, x_p\}$ est une p-combinaison de E, p sera alors le cardinal de E : pour une telle écriture, les x_i sont forcément deux à deux distincts.

Dans l'écriture $\{x_1, \ldots, x_p\}$, l'ordre d'écriture des x_i n'a aucune importance :

$\{1, 2, 3\}$ et $\{3, 2, 1\}$ sont la même 3-combinaison.

2.1 p-uplets d'un ensemble fini.

Proposition 15 (Compter les p-uplets d'éléments de E).

Soit E un ensemble fini de cardinal n et un entier naturel non nul p.

Le nombre de p-uplets d'éléments de E est n^p.

Soit E un ensemble. On s'intéresse dans ce paragraphe aux p-uplets d'éléments de E *distincts deux à deux*. Ainsi, un p-uplet $(x_1, \ldots, x_p) \in E^p$ est un tel p-uplet si

$$\forall i, j \in [\![1, p]\!] \quad i \neq j \Longrightarrow x_i \neq x_j$$

Ces p-uplets (ou p-listes) particuliers sont parfois désignés comme des **p-arrangements** de E. Ainsi, la liste $(1, 5, 3)$ est un 3-arrangement de $\mathbb{N}$, $(1, 5, 5)$ n'en est pas un.

Proposition 16 (Compter les p-uplets d'éléments distincts)**.**

Soit E un ensemble fini de cardinal n et un entier naturel non nul p.

Le nombre de p-uplets d'éléments de E deux à deux distincts est

$$n(n-1)\dots(n-p+1) = \begin{cases} \dfrac{n!}{(n-p)!} & \text{si} \quad p \leq n \\ 0 & \text{si} \quad p > n. \end{cases}$$

Si besoin : une proposition de notation pour l'ensemble des p-arrangements d'un ensemble E : $\mathcal{A}_p(E)$.
Le résultat principal de la proposition ci-dessus peut alors se récrire ainsi :

$$\text{si } E \text{ est un ensemble fini de cardinal } n \text{, et } p \in [\![0, n]\!] \text{, alors } \boxed{|\mathcal{A}_p(E)| = \frac{n!}{(n-p)!}}.$$

Corollaire 17 (Compter les injections, les bijections)**.**

Soient E et F deux ensembles finis de cardinaux respectifs p et n. On suppose $p \leq n$.

Le nombre d'applications injectives allant de E dans F est $\dfrac{n!}{(n-p)!}$.

Il existe donc $n!$ bijections définies entre deux ensembles de même cardinal n.

En particulier, si E est un ensemble fini de cardinal n, son groupe symétrique (le groupe de ses permutations) est de cardinal $n!$

2.2 Parties d'un ensemble fini.

Proposition 18 (Compter les parties d'un ensemble fini)**.**

Soit E un ensemble fini de cardinal n. Le nombre de parties de E vaut 2^n.

Le résultat peut se récrire ainsi : si E est un ensemble fini, $\boxed{|\mathcal{P}(E)| = 2^{|E|}}$.

Rappel : On avait défini le coefficient binomial $\dbinom{n}{p}$ comme le quotient $\dfrac{n!}{p!(n-p)!}$ (cas non dégénérés) et prouvé que c'est un entier. Il est temps de comprendre pourquoi il se lit « p parmi n ».

Proposition 19 (Compter les parties à p éléments d'un ensemble fini)**.**

Soient E un ensemble fini de cardinal n, et p un entier naturel.

Le nombre de parties de E ayant p éléments est $\dbinom{n}{p}$.

Si besoin : une proposition de notation pour l'ensemble des parties à p éléments d'un ensemble E : $\mathcal{P}_p(E)$.

Le résultat principal de la proposition ci-dessus peut se récrire ainsi :

$$\text{si } E \text{ est un ensemble fini de cardinal } n, \text{ et } p \in \mathbb{N}, \text{ alors } \boxed{|\mathcal{P}_p(E)| = \binom{n}{p}}.$$

On donne pour finir une preuve combinatoire des formules ci-dessous.

Proposition 20.

Soit $n \in \mathbb{N}$.

$$\forall p \in \mathbb{N}\ \binom{n}{p} = \binom{n}{n-p}, \qquad \forall p \in \mathbb{N}^*\ \binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1}, \qquad \forall p \in \mathbb{N}\ \binom{n+1}{p+1} = \binom{n}{p+1} + \binom{n}{p}.$$

(symétrie) (formule *sans nom*) (formule de Pascal)

Et pourquoi ne pas aussi poser un regard combinatoire sur la formule du binôme... qui devient alors (presque) une évidence : pour $(a,b) \in \mathbb{C}^2$ et $n \in \mathbb{N}$,

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

Écrire un terme du développement, c'est choisir a ou b dans chacune des n *boîtes*.
La question est de savoir, pour k donné, combien de fois on va trouver $a^k b^{n-k}$ en développant tout ?
Réponse : il y a $\binom{n}{k}$ façons de choisir k fois le terme a (et donc $n-k$ fois b)...

Et si on augmente le nombre de termes, à quoi ressemble la formule du *multinôme de Newton ?* Pour $p \in \mathbb{N}^*$ et $a_1, \dots, a_p$ des nombres complexes, on a

$$(a_1 + \dots, a_p)^n = \sum_{k_1 + \cdots k_p = n} \binom{n}{k_1, \dots, k_p} a_1^{k_1} \cdots a_p^{k_p}$$

Que vaut le *coefficient multinomial* $\binom{n}{k_1,\dots,k_p}$ pour un p-uplet $(k_1, \dots, k_p)$ d'entiers naturels qui somment à n ?
Choisir un tel p-uplet, c'est

1. Choisir k_1 $\longrightarrow \binom{n}{k_1}$ choix
2. Pour chaque valeur de k_1, on a $\binom{n-k_1}{k_2}$ choix pour k_2 $\longrightarrow \binom{n}{k_1} \times \binom{n-k_1}{k_2}$ choix pour (k_1, k_2)
3. Itérons , pour chaque $p-1$-uplet $(k_1, \dots, k_{p-1})$, on a $\binom{n-(k_1+\cdots+k_{p-1})}{k_p}$ choix pour k_p
   $\longrightarrow \binom{n}{k_1} \times \binom{n-k_1}{k_2} \cdots \binom{n-(k_1+\cdots+k_{p-1})}{k_p}$ choix pour $(k_1, \dots, k_p)$

Évidemment, il faudrait justifier correctement ce qui précède et notamment l'écriture de produits avec celle d'union, de principes des bergers, etc... On se contentera ici de ce qui est écrit. On a finalement

$$\binom{n}{k_1, \dots, k_p} = \frac{n!}{k_1!(n-k_1)!} \times \frac{(n-k_1)!}{k_2!(n-(k_1+k_2))!} \cdots \frac{(n-(k_1+\cdots+k_{p-1}))!}{k_p!(n-n)!} = \frac{n!}{k_1! k_2! \cdots k_p!}.$$

Exercices

$\boxed{\textbf{21.1}}$ **[♦◊◊]**
A Reuste-sur-Linuxe, charmant village francilien, il y a 52 célibataires : 20 femmes et 32 hommes.
Combien de nouveaux couples hétérosexuels peuvent être formés dans le village ? De couples homosexuels ?

$\boxed{\textbf{21.2}}$ **[♦◊◊]** A l'entrée d'un immeuble, on dispose d'un clavier de 12 touches : trois lettres A, B et C, et les neuf chiffres de 1 à 9. Le code d'ouverture de la porte est composé d'une lettre suivie d'un nombre de quatre chiffres. Par exemple $B2923$.

1. Combien existe-t-il de codes différents ?
2. Combien existe-t-il de codes comportant au moins une fois le chiffre 7 ?
3. Combien existe-t-il de codes pour lesquels tous les chiffres sont pairs ?
4. Combien existe-t-il de codes pour lesquels les quatres chiffres sont différents ?

$\boxed{\textbf{21.3}}$ **[♦◊◊]** Mes voisins font la fête et c'est l'heure de trinquer. J'entends 78 tintements de verres.
Combien sont-ils ?

$\boxed{\textbf{21.4}}$ **[♦♦◊]** Combien d'anagrammes ont les mots $MATHS$, $COLLE$, et $ABRACADABRA$?

$\boxed{\textbf{21.5}}$ **[♦♦◊]** On dispose de 8 professeurs, à répartir dans 4 écoles.
Combien de répartitions sont possibles ?
Et combien si on impose deux professeurs par école ?

$\boxed{\textbf{21.6}}$ **[♦◊◊]** Soit E un ensemble de cardinal $n \in \mathbb{N}^*$.

1. Rappeler le nombre de parties de E.
2. Pour $k \in [\![0, n]\!]$, rappeler combien il existe de parties de E ayant k éléments.
3. Sait-on retrouver le résultat de la question 1 en connaissant celui de la question 2 ?

$\boxed{\textbf{21.7}}$ **[♦♦◊]** Soit E un ensemble de cardinal $n \in \mathbb{N}^*$.

1. Combien existe-t-il de couples (A, x) avec A une partie de E et x un élément de E ?
2. Combien existe-t-il de couples (A, x) avec A une partie de E et x un élément de A ?

$\boxed{\textbf{21.8}}$ **[♦◊◊]** Soit $n \geq 1$. En développant $(1-1)^n$, démontrer qu'un ensemble E de cardinal n a autant de parties de cardinal pair que de parties de cardinal impair.

$\boxed{\textbf{21.9}}$ **[♦♦♦]** 112eme et dernier exercice de la banque CCINP.

Soit $n \in \mathbb{N}^*$ et E un ensemble possédant n éléments.
On désigne par $\mathcal{P}(E)$ l'ensemble des parties de E.

1. Déterminer le nombre a de couples $(A, B) \in (\mathcal{P}(E))^2$ tels que $A \subset B$.
2. Déterminer le nombre b de couples $(A, B) \in (\mathcal{P}(E))^2$ tels que $A \cap B = \emptyset$.
3. Déterminer le nombre c de triplets $(A, B, C) \in (\mathcal{P}(E))^3$ tels que A, B et C soient deux à deux disjoints et vérifient $A \cup B \cup C = E$.

$\boxed{21.10}$ **[♦♦◊]** Soit E un ensemble non vide et n son cardinal.
Exprimer en fonction de n les sommes

$$\sum_{X\in\mathcal{P}(E)} 1,\qquad \sum_{X\in\mathcal{P}(E)} |X|,\qquad \sum_{(X,Y)\in(\mathcal{P}(E))^2} |X\cap Y|,\qquad \sum_{(X,Y)\in(\mathcal{P}(E))^2} |X\cup Y|.$$

$\boxed{21.11}$ **[♦♦◊]**
Soit G un groupe fini de cardinal pair. On travaille en notation multiplicative et on note e le neutre du groupe. On souhaite prouver l'existence d'un élément x de G tel que $x^2=e$ et tel que $x\neq e$. On définit l'ensemble

$$E=\left\{x\in G \mid x^2\neq e\right\}.$$

1. On définit sur E la relation $\sim$ par

$$\forall (x,y)\in E^2\quad x\sim y \iff \left(x=y \ \text{ ou } \ x=y^{-1}\right).$$

   Démontrer que $\sim$ est une relation d'équivalence sur E.
2. Conclure.

$\boxed{21.12}$ **[♦♦◊]** [Théorème de Lagrange]
Soit $(G,\star)$ un groupe fini et H un sous-groupe de G ; on veut montrer que son cardinal divise celui de G.
Pour un élément x de G fixé, on note

$$x\star H=\{x\star h \mid h\in H\}.$$

On note aussi $\mathscr{R}$ la relation binaire sur G définie par

$$\forall (x,y)\in G^2\qquad x\,\mathscr{R}\,y \iff x^{-1}\star y\in H.$$

1. Soit $x\in G$. Démontrer que l'ensemble $x\star H$ a le même cardinal que H.
2. Démontrer que $\mathscr{R}$ est une relation d'équivalence sur G.
3. Soit $x\in G$. Démontrer que sa classe d'équivalence pour la relation $\mathscr{R}$ est $x\star H$.
4. Conclure.

$\boxed{21.13}$ **[♦♦♦]** Formule de Vandermonde
Soient $(p,q,n)\in\mathbb{N}^3$. Proposer une démonstration combinatoire de l'identité ci-dessous.

$$\sum_{k=0}^{n}\binom{p}{k}\binom{q}{n-k}=\binom{p+q}{n}.$$

$\boxed{21.14}$ **[♦♦◊]** Soit $(n,p)\in(\mathbb{N}^*)^2$.
Combien y a-t-il d'applications strictement croissantes de $[\![1,p]\!]$ dans $[\![1,n]\!]$?

$\boxed{21.15}$ **[♦♦♦]** Soient $n\in\mathbb{N}^*$ et $p\in\mathbb{N}$. Déterminer le nombre de solutions dans $\{0,1\}^n$ à l'équation

$$x_1+x_2+\cdots x_n=p$$

$\boxed{21.16}$ **[♦♦♦]** Soient $n\in\mathbb{N}^*$. Combien y a-t-il de surjections de $[\![1,n+1]\!]$ dans $[\![1,n]\!]$?

$\boxed{21.17}$ **[♦♦♦]** Soit E un ensemble à n éléments, où n est un entier supérieur à 2.
Combien existe-t-il de fonctions $f:E\to E$ telles que $\operatorname{Card}(\operatorname{Im}(f))=n-1$?

---

22 Limites et continuité d'une fonction

Notations.

Les lettres I et J désigneront dans ce chapitre des intervalles de $\mathbb{R}$ non vides et non réduits à un point.
La notation $\overline{\mathbb{R}}$ désigne ici l'ensemble $\mathbb{R} \cup \{+\infty\} \cup \{-\infty\}$.

Les fonctions considérées dans ce chapitre seront définies sur une partie de $\mathbb{R}$ qui sera notée D.
Cette partie est un intervalle I ou un intervalle privé d'un point $I \setminus \{a\}$ avec $a \in I$.

Ces fonctions sont à valeurs dans $\mathbb{K}$, où $\mathbb{K}$ désigne au choix le corps $\mathbb{R}$ ou $\mathbb{C}$.
Pour certains résultats nécessitant l'utilisation d'un ordre, il faudra prendre $\mathbb{K} = \mathbb{R}$.
Le choix $\mathbb{K} = \mathbb{R}$ est obligatoire aussi lorsqu'on veut donner la courbe représentative d'une fonction.

Autoriser l'ensemble de définition D à valoir $I \setminus \{a\}$ nous permettra notamment de traiter la convergence d'un taux d'accroissement $\frac{f(x)-f(a)}{x-a}$, bien défini sur $I \setminus \{a\}$ lorsque $f : I \to \mathbb{K}$ et $a \in I$.

Définition 1.

Soit I un intervalle, $a \in \overline{\mathbb{R}}$ un élément ou une borne de I et $f : D \to \mathbb{K}$ avec $D = I$ ou $D = I \setminus \{a\}$.
On dit qu'une propriété portant sur f est vraie **au voisinage de** a si

- [$a \in \mathbb{R}$, a *fini*] il existe $\eta > 0$ tel que la propriété est vraie sur $D \cap [a-\eta, a+\eta]$,
- [cas $a = +\infty$] il existe $A \in \mathbb{R}$ tel que la propriété est vraie sur $D \cap [A, +\infty[$,
- [cas $a = -\infty$] il existe $A \in \mathbb{R}$ tel que la propriété est vraie sur $D \cap]-\infty, A]$.

1 Limites et continuité d'une fonction en un point.

1.1 Limite d'une fonction en un point.

Définition 2 (Cas où $\mathbb{K} = \mathbb{R}$)**.**

Soit I un intervalle, $a \in \overline{\mathbb{R}}$ un élément ou une borne de I. Soit $D = I$ ou $D = I \setminus \{a\}$.
Soit $f : D \to \mathbb{K}$ et $L \in \overline{\mathbb{R}}$.
Les équivalences ci-dessous définissent l'assertion f **admet** L **pour limite en** a, ce qui sera notée

$$f(x) \underset{x \to a}{\longrightarrow} L.$$

I Cas a fini, $L = \ell$, finie :

$$f(x) \underset{x \to a}{\longrightarrow} \ell \iff \forall \varepsilon > 0 \quad \exists \eta > 0 \quad \forall x \in D \cap [a - \eta, a + \eta] \quad |f(x) - \ell| \leq \varepsilon.$$

II Cas $a = +\infty$, $L = \ell$, finie :

$$f(x) \underset{x \to +\infty}{\longrightarrow} \ell \iff \forall \varepsilon > 0 \quad \exists A \in \mathbb{R} \quad \forall x \in D \cap [A, +\infty[\quad |f(x) - \ell| \leq \varepsilon.$$

III Cas $a = -\infty$, $L = \ell$, finie :

$$f(x) \underset{x \to -\infty}{\longrightarrow} \ell \iff \forall \varepsilon > 0 \quad \exists A \in \mathbb{R} \quad \forall x \in D \cap] - \infty, A] \quad |f(x) - \ell| \leq \varepsilon.$$

IV Cas a fini, $L = +\infty$:

$$f(x) \underset{x \to a}{\longrightarrow} +\infty \iff \forall B \in \mathbb{R} \quad \exists \eta > 0 \quad \forall x \in D \cap [a - \eta, a + \eta] \quad f(x) \geq B.$$

V Cas $a = +\infty$, $L = +\infty$:

$$f(x) \underset{x \to +\infty}{\longrightarrow} +\infty \iff \forall B \in \mathbb{R} \quad \exists A \in \mathbb{R} \quad \forall x \in D \cap [A, +\infty[\quad f(x) \geq B.$$

VI Cas $a = -\infty$, $L = +\infty$:

$$f(x) \underset{x \to -\infty}{\longrightarrow} +\infty \iff \forall B \in \mathbb{R} \quad \exists A \in \mathbb{R} \quad \forall x \in D \cap] - \infty, A] \quad f(x) \geq B.$$

VII Cas a fini, $L = -\infty$:

$$f(x) \underset{x \to a}{\longrightarrow} -\infty \iff \forall B \in \mathbb{R} \quad \exists \eta > 0 \quad \forall x \in D \cap [a - \eta, a + \eta] \quad f(x) \leq B.$$

VIII Cas $a = +\infty$, $L = -\infty$:

$$f(x) \underset{x \to +\infty}{\longrightarrow} -\infty \iff \forall B \in \mathbb{R} \quad \exists A \in \mathbb{R} \quad \forall x \in D \cap [A, +\infty[\quad f(x) \leq B.$$

IX Cas $a = -\infty$, $L = -\infty$:

$$f(x) \underset{x \to -\infty}{\longrightarrow} -\infty \iff \forall B \in \mathbb{R} \quad \exists A \in \mathbb{R} \quad \forall x \in D \cap] - \infty, A] \quad f(x) \leq B.$$

Version commune pour I, II, et III : dire que la fonction f admet le nombre réel ℓ pour limite en a (qui est fini, ou pas selon les cas), c'est dire que pour tout $\varepsilon > 0$, on a $f(x) \in [\ell - \varepsilon, \ell + \varepsilon]$ *au voisinage de* a.

Voici d'abord une réécriture du cas a fini, $L = \ell$ finie :

$$f(x) \underset{x \to a}{\longrightarrow} \ell \qquad \Longleftrightarrow \qquad \forall \varepsilon > 0 \quad \exists \eta > 0 \quad \forall x \in D \quad |x - a| \leq \eta \implies |f(x) - \ell| \leq \varepsilon.$$

Dans les énoncés suivants, I est un intervalle, $a \in \overline{\mathbb{R}}$ un élément ou une borne de I, $D = I$ ou $D = I \setminus \{a\}$. La fonction f est définie sur D et à valeurs dans $\mathbb{K}$.

Définition 3 (Cas où $\mathbb{K} = \mathbb{C}$)**.**

Soit $\ell \in \mathbb{C}$. En remplaçant la valeur absolue par le module dans les cas I, II et III de 2, on définit

$$f(x) \underset{x \to a}{\longrightarrow} \ell.$$

Proposition 4.

Soit $\ell \in \mathbb{C}$.

$$f(x) \underset{x \to a}{\longrightarrow} \ell \iff \begin{cases} \mathrm{Re}(f(x)) \underset{x \to a}{\longrightarrow} \mathrm{Re}(\ell) \\ \mathrm{Im}(f(x)) \underset{x \to a}{\longrightarrow} \mathrm{Im}(\ell) \end{cases}$$

Remarque. On ne définit pas "tendre vers l'infini" pour une fonction f à valeurs complexes. Si besoin, on peut décider que pour une telle fonction, "tendre vers l'infini", c'est finir par quitter tout disque du plan complexe centré en 0, soit $|f(x)| \underset{x \to a}{\longrightarrow} +\infty$.

Proposition 5 (Unicité de la limite)**.**

Si f admet une limite en a, celle-ci est unique.
Plus précisément, pour L, L' dans $\overline{\mathbb{R}}$ ou dans $\mathbb{C}$, si f admet L et L' pour limite en a, alors $L = L'$.
On pourra donc parler, lorsqu'elle existe, de **la** limite de la fonction en a, que l'on notera $\lim\limits_{x \to a} f(x)$.

Une nuance (la même que pour les suites) :

$$f(x) \underset{x \to a}{\longrightarrow} L \qquad \text{signifie « } f \text{ admet une limite en } a \textbf{ et } \text{celle-ci vaut } L \text{ ».}$$

$$\lim_{x \to a} f(x) = L \qquad \text{signifie « la limite de } f \text{ en } a \text{ vaut } L \text{ ».}$$

Écrire la seconde phrase réclame de savoir que la limite de f en a existe.

Proposition 6 (Quand la limite est finie)**.**

- Si f admet une limite finie en a, alors elle est bornée au voisinage de a.
- Si de surcroît f est <u>définie</u> en a (qui est forcément fini, dans ce cas) alors $\lim\limits_{x \to a} f(x) = f(a)$.

Remarque. On rappelle qu'être "bornée" pour une fonction à valeurs réelles, c'est être majorée et minorée, ce qui est équivalent à être majorée en valeur absolue. Pour une fonction à valeurs complexes, être bornée c'est être majorée en module.

Lemme 7 (Cas $\mathbb{K} = \mathbb{R}$).

Soit $(\ell, m) \in \mathbb{R}^2$.

$$\text{Si } f(x) \underset{x\to a}{\longrightarrow} \ell \text{ et } \ell > m \text{ alors l'inégalité } f(x) > m \text{ est vraie au voisinage de } a.$$

Proposition 8 (Conservation des inégalités larges par passage à la limite)**.**

Soit I un intervalle, $a \in \overline{\mathbb{R}}$ un élément ou une borne de I. Soit $D = I$ ou $D = I \setminus \{a\}$.
Soient $f : D \to \mathbb{R}$ et $g : D \to \mathbb{R}$ et $(\ell, \ell') \in \mathbb{R}^2$.

$$\text{Si } \left\{ \begin{array}{c} \forall x \in D \quad f(x) \leq g(x) \\ f(x) \underset{x\to a}{\longrightarrow} \ell \;\text{ et }\; g(x) \underset{x\to a}{\longrightarrow} \ell' \end{array} \right. \qquad \text{alors } \ell \leq \ell'.$$

1.2 Continuité d'une fonction en un point.

Considérons d'abord le cas d'une limite finie en un point où la fonction *est définie*.

Définition 9.

Soit $f : I \to \mathbb{K}$ et $a \in I$. On dit que f est **continue en** a si

$$f(x) \underset{x\to a}{\to} f(a).$$

Remarque. La définition ci-dessus est un peu redondante. En effet, d'après P6 si f admet une limite en a *et* est définie en a, alors nécessairement, $\lim\limits_{x\to a} f(x) = f(a)$.

Considérons maintenant le cas d'une limite finie en un point où la fonction *n'est <u>pas</u> définie*.

Proposition-Définition 10.

Soit I un intervalle et $a \in I$. Soit une fonction $f : I \setminus \{a\} \to \mathbb{K}$ qui admet une limite finie ℓ en a.
On dit alors que f est **prolongeable par continuité** en a, et on définit ce prolongement en posant

$$\widetilde{f} : x \mapsto \left\{ \begin{array}{cl} f(x) & \text{si } x \in I \setminus \{a\} \\ \ell & \text{si } x = a. \end{array} \right.$$

La fonction $\widetilde{f}$ ainsi définie sur I est continue en a et appelée le **prolongement de f par continuité** en a. On pourra aussi noter simplement f ce prolongement.

Remarque. On ne parle pas de prolongement par continuité en a si f est déjà définie en a !
Dans ce cas où f est définie en a, alors f est continue en a... ou pas continue en a.

Exemple. La fonction $f : x \mapsto x^x$, définie sur $\mathbb{R}_+^*$ est-elle prolongeable par continuité en 0 ?
Si oui, définir ce prolongement.

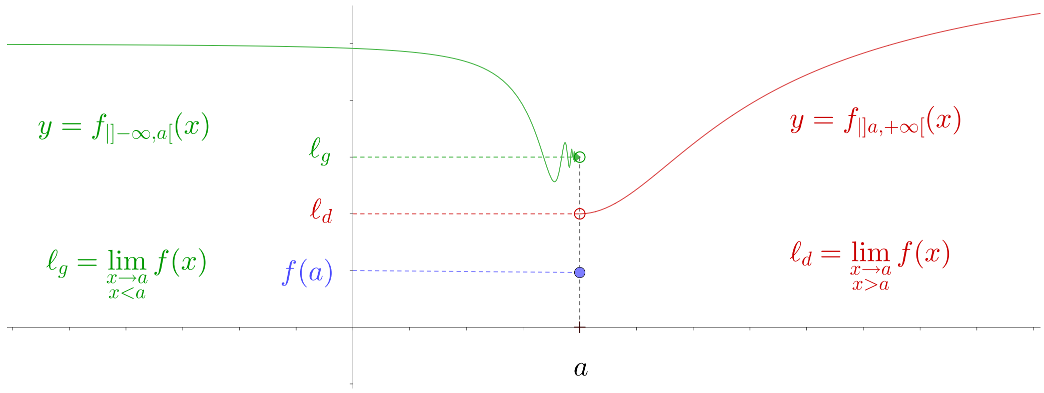
1.3 Limite et continuité à gauche et à droite.

Définition 11.

Soit I un intervalle, $a \in \overline{\mathbb{R}}$ un élément ou une borne de I. Soit $D = I$ ou $D = I \setminus \{a\}$.
Soit $f : D \to \mathbb{K}$ et $L \in \overline{\mathbb{R}}$ ou $L \in \mathbb{C}$. On dit que

- L est la **limite à gauche** de f en a si $a \neq \inf(I)$ et si $f_{|\,]-\infty,a[\cap I}$ admet L pour limite en a. On note alors
$$f(x) \underset{\substack{x\to a\\ x<a}}{\to} L \quad \text{et} \quad L = \lim_{\substack{x\to a\\ x<a}} f(x).$$
- L est la **limite à droite** de f en a si $a \neq \sup(I)$ et si $f_{|\,]a,+\infty[\cap I}$ admet L pour limite en a. On note alors
$$f(x) \underset{\substack{x\to a\\ x>a}}{\to} L \quad \text{et} \quad L = \lim_{\substack{x\to a\\ x>a}} f(x).$$

Autre notation pour les limites à gauche ou à droite : $\lim\limits_{x\to a-} f(x)$ et $\lim\limits_{x\to a+} f(x)$.



Proposition 12.

Soit I un intervalle et a un élément de I qui n'est pas une borne de I. Soit $D = I$ ou $D = I \setminus \{a\}$. Soit $f : D \to \mathbb{K}$.

1. <u>Cas $a \in D$.</u>

   La fonction f est continue en a si et seulement si $\begin{cases} f \text{ a une limite à gauche en } a \\ f \text{ a une limite à droite en } a \\ \lim\limits_{x\to a-} f(x) = \lim\limits_{x\to a+} f(x) = f(a). \end{cases}$

2. <u>Cas $a \notin D$.</u>

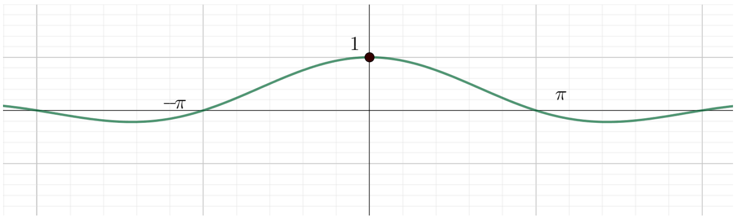
   La fonction f a une limite en a a si et seulement si $\begin{cases} f \text{ a une limite à gauche en } a \\ f \text{ a une limite à droite en } a \\ \lim\limits_{x\to a-} f(x) = \lim\limits_{x\to a+} f(x). \end{cases}$

   La limite de f en a est alors la valeur commune des limites à gauche et à droite.

Remarque. Si une fonction a des limites à gauche et à droite en a qui sont différentes, alors cette fonction n'a pas de limite en a.

Exemple 13 (quand les limites à gauche et à droite coïncident).

$$\frac{\sin x}{x} \underset{x\to 0}{\to} 1$$



La fonction **sinus cardinal**

$$f : \begin{cases} \mathbb{R}^* & \to & \mathbb{R} \\ x & \mapsto & \dfrac{\sin x}{x} \end{cases}$$

a une limite à droite en 0 qui vaut 1 (preuve géométrique à la fin du chapitre de trigonométrie).
Par parité, elle admet aussi 1 pour limite à gauche en 0.
Elle a donc 1 pour limite en 0 : elle est prolongeable par continuité en 0 en posant $f(0) = 1$.

Définition 14.

Soit $f : I \to \mathbb{R}$ et $a \in I$. On dit que

— f est **continue à gauche en** a si $f(x) \underset{x\to a-}{\to} f(a)$.

— f est **continue à droite en** a si $f(x) \underset{x\to a+}{\to} f(a)$.

Exemple 15.

La fonction $x \mapsto \lfloor x \rfloor$ est-elle continue à gauche en 2 ? continue à droite en 2 ?

Le premier résultat de la proposition 12 se récrit de la manière suivante.

Proposition 16.

Soit une fonction $f : I \to \mathbb{R}$ et $a \in I$.

f est continue en a si et seulement si elle est continue à gauche et à droite en a.

1.4 Caractérisation séquentielle de la limite, de la continuité.

Théorème 17 (Caractérisation séquentielle de la limite).

Soit I un intervalle, $a \in \overline{\mathbb{R}}$ un élément ou une borne de I. Soit $D = I$ ou $D = I \setminus \{a\}$.
Soit $f : D \to \mathbb{K}$ et $L \in \overline{\mathbb{R}}$ si $\mathbb{K} = \mathbb{R}$ ou $L \in \mathbb{C}$ si $\mathbb{K} = \mathbb{C}$.

$$f(x) \underset{x\to a}{\longrightarrow} L \qquad \Longleftrightarrow \qquad \Big(\forall (u_n) \in D^{\mathbb{N}} \quad u_n \to a \implies f(u_n) \to L\Big)$$

Corollaire 18.

Soit une fonction f telle que considérée dans le théorème précédent.
S'il existe deux suites (u_n) et (v_n) d'éléments de D telles que :

$$\begin{cases} u_n \to a \\ v_n \to a \end{cases} \quad \text{et} \quad \begin{array}{c} (f(u_n)) \text{ et } (f(v_n)) \\ \text{ne convergent pas vers la même limite.} \end{array}$$

alors f n'admet pas de limite en a.

Exemple. Montrer que cos et sin n'ont pas de limite en $+\infty$.

Corollaire 19 (Caractérisation séquentielle de la continuité en un point)**.**

Soit une fonction $f : I \to \mathbb{K}$ et $a \in I$. Il y a équivalence entre les deux assertions

1) f est continue en a.
2) Pour toute suite $u \in I^{\mathbb{N}}$ tendant vers a, $(f(u_n))$ tend vers $f(a)$.

Applications. On donne deux applications de 1) $\Longrightarrow$ 2). La première est le "théorème du point fixe" pour une suite définie par une relation du type $u_{n+1} = f(u_n)$. La seconde application est détermine les morphismes continus de $\mathbb{R}$ dans lui-même. Pour les applications de 2) $\Longrightarrow$ 1), on attendra le prochain paragraphe.

Proposition 20.

Soit $f : I \to I$ (l'intervalle I est stable par f), et (u_n) définie par $\begin{cases} u_0 \in I \\ \forall n \in \mathbb{N} \quad u_{n+1} = f(u_n). \end{cases}$
Si u converge vers une limite ℓ, que $\ell \in I$ et que f est continue en ℓ, alors $f(\ell) = \ell$

Exemple 21 ((*) Une équation fonctionnelle classique)**.**

Trouver toutes les fonctions f continues en tout point de $\mathbb{R}$ telles que

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

1.5 Limites et opérations.

Proposition 22 (opérations sur les limites finies)**.**

Soit I un intervalle, $a \in \overline{\mathbb{R}}$ un élément ou une borne de I. Soit $D = I$ ou $D = I \setminus \{a\}$.
Soit $f : D \to \mathbb{K}$ et $g : D \to \mathbb{K}$. Soient ℓ et ℓ' dans $\mathbb{K}$. Soient λ et μ dans $\mathbb{K}$.

1. La fonction $\lambda f + \mu g$ admet $\lambda \ell + \mu \ell'$ pour limite en a.
2. La fonction fg admet $\ell \ell'$ pour limite en a.
3. Si $\ell \neq 0$, alors $1/f$ est bien définie au voisinage de a et admet pour limite $1/\ell$ en a.

Pour les résultats sur les limites infinies, on fait confiance au lecteur, qui a déjà eu un cours sur la limite d'une suite.

Exemple 23 (Cas d'une limite infinie : débrouillez-vous)**.**

La limite $\lim\limits_{x\to 0+} \dfrac{1}{x\ln(x)}$ existe-t-elle ? Que vaut-elle ?

Corollaire 24 (opérations sur les fonctions continues en un point)**.**

Soient $f : I \to \mathbb{K}$, $g : I \to \mathbb{K}$ et $a \in I$. Soient λ et μ dans $\mathbb{K}$.
Si f et g sont continues en a alors

- la fonction $\lambda f + \mu g$ est continue en a,
- la fonction fg est continue en a,
- si $f(a) \neq 0$, alors $1/f$ est bien définie au voisinage de a et y est continue.

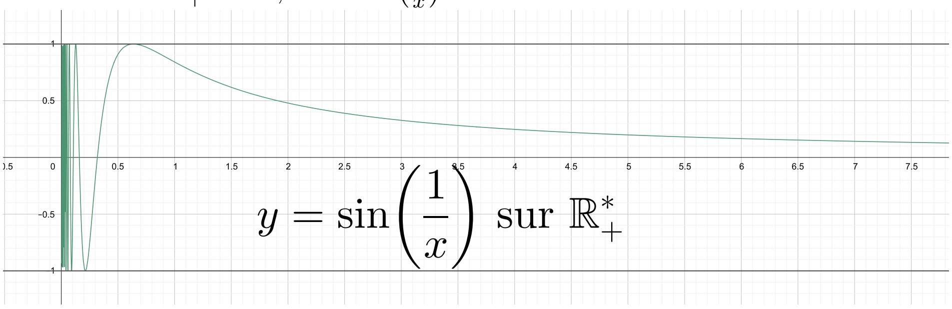
Proposition 25 (Composition des limites : deux fonctions)**.**

Soient I et J deux intervalles.
Soient $a, b, c \in \overline{\mathbb{R}}$, a étant un élément ou une borne de I et b un élément ou une borne de J.
On note D l'ensemble I ou $I \setminus \{a\}$ et D' l'ensemble J ou $J \setminus \{b\}$. Soient $f : D \to D'$ et $g : D' \to \mathbb{K}$

$$\text{Si} \quad \begin{cases} f(x) \underset{x\to a}{\longrightarrow} b \\ g(y) \underset{y\to b}{\longrightarrow} c \end{cases} \qquad \text{alors} \quad g\circ f(x) \underset{x\to a}{\longrightarrow} c.$$

Exemple 26.

Que dire de la fonction $\mathbb{R}_+^* \to \mathbb{R}\,;\, x \mapsto \sin\left(\frac{1}{x}\right)$ en $+\infty$? En 0 ?



Corollaire 27 (Composition de fonctions continues en un point)**.**

Soit $f : I \to J$ et $g : J \to \mathbb{K}$, où I et J sont des intervalles de $\mathbb{R}$. Soit $a \in I$.

Si f est continue en a et g continue en $f(a)$ alors $g \circ f$ est continue en a.

1.6 Théorèmes d'existence de limite.

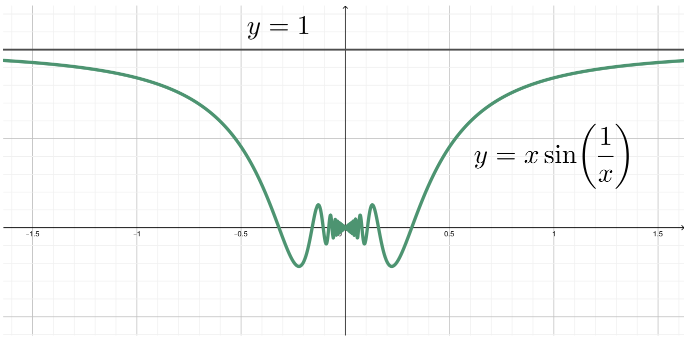
Théorème 28 (des gendarmes, pour les fonctions)**.**

Soit I un intervalle, $a \in \overline{\mathbb{R}}$ un élément ou une borne de I. Soit $D = I$ ou $D = I \setminus \{a\}$.
Soient f, g, h définies sur D et à valeurs réelles et $\ell \in \mathbb{R}$.

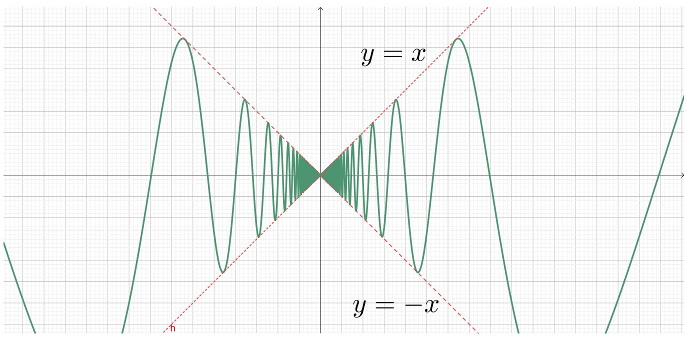
$$\text{Si} \quad \left\{ \begin{array}{c} \forall x \in D \quad f(x) \leq g(x) \leq h(x), \\ f(x) \underset{x \to a}{\to} \ell \quad \text{et} \quad h(x) \underset{x \to a}{\to} \ell \end{array} \right. \qquad \text{alors} \quad g(x) \underset{x \to a}{\to} \ell.$$

Exemple 29.

Étudier les limite en 0 et en $+\infty$ de $f : \left\{ \begin{array}{ccc} \mathbb{R}^* & \to & \mathbb{R} \\ x & \mapsto & x \sin\left(\frac{1}{x}\right) \end{array} \right.$.



La fonction $x \mapsto x \sin\left(\dfrac{1}{x}\right)$, sur $\mathbb{R}^*$.



La fonction $x \mapsto x \sin\left(\dfrac{1}{x}\right)$, zoom en 0.

Proposition 30 (de minoration, de majoration)**.**

Mêmes notations qu'au-dessus.

- Si $\forall x \in I \ f(x) \leq g(x)$ et $f(x) \underset{x \to a}{\to} +\infty$, alors $g(x) \underset{x \to a}{\to} +\infty$.
- Si $\forall x \in I \ f(x) \leq g(x)$ et $g(x) \underset{x \to a}{\to} -\infty$, alors $f(x) \underset{x \to a}{\to} -\infty$.

Théorème 31 (de la limite monotone pour les fonctions)**.**

Soit $I =]a, b[$ un intervalle ouvert, où $a \in \mathbb{R} \cup \{-\infty\}$ et $b \in \mathbb{R} \cup \{+\infty\}$.
Soit $f : I \to \mathbb{R}$ une fonction croissante sur I.

- En tout point c de $]a, b[$, f admet une limite finie à gauche et à droite. De plus,

$$\forall c \in]a, b[\quad \lim_{x \to c-} f(x) \leq f(c) \leq \lim_{x \to c+} f(x).$$

- En b, la fonction f admet une limite à gauche qui
  — est finie si f est majorée sur I,
  — vaut $+\infty$ sinon.

2 Fonctions continues sur un intervalle et à valeurs réelles.

2.1 Continuité sur un intervalle.

Définition 32.

Une fonction $f : I \to \mathbb{R}$ est dite **continue sur** I si elle est continue en tout point de I.
L'ensemble des fonctions continues sur I est noté $\mathcal{C}^0(I, \mathbb{R})$, ou seulement $\mathcal{C}^0(I)$.

Remarque. Si f est définie sur une réunion d'intervalles ouverts deux à deux disjoints $D = \cup_{j \in J} I_j$ (c'est le cas par exemple si elle est définie sur un intervalle privé d'un point), on dira que f est continue sur D si sa restriction à chacun des intervalles I_i est continue sur I_i.

Exemple 33.

Les fonctions usuelles, à l'exception de la partie entière sont continues sur leur ensemble de définition :

— Les fonctions polynomiales $P : x \mapsto \sum_{k=0}^{n} a_k x^k$ ($n \in \mathbb{N}$, $a_0, \dots, a_n \in \mathbb{R}$) sont continues sur $\mathbb{R}$;

— les fractions rationnelles $\frac{P}{Q}$ de deux fonctions polynomiales P et Q, sont continues sur la réunion disjointe d'intervalles $\mathbb{R} \setminus Z_Q$, où Z_Q est l'ensemble fini des racines réelles de Q.

— Les fonctions exp, ch, sh, cos, sin, arctan et $x \mapsto |x|$ sont continues sur $\mathbb{R}$

— ln est continue sur $\mathbb{R}_+^*$;

— Pour $a \in \mathbb{R}$, $x \mapsto x^a$ est continue sur $\mathbb{R}_+^*$, et prolongeable par continuité en 0 ssi $a \geq 0$;

— tan est continue sur la réunion disjointe des intervalles $]-\frac{\pi}{2} + k\pi, \frac{\pi}{2} + k\pi[$ avec $k \in \mathbb{Z}$;

— arccos et arcsin sont continues sur $[-1, 1]$.

Proposition 34.

$\mathcal{C}^0(I, \mathbb{R})$ est stable par combinaisons linéaires et par produit.
Soit $(f, g) \in (\mathcal{C}^0(I, \mathbb{R}))$. Si g ne s'annule pas sur I alors $f/g \in \mathcal{C}^0(I, \mathbb{R})$.

Proposition 35.

Soit $f : I \to J$ et $g : J \to \mathbb{R}$.

Si f est continue sur I et g continue sur J, alors $g \circ f$ est continue sur I.

Exemple 36 (jongler avec les théorèmes globaux et le point de vue local)**.**

Démontrer la continuité sur $\mathbb{R}$ de la fonction f définie sur $\mathbb{R}$ par

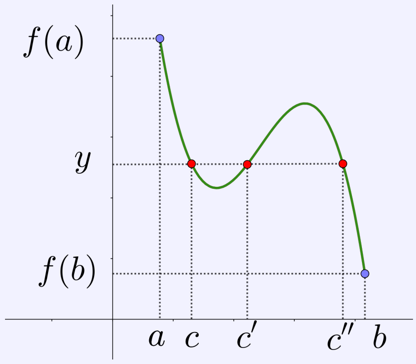
$$f(0) = 1 \quad \text{et} \quad \forall x \in \mathbb{R}^* \quad f(x) = \frac{\arctan(x)}{x}.$$

2.2 Théorème des valeurs intermédiaires.

Théorème 37 (des valeurs intermédiaires)**.**

Soient deux réels $a \leq b$ et $f : [a, b] \to \mathbb{R}$ continue. Alors, pour tout réel y entre $f(a)$ et $f(b)$,

$$\exists c \in [a, b] \quad y = f(c).$$



Corollaire 38.

Si une fonction continue sur un intervalle y change de signe, alors elle s'annule sur cet intervalle.
Si une fonction continue sur un intervalle ne s'y annule pas, alors $f > 0$ ou $f < 0$ sur I.

Exemple 39.

Soit $f : [a, b] \to [a, b]$, continue sur $[a, b]$.
Montrer l'existence d'un point fixe pour f (i.e. $\exists x_0 \in [a, b] : f(x_0) = x_0$).

Exemple 40.

Montrer qu'une fonction polynomiale de degré impair s'annule au moins une fois sur $\mathbb{R}$.

Corollaire 41.

L'image d'un intervalle par une fonction continue est un intervalle.

Corollaire 42 (TVI strictement monotone)**.**

Soit $f : [a, b] \to \mathbb{R}$ continue et strictement monotone sur $[a, b]$. Pour tout réel y entre $f(a)$ et $f(b)$,

$$\exists! c \in [a, b] \quad y = f(c).$$

2.3 Bijections continues.

Théorème 43 (Théorème de la bijection continue)**.**

Soit $f : I \to \mathbb{R}$ une fonction continue et strictement monotone sur I.

- Elle réalise une bijection de I dans $f(I)$, qui est un intervalle.
- Sa réciproque f^{-1} est strictement monotone sur $f(I)$, de même monotonie que f, et elle est continue sur $f(I)$.

Exemple 44.

Soit f la restriction de ch à $I = [0, +\infty[$. La fonction f est continue sur I et elle y est strictement croissante. La fonction f réalise donc une bijection de I vers $f(I)$. Ici $f(I)$ est l'intervalle $[1, +\infty[$.

Proposition 45 (preuve non exigible)**.**

Une fonction continue sur un intervalle est injective si et seulement si elle est strictement monotone.

2.4 Théorème des bornes atteintes.

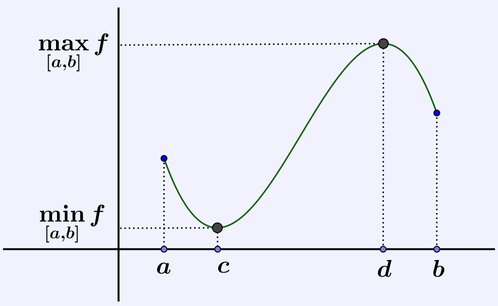
Théorème 46.

Soit $f : [a, b] \to \mathbb{R}$ une fonction <u>continue</u> sur le <u>segment</u> $[a, b]$.

Alors f est bornée et atteint ses bornes sur $[a, b]$:

$$\exists c \in [a, b] \quad : \quad f(c) = \min_{[a,b]} f$$

$$\exists d \in [a, b] \quad : \quad f(d) = \max_{[a,b]} f.$$



Corollaire 47 (Image d'un segment.)**.**

L'image d'un segment par une fonction continue est un segment.

2.5 Uniforme continuité.

Définition 48.

Une fonction $f : I \to \mathbb{R}$ est **uniformément continue** sur I si

$$\forall \varepsilon > 0 \quad \exists \eta > 0 \quad \forall (x, x') \in I^2 \quad |x - x'| \leq \eta \implies |f(x) - f(x')| \leq \varepsilon.$$

Exemple 49.

Toute fonction uniformément continue sur un intervalle y est continue.
La réciproque n'est pas vraie : la fonction exponentielle est continue sur $\mathbb{R}$ mais n'y est pas uniformément continue.

Théorème 50 (de Heine)**.**

Une fonction continue sur un segment y est uniformément continue.

On donne ci-dessous une propriété qui impliquera l'uniforme continuité.

Définition 51.

Soit $f : I \to \mathbb{R}$ et $K \geq 0$. On dit que f est K**-lipschitzienne** sur I si

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

On dira que f est **lipschitzienne** sur I s'il existe $K \geq 0$ tel que f est K-lipschitzienne.

Exemples 52.

- Toute fonction affine est lipschitzienne sur son intervalle de définition.
- Sur $[0, 1]$, $f : x \mapsto x^2$ est lipschitzienne et $g : x \mapsto \sqrt{x}$ ne l'est pas.

Proposition 53.

Une fonction lipschitzienne sur un intervalle y est uniformément continue. La réciproque est fausse.

Reste à savoir établir qu'une fonction est lipschitzienne. Le théorème des accroissements finis, dans le cours sur la dérivabilité, sera un bon outil pour ça.

2.6 Le cas des fonctions à valeurs complexes.

Une fonction $f : I \to \mathbb{C}$ est dite continue sur I si elle est continue en tout point de I ; on note alors $f \in \mathcal{C}^0(I, \mathbb{K})$. Les résultats sur la somme, le produit, le quotient, la composée s'étendent.

Si $f \in \mathcal{C}^0(I, \mathbb{C})$, alors $\overline{f} : x \mapsto \overline{f(x)}$ est continue sur I.

- Par somme et différence, on obtient que $\mathrm{Re}(f)$ et $\mathrm{Im}(f)$ sont des fonctions à valeurs réelles continues sur I. La réciproque est vraie, de sorte qu'une fonction est continue sur I ssi sa partie réelle et sa partie imaginaire le sont.
- Par produit de f et de son conjugué, on obtient que $x \mapsto |f(x)|^2$ est continue sur I, ainsi que $x \mapsto |f(x)|$ par composition avec la racine carrée.

Pas question d'étendre le TVI ou le théorème de la bijection continue pour des fonctions à valeurs complexes, faute d'ordre sur $\mathbb{C}$.

En revanche, une fonction à valeurs complexes continue sur un segment, y est bornée, au sens de majorée en module : il suffit d'appliquer le TBA à $x \mapsto |f(x)|$.

Les définitions de fonction uniformément continues, ou de fonction lipschitzienne s'étendent en remplaçant la valeur absolue par le module et on retrouve le théorème de Heine et le fait que les fonctions lipschitziennes sur un intervalle sont uniformément continues.

Preuves

Preuve du théorème de la limite monotone pour les fonctions (31)
On détaille seulement la preuve du premier point, le second est facile.

Soit une fonction définie et croissante sur un intervalle $]a, b[$, où on considère un point c. On va démontrer l'existence d'une limite à gauche en c pour f. Nous avons un candidat, que l'on définit par

$$s_g = \sup \{f(x)\ x \in]a, c[\}.$$

Cette définition a un sens : la partie dont on prend la borne supérieure est non vide (elle contient $f\left(\frac{a+c}{2}\right)$ par exemple) et majorée par $f(c)$, f étant croissante.
Soit $\varepsilon > 0$. D'après la caractérisation de la borne supérieure,

$$\exists x_0 \in]a, c[\quad s_g - \varepsilon < f(x_0) \leq s_g.$$

Par croissance de f, pour tout $x \in [x_0, c[$, $f(x) \geq f(x_0) \geq s_g - \varepsilon$ et puisque $f(c)$ majore f sur $]a, c[$ on a aussi $f(x) \leq s_g$. Posons $\eta = c - x_0$ on a bien

$$\forall x \in [c - \eta, c[\quad s_g - \varepsilon \leq f(x) \leq s_g,$$

ce qui montre $f(x) \underset{x \to c-}{\to} s_g$.
De manière analogue, on peut démontrer que

$$f(x) \underset{x \to c-}{\to} i_d, \qquad \text{où} \qquad i_d = \inf \{f(x)\ x \in]c, b[\}.$$

$\square$

Deuxième preuve (courte !) du TVI. Soit f une fonction continue sur $[a,b]$. Fixons y entre $f(a)$ et $f(b)$. Soit la partie

$$A = \{x \in [a,b] : f(x) \leq y\}.$$

Cette partie est non vide : puisque y est entre $f(a)$ et $f(b)$, on a $f(a) \leq y$ ou $f(b) \leq y$, donc $a \in A$ ou $b \in A$. La partie A est aussi majorée (par b). Posons donc $s = \sup(A)$.

• Pour $\varepsilon > 0$, $s + \varepsilon \notin A$. Ainsi, $f(s+\varepsilon) > y$. Or par continuité (à droite) de f en s, $f(s+\varepsilon) \underset{x \to s+}{\to} f(s)$. La stabilité des inégalités larges donne $f(s) \geq y$.

• On sait trouver une suite d'éléments de A tendant vers s : $\forall n \in \mathbb{N}^* \quad \exists x_n \in A \quad s - \frac{1}{n} < x_n \leq s$. Notamment, pour tout n entier, $f(x_n) \leq y$. En passant à la limite, par continuité (à gauche) de f en s, $f(s) \leq y$.
• Les deux inégalités donnent que $f(s) = y$: on a trouvé un antécédent de y par f. □

Preuve du théorème de la bijection continue (Th 43)
Pour fixer les idées, supposons f continue et strictement croissante sur I et notons $J = f(I)$.

• On a vu que l'image d'un intervalle par une fonction continue est un intervalle : c'est vrai en particulier pour $J = f(I)$. C'est par définition même de $J = f(I)$ que $f : I \to J$ est surjective. L'injectivité provient de la stricte monotonie (voir cours sur les applications). Ceci prouve la bijectivité de $f : I \to J$.

• Soit y et y' deux éléments de $J = f(I)$ tels que $y < y'$. Supposons $f^{-1}(y) \geq f^{-1}(y')$. En appliquant f qui est croissante, on obtient $y \geq y'$, ce qui n'est pas. On a donc $f^{-1}(y) < f^{-1}(y')$, ce qui montre la stricte monotonie de f^{-1}.

• Prouvons la continuité de f^{-1} sur J (démo non exigible). Si $b \in J$, d'après le théorème de la limite monotone, f^{-1} admet en b une limite à gauche et à droite que l'on note G et D (on suppose ici que b est à l'*intérieur* de J en laissant au lecteur le soin d'adapter si b est un bord) : $G \leq f^{-1}(b) \leq D$. Les limites à gauche et à droite G et D sont des éléments de I. Détaillons pour G : si y_0 est élément de J strictement inférieur à b, alors par passage à la limite, $f^{-1}(y_0) \leq G \leq f^{-1}(b)$. Encadré par deux éléments de l'intervalle I, G est encore un élément de I. Par continuité de f en G puis en D, on a

$$f(G) = \lim_{y \to b-} f(f^{-1}(y)) = b \qquad \text{et} \qquad f(D) = \lim_{y \to b-} f(f^{-1}(y)) = b.$$

Ainsi, $f(G) = f(D)$ et par injectivité de f, $G = D$. On obtient $G = f^{-1}(b) = D$, ce qui démontre la continuité de f^{-1} en b. □

Preuve de la proposition 45

L'implication réciproque est claire : la stricte monotonie implique l'injectivité (pas besoin d'être continue, ni définie sur un intervalle).

On suppose que f est continue sur I et injective. Si f est strictement monotone alors,

$$\forall (a,b,c) \in I^3, \quad a < b < c \Longrightarrow \begin{cases} f(a) < f(b) < f(c) \\ \text{ou} \\ f(a) > f(b) > f(c) \end{cases}$$

Autrement dit,

$$\forall (a,b,c) \in I^3, \quad a < b < c \Longrightarrow f(b) \in [\min(f(a), f(c)), \max(f(a), f(c))]$$

Raisonnons par contraposée et supposons qu'il existe $(a,b,c) \in I^3$ tel que

$$a < b < c \text{ et } \ f(b) \notin [\min(f(a), f(c)), \max(f(a), f(c))]$$

<u>1^{er} cas :</u> on suppose $f(a) < f(c)$.

$\boxed{\text{a}}$ On suppose $f(b) < f(a) < f(c)$. D'après le théorème des valeurs intermédiaires, il existe $(\alpha, \beta) \in I^2$ tel que

$$a < \alpha < b < \beta < c \text{ et } \ f(\alpha) = f(\beta) = \frac{f(a) - f(b)}{2}$$

ce qui contredit l'injectivité.

$\boxed{\text{b}}$ On suppose $f(a) < f(c) < f(b)$. Même démonstration.

<u>2^d cas :</u> on suppose $f(a) > f(c)$. Même démonstration.

□

Exercices

Limites.

$\boxed{\textbf{22.1}}$ **[♦◇◇]** Calculer (en montrant qu'elles existent) : $\lim\limits_{x \to 0+} x \lfloor \frac{1}{x} \rfloor \qquad \lim\limits_{x \to +\infty} x \lfloor \frac{1}{x} \rfloor$

$\boxed{\textbf{22.2}}$ **[♦◇◇]** Soient $f : [0,1] \to [0,1]$ et $g : [0,1] \to [0,1]$. On suppose que fg admet 1 pour limite en 0. Montrer que f et g admettent 1 pour limite en 0.

$\boxed{\textbf{22.3}}$ **[♦◇◇]** Dire si les fonctions

$$f : x \mapsto \exp\left(-\frac{1}{x}\right) \quad \text{ et } \quad g : x \mapsto \exp\left(-\frac{1}{x^2}\right),$$

définies sur $\mathbb{R}^*$, sont prolongeables par continuité en 0.

$\boxed{\textbf{22.4}}$ **[♦♦◇]** Montrer que la fonction $f : x \mapsto \frac{x^x}{\lfloor x \rfloor^{\lfloor x \rfloor}}$ n'a pas de limite en $+\infty$.

Continuité, en un point, sur un intervalle.

$\boxed{\textbf{22.5}}$ **[♦◇◇]** Montrer que la fonction $f : x \mapsto \ln(x)\ln(1-x)$ est prolongeable par continuité sur les bords de son intervalle de définition.
Indication : on pourra se convaincre que $x \mapsto \frac{\ln(1-x)}{x}$ possède une limite finie en 0.

$\boxed{\textbf{22.6}}$ **[♦◇◇]** Soit f une fonction continue sur I et à valeurs réelles.
Montrer qu'alors $x \mapsto |f(x)|$ est continue sur I. Prouver que la réciproque est fausse.

$\boxed{\textbf{22.7}}$ **[♦♦◊]** Soient f et g deux fonctions continues un intervalle I.
Montrer que $\max(f,g) : x \mapsto \max(f(x), g(x))$ et $\min(f,g) : x \mapsto \max(f(x), g(x))$ sont continues sur I.

$\boxed{\textbf{22.8}}$ **[♦♦◊]** Soit $f : \mathbb{R}_+^* \to \mathbb{R}$, croissante, et telle que $x \mapsto \dfrac{f(x)}{x}$ est décroissante.
Montrer que f est continue sur $\mathbb{R}_+^*$.

$\boxed{\textbf{22.9}}$ **[♦◊◊]** Soit $f : \mathbb{R} \to \mathbb{R}$, à la fois 1-périodique et $\sqrt{2}$-périodique, et continue en 0.

1. Soit $n \in \mathbb{N}$. Montrer que $(\sqrt{2}-1)^n$ est une période de f.
2. Montrer que f est constante.

$\boxed{\textbf{22.10}}$ **[♦♦◊]** Montrer que la fonction $\mathbf{1}_{\mathbb{Q}}$ n'est continue en aucun point de $\mathbb{R}$.

$\boxed{\textbf{22.11}}$ **[♦♦◊]** [CC-INP MPI 43]
Soit $x_0 \in \mathbb{R}$. On définit la suite (u_n) par $u_0 = x_0$ et, $\forall n \in \mathbb{N}$, $u_{n+1} = \mathrm{Arctan}(u_n)$.

1. (a) Démontrer que la suite (u_n) est monotone et déterminer, en fonction de la valeur de x_0, le sens de variation de (u_n).
   (b) Montrer que (u_n) converge et déterminer sa limite.
2. Déterminer l'ensemble des fonctions h, continues sur $\mathbb{R}$, telles que : $\forall x \in \mathbb{R}$, $h(x) = h(\mathrm{Arctan}\, x)$.

$\boxed{\textbf{22.12}}$ **[♦♦♦]** Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ continues en 0 telles que

$$\forall x \in \mathbb{R} \quad f(2x) - f(x) = x.$$

Propriétés des fonctions continues sur un intervalle.

$\boxed{\textbf{22.13}}$ **[♦◊◊]** Soit $f : \mathbb{R}_+ \to \mathbb{R}_+$ continue telle que $\lim\limits_{x\to+\infty} \frac{f(x)}{x} < 1$. Montrer que f possède un point fixe.

$\boxed{\textbf{22.14}}$ **[♦♦◊]** Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction décroissante et continue.
Prouver que f possède un unique point fixe, c'est-à-dire qu'il existe une unique solution à l'équation $f(x) = x$.

$\boxed{\textbf{22.15}}$ **[♦♦◊]** Soit f une fonction continue sur $\mathbb{R}$ et admettant des limites finies en $+\infty$ et $-\infty$.
Montrer que f est bornée.

$\boxed{\textbf{22.16}}$ **[♦◊◊]** Soient f et g deux fonctions de $\mathbb{R}$ dans $\mathbb{R}$. Montrer que si f est continue et que g est bornée, alors $g \circ f$ est $f \circ g$ sont bornées.

$\boxed{\textbf{22.17}}$ **[♦♦◊]** Soit f une fonction continue sur $\mathbb{R}$ telle que $\forall x \in \mathbb{R}^* \quad |f(x)| < |x|$.

1. Prouver que 0 est un point fixe de f et que c'est le seul.
2. Prouver que pour tout segment $[a,b]$ inclus dans $\mathbb{R}_+^*$, il existe $k \in [0,1[$ tel que $\forall x \in [a,b]$ $|f(x)| \leq k|x|$.

$\boxed{\textbf{22.18}}$ **[♦♦♦]** Soit $f : [0,1] \mapsto \mathbb{R}$, continue, telle que $f(0) = f(1)$. Montrer que, pour tout $p \in \mathbb{N}^*$, l'équation

$$f\left(x + \frac{1}{p}\right) = f(x)$$

admet au moins une solution.

Dérivabilité

Dans tout le cours, I désignera un intervalle de $\mathbb{R}$ non vide et non réduit à un point.

1 Dérivabilité.

1.1 Définition et exemples.

Définition 1 (Dérivabilité en un point)**.**

Soit $f : I \to \mathbb{K}$ et $a \in I$. La fonction f est dite **dérivable en** a si le taux d'accroissement

$$\frac{f(x) - f(a)}{x - a}$$

admet une limite finie quand x tend vers a.

Lorsqu'elle existe, cette limite est appelée **nombre dérivé** en a et notée $f'(a)$.

Une autre écriture du taux d'accroissement de f au point a est

$$\frac{f(a+h) - f(a)}{h},$$

(on se demande alors si une limite finie existe lorsque h tend vers 0, pour h différent de 0).

Figure. Dans le cas réel : fonction dérivable en un point, pentes des cordes, pente de la tangente.

Définition 2 (Dérivabilité sur un intervalle)**.**

On dit que $f : I \to \mathbb{K}$ est **dérivable sur** I si elle est dérivable en tout point de I.

On appelle alors **dérivée** de f la fonction $f' : \begin{cases} I & \to & \mathbb{K} \\ x & \mapsto & f'(x) \end{cases}$.

L'ensemble des fonctions dérivables sur I et à valeurs dans $\mathbb{K}$ sera noté $\mathcal{D}(I, \mathbb{K})$.

On peut étendre la définition précédente à une réunion disjointe d'intervalles ouverts : une fonction étant déclarée dérivable sur cet ensemble si sa restriction à chacun des intervalles y est dérivable.

Proposition 3.

Soit $f : I \to \mathbb{K}$ et $a \in I$.

1. Si f est dérivable en a, alors elle est continue en a.
2. Si f est dérivable sur I, alors elle est continue sur I. Ceci s'écrit aussi : $\mathcal{D}(I, \mathbb{K}) \subset \mathcal{C}^0(I, \mathbb{K})$.

La réciproque de la proposition précédente est fausse : on trouvera ci-dessous des exemples qui le montrent.

Exemple 4.

1. La fonction $x \mapsto |x|$ est continue en 0. Elle n'y est pas dérivable.

2. Soit $a \in \mathbb{R}$ et $f : x \mapsto x^a$, définie sur $\mathbb{R}_+^*$.
   Rappelez pour quelles valeurs de a la fonction f est prolongeable par continuité.
   Pour lesquelles de ces valeurs la fonction ainsi prolongée est-elle dérivable en 0 ?

3. Soient $f : x \mapsto x \sin\left(\dfrac{1}{x}\right)$ et $g : x \mapsto x^2 \sin\left(\dfrac{1}{x}\right)$ définies sur $\mathbb{R}^*$.
   Après avoir montré qu'on pouvait les prolonger par continuité en 0, établir si ces prolongements sont dérivables en 0.
   Représenter le graphe de ces fonctions au voisinage de 0.

On propose une caractérisation de la dérivabilité pour les fonctions à valeurs complexes.

Proposition 5.

Soit $f : I \to \mathbb{C}$ et $a \in I$. On note $\alpha : x \mapsto \mathrm{Re}\,(f(x))$ et $\beta : x \mapsto \mathrm{Im}\,(f(x))$.

$$f \text{ est dérivable en } a \quad \Longleftrightarrow \quad \alpha \text{ et } \beta \text{ sont dérivables en } a$$

Dans le cas où f est dérivable en a, on a

$$f'(a) = \alpha'(a) + i\beta'(a).$$

Exemple. Vérifier que $t \mapsto e^{it}$ est dérivable sur $\mathbb{R}$ et préciser sa dérivée.

Définition 6.

Soit $f : I \to \mathbb{K}$ et $a \in I$. On dit que f est
- **dérivable à gauche** en a si le taux d'accroissement en a admet une limite à gauche (finie).
- **dérivable à droite** en a si le taux d'accroissement en a admet une limite à droite (finie).

Lorsque ces limites existent, on note

$$f'_g(a) = \lim_{\substack{x\to a\\ x<a}} \frac{f(x)-f(a)}{x-a} \quad \text{et} \quad f'_d(a) = \lim_{\substack{x\to a\\ x>a}} \frac{f(x)-f(a)}{x-a}.$$

Figure. Dans le cas réel : demi-tangentes d'une fonction dérivable à gauche et à droite.

Proposition 7 (Caractérisation de la dérivabilité en a)**.**

Soit $f : I \to \mathbb{K}$ et a un élément de I qui n'est pas une borne de I.

$$f \text{ est dérivable en } a \iff \begin{cases} f \text{ est dérivable à gauche en } a \\ f \text{ est dérivable à droite en } a \\ f'_g(a) = f'_d(a) \end{cases}$$

Dans le cas où f est dérivable en a, on a $f'(a) = f'_g(a) = f'_d(a)$.

On termine avec la définition suivante, qui décrit des fonctions « un peu mieux que dérivable ».

Définition 8.

Une fonction $f : I \to \mathbb{K}$ est dite **de classe $\mathcal{C}^1$** sur I si
- elle est dérivable sur I
- sa dérivée f' est continue sur I

Certains auteurs parlent aussi de fonctions « continûment dérivables ».
L'ensemble des fonctions de classe $\mathcal{C}^1$ sur I et à valeurs dans $\mathbb{K}$ sera noté $\mathcal{C}^1(I, \mathbb{K})$.

Exemple 9 (Une fonction dérivable mais pas $\mathcal{C}^1$: un exemple en cinq étapes)**.**

1. Une définition sur $\mathbb{R}^*$: $g : \mathbb{R}^* \to \mathbb{R}; x \mapsto x^2 \sin\left(\frac{1}{x}\right)$.
2. Prolongement en 0. Pour $x \in \mathbb{R}^*$ $|g(x)| \leq x^2$ donc g a une limite nulle en 0.
   On prolonge g par continuité en posant $g(0) = 0$.
3. Dérivabilité de g sur $\mathbb{R}^*$? **Oui** : par produit et composée. On a
$$\forall x \in \mathbb{R}^* \quad g'(x) = 2x\sin(1/x) - \cos(1/x).$$
4. Dérivabilité de g en 0 ? **Oui** : on l'a vu en début de cours : le taux d'accroissement en 0 tend vers 0 et on a $g'(0) = 0$.
5. g est-elle de classe $\mathcal{C}^1$ sur $\mathbb{R}$? **Non** : g' est continue sur $\mathbb{R}^*$ par produit et composée mais à cause de $\cos(1/x)$, g' n'a pas de limite en 0 ! Elle ne saurait donc y être continue.

1.2 Dérivabilité en un point et développement limite à l'ordre 1.

Lemme 10.

Soit $f : I \to \mathbb{K}$ et $a \in I$.
Si f est dérivable en a, il existe une fonction ε définie au voisinage de 0 telle que

$$f(a+h) = f(a) + hf'(a) + h\varepsilon(h) \quad \text{et} \quad \varepsilon(h) \underset{h\to 0}{\longrightarrow} 0.$$

Plus précisément, l'égalité ci-dessus est vraie pour tout $h \in \{x - a \mid x \in I \setminus \{a\}\}$.

Définition 11.

Soit $f : I \to \mathbb{K}$ et $a \in I$. On dit que f admet un **développement limité** en a **à l'ordre** 1 s'il existe deux nombres a_0 et a_1 dans $\mathbb{K}$ et une fonction ε définie au voisinage de 0 tels que

$$f(a+h) = a_0 + a_1 h + h\varepsilon(h) \quad \text{et} \quad \varepsilon(h) \underset{h\to 0}{\longrightarrow} 0.$$

Lemme 12.

Soit $f : I \to \mathbb{K}$ et $a \in I$.
On suppose que f admet un DL en a à l'ordre 1 : il existe deux nombres a_0 et a_1 dans $\mathbb{K}$ et une fonction ε définie au voisinage de 0 tels que

$$f(a+h) = a_0 + a_1 h + h\varepsilon(h) \quad \text{et} \quad \varepsilon(h) \underset{h\to 0}{\longrightarrow} 0.$$

La fonction f est dérivable en a et nécessairement,

$$a_0 = f(a) \quad \text{et} \quad a_1 = f'(a).$$

Les deux lemmes précédents sont les deux implications d'une caractérisation énoncée comme suit :

Théorème 13.

Une fonction est dérivable en un point ssi elle y admet un développement limité à l'ordre 1.

Soit $f : I \to \mathbb{K}$ dérivable en a. On vient de comprendre qu'il existe une fonction ε qui tend vers 0 en a telle que pour tout $x \in I \setminus \{a\}$, on a

$$f(x) = f(a) + f'(a)(x-a) + (x-a)\varepsilon(x).$$

Dans ce développement limité de f en a à l'ordre 1, les termes sont écrits du plus *grand* au plus *petit* (on rendra cela rigoureux). Le terme $(x-a)\varepsilon(x)$ peut être vu comme l'erreur d'approximation lorsqu'on écrit

$$f(x) \approx f(a) + f'(a)(x-a).$$

Une fonction dérivable en a, c'est une fonction qui se comporte au voisinage de a comme une fonction affine. Sa courbe représentative y admet pour tangente la droite d'équation $y = f'(a)(x-a) + f(a)$.

1.3 Dérivabilité et opérations.

Proposition 14 (Somme, produit, quotient).

Soient $f, g : I \to \mathbb{K}$ deux fonctions dérivables en $a \in I$. Alors,

- pour tous λ et μ dans $\mathbb{K}$, $\lambda f + \mu g$ est dérivable en a et
$$(\lambda f + \mu g)'(a) = \lambda f'(a) + \mu g'(a),$$
- fg est dérivable en a et
$$(fg)'(a) = f'(a)g(a) + f(a)g'(a),$$
- Si $g(a) \neq 0$, alors g ne s'annule pas au voisinage de a et f/g est dérivable en a : on a
$$\left(\frac{f}{g}\right)'(a) = \frac{g(a)f'(a) - f(a)g'(a)}{g(a)^2}.$$

Corollaire 15 (du local au global).

Soient $f, g \in \mathcal{D}(I, \mathbb{K})$. Alors,

- $\forall (\lambda, \mu) \in \mathbb{K}^2 \quad \lambda f + \mu g \in \mathcal{D}(I, \mathbb{K})$ et $(\lambda f + \mu g)' = \lambda f' + \mu g'$,
- $fg \in \mathcal{D}(I, \mathbb{K})$ et $(fg)' = f'g + fg'$,
- Si g ne s'annule pas sur I, alors $f/g \in \mathcal{D}(I, \mathbb{K})$ et $(f/g)' = (gf' - fg')/g^2$.

Théorème 16 (Composition).

Soit $f : I \to J$ et $g : J \to \mathbb{K}$. Soit $a \in I$.
Si f est dérivable au point a et g dérivable au point $f(a)$, alors

$$g \circ f \text{ est dérivable en } a \quad \text{et} \quad (g \circ f)'(a) = f'(a) \cdot g'(f(a)).$$

Corollaire 17 (du local au global).

Soit $f : I \to J$ et $g : J \to \mathbb{K}$. Supposons que f est dérivable sur I et g dérivable sur J. Alors,

$$g \circ f \text{ est dérivable sur } I \quad \text{et} \quad (g \circ f)' = f' \times g' \circ f.$$

Exemple 18 (jongler avec les théorèmes globaux et le point de vue local).

Établir la dérivabilité de $f : x \mapsto \sqrt{x \sin(x)}$ sur $[0, \pi[$ et préciser sa dérivée.

1.4 Dérivabilité d'une réciproque.

Théorème 19 (Dérivabilité d'une réciproque)**.**

Soit f une fonction continue réalisant une bijection de I dans J, de réciproque $f^{-1} : J \to I$. Supposons que f est dérivable en un point $a \in I$.

$$f^{-1} \text{ est dérivable au point } f(a) \quad \text{si et seulement si} \quad f'(a) \neq 0.$$

Lorsqu'il y a dérivabilité en $f(a)$, on a $\left(f^{-1}\right)'(f(a)) = \dfrac{1}{f'(a)}$.

Corollaire 20 (du local au global)**.**

Soit f une fonction réalisant une bijection de I dans J, de réciproque $f^{-1} : J \to I$.
Si f est dérivable sur I et que f' ne s'annule pas sur I, alors f^{-1} est dérivable sur J et

$$\left(f^{-1}\right)' = \frac{1}{f' \circ f^{-1}}.$$

Exemple 21.

Justifier brièvement que sh réalise une bijection de $\mathbb{R}$ dans $\mathbb{R}$. Notons argsh sa réciproque.
Sans chercher à l'expliciter, montrer que argsh est dérivable sur $\mathbb{R}$ et calculer sa dérivée.

1.5 Extremum local et point critique.

Définition 22.

On dit que $f : I \to \mathbb{R}$ admet un **extremum local** en $a \in I$ si $f(a)$ est un extremum de f au voisinage de a. Plus précisément, on dit que f admet un maximum local en a si

$$\exists \eta > 0 \quad \forall x \in I \cap [a - \eta, a + \eta] \quad f(x) \leq f(a)$$

Proposition 23 (Extremum local et dérivabilité)**.**

Soit $f :]a, b[\to \mathbb{R}$ une fonction définie sur un intervalle ouvert et $c \in]a, b[$.
Si f admet un extremum local en c et y est dérivable, alors $f'(c) = 0$.
Un point c où la dérivée de f s'annule est appelé un **point critique** de f.

Exemple 24 (la réciproque est fausse et toutes les hypothèses comptent)**.**

1. $x \mapsto x^3$ a un point critique en 0 qui n'est pas un extremum local.
2. $x \mapsto |x|$ a un minimum global en 0 : elle n'y est pas dérivable.
3. Montrer qu'il est essentiel que c soit à l'*intérieur* de l'intervalle.

2 Fonctions dérivables sur un intervalle et à valeurs réelles.

Dans tout ce qui suit, a et b sont deux réels tels que $a < b$.

2.1 Théorème de Rolle.

Théorème 25 (de Rolle)**.**

Soit $f : [a, b] \to \mathbb{R}$, continue sur $[a, b]$ et dérivable sur $]a, b[$ et telle que $f(a) = f(b)$, alors

$$\exists c \in]a, b[\quad f'(c) = 0.$$

Exemple 26.

Soit $f \in \mathcal{D}(I, \mathbb{R})$. Montrer que si f s'annule n fois ($n \in \mathbb{N}^*$), alors f' s'annule (au moins) $n-1$ fois.

2.2 Egalité des accroissements finis.

Théorème 27 (Égalité des accroissements finis)**.**

Soit $f : [a, b] \to \mathbb{R}$ une fonction continue sur $[a, b]$ et dérivable sur $]a, b[$. Alors,

$$\exists c \in]a, b[\quad \frac{f(b) - f(a)}{b - a} = f'(c).$$

Remarque. Idée de preuve à retenir : on pose une fonction auxiliaire $\Phi : x \mapsto f(x) - A(x-a)$, en choisissant la constante A de manière à "compenser la pente" et ainsi pouvoir appliquer le théorème de Rolle à Φ.

Remarque. Notons que le théorème ci-dessus concerne des accroissements où b ne tend pas vers a ! C'est en ce sens que les accroissements sont **finis**, là où dans la partie 1, le passage à la limite les rendait *infinitésimaux*. On pourrait donc renommer ce résultat : théorème des accroissements **macroscopiques**.

En guise de première application des accroissements finis, on propose (enfin !) la démonstration d'un théorème bien connu des lycéens.

Théorème 28 (Caractérisation des fonctions monotones parmi les fonctions dérivables)**.**

Soit I un intervalle, et $f : I \to \mathbb{R}$ une fonction dérivable sur I.

- f est croissante sur I si et seulement si f' est positive sur I.
- f est décroissante sur I si et seulement si f' est négative sur I.
- f est constante sur I si et seulement si f' est nulle sur I.

- Si f' est strictement positive sur I, alors f y est strictement croissante. Réciproque fausse.
- Si f' est strictement négative sur I, alors f y est strictement décroissante. Réciproque fausse.

2.3 Inégalité des accroissements finis.

Théorème 29 (Inégalité des accroissements finis)**.**

Soit $f \in \mathcal{D}(I, \mathbb{R})$. Si $|f'|$ est majorée par un réel K, alors f est K-lipschitzienne.

Exemple 30.

(Re)-démontrer que

$$\forall x \in \mathbb{R} \quad |\sin x| \leq |x|.$$

Exemple 31.

Démontrer

$$\forall x, y \in [1, +\infty[\quad \left| \frac{\sin x}{x} - \frac{\sin y}{y} \right| \leq 2|x - y|.$$

Exemple 32.

Montrer qu'une fonction de classe $\mathcal{C}^1$ sur un segment y est lipschitzienne.

Application. Fonction contractante et convergence linéaire vers le point fixe.

Soit $f : I \to I$ une application k-lipschitzienne, avec $0 \leq k < 1$: elle est dite *contractante*.
On suppose de surcroît que f admet un point fixe $\alpha \in I$: $f(\alpha) = \alpha$.
Ce point fixe est alors unique (on le montre).

Soit (u_n) une suite définie par $\begin{cases} u_0 \in I \\ \forall n \in \mathbb{N} \quad u_{n+1} = f(u_n). \end{cases}$

On montre que $\underline{(u_n) \text{ converge vers } \alpha}$. En effet, pour tout $n \in \mathbb{N}$, on a

$$|u_{n+1} - \alpha| = |f(u_n) - f(\alpha)| \leq k|u_n - \alpha|.$$

Une récurrence amène immédiatement

$$\forall n \in \mathbb{N} \quad |u_n - \alpha| \leq k^n |u_0 - \alpha|.$$

La convergence de u vers α est linéaire, en échelle logarithmique : $-\ln|u_n - \alpha|$ est majorée par une fonction linéaire de n. Si on regarde u_n comme une approximation de α, le nombre de *décimales exactes* dans l'approximation croît comme une fonction linéaire de n.
Voir le TD pour un exemple de convergence linéaire vers le point fixe.

Une méthode offrant de meilleurs résultats numériques : la **méthode de Newton**, pour laquelle la vitesse de convergence est quadratique, avec une majoration de l'erreur de la forme

$$\forall n \in \mathbb{N} \quad |u_n - \alpha| \leq k^{2^n} |u_0 - \alpha|,$$

où $0 \leq k < 1$. Cette fois, le nombre de décimales exactes double à chaque itération !

2.4 Théorème de la limite de la dérivée.

Théorème 33 (de la limite de la dérivée)**.**

Soit $a \in I$. Soit $f : I \to \mathbb{R}$ dérivable sur $I \setminus \{a\}$ et continue en a. Soit $\ell \in \mathbb{R}$.

$$\text{Si} \quad f'(x) \underset{\substack{x \to a \\ x \neq a}}{\longrightarrow} \ell \quad \text{alors} \quad f \text{ est dérivable en } a \text{ de dérivée } f'(a) = \ell.$$

Automatiquement f' est continue en a.
Si de surcroît la fonction f' est continue sur $I \setminus \{a\}$, alors f est de classe $\mathcal{C}^1$ sur I.

La réciproque est fausse, on le constate sur l'exemple de $g : x \mapsto x^2 \sin(\frac{1}{x})$: cette fonction est dérivable sur $\mathbb{R}$, et en particulier en 0, alors que sa dérivée sur $\mathbb{R}^*$ n'a pas de limite en 0.

Proposition 34 (limite $\pm\infty$ pour la dérivée)**.**

Soit $a \in I$. Soit $f : I \to \mathbb{R}$ dérivable sur $I \setminus \{a\}$ et continue en a.

$$\text{Si} \quad f'(x) \underset{\substack{x \to a \\ x \neq a}}{\longrightarrow} +\infty \quad \text{alors} \quad \frac{f(x)-f(a)}{x-a} \underset{\substack{x \to a \\ x \neq a}}{\longrightarrow} +\infty.$$

Exemple 35 (Un prolongement $\mathcal{C}^1$)**.**

Soit f une fonction deux fois dérivable sur $\mathbb{R}_+$ telle que $f'(0) = 0$.
Démontrer que $g : x \mapsto f(\sqrt{x})$ est sur $\mathbb{R}_+$ et que sa dérivée y est continue.

2.5 Le cas des fonctions à valeurs complexes.

Exemple 36 (Pas de théorème de Rolle lorsque les images sont complexes)**.**

Soit $f : t \mapsto e^{it}$, $\mathbb{R} \to \mathbb{C}$.
Vérifier que f est continue sur $[0, 2\pi]$, dérivable sur $]0, 2\pi[$ et que $f(0) = f(2\pi)$.
Montrer ensuite que f' ne s'annule pas sur $]0, 2\pi[$.

Puisque le théorème de Rolle peut être vu comme un cas particulier de l'égalité des accroissements finis, on comprend que ce théorème ne s'étend pas aux fonctions à valeurs complexes. L'inégalité des accroissements finis, elle, demeure vraie comme on le voit ci-dessous.

Proposition 37 (Inégalité des accroissements finis pour des images complexes)**.**

Soit $f : I \to \mathbb{C}$ une fonction de classe $\mathcal{C}^1$ sur I, telle que le module de la dérivée est majoré sur I par une constante $K \geq 0$. Alors f est K-lipschitzienne sur I, on a cette inégalité pour les modules :

$$\forall (x, y) \in I^2 \quad |f(x) - f(y)| \leq K|x - y|,$$

3 Fonctions de classe $\mathcal{C}^n$.

3.1 Définition de la classe $\mathcal{C}^n$.

Définition 38.

On définit pour tout $n \in \mathbb{N}$ l'ensemble des fonctions n **fois dérivables** sur I, noté $\mathcal{D}^n(I, \mathbb{K})$, et pour f dans cet ensemble, sa **dérivée $n$ème** $f^{(n)}$, ou dérivée à l'ordre n.

- On pose $\mathcal{D}^0(I, \mathbb{K}) = \mathcal{F}(I, \mathbb{K})$: toutes les fonctions définies sur I sont 0 fois dérivables, et pour $f : I \to \mathbb{K}$, on pose $f^{(0)} := f$.
- Supposons $\mathcal{D}^n(I, \mathbb{K})$ bien défini pour $n \in \mathbb{N}$, ainsi que $f^{(n)}$ pour $f \in \mathcal{D}^n(I, \mathbb{K})$.
Alors, $\mathcal{D}^{n+1}(I, \mathbb{K})$ est l'ensemble des fonctions $f \in \mathcal{D}^n(I, \mathbb{K})$ telle que $f^{(n)}$ est dérivable sur I ; on pose alors
$$f^{(n+1)} := \left(f^{(n)}\right)'.$$

Remarques. $\mathcal{D}^1(I, \mathbb{K}) = \mathcal{D}(I, \mathbb{K})$ et la dérivée à l'ordre 1 est la dérivée... tout court.
Si $f \in \mathcal{D}^2(I, \mathbb{K})$, elle est dérivable et sa dérivée f' est elle-même dérivable, f a une dérivée d'ordre 2, dite aussi dérivée seconde : $f^{(2)} = (f')'$ souvent notée f''.

Lemme 39.

Soit $n \in \mathbb{N}$. Si f est n fois dérivable sur I et si $(k, \ell) \in \mathbb{N}^2$ vérifie $k + l \leq n$, alors
$$f^{(k+\ell)} = \left(f^{(k)}\right)^{(\ell)}.$$

En particulier, si f est dérivable $n+1$ fois sur I, on a : $\quad f^{(n+1)} = \left(f^{(n)}\right)'$ et $f^{(n+1)} = \left(f'\right)^{(n)}$.

Définition 40.

Soit $n \in \mathbb{N}$. On dit que $f : I \to \mathbb{K}$ est **de classe $\mathcal{C}^n$** sur I si
— elle est dérivable n fois sur I
— sa dérivée $n$ème $f^{(n)}$ est continue sur I.
Notamment, les fonctions de classe $\mathcal{C}^0$ sur I sont les fonctions qui y sont continues.
L'ensemble des fonctions de classe $\mathcal{C}^n$ sur I sera noté $\mathcal{C}^n(I, \mathbb{R})$.

$$\boxed{\mathcal{D}^{n+1}(I, \mathbb{K}) \subset \mathcal{C}^n(I, \mathbb{K}) \subset \mathcal{D}^n(I, \mathbb{K}) \ldots \subset \mathcal{C}^1(I, \mathbb{K}) \subset \mathcal{D}^1(I, \mathbb{K}) \subset \mathcal{C}^0(I, \mathbb{K}).}$$

Proposition 41.

Soit $n \in \mathbb{N}$ et $f : I \to \mathbb{K}$.
$$f \in \mathcal{C}^{n+1}(I, \mathbb{K}) \iff (f \text{ est dérivable sur } I \text{ et } f' \in \mathcal{C}^n(I, \mathbb{K})).$$

Définition 42.

On appelle fonction **de classe** $\mathcal{C}^\infty$ sur I une fonction qui est de classe $\mathcal{C}^n$ sur I pour tout $n \in \mathbb{N}$:

$$\mathcal{C}^\infty(I, \mathbb{K}) := \bigcap_{n \in \mathbb{N}} \mathcal{C}^n(I, \mathbb{K}).$$

Exemples.

- Les fonctions exp, ln, cos, sin, tan, ch, sh, ainsi que les fonction polynomiales et leurs quotients sont de classe $\mathcal{C}^\infty$ sur leur domaine de définition, et cela peut être affirmé sans démonstration.
- Les fonctions $x \mapsto x^a$ sont de classe $\mathcal{C}^\infty$ sur $\mathbb{R}_+^*$.
- Les fonction arcsin et arccos, définies sur $[-1, 1]$, sont de classe $\mathcal{C}^\infty$ sur $]-1, 1[$.

3.2 Stabilité par opérations de la classe $\mathcal{C}^n$.

Dans ce qui suit, $n \in \mathbb{N} \cup \{\infty\}$.

Proposition 43 ($\mathcal{C}^n(I, \mathbb{K})$ est stable par combinaison linéaire.)**.**

Si f et g sont de classe $\mathcal{C}^n$ sur I, alors pour tous λ et μ réels, $\lambda f + \mu g$ est de classe $\mathcal{C}^n$ sur I.
Dans le cas où n est fini,

$$(\lambda f + \mu g)^{(n)} = \lambda f^{(n)} + \mu g^{(n)}.$$

Proposition 44 ($\mathcal{C}^n(I, \mathbb{K})$ est stable par produit/Formule de Leibniz)**.**

Soient f et g deux fonctions de classe $\mathcal{C}^n$ sur I, Alors, la fonction fg est de classe $\mathcal{C}^n$ sur I.
Dans le cas où n est fini,

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

Exemple 45.

Soit $n \in \mathbb{N}^*$ et $f : x \mapsto x^n \cos(x)$.
Justifier que f est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$ et calculer $f^{(k)}(0)$ pour $k \in [\![0, n]\!]$.

Proposition 46.

- Si f et g sont deux fonctions de classe $\mathcal{C}^n$ sur I, avec g ne s'annulant pas sur I, alors (f/g) est de classe $\mathcal{C}^n$ sur I.
- Soient $f : I \to J$ et $g : J \to \mathbb{R}$. Si f est de classe $\mathcal{C}^n$ sur I et g est de classe $\mathcal{C}^n$ sur J alors, $g \circ f$ est de classe $\mathcal{C}^n$ sur I.
- Soit $f : I \to J$ bijective et de classe $\mathcal{C}^n$ sur I $(n \geq 1)$.
  Si f' ne s'annule pas sur I, alors f^{-1} est de classe $\mathcal{C}^n$ sur J.

Exercices

$\boxed{\textbf{23.1}}$ **[♦◇◇]** Soit f une fonction définie au voisinage d'un réel a et dérivable en a. Montrer que la limite suivante existe et la calculer :

$$\lim_{h \to 0} \frac{f(a+h) - f(a-h)}{2h}.$$

$\boxed{\textbf{23.2}}$ **[♦♦◇]** Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que $\forall x, y \in \mathbb{R} \quad f(x) - f(y) \leq (x-y)^2$.

$\boxed{\textbf{23.3}}$ **[♦♦♦]** Montrer qu'il n'existe pas de fonction $f : \mathbb{R} \to \mathbb{R}_+^*$ dérivable telle que $f' = f \circ f$.

$\boxed{\textbf{23.4}}$ **[♦♦◇]** Soit $f : \mathbb{R} \to \mathbb{R}$, dérivable et tendant vers une même limite finie en $+\infty$ et $-\infty$.
Montrer que la dérivée de f s'annule sur $\mathbb{R}$.
Indication : on pourra s'intéresser à la fonction $g : \left\{ \begin{array}{ccc}]-\frac{\pi}{2}, \frac{\pi}{2}[& \to & \mathbb{R} \\ x & \mapsto & f(\tan(x)) \end{array} \right.$.

$\boxed{\textbf{23.5}}$ **[♦♦◇]** Soit $n \in \mathbb{N}^*$ et f de classe $\mathcal{C}^n$ sur $[a, b]$ telle que $f(a) = 0$ et $\forall k \in [\![0, n-1]\!] \ f^{(k)}(b) = 0$.
Démontrer que les fonctions $f', f^{(2)}, \ldots$ et $f^{(n)}$ s'annulent sur $]a, b[$.

$\boxed{\textbf{23.6}}$ **[♦♦♦]** Soit f une fonction dérivable sur $[0, 1]$ telle que $f(0) = f(1) = f'(0) = 0$.
Montrer que la tangente à la courbe de f en un certain point de $]0, 1[$ est une droite qui passe par l'origine.

$\boxed{\textbf{23.7}}$ **[♦♦◇]** En appliquant le théorème des accroissements finis entre k et $k+1$ à la fonction $x \mapsto \ln|\ln(x)|$, démontrer que la suite de terme général $\sum\limits_{k=2}^{n} \frac{1}{k \ln(k)}$ diverge.

$\boxed{\textbf{23.8}}$ **[♦♦◇]** La fonction $x \mapsto x^x$ est définie sur $\mathbb{R}_+$ (on rappelle que $0^0 = 1$).
Démontrer qu'elle est continue en 0 mais qu'elle n'y est pas dérivable.

$\boxed{\textbf{23.9}}$ **[♦♦◇]** Soit $a \in \mathbb{R}_+^*$ On définit sur $\mathbb{R}_+^*$ la fonction $f : x \mapsto \frac{1}{2}\left(x + \frac{a}{x}\right)$

1. Démontrer que f possède un unique point fixe ℓ sur $\mathbb{R}_+^*$ que l'on exprimera à l'aide de a.
   Justifier que $[\ell, +\infty[$ est stable par f.
2. Démontrer que f est $\frac{1}{2}$-lipschitzienne sur $[\ell, +\infty[$.
3. Soit u la suite définie par $u_0 \in [\ell, +\infty[$ et par $\forall n \in \mathbb{N} \quad u_{n+1} = f(u_n)$.
   Démontrer qu'il existe une constante $C > 0$ telle que

$$\forall n \in \mathbb{N} \quad |u_n - \ell| \leq C \cdot \left(\frac{1}{2}\right)^n.$$

$\boxed{\textbf{23.10}}$ **[♦♦◇]** Démontrer que

$$\forall n \in \mathbb{N} \quad \forall x \in [0, \frac{\pi}{2}[\quad \tan^{(n)}(x) \geq 0.$$

$\boxed{\textbf{23.11}}$ **[♦♦◇]** Montrer que pour tout $n \in \mathbb{N}^*$ et pour tout $x > 0$,

$$\frac{\mathrm{d}^n}{\mathrm{d}x^n}\Big(x^{n-1}\ln(x)\Big) = \frac{(n-1)!}{x}$$

$\boxed{\textbf{23.12}}$ **[♦♦♦]** Soit $n \in \mathbb{N}$ et $f \in \mathcal{C}^n(\mathbb{R}, \mathbb{R})$. Montrer que pour tout $x \in \mathbb{R}^*$,

$$\frac{\mathrm{d}^n}{\mathrm{d}x^n}\left(x^{n-1} f\left(\frac{1}{x}\right)\right) = \frac{(-1)^n}{x^{n+1}} f^{(n)}\left(\frac{1}{x}\right)$$

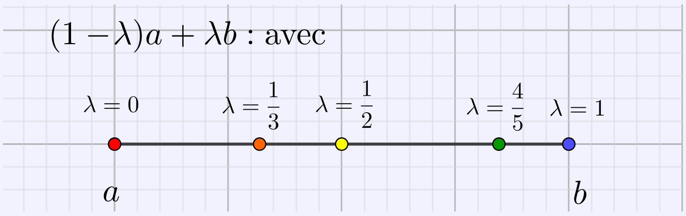
I est un intervalle de $\mathbb{R}$. Rappelons que c'est une partie *convexe* de $\mathbb{R}$: si $a, b \in I$ avec $a \leq b$, alors $[a, b] \subset I$.

1 Convexité d'une fonction.

Lemme 1.

Soient a et b deux réels tels que $a \leq b$. On a

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

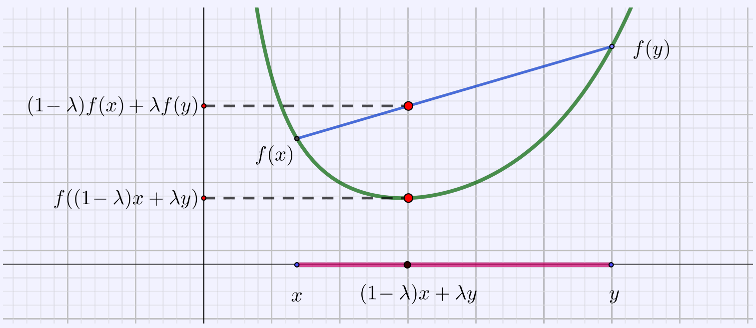


Définition 2.

Une fonction $f : I \to \mathbb{R}$ est dite **convexe** sur I si pour tout $(x, y) \in I^2$ et tout $\lambda \in [0,1]$,

$$f((1-\lambda)x + \lambda y) \leq (1-\lambda)f(x) + \lambda f(y).$$

L'opposé d'une fonction convexe est dite **concave**.



Exemple 3.

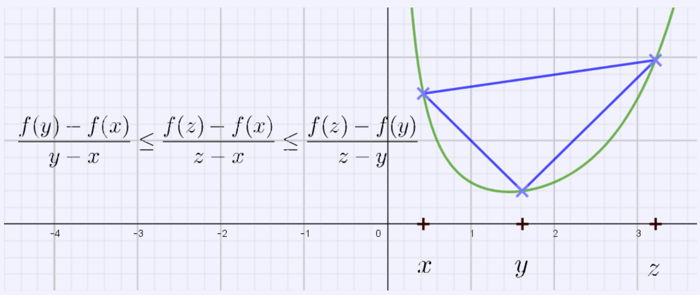
1. Les fonctions affines sont convexes sur $\mathbb{R}$ ... et concaves !
2. La fonction $x \mapsto |x|$ est convexe sur $\mathbb{R}$.

2 Inégalité des pentes.

Proposition 4 (Inégalité des pentes)**.**

Si f est une fonction convexe sur I, alors

$$\forall (x,y,z) \in I^3 \quad (x<y<z) \Longrightarrow \left(\frac{f(y)-f(x)}{y-x} \leq \frac{f(z)-f(x)}{z-x} \leq \frac{f(z)-f(y)}{z-y} \right).$$



Proposition 5 (Caractérisation de la convexité par la croissance des pentes des sécantes)**.**

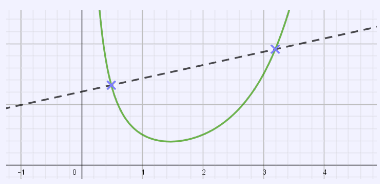
Soit $f : I \to \mathbb{R}$. Il y a équivalence entre

1. f est convexe sur I.
2. Pour tout $a \in I$, la fonction $T_a : x \mapsto \frac{f(x)-f(a)}{x-a}$ est croissante sur $I \setminus \{a\}$.

Remarque : Si a est un point à l'intérieur de I (c'est-à-dire un élément de I qui n'est pas une borne de I), on peut appliquer le théorème de la limite monotone au taux d'accroissement de f en a et prouver qu'il admet une limite finie à gauche et à droite de a (exercice). Ceci permet de prouver qu'une fonction convexe est dérivable à gauche et à droite (et partant continue) en tout point intérieur de son intervalle de définition.

Proposition 6 (Position du graphe par rapport aux sécantes)**.**

Soit f une fonction convexe sur I et $a, b \in I$ tels que $a < b$.
Considérons l'unique droite affine passant par les points $(a, f(a))$ et $(b, f(b))$, **sécante** de f.
Le graphe de f est en dessous de cette sécante sur $[a,b]$ et au dessus à l'extérieur de $[a,b]$.



3 Fonctions convexes dérivables.

Proposition 7 (Caractérisation des fonctions convexes parmi les fonctions dérivables)**.**

Soit $f : I \to \mathbb{R}$ une fonction dérivable sur I. Il y a équivalence entre

1. f est convexe sur I.
2. f' est croissante sur I.

Notamment, si f est une fonction deux fois dérivable sur I, f est convexe sur I ssi $f'' \geq 0$ sur I.

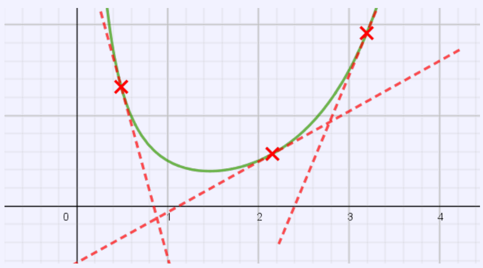
Exemple 8.

- exp, ch, et les puissances paires $x \mapsto x^{2p}$ ($p \in \mathbb{N}$) sont convexes sur $\mathbb{R}$.
  Les fonctions $x \mapsto x^a$ avec $a \geq 1$ et $a \leq 0$ sont convexes sur $\mathbb{R}_+^*$.
- ln est concave sur $\mathbb{R}_+^*$. Les fonctions $x \mapsto x^a$ avec $0 \leq a \leq 1$ sont concaves sur $\mathbb{R}_+^*$.
- Les puissances impaires $x \mapsto x^{2p+1}$ ($p \in \mathbb{N}$) sont concaves sur $\mathbb{R}_-$ et convexes sur $\mathbb{R}_+$: on observe en 0 un *point d'inflexion.*

Proposition 9 (Position du graphe par rapport aux tangentes)**.**

Le graphe d'une fonction $f \in \mathcal{D}(I, \mathbb{R})$ convexe est au-dessus de toutes ses tangentes : si $a \in I$,

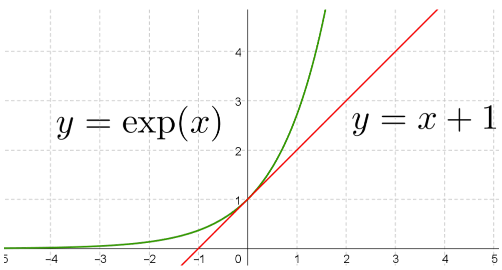
$$\forall x \in I \quad f(x) \geq f'(a)(x-a) + f(a).$$

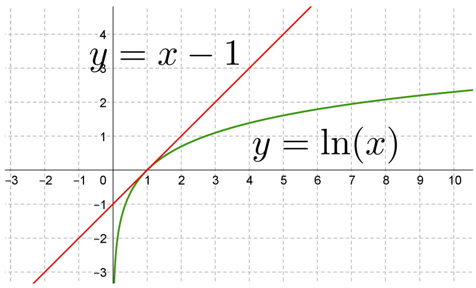


Exemple 10.

Les fonctions exp et ln sont respectivement convexe et concave.

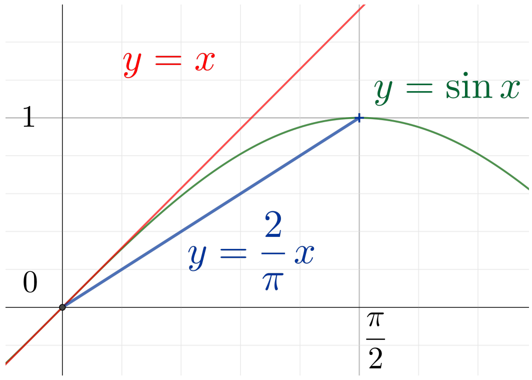
$$\forall x \in \mathbb{R} \quad e^x \geq x+1 \qquad\qquad \forall x \in \mathbb{R}_+^* \quad \ln(x) \leq x-1$$





Exemple 11.

La fonction sin est concave sur $[0, \frac{\pi}{2}]$: on a l'encadrement $\forall x \in [0, \frac{\pi}{2}] \quad \frac{2}{\pi}x \leq \sin x \leq x$.



4 Inégalité de Jensen.

Lemme 12.

Soient $x_1, \ldots, x_n$ n éléments d'un intervalle I et $\lambda_1, \ldots, \lambda_n \in \mathbb{R}_+$ tels que $\sum_{k=1}^{n} \lambda_k = 1$.

Alors tous les λ_i sont inférieurs à 1 et le nombre $\sum_{i=1}^{n} \lambda_i x_i$ est encore un élément de I.

Remarque. On peut voir le nombre $\sum_{i=1}^{n} \lambda_i x_i$ comme une *moyenne pondérée* des x_i.
On peut aussi emprunter son vocabulaire à la géométrie et parler de cette somme comme d'un *barycentre* des x_i. Un exemple important : celui où les n scalaires λ_i sont égaux (à $\frac{1}{n}$, donc)

$$\frac{1}{n}\sum_{i=1}^{n} x_i.$$

Alors tous les x_i ont le *même poids dans la moyenne* : on parlera d'*isobarycentre* en géométrie.

Théorème 13 (Inégalité de Jensen)**.**

Soit $n \in \mathbb{N}^*$. Si f est une fonction convexe sur un intervalle I, l'inégalité

$$f\left(\sum_{i=1}^{n} \lambda_i x_i\right) \leq \sum_{i=1}^{n} \lambda_i f(x_i),$$

est vraie pour tous $x_1, \ldots, x_n$ dans I et $\lambda_1, \ldots, \lambda_n$ positifs de somme égale à 1.

Remarque : on retrouve l'inégalité définissant la convexité dans le cas $n = 2$.

L'inégalité de Jensen sera souvent écrite pour des scalaires λ_i tous égaux. Ainsi, pour $n \in \mathbb{N}^*$, f convexe sur I, et $x_1, \ldots x_n \in I$, on a

$$f\left(\frac{1}{n}\sum_{i=1}^{n} x_i\right) \leq \frac{1}{n} f\left(\sum_{i=1}^{n} x_i\right).$$

Exemple 14 (Inégalité arithmético-géométrique)**.**

En utilisant la concavité de ln sur $\mathbb{R}_+^*$, on démontre que

$$\forall n \in \mathbb{N}^* \quad \forall x_1, \ldots, x_n \in \mathbb{R}_+^* \quad (x_1 x_2 \cdots x_n)^{\frac{1}{n}} \leq \frac{x_1 + x_2 + \cdots + x_n}{n}.$$

Le membre de droite est appelé moyenne arithmétique des x_i : pour le grand public, c'est « la » moyenne. Le membre de gauche est appelé **moyenne géométrique** des x_i.

L'inégalité arithmético-géométrique montre que si l'on remplaçait la moyenne arithmétique par la géométrique sur les bulletins de notes des étudiants, cela se ferait toujours à leur désavantage !

Exercices

$\boxed{\textbf{24.1}}$ **[♦◊◊]**

1. Démontrer que la fonction $x \mapsto \ln(\ln(x))$ est concave sur $]1, +\infty[$.
2. Montrer que
$$\forall a, b > 1 \;\; \ln\left(\frac{a+b}{2}\right) \geq \sqrt{\ln(a)\ln(b)}.$$

$\boxed{\textbf{24.2}}$ **[♦◊◊]** Soit $n \in \mathbb{N}^*$ et $(x_1, \ldots, x_n) \in \left(\mathbb{R}_+^*\right)^n$ et $\alpha \in \mathbb{R}$.
En discutant selon les valeurs de α, comparer

$$\left(\sum_{i=1}^{n} x_i\right)^{\alpha} \quad \text{et} \quad n^{\alpha-1}\sum_{i=1}^{n} x_i^{\alpha}.$$

$\boxed{\textbf{24.3}}$ **[♦◊◊]** Soit $n \in \mathbb{N}^*$

1. Montrer que $f : x \mapsto \ln(1 + e^x)$ est convexe sur $\mathbb{R}$.
2. Montrer que
$$\forall (x_1, \ldots, x_n) \in (\mathbb{R}_+^*)^n \quad 1 + \left(\prod_{k=1}^{n} x_k\right)^{\frac{1}{n}} \leq \left(\prod_{k=1}^{n}(1 + x_k)\right)^{\frac{1}{n}}$$
3. Montrer que
$$\forall (a_1, \ldots, a_n, b_1, \ldots, b_n) \in (\mathbb{R}_+^*)^{2n} \quad \left(\prod_{k=1}^{n} a_k\right)^{\frac{1}{n}} + \left(\prod_{k=1}^{n} b_k\right)^{\frac{1}{n}} \leq \left(\prod_{k=1}^{n}(a_k + b_k)\right)^{\frac{1}{n}}.$$

$\boxed{\textbf{24.4}}$ **[♦♦◊]**

1. Montrer que la fonction $x \mapsto \dfrac{1}{e^x+1}$ est convexe sur $\mathbb{R}_+$.
2. En déduire que pour tout $x_1, \dots, x_n \geq 1$,

$$\sum_{k=1}^{n} \frac{1}{1+x_k} \geq \frac{n}{1+\sqrt[n]{x_1 \dots x_n}}.$$

$\boxed{\textbf{24.5}}$ **[♦♦◊]** Soit $f : [0,1] \to \mathbb{R}$ deux fois dérivable et telle que $\forall x \in [0,1]\ f''(x) \geq 1$.
Montrer que $f(0) - 2f(\frac{1}{2}) + f(1) \geq \frac{1}{4}$.

$\boxed{\textbf{24.6}}$ **[♦♦◊]** *avec les propriétés de l'intégrale*
Soit f une fonction convexe et de classe $\mathcal{C}^1$ sur $[a,b]$. Prouver que

$$(b-a)f\left(\frac{a+b}{2}\right) \leq \int_a^b f(t)\mathrm{d}t \leq (b-a)\frac{f(a)+f(b)}{2}.$$

$\boxed{\textbf{24.7}}$ **[♦♦◊]** Montrer que toute fonction convexe sur $\mathbb{R}$ et majorée, est constante.

$\boxed{\textbf{24.8}}$ **[♦♦◊]** Soient deux réels $a < b$ et $f : [a,b] \to \mathbb{R}_+$ une fonction convexe.

1. Montrer que f est continue sur $]a,b[$.
2. Donner le graphe d'une fonction convexe sur $[a,b]$ et discontinue en a et b.

$\boxed{\textbf{24.9}}$ **[♦♦◊]** Soit f une fonction convexe sur un intervalle I et admettant sur I un minimum.
Démontrer que l'ensemble des points pour lesquels ce minimum est atteint est un intervalle.

$\boxed{\textbf{24.10}}$ **[♦♦♦]** [Inégalités de Hölder et de Minkowski]

Soit $(p,q) \in]0,+\infty[^2$ tel que $\frac{1}{p} + \frac{1}{q} = 1$.

1. À l'aide de ln, montrer que $\forall (\alpha,\beta) \in]0,\infty[^2\ \alpha\beta \leq \frac{1}{p}\alpha^p + \frac{1}{q}\beta^q$.
2. Montrer l'inégalité de Hölder

$$\forall (a_1, \dots, a_n, b_1, \dots, b_n) \in \mathbb{R}^{2n} \quad \sum_{i=1}^{n} |a_i||b_i| \leq \left(\sum_{i=1}^{n} |a_i|^p\right)^{\frac{1}{p}} \times \left(\sum_{i=1}^{n} |b_i|^q\right)^{\frac{1}{q}}.$$

   On pourra poser $A = \left(\sum_{i=1}^{n} |a_i|^p\right)^{\frac{1}{p}}$ *et* $B = \left(\sum_{i=1}^{n} |b_i|^q\right)^{\frac{1}{q}}$, *traiter le cas où* $A = 0$ *ou* $B = 0$ *puis appliquer 1) avec* $\alpha = \frac{|a_i|}{A}$ *et* $\beta = \frac{|b_i|}{B}$.
3. Montrer l'inégalité de Minkowski :

$$\forall p \in]1,+\infty[\quad \forall (a_1, \dots, a_n, b_1, \dots, b_n) \in \mathbb{R}^{2n} \quad \left(\sum_{i=1}^{n} |a_i + b_i|^p\right)^{\frac{1}{p}} \leq \left(\sum_{i=1}^{n} |a_i|^p\right)^{\frac{1}{p}} + \left(\sum_{i=1}^{n} |b_i|^p\right)^{\frac{1}{p}}.$$

   Indication : on pourra remarquer que $|a_i + b_i|^p \leq |a_i + b_i|^{p-1}(|a_i| + |b_i|)$ *et appliquer l'inégalité de Hölder.*

---

25 # Polynômes

1 L'anneau des polynômes.

1.1 Combinaisons linéaires, degré.

Définition 1.

On appelle **polynôme** à coefficients dans $\mathbb{K}$ une suite d'éléments de $\mathbb{K}$ nulle à.p.d.c.r.

L'**ensemble des polynômes** à coefficients dans $\mathbb{K}$ sera noté $\mathbb{K}[X]$.

- La suite nulle est un polynôme. Il est appelé **polynôme nul** et noté 0, ou $0_{\mathbb{K}[X]}$.
- La suite $(1, 0, 0, 0, \dots)$ est un polynôme. Il est appelé polynôme constant égal à 1 et noté 1.
- La suite $(0, 1, 0, 0, \dots)$ est un polynôme. Il est noté X et appelé **indéterminée**.
- Soit $n \in \mathbb{N}$. La suite dont tous les termes sont nuls sauf celui au rang n qui vaut 1 est un polynôme que l'on notera X^n. On l'appelle **monôme** d'ordre n :

$$X^n = (0, 0, \dots, 0, \underbrace{1}_{\text{rang } n}, 0, 0, \dots).$$

Définition 2.

Soit $P = (a_k)_{k \in \mathbb{N}}$ un polynôme de $\mathbb{K}[X]$, <u>non nul</u>.
On appelle **degré** de P, et on note $\deg(P)$ l'indice du dernier coefficient non nul de P :

$$\deg(P) = \max \{k \in \mathbb{N} : a_k \neq 0\}.$$

Par ailleurs, on pose $\deg(0_{\mathbb{K}[X]}) = -\infty$.

Pour $n \in \mathbb{N}$, on a $\deg(X^n) = n$.

Proposition-Définition 3 (Somme de polynômes et son degré)**.**

Soient $P = (a_k)_{k \in \mathbb{N}}$ et $Q = (b_k)_{k \in \mathbb{N}}$ deux polynômes de $\mathbb{K}[X]$.
On appelle somme de P et Q, notée $P + Q$ la suite $(a_k + b_k)_{k \in \mathbb{N}}$.
C'est un polynôme de $\mathbb{K}[X]$ et

$$\deg(P + Q) \leq \max(\deg(P), \deg(Q)), \text{ avec égalité si } \deg(P) \neq \deg(Q);$$

Proposition 4.

$(\mathbb{K}[X], +)$ est un <u>groupe abélien</u>. Plus précisément,

1. $+$ est une loi de composition interne sur $\mathbb{K}[X]$, associative et commutative ;
2. il existe un polynôme dans $\mathbb{K}[X]$ qui est neutre pour l'addition : c'est le polynôme nul $0_{\mathbb{K}[X]}$;
3. tout polynôme P de $\mathbb{K}[X]$ possède un symétrique $-P$ dans $K[X]$.
   Si $P = (a_k)$, le polynôme $-P$ est la suite $(-a_k)$ et on a $-P + P = P + (-P) = 0_{\mathbb{K}[X]}$.

Proposition-Définition 5 (Multiplication par un scalaire et son degré)**.**

Soient $P = (a_k)_{k\in\mathbb{N}} \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.
On note $\lambda \cdot P$, ou encore λP la suite $(\lambda a_k)_{k\in\mathbb{N}}$.
C'est un polynôme de $\mathbb{K}[X]$ et

$$\deg(\lambda P) \leq \deg(P), \text{ avec égalité si } \lambda \neq 0.$$

Proposition 6 (Propriétés de la multiplication par un scalaire)**.**

- $\forall P \in \mathbb{K}[X] \quad 1_{\mathbb{K}} \cdot P = P$;
- $\cdot$ est distributive par rapport à l'addition dans $\mathbb{K}[X]$:

$$\forall (P,Q) \in (\mathbb{K}[X])^2 \quad \forall \lambda \in \mathbb{K} \quad \lambda \cdot (P+Q) = \lambda \cdot P + \lambda \cdot Q;$$

- $\cdot$ est distributive par rapport à l'addition dans $\mathbb{K}$:

$$\forall P \in \mathbb{K}[X] \quad \forall \lambda, \mu \in \mathbb{K} \quad (\lambda + \mu) \cdot P = \lambda \cdot P + \mu \cdot P;$$

- $\forall \lambda, \mu \in \mathbb{K} \quad \forall P \in \mathbb{K}[X] \quad \lambda \cdot (\mu \cdot P) = (\lambda\mu) \cdot P$.

Proposition-Définition 7.

Soit $n \in \mathbb{N}$.
On note $\mathbb{K}_n[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$, de degré inférieur ou égal à n.
Un polynôme $P = (a_k)_{k\in\mathbb{N}}$ qui appartient à $\mathbb{K}_n[X]$ s'écrit

$$P = \sum_{k=0}^{n} a_k X^k.$$

On a en particulier

$\boxed{\mathbb{K}_0[X] = \left\{a \cdot 1_{\mathbb{K}[X]} \mid a \in \mathbb{K}\right\}}$ $\boxed{\mathbb{K}_1[X] = \left\{aX + b \mid (a,b) \in \mathbb{K}^2\right\}}$ $\boxed{\mathbb{K}_2[X] = \left\{aX^2 + bX + c \mid (a,b,c) \in \mathbb{K}^3\right\}}$

Définition 8.

Les polynômes de $\mathbb{K}_0[X]$ sont appelés **polynômes constants**.

Attention, un polynôme constant est de degré 0... ou $-\infty$ s'il est nul !

Proposition 9.

Soit $n \in \mathbb{N}$. L'ensemble $\mathbb{K}_n[X]$ est stable par combinaisons linéaires :

$$\forall (P,Q) \in (\mathbb{K}_n[X])^2 \quad \forall (\lambda,\mu) \in \mathbb{K}^2 \quad \lambda P + \mu Q \in \mathbb{K}_n[X].$$

Notation.

Un polynôme $P = (a_k)_{k\in\mathbb{N}}$ de $\mathbb{K}[X]$ sera désormais noté

$$P = \sum a_k X^k,$$

Remarque. Soient $P = \sum a_k X^k$ et $Q = \sum b_k X^k$. Par définition, les polynômes P et Q sont égaux si et seulement si les suites P et Q sont égales. Cela permettra « d'identifier » le coefficient devant X^k. Ainsi,

$$\boxed{\sum a_k X^k = \sum b_k X^k \quad \Longleftrightarrow \quad \forall k \in \mathbb{N} \ \ a_k = b_k.}$$

Proposition-Définition 10.

Soit P un polynôme de $\mathbb{K}[X]$ et $d \in \mathbb{N}$.

$$\deg(P) = d \quad \Longleftrightarrow \quad \Big(\exists (\lambda, R) \in \mathbb{K} \times \mathbb{K}[X] \ \mid \ P = \lambda X^d + R, \ \lambda \neq 0 \ \text{ et } \ \deg(R) < d\Big).$$

Si P est non nul et de degré $d \in \mathbb{N}$, alors λ est appelé **coefficient dominant** de P.
On pourra noter ce coefficient $\mathrm{cd}(P)$. Si ce coefficient vaut 1, le polynôme P est dit **unitaire**.

1.2 Produit.

Proposition-Définition 11 (Produit de deux polynômes)**.**

Soient $P = \sum a_k X^k$ et $Q = \sum b_k X^k$ deux polynômes de $\mathbb{K}[X]$.
Soit $(c_k)_{k\geq 0}$ la suite définie par

$$\forall k \in \mathbb{N} \quad c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

La suite c est un polynôme : on l'appelle **produit** de P et Q, noté $P \times Q$, ou encore PQ :

$$\left(\sum_{k\in\mathbb{N}} a_k X^k\right)\left(\sum_{k\in\mathbb{N}} b_k X^k\right) = \sum_{k\in\mathbb{N}} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) X^k.$$

Proposition 12 (Degré et coefficient dominant d'un produit)**.**

$$\boxed{\forall (P,Q) \in (\mathbb{K}[X])^2 \quad \deg(P \times Q) = \deg(P) + \deg(Q)}$$

$$\forall (P,Q) \in (\mathbb{K}[X] \setminus \{0\})^2 \quad \mathrm{cd}(P \times Q) = \mathrm{cd}(P) \times \mathrm{cd}(Q).$$

Proposition 13 (la balade du scalaire)**.**

$$\forall (P,Q) \in (\mathbb{K}[X])^2 \quad \forall (\lambda,\mu) \in \mathbb{K}^2 \quad (\lambda P)Q = P(\lambda Q) = \lambda(PQ) \quad \text{et} \quad (\lambda P)(\mu Q) = (\lambda\mu)PQ.$$

1.3 Structure d'anneau de $\mathbb{K}[X]$.

Théorème 14.

$(\mathbb{K}[X], +, \times)$ est un anneau commutatif.

Proposition 15 (Cohérence de la notation X^n)**.**

Pour tout $n \in \mathbb{N}$, le polynôme X^n est bien le $n$ème itéré de X.

La preuve des deux résultats ci-dessus est en annexe.

Proposition 16 (Propriétés de l'anneau des polynômes)**.**

L'anneau $\mathbb{K}[X]$ est intègre : il est commutatif, et sans diviseurs de zéro :

$$\forall P, Q \in \mathbb{K}[X] \qquad PQ = 0 \implies (P = 0 \text{ ou } Q = 0)\,.$$

Ainsi pouvons nous « simplifier » par un polynôme non nul :

$$\forall A, B, C \in \mathbb{K}[X] \quad (AB = AC \quad \text{et} \quad A \neq 0) \implies B = C.$$

Les inversibles de l'anneau $\mathbb{K}[X]$ sont les polynômes constants non nuls :

$$U\left(\mathbb{K}[X]\right) = \mathbb{K}_0[X] \setminus \{0\}.$$

Comme dans tout anneau commutatif, il est possible d'écrire des identités remarquables dans $\mathbb{K}[X]$, notamment le binôme, ou la factorisation de $P^n - Q^n$ par $P - Q$.

Exemple 17.

À l'aide d'identités remarquables, factoriser

$$X^3 - 1; \qquad X^3 + 1; \qquad X^4 - 1; \qquad 1 + X^4 + X^8.$$

Exemple 18.

Soit $n \in \mathbb{N}^*$ et $P = (X+2)^n - (X+1)^n$. Calculer le degré de P et son coefficient dominant.

Exemple 19 (Formule de Vandermonde)**.**

Soient $(p, q, n) \in \mathbb{N}^3$. En considérant $(X+1)^p(X+1)^q$, montrer que

$$\sum_{k=0}^{n} \binom{p}{k}\binom{q}{n-k} = \binom{p+q}{n}.$$

1.4 Évaluation.

Définition 20 (où l'on retrouve les fonctions polynomiales).

Soit $P = \sum a_k X^k$ un polynôme de $\mathbb{K}[X]$.
Pour $x \in \mathbb{K}$, on appelle **évaluation** de P en x, et on note $P(x)$ le nombre

$$P(x) = \sum_{k=0}^{+\infty} a_k x^k \qquad (P \in \mathbb{K}[X] \;\text{ et }\; P(x) \in \mathbb{K}).$$

La somme précédente est *finie* puisque la suite (a_n) est par définition nulle à.p.d.c.r.
On parlera de $\widetilde{P} : x \mapsto P(x)$ comme de la **fonction polynomiale associée** au polynôme P.

Exemples 21.

1. Soit $P = X^3 - 3X + 4$. Évaluer P en 2 et -1.
2. Quelle est la fonction polynomiale associée à $X^2 - 1$? à X ?
3. Quel coefficient du polynôme obtient-on lorsqu'on l'évalue en 0 ?

Proposition 22 (opérations et évaluation).

Soient $P, Q \in \mathbb{K}[X]$, $x \in \mathbb{K}$ et $(\lambda, \mu) \in \mathbb{K}^2$.

$$(\lambda P + \mu Q)(x) = \lambda P(x) + \mu Q(x), \quad \text{ et } \quad (PQ)(x) = P(x) \cdot Q(x).$$

Exemple 23 (Polynômes de Tchebychev.).

Soit $(T_n)_{n\in\mathbb{N}}$ une suite de polynômes définie par

$$T_0 = 1, \qquad T_1 = X \qquad \forall n \in \mathbb{N} \;\; T_{n+2} = 2XT_{n+1} - T_n.$$

1. Calculer T_2, T_3, T_4 et T_5.
2. Donner pour tout entier n le degré et le coefficient dominant de T_n.
3. Démontrer que pour tout $n \in \mathbb{N}$, et tout $\theta \in \mathbb{R}$, $\cos(n\theta) = T_n(\cos(\theta))$.

Définition 24.

Soit $P \in \mathbb{K}[X]$. Une **racine** (ou un zéro) de P dans $\mathbb{K}$ est un nombre $\alpha \in \mathbb{K}$ tel que $P(\alpha) = 0$.

Exemple 25.

Donner une racine réelle de $P = X^5 - X^4 + X^3 - X^2 + X - 1$.
Donner les racines de $X^5 - 1$ dans $\mathbb{C}$.

1.5 Composition.

Définition 26.

Soient deux polynômes $P = \sum a_k X^k$ et Q. Leur **composée** $P \circ Q$ est définie par

$$P \circ Q = \sum_{k=0}^{+\infty} a_k Q^k.$$

La somme ci-dessus a un nombre fini de termes non nuls, la suite $(a_k)_{k\in\mathbb{N}}$ étant nulle à.p.d.c.r.

Exemple : Calcul de $P \circ Q$ et $Q \circ P$ avec $P = 1 + X^2$ et $Q = 2 - X$.

Remarques.

1. On vérifiera que $X \circ P = P$ et que $P \circ X = P$. Cette dernière égalité explique que l'on écrit parfois $P(X)$ à la place de P. De la même façon, on écrira $P(X^2)$ ou $P(Q(X))$ pour désigner respectivement les polynômes $P \circ X^2$ et $P \circ Q$.
2. L'écriture $P(X + 1)$ peut alors prêter à confusion : s'agit-il de $P \circ (X + 1)$ ou de $P \times (X + 1)$? La bonne réponse, c'est la composition : pour le produit, on préfèrera l'écriture $(X + 1)P$.
3. Assez clairement, si P et Q sont deux polynômes de $\mathbb{K}[X]$ et $x \in \mathbb{K}$, on a $P \circ Q(x) = P(Q(x))$.

Proposition 27.

$$\forall P \in \mathbb{K}[X] \quad \forall Q \in \mathbb{K}[X] \setminus \mathbb{K}_0[X] \quad \deg(P \circ Q) = \deg(P) \times \deg(Q).$$

1.6 Dérivation.

Définition 28.

Soit $P = \sum a_k X^k$ un polynôme de $\mathbb{K}[X]$. Le polynôme

$$P' = \sum_{k\in\mathbb{N}} (k + 1)a_{k+1} X^k$$

est appelé **polynôme dérivé** de P.

Remarque. Pas besoin de parler de dérivabilité ci-dessus : la définition ci-dessus est une opération purement *formelle* qui à la suite (a_k) associe la suite $((k + 1)a_{k+1})$.

Proposition 29.

Si P est un polynôme de $\mathbb{R}[X]$, la fonction polynomiale associée au polynôme dérivé P' est la dérivée de la fonction polynomiale associée à P.

Proposition 30.

$$\forall P \in \mathbb{K}[X] \qquad P \text{ est constant} \quad \iff \quad P' = 0_{\mathbb{K}[X]}.$$

Proposition 31 (Degré du polynôme dérivé)**.**

$$\forall P \in \mathbb{K}[X] \quad \deg(P') = \begin{cases} \deg(P)-1 & \text{si } P \text{ n'est pas constant,} \\ -\infty & \text{si } P \text{ est constant.} \end{cases}$$

Proposition 32 (Dérivation et opérations)**.**

Pour tous $P, Q \in \mathbb{K}[X]$, pour tous scalaires $\lambda, \mu \in \mathbb{K}$,

$$(\lambda P + \mu Q)' = \lambda P' + \mu Q' \qquad \text{et} \qquad (PQ)' = P'Q + PQ'.$$

$$\forall n \in \mathbb{N} \quad (P^n)' = nP'P^{n-1} \qquad \text{et} \qquad (P \circ Q)' = Q' \cdot P' \circ Q.$$

On peut s'étonner qu'une preuve soit nécessaire : ces résultats sont bien connus pour les *fonctions*... Mais attention : ici, la dérivation est une opération définie directement sur les suites de coefficients : pas de taux d'accroissement ici. Une preuve est donnée en annexe, à base de calculs formels sur les coefficients.
On peut se demander si le fait qu'on connaisse ces identités pour les fonctions polynomiales peut nous aider à prouver que le résultat est vrai pour les objets algébriques. La réponse est oui (voir la notion de rigidité polynomiale à la fin du cours).

Définition 33.

Soit $P \in \mathbb{K}[X]$ et $k \in \mathbb{N}$. On définit la **dérivée k-eme** de P, que l'on note $P^{(k)}$, en posant

$$P^{(0)} = P \qquad \text{et} \qquad \forall k \geq 1 \quad P^{(k)} = \left(P^{(k-1)}\right)'.$$

Exemple 34.

$$\forall n, k \in \mathbb{N} \quad \forall a \in \mathbb{K} \quad ((X-a)^n)^{(k)} = \begin{cases} \dfrac{n!}{(n-k)!}(X-a)^{n-k} & \text{si } 0 \leq k \leq n \\ 0 & \text{si } k > n \end{cases}$$

Proposition 35 (Linéarité de la dérivée $n$ème et formule de Leibniz)**.**

$$\forall (P,Q) \in (\mathbb{K}[X])^2 \quad \forall (\lambda, \mu) \in \mathbb{K}^2 \quad \forall n \in \mathbb{N} \quad (\lambda P + \mu Q)^{(n)} = \lambda P^{(n)} + \mu Q^{(n)}$$

$$\forall (P,Q) \in (\mathbb{K}[X])^2 \quad \forall n \in \mathbb{N} \quad (PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

Théorème 36 (Formule de Taylor pour les polynômes)**.**

Soit $n \in \mathbb{N}$, $P \in \mathbb{K}_n[X]$ et $a \in \mathbb{K}$. Alors,

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k.$$

Corollaire 37 (coefficients du polynôme à l'aide des dérivées)**.**

Soit $P = \sum a_k X^k$ un polynôme de $\mathbb{K}[X]$. Alors,

$$\forall k \in \mathbb{N} \quad a_k = \frac{P^{(k)}(0)}{k!}.$$

2 Arithmétique dans $\mathbb{K}[X]$.

2.1 Divisibilité et division euclidienne dans $\mathbb{K}[X]$.

Définition 38.

Soit $(A, B) \in \mathbb{K}[X]^2$. On dit que B **divise** A s'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $A = BQ$. On note alors $B \mid A$.

Exemple 39.

Tous les polynômes divisent le polynôme nul.

Pour $n \in \mathbb{N}^*$, $X-1$ divise $X^n - 1$ dans $\mathbb{R}[X]$: on a $X^n - 1 = (X-1)\sum_{k=0}^{n-1} X^k$.

Proposition 40.

Soient deux polynômes A et B de $\mathbb{K}[X]$, A étant non nul. Si B divise A, alors $\deg(B) \leq \deg(A)$.

Proposition-Définition 41.

La relation divise sur $\mathbb{K}[X]$ est réflexive et transitive, mais elle n'est *pas* antisymétrique.
En effet, pour A et B deux polynômes,

$$(A \mid B \text{ et } B \mid A) \iff \exists \lambda \in \mathbb{K}^* \ A = \lambda B.$$

On dit alors que A et B sont **associés**.

Tout polynôme non nul P est associé à un unique polynôme unitaire : λP, où $\lambda = \mathrm{cd}(P)^{-1}$.

Théorème 42 (de division euclidienne).

Soit $(A,B) \in \mathbb{K}[X]^2$, avec $B \neq 0$. Il existe un unique couple $(Q,R) \in \mathbb{K}[X]^2$ tel que

$$A = BQ + R \quad \text{et} \quad \deg(R) < \deg(B).$$

Exemple 43.

Poser la division de $A = X^5 + 3X^3 - 2X^2 + 1$ par $B = X^2 - 2X - 1$.
L'évaluation (en 1 ou -1 par exemple) permet parfois de détecter une éventuelle erreur de calcul.

Corollaire 44.

Soit $(A,B) \in \mathbb{K}[X]^2$, avec $B \neq 0$.
On a que B divise A ssi le reste dans la division euclidienne de A par B est le polynôme nul.

Exemple 45 (juste le reste).

Soit $\theta \in \mathbb{R}$ et $n \geq 2$.
Déterminer le reste dans la division euclidienne de $(\sin\theta X + \cos\theta)^n$ par $X^2 + 1$.
Prouver qu'il n'existe aucune valeur de θ ni de n pour lesquelles $X^2 + 1$ divise $(\sin\theta X + \cos\theta)^n$.

2.2 PGCD de deux polynômes (ou plus).

L'ensemble des diviseurs d'un polynôme A sera noté $\mathcal{D}(A)$. Cet ensemble contient tous les polynômes constants non nuls. De plus, si $A \neq 0_{\mathbb{K}[X]}$, tous les éléments de $\mathcal{D}(A)$ ont un degré majoré par $\deg(A)$.

Ainsi, dans le cas où l'un des polynômes A ou B est non nul, les polynômes de $\mathcal{D}(A) \cap \mathcal{D}(B)$ ont leur degré majoré par $\max(\deg(A), \deg(B))$, ce qui permet de donner du sens à la définition ci-dessous.

Définition 46.

Soient A et B deux polynômes de $\mathbb{K}[X]$.

- Si $(A,B) \neq (0,0)$,
  — tout diviseur commun à A et B de degré maximal est appelé *un* **PGCD** de A et B ;
  — l'unique polynôme unitaire parmi eux est appelé **PGCD unitaire** et noté $A \wedge B$.
- Si $A = B = 0$, on pose $A \wedge B = 0$.

Proposition 47.

Deux PGCD d'un même couple de polynômes sont associés.

Théorème 48 (PGCD par une relation de Bézout)**.**

Soient A et B deux polynômes de $\mathbb{K}[X]$. Il existe $(U,V) \in (\mathbb{K}[X])^2$ tel que

$$A \wedge B = AU + BV.$$

L'égalité ci-dessus est appelée une **relation de Bézout**.
Le couple (U,V) peut-être désigné comme un couple de *coefficients de Bézout*, il n'est pas unique.

Remarque. Lorsque l'un des deux polynômes A ou B est non nul, on comprend dans la preuve que le PGCD est le polynôme unitaire de degré minimal appartenant à l'ensemble

$$A\mathbb{K}[X] + b\mathbb{K}[X] = \left\{ AU + BV \ : \ (U,V) \in (\mathbb{K}[X]^2 \right\}.$$

Proposition 49 (Les diviser tous les deux, c'est diviser leur PGCD)**.**

Soit $(A,B) \in (\mathbb{K}[X])^2$. Alors

$$\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(A \wedge B).$$

Les diviseurs communs de A et B sont exactement les diviseurs du PGCD unitaire de A et B. Le PGCD unitaire peut être remplacé ici par n'importe quel PGCD.

Proposition 50.

$$\forall (A,B) \in \mathbb{K}[X]^2, \quad \forall P \in \mathbb{K}[X] \text{ (unitaire)}, \quad \mathrm{PGCD}\,(PA, PB) = P \cdot \mathrm{PGCD}(A,B).$$

Proposition 51 (Réduction du problème)**.**

Soit $(A,B,C,Q) \in (\mathbb{K}[X])^4$ tel que $A = BQ + C$.
Alors $\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(B) \cap \mathcal{D}(C)$. En particulier, $A \wedge B = B \wedge C$.

Théorème 52 (Algorithme d'Euclide)**.**

Soit $(A,B) \in \mathbb{K}[X]^2$, $B \neq 0$.

- On note $R_0 = A$ et $R_1 = B$.
- Tant qu'il existe $i \in \mathbb{N}^*$ tel que R_i est non nul, on définit R_{i+1} comme le reste dans la division euclidienne de R_{i-1} par R_i.

Cet algorithme termine : il existe $p \in \mathbb{N}^*$ tel que $R_1, \ldots, R_p$ sont non nuls et $R_{p+1} = 0$. Alors,

$$\boxed{R_p \text{ est un PGCD de } A \text{ et } B}$$

Méthode (Algorithme d'Euclide étendu).

Comme dans $\mathbb{Z}$, la remontée des divisions euclidienne fournit des coefficients de Bézout

Exemple 53.

Calculer un PGCD, ainsi qu'une relation de Bézout pour $A = X^3 - 2X^2 + 2X - 1$ et $B = X^3 - 1$.

Extension à un nombre fini de polynômes.

De la même façon que dans $\mathbb{Z}$, on peut définir les PGCD de n polynômes $A_1, \dots, A_n$ de $\mathbb{K}[X]$ non tous nuls. Le diviseur maximal en degré et unitaire étant noté

$$A_1 \wedge \cdots \wedge A_n.$$

Les résultats de l'arithmétique classique s'étendent, en particulier l'*associativité* du PGCD. Pour alléger cet exposé, on renvoie au cours d'arithmétique dans $\mathbb{Z}$ pour un énoncé précis.

2.3 PPCM de deux polynômes.

Soient A et B polynômes de $\mathbb{K}[X]$. L'ensemble $A\mathbb{K}[X] \cap B\mathbb{K}[X]$ est celui de leurs multiples communs. Si A et B sont non nuls, cette intersection contient au moins un polynôme non nul : AB.

Définition 54.

Soient A et B deux polynômes de $\mathbb{K}[X]$.

- Si A et B sont non nuls,
  - tout multiplie commun de A et B de degré minimal est appelé un **PPCM** de A et B ;
  - l'unique polynôme unitaire parmi eux est appelé **PPCM** unitaire et noté $A \vee B$.
- Si A ou B vaut 0, on pose $a \vee b = 0$.

Proposition 55.

Soit A et B dans $\mathbb{K}[X]$. Alors

$$A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X].$$

Les multiples communs de A et B sont exactement les multiples du PPCM unitaire de A et B. Le PPCM unitaire peut être remplacé ici par n'importe quel PPCM.

Proposition 56.

$$\forall (A, B) \in (\mathbb{K}[X])^2 \quad (A \wedge B) \cdot (A \vee B) \text{ et } AB \text{ sont associés.}$$

2.4 Polynômes premiers entre eux.

Définition 57 (le cas d'un couple)**.**

On dit que deux polynômes sont **premiers entre eux** si leur PGCD unitaire est égal à $1_{\mathbb{K}[X]}$. Ainsi, deux polynômes sont premiers entre eux si et seulement leurs seuls diviseurs communs sont les polynômes constants non nuls

Si deux polynômes sont premiers entre eux, au moins l'un d'entre eux est non nul.

Proposition 58 (se ramener à deux polynômes premiers entre eux)**.**

Soient $(A, B) \in (\mathbb{K}[X])^2 \setminus \{(0, 0)\}$ et D un PGCD de A et B.
Si A^* et B^* sont les deux polynômes tels que $A = DA^*$, $B = DB^*$, alors $A^* \wedge B^* = 1$.

Proposition 59.

Deux polynômes non nuls A et B sont premiers entre eux ssi AB est un PPCM de A et B.

Théorème 60 (de Bézout)**.**

$$\forall A, B \in \mathbb{K}[X] \qquad A \wedge B = 1 \quad \Longleftrightarrow \quad \exists (U, V) \in (\mathbb{K}[X])^2 \ \ AU + BV = 1.$$

Corollaire 61.

Si A, B, C sont trois polynômes de $\mathbb{K}[X]$, alors

1. Si $A \wedge B = 1$ et $A \wedge C = 1$, alors $A \wedge (BC) = 1$.
2. Plus généralement, si A est premier avec chacun des m polynômes $B_1, \ldots, B_m$ où $m \in \mathbb{N}^*$, alors il est premier avec leur produit $B_1 \cdots B_m$.
3. Si $A \wedge B = 1$, alors pour tout $(n, p) \in \mathbb{N}^2$, $A^n \wedge B^p = 1$.

Exemple 62 (important)**.**

Soient $(\alpha, \beta) \in \mathbb{K}^2$ tel que $\alpha \neq \beta$ et $(n, p) \in \mathbb{N}^2$. Montrer que $(X - \alpha)^n \wedge (X - \beta)^p = 1$.

Le produit de deux diviseurs n'est pas toujours un diviseur, mais...

Proposition 63 (Produit de diviseurs premiers entre eux)**.**

$$\forall (A, B, C) \in (\mathbb{K}[X])^3 \qquad \begin{cases} A \mid C \ \text{ et } \ B \mid C \\ A \wedge B = 1 \end{cases} \quad \Longrightarrow \quad AB \mid C.$$

Diviser un produit, ce n'est pas forcément diviser l'un des facteurs, mais...

Théorème 64 (Lemme de Gauss)**.**

$$\forall (A,B,C) \in (\mathbb{K}[X])^3 \qquad \left\{ \begin{array}{c} A \mid BC \\ A \wedge B = 1 \end{array} \right. \implies \quad A \mid C.$$

Extension à un nombre fini de polynômes.

Dans ce paragraphe, n est un entier naturel supérieur à 2.

Définition 65.

Des polynômes $A_1, \dots, A_n$ sont dits **premiers entre eux dans leur ensemble** si leur PGCD unitaire est égal à 1, ou de manière équivalente les seuls diviseurs communs à ces polynômes sont les polynômes constants non nuls.

Remarque. Si n polynômes non tous nuls ne sont pas premiers entre eux dans leur ensemble, on peut les diviser par leur PGCD pour obtenir n polynômes qui cette fois le sont.

Définition 66.

Les polynômes $A_1, \dots, A_n$ sont **deux à deux premiers entre eux** si

$$\forall (i,j) \in [\![1,n]\!]^2 \quad i \neq j \implies A_i \wedge A_j = 1.$$

Exemple 67 (*dans leur ensemble* VS *deux à deux*)**.**

Si n polynômes sont premiers entre eux deux à deux, ils le sont dans leur ensemble.
Les polynômes $X(X+1)$, $X(X+2)$ et $(X+1)(X+2)$ sont premiers entre eux dans leur ensemble, mais deux quelconques d'entre eux ne sont pas premiers entre eux.

Proposition 68 (Théorème de Bezout généralisé)**.**

Soit $(A_1, \dots, A_n) \in (\mathbb{K}[X])^n$

$$A_1, \dots, A_n \text{ premiers entre eux dans leur ensemble } \iff \exists (U_1, \dots, U_n) \in (\mathbb{K}[X])^n \quad \sum_{i=1}^{n} A_i U_i = 1.$$

Proposition 69 (Produit de diviseurs deux à deux premiers entre eux)**.**

Soient n polynômes $A_1, A_2, \dots, A_n$ et un polynôme B.

Si tous les A_i divisent B et si les A_i sont deux à deux premiers entre eux,
alors le produit $A_1 \cdots A_n$ divise B.

3 Racines et factorisation.

3.1 Racines et divisibilité.

Théorème 70 (Racine et divisibilité par un polynôme de degré 1)**.**

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Il y a équivalence entre les deux assertions suivantes.

1. α est une racine de P.
2. $X - \alpha$ divise P.

Proposition 71.

Soit $P \in \mathbb{K}[X]$, $p \in \mathbb{N}^*$ et $\alpha_1, \alpha_2, \dots \alpha_p \in \mathbb{K}$ des scalaires de $\mathbb{K}$ deux à deux distincts. On a

$$\alpha_1, \alpha_2 \dots, \alpha_p \text{ sont racines de } P \quad \Longleftrightarrow \quad \prod_{k=1}^{p} (X - \alpha_k) \text{ divise } P.$$

Exemple 72.

Soit $(p, q, r) \in \mathbb{N}^3$. Justifier qu'il existe $Q \in \mathbb{C}[X]$ tel que $X^{3p+2} + X^{3q+1} + X^{3r} = (X^2 + X + 1)Q$.

Définition 73.

Un polynôme est dit **scindé** dans $\mathbb{K}[X]$ (ou « sur $\mathbb{K}$ ») s'il s'écrit comme produit polynômes de degré 1 à coefficients dans $\mathbb{K}$.

Exemple. Pour tout $n \in \mathbb{N}^*$, $X^n - 1$ est scindé sur $\mathbb{C}$: $X^n - 1 = \prod_{k=0}^{n-1} \left(X - e^{\frac{2ik\pi}{n}}\right)$.

Corollaire 74 (Condition suffisante pour que le polynôme soit scindé)**.**

Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n \in \mathbb{N}^*$.
Si P possède n racines deux à deux distinctes $\alpha_1, \dots, \alpha_n$ dans $\mathbb{K}$, alors il est scindé sur $\mathbb{K}$.

$$\exists \lambda \in \mathbb{K}^* \quad P = \lambda \prod_{k=1}^{n} (X - \alpha_k), \quad (\lambda \text{ est le coefficient dominant de } P).$$

Exemple 75 (Factorisation des polynômes de Tchebychev)**.**

Reprenons la suite $(T_n)_{n\in\mathbb{N}}$ définie par $T_0 = 1$, $T_1 = X$ et $\forall n \in \mathbb{N} \;\; T_{n+2} = 2XT_{n+1} - T_n$.
Fixons $n \in \mathbb{N}^*$. On a prouvé que T_n est de degré n, de coefficient dominant 2^{n-1} et on a prouvé que pour tout θ réel , $T_n(\cos\theta) = \cos(n\theta)$. Démontrer que

$$T_n = 2^{n-1} \prod_{k=0}^{n-1} \left(X - \cos\left(\frac{(2k+1)\pi}{2n}\right)\right).$$

3.2 Racines et rigidité des polynômes.

Théorème 76.

Le nombre de racines distinctes d'un polynôme non nul est majoré par son degré.

Corollaire 77 (Montrer qu'un polynôme est nul en prouvant qu'il a trop de racines)**.**

Soient $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$.

1. Si $P \in \mathbb{K}_n[X]$ et P admet au moins $n+1$ racines deux à deux distinctes, alors $P = 0$.
2. Si P admet une infinité de racines alors $P = 0$.

Corollaire 78 (Montrer que $P = Q$ en prouvant que $P - Q$ a "trop" de racines)**.**

Si P et Q sont de degré inférieur à n et que $P - Q$ possède $n+1$ racines, alors $P = Q$.
Notamment, si P et Q coïncident sur une infinité de valeurs de $\mathbb{K}$, P et Q sont le même polynôme.
En particulier, lorsque les fonctions polynomiales associées à P et Q sont égales, alors $P = Q$.

Exemple 79.

1. Trouver tous les polynômes P de $\mathbb{R}[X]$ tels que $\forall n \in \mathbb{N} \quad P(n) = n^{666}$.
2. Soit $n \in \mathbb{N}^*$. Prouver l'unicité du polynôme $T_n \in \mathbb{R}[X]$ tel que $\forall \theta \in \mathbb{R}\ T_n(\cos\theta) = \cos(n\theta)$.

3.3 Multiplicité d'une racine.

Définition 80.

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$ une racine de P. On dit que la racine α est de **multiplicité** $m \in \mathbb{N}^*$ si

$$(X-\alpha)^m \text{ divise } P \quad \text{ et } \quad (X-\alpha)^{m+1} \text{ ne divise pas } P.$$

On dira que α est de multiplicité **au moins** égale à $k \in \mathbb{N}$ si $(X-\alpha)^k$ divise P.
Une racine de multiplicité 1 est dite **simple**. Une racine qui n'est pas simple est dite **multiple**.

Proposition 81.

Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. Il y a équivalence entre les deux assertions suivantes.

1. α est racine de P de multiplicité m.
2. $\exists Q \in \mathbb{K}[X] \quad P = (X-\alpha)^m Q \;$ et $\; Q(\alpha) \neq 0$.

Le polynôme $(X+1)X^2(X-5)^3$ a pour racines -1 (racine simple), 0 (racine double) et 5 (multiplicité 3).

Lemme 82.

Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $k \in \mathbb{N}^*$. Si $(X-\alpha)^k$ divise P, alors $(X-\alpha)^{k-1}$ divise P'.

Théorème 83 (Caractérisation de la multiplicité)**.**

Soit $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. On a (1) $\iff$ (2), ainsi que (3) $\iff$ (4).

1. α est une racine de P de multiplicité au moins m.
2. $P(\alpha) = P'(\alpha) = P''(\alpha) = \ldots = P^{(m-1)}(\alpha) = 0$.

3. α est une racine de P de multiplicité m.
4. $P(\alpha) = P'(\alpha) = P''(\alpha) = \ldots = P^{(m-1)}(\alpha) = 0 \quad \text{et} \quad P^{(m)}(\alpha) \neq 0$.

Exemple 84.

En nous appuyant sur une racine multiple "facile", factorisons $P = X^4 + X^3 - 7X^2 - 13X - 6$.

Corollaire 85 (Caractérisation des racines simples)**.**

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$.

$$\alpha \text{ est une racine simple de } P \quad \text{si et seulement si} \quad P(\alpha) = 0 \text{ et } P'(\alpha) \neq 0.$$

Proposition 86.

Soit $P \in \mathbb{K}[X]$ et $\alpha_1, \ldots, \alpha_p$, p racines de P distinctes deux à deux, de multiplicités respectives au moins égales à $k_1, \ldots, k_p$. Alors, $\prod_{i=1}^{p} (X - \alpha_i)^{k_i}$ divise P.

Exemple 87.

On peut compter les racines d'un polynôme
- en considérant les racines deux à deux distinctes,
- ou bien *avec leur multiplicité*, en répétant m fois une racine dans la liste lorsque sa multiplicité vaut m.

Par exemple, le polynôme $(X+1)X^2(X-5)^3$ possède
- trois racines distinctes : $-1, 0$ et 5,
- six racines comptées avec leur multiplicité : $-1, 0, 0, 5, 5, 5$.

Corollaire 88.

Soient $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$.

1. Si P est non nul, alors le nombre de ses racines dans $\mathbb{K}$, comptées avec multiplicité, est majoré par son degré.
2. Si $P \in \mathbb{K}_n[X]$ et P admet au moins $n+1$ racines comptées avec leur multiplicité, alors P est le polynôme nul.

Corollaire 89 (Cas d'un degré égal au nombre de racines, comptées avec leur multiplicité)**.**

Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n \in \mathbb{N}^*$.
Si P possède p racines $\alpha_1, \dots, \alpha_p$ dans $\mathbb{K}$, de multiplicités $m_1, \dots, m_p$, et si $m_1 + \cdots + m_p = n$, alors P est scindé sur $\mathbb{K}$. Plus précisément, il existe $\lambda \in \mathbb{K}^*$ tel que

$$P = \lambda \prod_{k=1}^{p} (X - \alpha_k)^{m_k}, \quad (\lambda \text{ étant le coefficient dominant de } P).$$

3.4 Existence de racines : théorème de d'Alembert-Gauss.

Théorème 90 (de d'Alembert-Gauss, ou théorème fondamental de l'algèbre)**.**

Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine dans $\mathbb{C}$.

Proposition 91.

Deux polynômes de $\mathbb{C}[X]$ sont premiers entre eux si et seulement si ils n'ont pas de racine commune.

Exemple 92.

Soit $P \in \mathbb{C}[X] \setminus \mathbb{C}_0[X]$. Montrer que $\widetilde{P} : z \mapsto P(z)$, application de $\mathbb{C}$ vers $\mathbb{C}$ est surjective.

Proposition 93 (une racine réelle)**.**

Un polynôme de $\mathbb{R}[X]$ de <u>degré impair</u> possède au moins une racine réelle.

Exemple 94 (Recherche d'une racine rationnelle)**.**

1. Soit $P = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$.
   Montrer que si $\frac{p}{q}$ est racine de P avec $p \wedge q = 1$, alors p divise a_0 et q divise a_n.
2. Factoriser $X^3 + 2X^2 - 4X - 3$ dans $\mathbb{R}[X]$.

3.5 Décomposition en facteurs irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$.

Définition 95.

Soit $P \in \mathbb{K}[X]$ un polynôme non constant. Il est dit **irréductible** dans $\mathbb{K}[X]$ si ses seuls diviseurs dans $\mathbb{K}[X]$ sont les polynômes constants (non nuls) et les polynômes associés à P, c'est-à-dire ceux de la forme λP, $\lambda \in \mathbb{K}^*$.

Proposition 96.

Un polynôme non constant P est irréductible ssi tous ses diviseurs sont de degré 0 ou $\deg(P)$.

Les polynômes irréductibles sont à $\mathbb{K}[X]$ ce que les entiers premiers sont à $\mathbb{N}$ (ou $\mathbb{Z}$).

Proposition 97.

Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1 à coefficients dans $\mathbb{C}$.

Proposition 98 (Factorisation en produit d'irréductibles à coeff. dans $\mathbb{C}$)**.**

Tout polynôme non constant de $\mathbb{C}[X]$ est scindé dans $\mathbb{C}[X]$.

Plus précisément, pour tout $P \in \mathbb{C}[X] \setminus \mathbb{C}_0[X]$, il existe $\lambda \in \mathbb{C}^*$, $p \in \mathbb{N}^*$, $\alpha_1, \dots \alpha_p \in \mathbb{C}$, deux à deux distincts et $m_1, \dots m_p \in \mathbb{N}^*$ tels que

$$P = \lambda \prod_{k=1}^{p} (X - \alpha_k)^{m_k}.$$

En particulier, le nombre de racines de P comptées avec multiplicité est égale au degré de P :

$$\sum_{k=1}^{p} m_k = \deg(P).$$

Lemme 99.

Soit $P \in \mathbb{R}[X]$, $\alpha \in \mathbb{C} \setminus \mathbb{R}$ et $m \in \mathbb{N}^*$. Si α est racine de P alors $\overline{\alpha}$ l'est aussi et

$$B_\alpha = (X - \alpha)(X - \overline{\alpha}) = (X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2)$$

divise P <u>dans $\mathbb{R}[X]$</u>.

Si α a pour multiplicité m, alors $\overline{\alpha}$ aussi et B_α^m divise P dans $\mathbb{R}[X]$.

Proposition 100.

Les polynômes irréductibles de $\mathbb{R}[X]$ sont
- les polynômes de degré 1,
- les polynômes de degré 2, n'ayant pas de racines réelles.

Proposition 101 (Factorisation en produit d'irréductibles à coeff. dans $\mathbb{R}$)**.**

Tout polynôme non constant de $\mathbb{R}[X]$ s'écrit comme produit de polynômes irréductibles de $\mathbb{R}[X]$.

Plus précisément, si $P \in \mathbb{R}[X] \setminus \mathbb{R}_0[X]$, il existe $\lambda \in \mathbb{R}^*$, $p \in \mathbb{N}$, $\alpha_1, \dots \alpha_p \in \mathbb{R}$ deux à deux distincts, et $m_1, \dots m_p \in \mathbb{N}^*$, et il existe $p' \in \mathbb{N}$, $(\beta_1, \gamma_1), \dots, (\beta_{p'}, \gamma_{p'}) \in \mathbb{R}^2$, $v_1, \dots v_{p'} \in \mathbb{N}^*$ tels que

$$P = \lambda \prod_{k=1}^{p} (X - \alpha_k)^{m_k} \prod_{k=1}^{p'} \left(X^2 + \beta_k X + \gamma_k\right)^{v_k} \quad \text{avec} \quad \forall k \in [\![1, p']\!] \;\; \beta_k^2 - 4\gamma_k < 0.$$

Méthode (Factorisation d'un polynôme en produit d'irréductibles)**.**

- On repère le degré de P : il majore le nombre de racines. Il est même égal au nombre de racines comptées avec multiplicité dans $\mathbb{C}$.
- On repère le coefficient dominant : il figure dans la factorisation.
- On cherche les racines complexes de P en posant l'équation $P(z) = 0$ avec $z \in \mathbb{C}$, ainsi que la multiplicité de ces racines. On obtient une factorisation dans $\mathbb{C}[X]$ (cf P98).
- Les racines réelles donnent des facteurs de degré 1. Les racines non réelles sont "couplées" avec leur conjuguées pour obtenir des polynômes de degré 2 sans racines réelles, comme dans le lemme 99. On obtient une factorisation dans $\mathbb{R}[X]$ (du type de celle de la proposition 101)

Exemple 102.

Factorisation de $X^6 - 1$ en produit d'irréductibles de $\mathbb{R}[X]$.

Quelques exemples de factorisation (dans $\mathbb{C}[X]$ puis $\mathbb{R}[X]$), laissées en exercice.

$$\begin{aligned} X^6 + 1 &= \left(X - e^{i\frac{\pi}{6}}\right)(X - i)\left(X - e^{5i\frac{\pi}{4}}\right)\left(X - e^{-5i\frac{\pi}{4}}\right)(X + i)\left(X - e^{-i\frac{\pi}{6}}\right) \\ &= \left(X^2 - \sqrt{3}X + 1\right)\left(X^2 + 1\right)\left(X^2 + \sqrt{3}X + 1\right). \end{aligned}$$

$$\begin{aligned} X^8 - 1 &= (X-1)(X+1)(X - e^{\frac{ik\pi}{4}})(X - e^{-\frac{ik\pi}{4}})(X - i)(X + i)(X - e^{\frac{3ik\pi}{4}})(X - e^{-\frac{3ik\pi}{4}}) \\ &= (X-1)(X+1)(X^2 - \sqrt{2}X + 1)(X^2 + 1)(X^2 + \sqrt{2}X + 1). \end{aligned}$$

4 Compléments.

4.1 Relations coefficients-racines pour un polynôme scindé.

Définition 103.

Soient $x_1, \dots, x_n \in \mathbb{K}$. On appelle **fonctions symétriques élémentaires** de $x_1, \dots, x_n$ les nombres définis par

$$\forall k \in [\![1, n]\!] \qquad \sigma_k = \sum_{A \in \mathcal{P}_k([\![1,n]\!])} \prod_{i \in A} x_i = \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

On a notamment

$$\sigma_1 = \sum_{i=1}^{n} x_i, \qquad \sigma_n = \prod_{i=1}^{n} x_i, \qquad \sigma_2 = \sum_{i<j} x_i x_j.$$

Remarque. Dans le cas $n = 2$, il y a deux fonctions symétriques élémentaires de x_1, x_2 :

$$\sigma_1 = x_1 + x_2 \qquad \sigma_2 = x_1 x_2.$$

Dans le cas $n = 3$, il y a trois fonctions symétriques élémentaires de x_1, x_2, x_3 :

$$\sigma_1 = x_1 + x_2 + x_3, \qquad \sigma_2 = x_1 x_2 + x_1 x_3 + x_2 x_3, \qquad \sigma_3 = x_1 x_2 x_3.$$

Exemple 104.

Soient x, y, z trois scalaires de $\mathbb{K}$ et $\sigma_1, \sigma_2, \sigma_3$ les fonctions symétriques élémentaires associées. Démontrer que

$$\begin{array}{rcl} x^2 + y^2 + z^2 & = & \sigma_1^2 - 2\sigma_2 \\ x^3 + y^3 + z^3 & = & \sigma_1^3 + 3\sigma_3 - 3\sigma_1\sigma_2 \end{array}.$$

Théorème 105 (Relations coefficients-racines : formules de Viète)**.**

Soit P un polynôme de degré $n \in \mathbb{N}^*$, scindé sur $\mathbb{K}$: il s'écrit donc

$$P = \sum_{k=0}^{n} a_k X^k \quad \text{et} \quad P = a_n \prod_{k=1}^{n} (X - \alpha_k),$$

où $a_0, \dots, a_n$ sont ses coefficients et $\alpha_1, \dots, \alpha_n$ ses racines, répétées avec leur multiplicité. On a

$$\boxed{P = a_n \left(X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \ldots + (-1)^k \sigma_k X^{n-k} + \cdots + (-1)^n \sigma_n \right)},$$

avec $\sigma_1, \dots, \sigma_n$ les fonctions symétriques élémentaires des racines $\alpha_1, \dots, \alpha_n$.

Ces nombres s'expriment donc en fonction des coefficients de P :

$$\boxed{\forall k \in [\![1, n]\!] \quad \sigma_k = (-1)^k \frac{a_{n-k}}{a_n}.}$$

Corollaire 106 (Somme et produit des racines d'un polynôme scindé)**.**

Soit $P = \sum a_k X^k$ un polynôme de degré $n \in \mathbb{N}^*$, scindé sur $\mathbb{K}$.
La somme des racines σ_1 et le produit des racines σ_n valent

$$\sigma_1 = -\frac{a_{n-1}}{a_n} \quad \text{et} \quad \sigma_n = (-1)^n \frac{a_0}{a_n}.$$

Remarque. Soit $aX^2 + bX + c$ un polynôme de degré 2 et α_1 et α_2 ses deux racines complexes. On retrouve

$$\alpha_1 + \alpha_2 = -\frac{b}{a} \quad \text{et} \quad \alpha_1 \alpha_2 = \frac{c}{a}.$$

Preuve du théorème. Avant de développer $a_n(X - \alpha_1) \cdots (X - \alpha_n)$, on pourra commencer par examiner le cas $n = 3$ pour un polynôme unitaire :

$$P = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3) = X^3 - \underbrace{(\alpha_1+\alpha_2+\alpha_3)}_{=\sigma_1} X^2 \; + \; \underbrace{(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)}_{=\sigma_2} X \; - \; \underbrace{\alpha_1\alpha_2\alpha_3}_{=\sigma_3}.$$

□

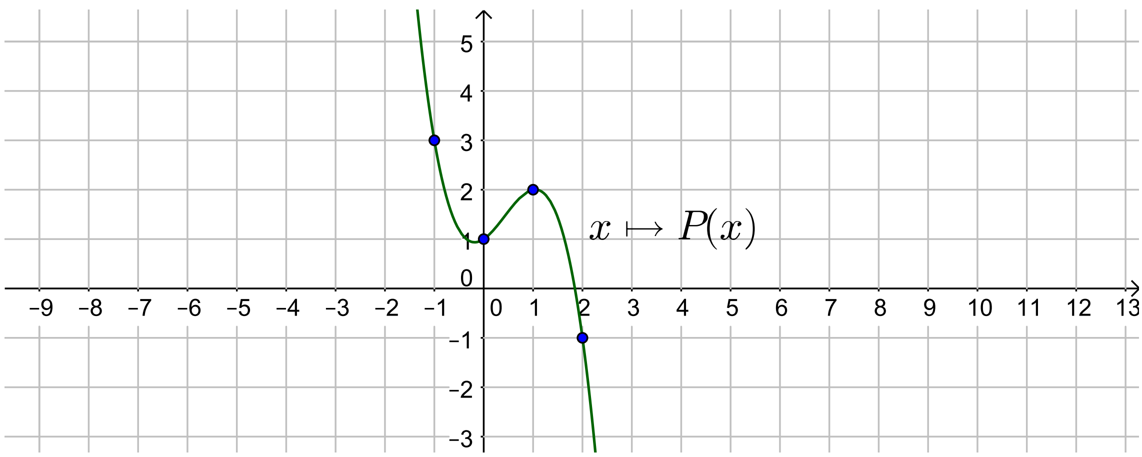
Exemple 107.

Trouver tous les triplets $(x, y, z) \in \mathbb{R}^3$ tels que

$$\begin{array}{rcl} x + \ y + \ z & = & 2 \\ x^2 + y^2 + z^2 & = & 14 \\ x^3 + y^3 + z^3 & = & 20 \end{array}.$$

4.2 Interpolation de Lagrange.

Interpoler, c'est proposer une fonction qui passe par un ensemble de points donnés. Ici, on a donné l'unique polynôme P de degré inférieur à 3 passant par les quatre points $(-1, 3)$, $(0, 1)$, $(1, 2)$ et $(2, -1)$.



Polynôme interpolateur.

Définition 108.

Soit $n \in \mathbb{N}^*$ et $(x_1, \dots, x_n) \in \mathbb{K}^n$, où les x_i sont deux à deux distincts. On pose

$$\forall i \in [\![1, n]\!] \quad L_i = \frac{\prod\limits_{\substack{k=1 \\ k \neq i}}^{n} (X - x_k)}{\prod\limits_{\substack{k=1 \\ k \neq i}}^{n} (x_i - x_k)}.$$

Les polynômes $(L_1, \dots, L_n)$ sont appelés **polynômes de Lagrange** associés à $(x_1, \dots, x_n)$.

Exemple 109 (Comprendre la définition avec un exemple)**.**

Écrire la famille des quatre polynômes de Lagrange associés à $(x_1, x_2, x_3, x_4) = (-1, 0, 1, 2)$.

Proposition 110.

Soit $n \in \mathbb{N}^*$ et $(L_1, \dots, L_n)$ la famille de polynômes de Lagrange associés à un n-uplet $(x_1, \dots, x_n)$ de scalaires deux à deux distincts. Tous les polynômes L_i sont de degré $n - 1$ et

$$\forall (i, j) \in [\![1, n]\!]^2 \quad L_i(x_j) = \delta_{i,j}.$$

Théorème 111 (Interpolation de Lagrange)**.**

Soit $n \in \mathbb{N}^*$, $(x_1, \dots, x_n) \in \mathbb{K}^n$ (scalaires deux à deux distincts) et $(y_1, \dots, y_n) \in \mathbb{K}^n$.

$$\exists! P \in \mathbb{K}_{n-1}[X] \quad \forall i \in [\![1, n]\!] \quad P(x_i) = y_i.$$

En notant $(L_1, \dots, L_n)$ la famille de polynômes de Lagrange associés à $(x_1, \dots, x_n)$, on a

$$P = \sum_{i=1}^{n} y_i L_i.$$

Corollaire 112 (L'ensemble des polynômes interpolateurs)**.**

Soit $n \in \mathbb{N}^*$, $(x_1, \dots, x_n) \in \mathbb{K}^n$ (scalaires deux à deux distincts) et $(y_1, \dots, y_n) \in \mathbb{K}^n$.
Soit P l'unique polynôme de $\mathbb{K}_{n-1}[X]$ tel que $\forall i \in [\![1, n]\!]$ $P(x_i) = y_i$.

Les polynômes $Q \in \mathbb{K}[X]$ tels que $\forall i \in [\![1, n]\!]$ $Q(x_i) = y_i$ sont ceux de la forme

$$Q = P + A \cdot \prod_{i=1}^{n} (X - x_i), \quad \text{où } A \in \mathbb{K}[X].$$

Preuves

Preuve du théorème 14.

Pour ne pas avoir à introduire des coefficients pour chaque polynôme ci-dessous, on convient de noter $[A]_k$, pour $k \in \mathbb{N}$ le coefficient d'ordre k d'un polynôme A. Dans toute la suite, k est un entier naturel fixé.

On se donne pour les calculs ci-dessous P, Q, R trois polynômes de $\mathbb{K}[X]$.

1) $(\mathbb{K}[X], +)$ est un groupe abélien, de neutre le polynôme nul.
Il est assez facile de vérifier, en effet, qu'il s'agit d'un sous-groupe de $(\mathbb{K}^{\mathbb{N}}, +)$, groupe abélien connu.

2) La loi $\times$ est une loi de composition interne sur $\mathbb{K}[X]$, cela a été établi par la proposition 11.

3) La loi $\times$ est commutative.

$$[PQ]_k = \sum_{i=0}^{k} [P]_i [Q]_{k-i} \underset{j=k-i}{=} \sum_{j=0}^{k} [P]_{k-j} [Q]_j = \sum_{i=0}^{k} [Q]_i [P]_{k-i} = [QP]_k.$$

4) Le polynôme $1 (= 1_{\mathbb{K}[X]})$ est neutre pour le produit.
Rappelons la définition du *symbole de Kronecker*, défini pour i et j entiers par

$$\delta_{i,j} = \begin{cases} 1 & \text{si} \quad i = j \\ 0 & \text{si} \quad i \neq j \end{cases}$$

Le polynôme constant égal à 1 a tous ses coefficients nuls saufs celui d'ordre 0 qui vaut 1. Pour tout $i \in \mathbb{N}$, on a donc

$$[1_{\mathbb{K}[X]}]_i = \delta_{i,0}.$$

On calcule alors

$$[1_{\mathbb{K}[X]} \cdot P]_k \underset{3)}{=} [P \cdot 1_{\mathbb{K}[X]}]_k = \sum_{i=0}^{k} [P]_i \cdot [1_{\mathbb{K}[X]}]_{k-i} = \sum_{i=0}^{k} [P]_i \cdot \delta_{0,k-i} = 0 + [P]_k \cdot 1 = [P]_k.$$

5) Associativité. En écrivant de deux façons une somme triangulaire

$$\begin{aligned} [(PQ)R)]_k = \sum_{i=0}^{k} [PQ]_i [R]_{k-i} &= \sum_{i=0}^{k} \left(\sum_{j=0}^{i} [P]_j [Q]_{i-j} \right) [R]_{k-i} \\ &= \sum_{j=0}^{k} [P]_j \left(\sum_{i=j}^{k} [Q]_{i-j} [R]_{k-i} \right) \\ &\underset{l=i-j}{=} \sum_{j=0}^{k} [P]_j \left(\sum_{l=0}^{k-j} [Q]_l [R]_{k-j-l} \right) \\ &= \sum_{j=0}^{k} [P]_j [QR]_{k-j} = [P(QR)]_k. \end{aligned}$$

6) Distributivité.

$$[P(Q+R)]_k = \sum_{i=0}^{k} [P]_i [Q+R]_{k-i} = \sum_{i=0}^{k} [P]_i \left([Q]_{k-i} + [R]_{k-i} \right) = \sum_{i=0}^{k} [P]_i [Q]_{k-i} + \sum_{i=0}^{k} [P]_i [R]_{k-i} = [PQ]_k + [PR]_k.$$

□

Preuve de la proposition 15
• Le polynôme X^0 est la suite $(1, 0, \ldots)$: c'est bien le polynôme 1, par définition.
• Soit $n \in \mathbb{N}$. Vérifions que $X^{n+1} = X \times X^n$. Par définition, X^n est la suite dont tous les termes sont nuls saufs celui au rang n qui vaut 1. Ceci s'écrit

$$\forall k \in \mathbb{N} \quad [X^n]_k = \delta_{k,n}.$$

Fixons k et calculons le coefficient d'ordre k pour $X \times X^n$:

$$[X \times X^n]_k = \sum_{i=0}^{k} [X]_i [X^n]_{k-i} = \sum_{i=0}^{k} \delta_{i,1}\delta_{k-i,n}.$$

Le terme $\delta_{i,1}\delta_{k-i,n}$ est nul sauf si $i = 1$ **et** $k - i = n$, c'est-à-dire si $k = n + 1$ **et** $i = 1$. Ainsi,

$$[X \times X^n]_k = \begin{cases} 0 & \text{si} \quad k \neq n+1 \\ \delta_{1,1}\delta_{n,n} = 1 & \text{si} \quad k = n+1 \end{cases}$$

On a bien $[X \times X^n]_k = \delta_{k,n+1} = [X^{n+1}]_k$, et ce pour tout k. On a bien vérifié que les polynômes $X \times X^n$ et X^{n+1} ont mêmes coefficients : ils sont égaux. □

Preuve de la proposition 32 Soient $P = \sum_{k \in \mathbb{N}} a_k X^k$ et $Q = \sum_{k \in \mathbb{N}} b_k X^k$ deux polynômes de $\mathbb{K}[X]$, et $\lambda, \mu \in \mathbb{K}$.

• La preuve de la première égalité est de routine. Fixons un entier naturel k et comparons les coefficients d'ordre k.

$$[(\lambda P + \mu Q)']_k = (k+1)[\lambda P + \mu Q]_{k+1} = (k+1)\left(\lambda a_{k+1} + \mu b_{k+1}\right) = \lambda [P']_{k+1} + \mu [Q']_{k+1} = [\lambda P' + \mu Q']_k.$$

• Pour la seconde égalité, on calcule le coefficient d'ordre k du membre de droite :

$$\begin{aligned}
[P'Q + PQ']_k &= [P'Q]_k + [PQ']_k \\
&= \sum_{i=0}^{k} [P']_i [Q]_{k-i} \; + \; \sum_{i=0}^{k} [P]_i [Q']_{k-i} \\
&= \sum_{i=0}^{k} (i+1) a_{i+1} b_{k-i} \; + \; \sum_{i=0}^{k} a_i (k - i + 1) b_{k-i+1} \\
&= \sum_{j=1}^{k+1} j a_j b_{k-j+1} + \sum_{j=0}^{k} a_j (k - j + 1) b_{k-j+1} \qquad \left\{ \begin{array}{ll} \text{première somme :} & j = i+1 \\ \text{seconde somme :} & i = j \end{array} \right. \\
&= (k+1) a_{k+1} b_0 + \sum_{j=1}^{k} (\cancel{j} + k - \cancel{j} + 1) a_j b_{k-j+1} + (k+1) a_0 b_{k+1} \\
&= (k+1) \sum_{j=0}^{k+1} a_j b_{k+1-j} = (k+1)[(PQ)]_{k+1} = [(PQ)']_k.
\end{aligned}$$

• L'identité $(P^n)' = nP'P^{n-1}$ est vraie pour $n = 0$. Supposons qu'elle le soit pour un entier naturel n donné. Alors, en utilisant la formule pour la dérivée d'un produit, on montre l'identité au rang $n + 1$:

$$\left(P^{n+1}\right)' = (P \cdot P^n)' = P'P^n + P\,(P^n)' = P'P^n + P\left(nP'P^{n-1}\right) = (n+1)P'P^n,$$

• Notons $P = \sum_{k=0}^{n} a_k X^k$, où $n \geq \deg(P)$. On a

$$(P \circ Q)' = \left(\sum_{k=0}^{n} a_k Q^k \right)' = \sum_{k=0}^{n} a_k \left(Q^k\right)' = \sum_{k=0}^{n} a_k k Q' Q^{k-1} = Q' \sum_{k=0}^{n} k a_k Q^{k-1} = Q' \cdot P' \circ Q.$$

□

Preuve du théorème 42.
• $\boxed{\text{Unicité}}$. Preuve en classe.

• $\boxed{\text{Existence}}$. On va raisonner par récurrence sur le degré du polynôme à diviser.
Pour cela, fixons pour toute la preuve un polynôme B non nul, et notons p son degré qui est donc un entier naturel.

Pour $n \in \mathbb{N}$, on note

$\mathcal{P}(n)$ « Pour tout polynôme A de $\mathbb{K}_n[X]$ il existe un couple de polynômes (Q, R) tel que $A = BQ + R$ et $\deg(R) < \deg(B)$. »

⋆ <u>Initialisation</u>. Soit A un polynôme de $\mathbb{K}_0[X]$, c'est-à-dire un polynôme constant. On peut écrire $A = a_0 \cdot 1$. Deux cas se présentent. Si B est constant, alors on peut écrire $B = b_0 \cdot 1$, avec $b_0 \neq 0$ puisque B n'est pas nul. On écrit alors
$$a_0 \cdot 1 = \frac{a_0}{b_0} 1 \cdot b_0 1 + 0_{\mathbb{K}[X]}.$$
Cette division convient puisque le degré du reste $(-\infty)$ est strictement inférieur au degré de B (nul). Si B n'est pas constant, alors écrivons
$$A = B \cdot 0_{\mathbb{K}[X]} + A.$$
De plus le degré du reste vaut $\deg(A) = 0 < \deg(B)$ (puisque B est non constant dans ce cas).

⋆ <u>Hérédité</u>. Soit $n \in \mathbb{N}$. Supposons $\mathcal{P}(n)$. Pour démontrer $\mathcal{P}(n+1)$ prenons A dans $\mathbb{K}_{n+1}[X]$. Si A est de degré inférieur à n, $\mathcal{P}(n)$ s'applique et nous donne l'existence d'un couple quotient reste comme il faut. Supposons dorénavant que A est de degré $n+1$.

♢ Si le degré de B, noté p, satisfait $p > n+1$, alors il suffit de poser
$$A = B \cdot 0_{\mathbb{K}[X]} + A.$$
Le reste vaut A et on a bien $\deg(A) = n + 1 < p = \deg(B)$.

♢ Si $p \leq n+1$.
On peut écrire A et B sous la forme
$$\begin{array}{rcll} A = & a_{n+1}X^{n+1} & +\widetilde{A} & \text{avec } a_{n+1} \neq 0 \quad \text{et} \quad \deg(\widetilde{A}) \leq n. \\ B = & b_pX^p & +\widetilde{B} & \text{avec } b_p \neq 0 \quad \text{et} \quad \deg(\widetilde{B}) \leq p-1. \end{array}$$
On "commence" alors une division par B en s'occupant d'abord du terme de plus haut degré de A :
$$\begin{aligned} A &= \left(b_pX^p + \widetilde{B}\right) \cdot \frac{a_{n+1}}{b_p} X^{n+1-p} - \frac{a_{n+1}}{b_p} X^{n+1-p} \widetilde{B} + \widetilde{A} \\ &= B \cdot \frac{a_{n+1}}{b_p} X^{n+1-p} + C, \end{aligned}$$
où $C = \widetilde{A} - \frac{a_{n+1}}{b_p} X^{n+1-p} \widetilde{B}$. Le polynôme C est un polynôme de $\mathbb{K}_n[X]$, comme démontré par le calcul suivant :
$$\begin{aligned} \deg(C) \leq \max \left[\underbrace{\deg(\widetilde{A})}_{\leq n}, \deg\left(\frac{a_{n+1}}{b_p} X^{n+1-p} \widetilde{B}\right)\right] &\leq \max \left(n, (n+1-p) + \underbrace{\deg(\widetilde{B})}_{\leq p-1} \right) \\ &\leq \max(n, n) = n. \end{aligned}$$
D'après $\mathcal{P}(n)$, il existe deux polynômes ($\widetilde{Q}$ et $\widetilde{R}$) tels que $C = B\widetilde{Q} + \widetilde{R}$ avec $\deg(\widetilde{R}) < \deg(B)$. Réinjectons dans la division de A par B commencée plus haut :
$$A = B \cdot \frac{a_{n+1}}{b_p} X^{n+1-p} + B\widetilde{Q} + \widetilde{R} = B\left(\frac{a_{n+1}}{b_p} X^{n+1-p} + \widetilde{Q}\right) + \widetilde{R}.$$
On a bien ici une écriture du type $A = BQ + R$ avec $\deg(R) < \deg(B)$: $\mathcal{P}(n+1)$ est démontrée.

⋆ <u>Conclusion.</u> D'après le principe de récurrence, l'existence du couple quotient-reste est établie lorsque $A \in \mathbb{K}_n[X]$ et ce pour tout $n \in \mathbb{N}$. Puisque $\mathbb{K}[X] = \bigcup_{n=0}^{+\infty} \mathbb{K}_n[X]$, l'existence est établie pour tout polynôme A.

□

Exercices

Polynômes à travers leurs coefficients/ L'anneau $\mathbb{K}[X]$.

$\boxed{\textbf{25.1}}$ **[♦♦◇]** (1er TD : admettre la question 2)
On note $I =]-\frac{\pi}{2}, \frac{\pi}{2}[$.

1. Montrer que pour tout $n \in \mathbb{N}$, il existe un polynôme $P_n \in \mathbb{R}[X]$ tel que
$$\forall x \in I \quad \tan^{(n)}(x) = P_n(\tan(x)).$$
2. Montrer qu'un tel polynôme P_n est unique.
3. Donner pour tout entier n le degré et le coefficient dominant de P_n.
4. Démontrer que pour tout entier naturel n, les coefficients de P_n sont des entiers.

$\boxed{\textbf{25.2}}$ **[♦◇◇]** En calculant de deux façons différentes le coefficient devant X^n dans l'écriture développée de $(1-X^2)^n$, obtenir une identité sur les coefficients binomiaux.

$\boxed{\textbf{25.3}}$ **[♦♦◇]** Trouver tous les polynômes P de $\mathbb{R}[X]$ tels que $4P = (P')^2$.

$\boxed{\textbf{25.4}}$ **[♦♦◇]** Trouver tous les polynômes P dans $\mathbb{R}[X]$ qui satisfont
$$P(X+1) = XP'.$$

$\boxed{\textbf{25.5}}$ **[♦♦♦]** Soit Q un polynôme de $\mathbb{K}[X]$.
Démontrer que l'équation $P - P' = Q$ possède une unique solution dans $\mathbb{K}[X]$.

Racines et factorisation d'un polynôme.

$\boxed{\textbf{25.6}}$ **[♦♦◇]** Approximation de π par $\frac{22}{7}$.

1. Poser la division euclidienne de $X^4(1-X)^4$ par $1+X^2$.
2. Démontrer l'égalité $\int_0^1 \frac{x^4(1-x)^4}{1+x^2}\mathrm{d}x = \frac{22}{7} - \pi$.
3. Prouver l'inégalité $\frac{1}{1260} \leq \frac{22}{7} - \pi \leq \frac{1}{630}$.

$\boxed{\textbf{25.7}}$ **[♦♦◇]** Donner le reste dans la division euclidienne de $X^{2025} + X^3 + 1$ par
a) $X^2 - 1$, b) $(X-1)^2$.

$\boxed{\textbf{25.8}}$ **[♦♦◇]** Soient $(A, B, P) \in (\mathbb{K}[X])^3$ tels que P est non constant et $A \circ P | B \circ P$. Montrer que $A|B$.

$\boxed{\textbf{25.9}}$ **[♦♦◇]** Trouver tous les polynômes de $\mathbb{R}[X]$ tels que $(X+4)P(X) = XP(X+1)$.

$\boxed{\textbf{25.10}}$ **[♦◇◇]** Démontrer qu'il n'existe pas de polynôme P dans $\mathbb{R}[X]$ tel que
$$\forall n \in \mathbb{N} \quad P(n) = n^{666} + (-1)^n.$$

$\boxed{\textbf{25.11}}$ **[♦◇◇]** Soit $n \in \mathbb{N}^*$. Montrer que $(X-1)^3$ divise $P_n = nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$.

$\boxed{\textbf{25.12}}$ **[♦◇◇]** Montrer que, pour tout $n \in \mathbb{N}^*$, le polynôme $P = \sum_{k=0}^{n} \frac{X^k}{k!}$ n'a que des racines simples dans $\mathbb{C}$.

Arithmétique dans $\mathbb{K}[X]$

$\boxed{25.13}$ **[♦♦◊]** Soient p et q deux entiers naturels non nuls et r le reste dans la division euclidienne de p par q.

1. Montrer que $X^r - 1$ est le reste dans la division euclidienne de $X^p - 1$ par $X^q - 1$.
2. En déduire que $(X^p - 1) \wedge (X^q - 1) = X^{p\wedge q} - 1$.

$\boxed{25.14}$ **[♦♦♦]** Pour $n \in \mathbb{N}^*$, on pose $P_n = (X+1)^{n+1} - X^{n+1} - 1$. Donner une condition nécessaire et suffisante sur n pour que P_n et P_n' soient premiers entre eux.
Calculer leur PGCD quand ce n'est pas le cas.

Factorisation de polynômes

$\boxed{25.15}$ **[♦♦◊]** Factoriser $X^6 + X^3 + 1$ en produit d'irréductibles de $\mathbb{R}[X]$.

$\boxed{25.16}$ **[♦♦♦]** Soit $n \geq 2$. Factoriser $(X+i)^n - (X-i)^n$ en produit d'irréductibles de $\mathbb{C}[X]$.

$\boxed{25.17}$ **[♦♦♦]** Soit $n \in \mathbb{N}^*$. Factoriser $\sum_{k=0}^{n-1} X^k$ dans $\mathbb{C}[X]$. En déduire $\prod_{k=1}^{n-1} \sin\left(\frac{k\pi}{n}\right) = \frac{n}{2^{n-1}}$.

$\boxed{25.18}$ **[♦♦♦]** Soit $n \in \mathbb{N}^*$. Factoriser en produit d'irréductibles de $\mathbb{R}[X]$ le polynôme

$$\sum_{k=0}^{2n} X^k.$$

Divers

$\boxed{25.19}$ **[♦◊◊]** Soit P un polynôme de $\mathbb{R}[X]$ de degré $n \geq 2$ scindé dans $\mathbb{R}[X]$ à racines simples.

1. Montrer que P' est scindé à racines simples.
2. Prouver que la moyenne arithmétique des racines de P et celle des racines de P' sont égales.

$\boxed{25.20}$ **[♦♦◊]** Démontrer qu'il existe un nombre fini de polynômes unitaires de $\mathbb{Z}[X]$ ayant un degré égal à n et des racines complexes de module inférieur à 1.

$\boxed{25.21}$ **[♦♦◊]** Soit $n \in \mathbb{N}^*$ et $P = nX^n - \sum_{k=0}^{n-1} X^k$.

1. Prouver que 1 est racine simple de P.
2. (*) En vous intéressant à $(X-1)P$, démontrer que toutes les racines complexes de P sont simples.
3. Donner la somme et le produit des racines.

$\boxed{25.22}$ **[♦♦♦]** Soit $n \in \mathbb{N}$.

1. Exprimer de deux façons différentes l'unique polynôme P de degré n tel que $\forall i \in [\![0, n]\!]\ P(i) = i^n$.
2. En considérant son coefficient dominant, démontrer l'identité

$$\sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^n = n!$$

Fractions rationnelles

1 Fractions rationnelles.

1.1 Le corps $\mathbb{K}(X)$.

L'énoncé suivant (admis) a été donné à la fin du cours Structures algébriques.

Pour tout anneau intègre A, il existe un unique corps (commutatif) K contenant A et vérifiant

$$\forall x \in K \quad \exists a \in A \; \exists b \in A \setminus \{0_A\} \; x = ab^{-1}.$$

Le corps K est appelé **corps des fractions** de l'anneau A.

Par exemple, le corps $\mathbb{Q}$ est le corps des fractions de l'anneau $\mathbb{Z}$.

Définition 1.

On note $\mathbb{K}(X)$ le corps des fractions de l'anneau $\mathbb{K}[X]$.
Ses éléments, appelés **fractions rationnelles** sont de la forme

$$F = AB^{-1} \quad \left(\text{soit en notation fractionnaire } F = \frac{A}{B}\right),$$

où A et B appartiennent à $\mathbb{K}[X]$ avec $B \neq 0$. Le couple (A, B) est appelé un **représentant** de F.

Remarque. Le théorème d'existence du corps des fractions dit que le corps $\mathbb{K}(X)$ *contient* l'anneau $\mathbb{K}[X]$.
Cela signifie que la somme et le produit sur $\mathbb{K}(X)$ prolongent la somme et le produit de $\mathbb{K}[X]$.
Autrement dit, $\mathbb{K}[X]$ est un sous-anneau de $\mathbb{K}(X)$.

Remarque. L'écriture B^{-1} désigne l'inverse de B dans le corps $\mathbb{K}(X)$. On verra que, sauf dans le cas où B est un polynôme constant non nul, B^{-1} n'est pas un polynôme.

Comme pour les polynômes, à la place de $F = \dfrac{A}{B}$, on pourra écrire $F(X) = \dfrac{A(X)}{B(X)}$.

Calculs dans $\mathbb{K}(X)$ Soient $A_1, B_1, A_2, B_2 \in \mathbb{K}(X)$ telles que $B_1 \neq 0$ et $B_2 \neq 0$.

1. Cas d'égalité
$$\frac{A_1}{B_1} = \frac{A_2}{B_2} \iff A_1B_2 = A_2B_1.$$

2. Produit et inverse.
$$\frac{A_1}{B_1} \cdot \frac{A_2}{B_2} = \frac{A_1A_2}{B_1B_2} \qquad \text{Si } A_1 \neq 0 \text{ alors } \left(\frac{A_1}{B_1}\right)^{-1} = \frac{B_1}{A_1}.$$

3. Somme
$$\frac{A_1}{B_1} + \frac{A_2}{B_2} = \frac{A_1B_2 + A_2B_1}{B_1B_2}.$$

Proposition 2.

Soit $F \in \mathbb{K}(X)$. Il existe un unique $(A, B) \in \mathbb{K}[X]^2$ tel que
$$B \text{ est unitaire (et non nul)}, \quad A \wedge B = 1 \quad \text{et} \quad F = \frac{A}{B}.$$
C'est la **forme irréductible** de la fraction F.

Si P est un polynôme, alors P est a fortiori une fraction rationnelle. Sa forme irréductible est $P = \frac{P}{1}$.

1.2 Fonction rationnelle associée, composée, dérivation.

Définition 3 (Fonction rationnelle associée à une fraction rationnelle)**.**

Soit $F \in \mathbb{K}(X)$ de forme irréductible $F = \frac{A}{B}$. On pose $D_F = \mathbb{K} \setminus \{\alpha \in \mathbb{K} \mid B(\alpha) = 0\}$.

On appelle **fonction rationnelle** associée à F l'application $\widetilde{F} : \left\{ \begin{array}{ccc} D_F & \to & \mathbb{K} \\ x & \mapsto & \frac{A(x)}{B(x)} \end{array} \right.$.

Il faudrait peut-être définir de manière formelle la composée de deux fractions rationnelles, ou encore sa dérivée. Pour alléger l'exposé, on se contentera d'exploiter les réflexes qu'on a sur les fonctions rationnelles.

Exemple 4.

Soit $F = \dfrac{X^4+1}{X^4+X^2+1}$. Montrer que $F(-X) = F(X)$ et $F\left(\frac{1}{X}\right) = F(X)$.

Exemple 5.

Soit P un polynôme de $\mathbb{K}[X]$, non nul, de degré d. Justifier que $X^dP(\frac{1}{X})$ est un polynôme. Pourquoi l'appelle-t-on parfois polynôme symétrique de P ?

1.3 Degré et partie entière d'une fraction rationnelle.

Définition-Proposition 6.

Soit $F = \dfrac{A}{B} \in \mathbb{K}(X)$. On définit le **degré** de F comme

$$\deg(F) = \deg(A) - \deg(B).$$

(ce nombre étant indépendant du représentant (A, B)). On a donc $\deg(F) \in \mathbb{Z} \cup \{-\infty\}$.

Remarque. Si $P \in \mathbb{K}[X]$, sa forme irréductible en tant que fraction rationnelle est $P = \dfrac{P}{1}$. Les degrés de P dans l'anneau $\mathbb{K}[X]$ et dans le corps $\mathbb{K}(X)$ sont donc égaux.

Proposition 7 (Degré et opérations)**.**

Soient $F, G \in \mathbb{K}(X)$.

1. $\deg(F + G) \leq \max(\deg(F), \deg(G))$ avec égalité si $\deg(F) \neq \deg(G)$;
2. $\forall \lambda \in \mathbb{K}\ \ \deg(\lambda F) \leq \deg(F)$, avec égalité si $\lambda \neq 0$;
3. $\deg(FG) = \deg(F) + \deg(G)$.
4. Si $G \neq 0$, $\deg\left(\dfrac{F}{G}\right) = \deg(F) - \deg(G)$.

Exemple 8.

$$\deg\left(\frac{X^4}{X^2+1}\right) = 4 - 2 = 2\,; \quad \deg\left(\frac{X-1}{X^3+1}\right) = 1 - 3 = -2\,; \quad \deg\left(\frac{X^2+1}{X^2-1}\right) = 2 - 2 = 0.$$

Proposition-Définition 9.

Soit $F = \frac{A}{B} \in \mathbb{K}(X)$. On note E le quotient dans la division euclidienne de A par B.

Il existe une unique fraction rationnelle $G \in \mathbb{K}(X)$ tels que

$$F = E + G \quad \text{et} \quad \deg(G) < 0.$$

Le polynôme E est appelé **partie entière** de F. Elle est nulle ssi $\deg(F) < 0$.

Exemple 10.

Soit $n \in \mathbb{N}^*$. Quelle est la partie entière de $\dfrac{X^n}{X-1}$?

1.4 Zéros et pôles d'une fraction rationnelle.

Définition 11.

Soit $F \in \mathbb{K}(X)$ de forme irréductible $F(X) = \frac{A(X)}{B(X)}$. Soient $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}$.

1. α est un **zéro** (de multiplicité m) de F si α est racine de A (de multiplicité m).
2. α est un **pôle** (de multiplicité m) de F si α est racine de B (de multiplicité m).

On parlera de **pôle simple** au sujet d'un pôle de multiplicité 1.

Exemple 12.

Déterminer les pôles de $\dfrac{1}{X^2+1}$ dans $\mathbb{R}$ et dans $\mathbb{C}$.

Exemple 13.

Justifier qu'une fraction rationnelle de $\mathbb{C}(X)$ sans pôle ne peut être qu'un polynôme.

Proposition 14.

Soit $F \in \mathbb{R}(X)$ et $\alpha \in \mathbb{C}$.
Alors α est pôle de F de multiplicité m si et seulement si $\overline{\alpha}$ est pôle de F de multiplicité m.

2 Décomposition en éléments simples.

2.1 Les deux théorèmes.

Théorème 15 (Décomposition en éléments simples dans $\mathbb{C}(X)$)**.**

Soit $F \in \mathbb{C}(X)$ que l'on écrit sous forme irréductible, le dénominateur étant décomposé en facteurs irréductibles :

$$F(X) = \frac{A(X)}{\displaystyle\prod_{k=1}^{r}(X-\alpha_k)^{m_k}}.$$

(les complexes α_k sont distincts deux à deux, les m_k sont des entiers naturels non nuls.) Alors il existe

- un unique polynôme $E \in \mathbb{C}[X]$ (la partie entière de F) ;
- une unique famille $(a_{k,j})_{\substack{1\le k\le r\\ 1\le j\le m_k}}$ de complexes

tels que

$$F(X) = E(X) + \sum_{k=1}^{r} \underbrace{\left(\sum_{j=1}^{m_k} \frac{a_{k,j}}{(X-\alpha_k)^j}\right)}_{\text{relatif à } (X-\alpha_k)^{m_k}}.$$

Théorème 16 (Décomposition en éléments simples dans $\mathbb{R}(X)$)**.**

Soit $F \in \mathbb{R}(X)$ que l'on écrit sous forme irréductible, le dénominateur étant décomposé en facteurs irréductibles :

$$F(X) = \frac{A(X)}{\displaystyle\prod_{k=1}^{r}(X-\alpha_k)^{m_k}\prod_{\ell=1}^{s}(X^2+p_\ell X+q_\ell)^{n_\ell}}.$$

(les réels α_k sont distincts deux à deux ; les irréductibles de degré 2 $X^2+p_\ell X+q_\ell$ sont distincts deux à deux, les m_k et les n_ℓ sont dans $\mathbb{N}^*$).
Alors il existe

— un unique polynôme $E \in \mathbb{R}[X]$ (la partie entière de F) ;
— une unique famille $(a_{k,j})_{\substack{1\leq k\leq r\\ 1\leq j\leq m_k}}$ de réels ;
— une unique famille $(b_{\ell,j}X+c_{\ell,j})_{\substack{1\leq \ell\leq s\\ 1\leq j\leq n_\ell}}$ de polynômes de $\mathbb{R}_1[X]$

tels que

$$F(X) = E(X) + \sum_{k=1}^{r}\underbrace{\left(\sum_{j=1}^{n_k}\frac{a_{k,j}}{(X-\alpha_k)^j}\right)}_{\text{relatif à } (X-\alpha_k)^{m_k}} + \sum_{\ell=1}^{s}\underbrace{\left(\sum_{j=1}^{n_\ell}\frac{b_{\ell,j}X+c_{\ell,j}}{(X^2+p_\ell X+q_\ell)^j}\right)}_{\text{relatif à } (X^2+p_\ell X+q_\ell)^{n_\ell}}.$$

Exemple 17 (Forme d'une décomposition en éléments simples (sans calculer les coefficients))**.**

1. Donner la forme de la décomposition en éléments simples dans $\mathbb{C}(X)$ de

$$F(X) = \frac{X}{(X+1)^3(X^2+X+1)}.$$

2. Donner la forme de la décomposition en éléments simples dans $\mathbb{R}(X)$ de

$$F(X) = \frac{X^2+2}{(X-1)^2(X+2)(X^2+X+1)}.$$

2.2 Coefficient relatif à un pôle simple

Proposition 18 (Calcul du coefficient relatif à un pôle simple)**.**

Soit $F \in \mathbb{K}(X)$ et $\alpha \in \mathbb{K}$ un **pôle simple** de F.
La décomposition en éléments simples de F s'écrit donc

$$F = \frac{c}{X-\alpha} + G \quad \text{où } \alpha \text{ n'est pas un pôle de } G.$$

1. Formule du cache (utilisation pour des calculs explicites) : $\boxed{c = [(X-\alpha)F(X)]\,(\alpha)}$.
2. Formule théorique : si $F = \dfrac{A}{B}$ et $B'(\alpha) \neq 0$, alors $\boxed{c = \dfrac{A(\alpha)}{B'(\alpha)}}$.

Exemple 19.

Décomposer en éléments simples dans $\mathbb{R}(X)$:

$$F = \frac{2X-1}{X^3+3X^2+2X}$$

$$G = \frac{n!}{X(X-1)\dots(X-n)} \ (n \in \mathbb{N}^*)$$

Exemple 20 (Utilisation d'une décomposition en éléments simples)**.**

Soit $P \in \mathbb{K}[X]$ de degré $n \geq 1$ admettant n racines distinctes non nulles $z_1, \dots, z_n$.

1. Décomposer en éléments simples la fraction $\dfrac{1}{P}$.
2. En déduire la valeur de

$$\sum_{k=1}^{n} \frac{1}{z_k P'(z_k)}.$$

2.3 Une décomposition importante : celle de $\frac{P'}{P}$.

Lemme 21 (Dérivée logarithmique d'un produit)**.**

Soient $P_1, \dots, P_r \in \mathbb{K}[X] \setminus \{0\}$. Alors

$$\frac{\left(\prod_{k=1}^{r} P_k\right)'}{\prod_{k=1}^{r} P_k} = \sum_{k=1}^{r} \frac{P_k'}{P_k}.$$

Théorème 22 (Décomposition en éléments simples de $\frac{P'}{P}$)**.**

Soit P un polynôme scindé sur $\mathbb{K}$:

$$P = \lambda \prod_{k=1}^{r} (X-\alpha_k)^{m_k}.$$

Alors

$$\frac{P'}{P} = \sum_{k=1}^{r} \frac{m_k}{X-\alpha_k}.$$

Exemple 23 (Utilisation d'une décomposition en éléments simples)**.**

Soit $n \in \mathbb{N}$, $n \geq 2$. Déterminer la forme irréductible de

$$F = \sum_{k=1}^{n-1} \frac{1}{X - e^{\frac{2ik\pi}{n}}}.$$

En déduire la valeur de

$$\sum_{k=1}^{n-1} \frac{1}{1 - e^{\frac{2ik\pi}{n}}}.$$

2.4 Pratique de la décomposition en éléments simples

Méthode (comment aborder un calcul de décomposition en éléments simples)**.**

Soit $F \in \mathbb{K}(X)$ dont on cherche la décomposition en éléments simples.

i) On écrit F sous forme irréductible.
On décompose le dénominateur en facteurs irréductibles.

ii) On cherche la partie entière de F (si $\deg F < 0$, la partie entière est nulle).

iii) On écrit *a priori* la décomposition en éléments simples de F.
Elle fait intervenir des coefficients qu'il reste à calculer.

iv) On calcule les coefficients relatifs aux pôles simples (formule du cache).

v) On calcule les autres coefficients comme on peut.
Pour cela on peut s'aider de la parité, de la conjugaison complexe, de l'évaluation en quelques valeurs, des limites en $\pm\infty$...

Exemple 24.

Décomposer en éléments simples dans $\mathbb{C}(X)$.

$$F = \frac{X^2 + 2}{X^2(X^2 + 1)} \quad \text{et} \quad G = \frac{1}{X^n - 1} \ (n \in \mathbb{N}^*)$$

Exemple 25.

Décomposer en éléments simples dans $\mathbb{R}(X)$.

$$F = \frac{1}{X^3 + 1} \quad \text{et} \quad G = \frac{4X^2}{X^4 + 1}.$$

Exercices

26.1 **[♦◇◇]** Décomposer en éléments simples dans $\mathbb{C}[X]$ la fraction rationnelle

$$\frac{X}{(X^2+X+1)^2}.$$

26.2 **[♦◇◇]** Décomposer en éléments simples dans $\mathbb{R}[X]$ la fraction rationnelle

$$\frac{X^2-2X-1}{(X^2+1)^2}.$$

26.3 **[♦◇◇]**

1. Décomposer en éléments simples la fraction rationnelle $\dfrac{1}{X(X+1)(X+2)}$.
2. Calculer la limite quand n tend vers $+\infty$ de

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

26.4 **[♦♦◇]** Soit P un polynôme scindé sur $\mathbb{R}$ et à racines simples $x_1, \ldots, x_n$ avec $n > 1$. Démontrer que

$$\sum_{i=1}^{n} \frac{1}{P'(x_i)} = 0.$$

26.5 **[♦♦◇]**
Pour chacune des fonctions ci-dessous, proposer une primitive sur un intervalle que vous préciserez :

$$f : x \mapsto \frac{1}{1-x^4} \qquad \text{et} \qquad g : x \mapsto \frac{x^2}{x^3-1}.$$

26.6 **[♦♦♦]** Racines multiples de P'
Soit $P \in \mathbb{R}[X]$ un polynôme non constant.

1. On suppose que P est scindé sur $\mathbb{R}$.
   (a) Donner la décomposition en éléments simples de $\frac{P'}{P}$.
   (b) En déduire que
   $$\forall x \in \mathbb{R} \quad P'(x)^2 \geq P(x)P''(x),$$
   avec égalité si et seulement si x est une racine multiple de P.
   (c) Rappeler pourquoi P' est scindé sur $\mathbb{R}$, puis montrer que toute racine multiple de P' est racine de P.
2. (a) Est-il vrai en général que toute racine multiple de P' est racine de P.
   (b) Est-il vrai, sous l'hypothèse que P est scindé sur $\mathbb{R}$, que toute racine de P' est racine de P ?

26.7 **[♦♦♦]** Calculer la limite lorsque x tend vers $\frac{\pi}{2}$ par valeurs inférieures de

$$\int_0^x \sqrt{\tan(t)}\mathrm{d}t.$$

---

27 Espaces vectoriels

Mis à part le calcul booléien, on peut dire qu'il n'y a sans doute pas de théorie plus universellement utilisée en Mathématique que l'Algèbre linéaire ; il n'y en a presque pas non plus qui soit plus élémentaire, bien que des générations de professeurs et de faiseurs de manuels se soient ingéniés à la compliquer à plaisir par de ridicules calculs de matrices.

Jean Dieudonné,
Éléments d'Algèbre linéaire,
Annexe aux Éléments d'Analyse.

Dans ce cours, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$, et sauf indication contraire, n et p sont des entiers naturels non nuls.

1 Espaces et sous-espaces vectoriels.

1.0 Avant-propos : combinaisons linéaires dans $\mathbb{K}^n$.

Définition 1 (Somme de n-uplets, multiplication d'un n-uplet par un scalaire)**.**

Pour tous $x = (x_1, \dots, x_n) \in \mathbb{K}^n$, $y = (y_1, \dots, y_n) \in \mathbb{K}^n$, pour tout $\lambda \in \mathbb{K}$, on pose

$$x + y := (x_1 + y_1, \dots, x_n + y_n) \quad \text{et} \quad \lambda \cdot x := (\lambda x_1, \dots, \lambda x_n).$$

Proposition 2 ($(\mathbb{K}^n, +)$ est un groupe abélien)**.**

Le neutre de ce groupe est le n-uplet $(0, \dots, 0)$.
Le symétrique d'un n-uplet $(x_1, \dots, x_n)$ est le n-uplet $(-x_1, \dots, -x_n)$.

Un calcul dans $\mathbb{R}^3$:

$$3(0, 1, 2) - (0, 2, 1) = (0, 3, 6) - (0, 2, 1) = (0, 1, 5).$$

Définition 3 (Base canonique de $\mathbb{K}^n$)**.**

Pour tout $i \in [\![1, n]\!]$, on note

$$e_i = (0, \dots, 0, 1, 0, \dots, 0),$$

où le 1 est écrit sur la $i$ème coordonnée.
La famille $(e_1, \dots, e_n)$ est appelée **base canonique** de $\mathbb{K}^n$.

La base canonique de $\mathbb{R}^3$ est (e_1, e_2, e_3) où

$$e_1 = (1, 0, 0), \qquad e_2 = (0, 1, 0), \qquad e_3 = (0, 0, 1).$$

Proposition 4.

Tout vecteur de $\mathbb{K}^n$ s'écrit de façon unique comme combinaison linéaire des vecteurs de $(e_1, \dots, e_n)$, base canonique de $\mathbb{K}^n$:

$$\forall x \in \mathbb{K}^n \quad , \exists! (x_1, \dots, x_n) \in \mathbb{K}^n \quad x = \sum_{i=1}^{n} x_i e_i.$$

Par exemple, voici l'unique décomposition de $(1, 2, 3)$ sur la base canonique de $\mathbb{R}^3$:

$$(1, 2, 3) = e_1 + 2e_2 + 3e_3.$$

1.1 Structure de $\mathbb{K}$-espace vectoriel.

On appelle **loi de composition externe** sur un ensemble E à scalaires dans $\mathbb{K}$ une application

$$\cdot : \left\{ \begin{array}{ccc} E \times \mathbb{K} & \to & E \\ (x, \lambda) & \mapsto & \lambda \cdot x \end{array} \right. .$$

L'idée est que si x est un *bidule* et λ un scalaire, alors $\lambda \cdot x$ est un *bidule*.

Définition 5.

On appelle $\mathbb{K}$-**espace vectoriel** un triplet $(E, +, \cdot)$, où E est un ensemble, $+$ une loi de composition interne, et $\cdot$ une loi de composition externe, avec scalaires dans $\mathbb{K}$ vérifiant

1. $(E, +)$ est un groupe abélien, c'est-à-dire
   (a) $+$ est associative : $\forall x, y, z \in E \quad (x + y) + z = x + (y + z)$;
   (b) $+$ est commutative : $\forall x, y \in E \quad x + y = y + x$;
   (c) Il existe dans E un unique élément neutre pour $+$, appelé "zéro" de E et noté 0_E :
   $$\forall x \in E \quad x + 0_E = 0_E + x = x;$$
   (d) Tout élément x de E admet un (unique) symétrique dans E, noté $(-x)$, tel que
   $$x + (-x) = -x + x = 0_E.$$
2. Propriétés de $\cdot$
   (a) $\forall x \in E \quad 1_{\mathbb{K}} \cdot x = x$;
   (b) $\cdot$ est distributive par rapport à l'addition dans E :
   $$\forall (x, y) \in E^2 \quad \forall \lambda \in \mathbb{K} \quad \lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y;$$
   (c) $\cdot$ est distributive par rapport à l'addition dans $\mathbb{K}$:
   $$\forall x \in E \quad \forall (\lambda, \mu) \in \mathbb{K}^2 \quad (\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x;$$
   (d) $\forall (\lambda, \mu) \in \mathbb{K}^2 \quad \forall x \in E \quad \lambda \cdot (\mu \cdot x) = (\lambda\mu) \cdot x$.

Les éléments de E sont appelés des **vecteurs**.

Un abus fréquent consiste à parler de "l'espace vectoriel E" en omettant de mentionner les lois $+$ et $\cdot$.

Attention : dans un espace vectoriel, le produit de deux vecteurs n'a pas de sens a priori.

Proposition 6 (Autour de zéro et du symétrique)**.**

Soit E un $\mathbb{K}$-espace vectoriel.

(i) $\forall x \in E \quad 0_{\mathbb{K}} \cdot x = 0_E$.
(ii) $\forall \lambda \in \mathbb{K} \quad \lambda \cdot 0_E = 0_E$.
(iii) $\forall x \in E \quad (-x) = (-1) \cdot x$.
(iv) $\forall \lambda \in \mathbb{K}\ \forall x \in E \quad \lambda \cdot x = 0_E \implies (\lambda = 0_{\mathbb{K}} \text{ ou } x = 0_E)$.

Preuve. Dans ce qui suit, lorsqu'on utilise une propriété de la définition 5, on signale son numéro.
(i) Soit $x \in E$. On peut écrire

$$0_{\mathbb{K}} \cdot x = (0_{\mathbb{K}} + 0_{\mathbb{K}}) \cdot x \underset{2.(c)}{=} 0_{\mathbb{K}} \cdot x + 0_{\mathbb{K}} \cdot x.$$

La propriété 1.(d) nous rappelle que le vecteur $0_{\mathbb{K}} \cdot x$ admet un symétrique dans le groupe $(E, +)$ noté $-0_{\mathbb{K}} \cdot x$.
On ajoute ce symétrique à l'égalité précédente :

$$\underbrace{0_{\mathbb{K}} \cdot x + (-0_{\mathbb{K}} \cdot x)}_{=0_E} = (0_{\mathbb{K}} \cdot x + 0_{\mathbb{K}} \cdot x) + (-0_{\mathbb{K}} \cdot x) \underset{1.(a)}{=} 0_{\mathbb{K}} \cdot x + \underbrace{(0_{\mathbb{K}} \cdot x + (-0_{\mathbb{K}} \cdot x))}_{=0_E} \underset{1.(c)}{=} 0_{\mathbb{K}} \cdot x,$$

ce qui montre bien $0_{\mathbb{K}} \cdot x = 0_E$.
(ii) Soit $\lambda \in \mathbb{K}$. On a

$$\lambda \cdot 0_E \underset{(i)}{=} \lambda \cdot (0_{\mathbb{K}} \cdot 0_E) \underset{2.(d)}{=} (\lambda \cdot 0_{\mathbb{K}}) \cdot 0_E = 0_{\mathbb{K}} \cdot 0_E = 0_E.$$

(iii) Soit $x \in E$. On a

$$x + (-1) \cdot x \underset{2.(c)}{=} (1 + (-1)) \cdot x = 0_{\mathbb{K}} \cdot x = 0_E.$$

On a montré que $(-1) \cdot x$ est un symétrique de x, donc <u>le</u> symétrique : $(-1) \cdot x = -x$.
(iv) Soient $\lambda \in \mathbb{K}$ et $x \in E$ tels que $\lambda \cdot x = 0_E$. Supposons que $\lambda \neq 0_{\mathbb{K}}$. Alors λ possède un inverse λ^{-1}.
En multipliant par ce scalaire,

$$\lambda^{-1} (\lambda \cdot x) = \lambda^{-1} \cdot 0_E \quad \text{d'où} \quad (\lambda^{-1}\lambda) \cdot x = 0_E \quad \text{d'où} \quad 1_{\mathbb{K}} \cdot x = 0_E.$$

D'après 2.(a), $1_{\mathbb{K}} \cdot x = x$, ce qui montre bien que $x = 0_E$.

□

Exemple 7 (L'espace vectoriel $\mathbb{K}^n$)**.**

Muni des lois + et · définies dans l'avant-propos, $(\mathbb{K}^n, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.
Le zéro de cet espace vectoriel est le n-uplet $(0, \dots, 0)$.
Le symétrique du vecteur $(x_1, \dots, x_n)$ est le vecteur $(-x_1, \dots, -x_n)$.

Exemples :

1. Le cas $n = 2$ et $\mathbb{K} = \mathbb{R}$.
   L'espace vectoriel $\mathbb{R}^2$ est le premier espace vectoriel dans lequel on a travaillé. Par définition, un vecteur u de $\mathbb{R}^2$ s'écrit $u = (x, y)$, où x et y sont deux réels.
   Les nostalgiques pourront écrire $\overrightarrow{u}$ cet élément de $\mathbb{R}^2$. L'ensemble $\mathbb{R}^2$ peut être identifié au plan en se donnant un repère orthonormé : $\overrightarrow{u}$ est alors associé au point de coordonnées x et y.
2. Le cas $n = 3$ et $\mathbb{K} = \mathbb{R}$.
   L'espace $\mathbb{R}^3$ est celui de la mécanique newtonienne : il modélise l'espace en trois dimensions dans lequel nous vivons.
3. Le cas $n = 1$.
   $\mathbb{R}$ est un $\mathbb{R}$-espace vectoriel. $\mathbb{C}$ est un $\mathbb{C}$-espace vectoriel.

Exemple 8 ($\mathbb{C}$ vu comme $\mathbb{R}$-espace vectoriel)**.**

Si $\mathbb{C}$ est un $\mathbb{C}$-espace vectoriel, comme on vient de le dire, c'est aussi un $\mathbb{R}$-espace vectoriel.

On sait déjà identifier $\mathbb{C}$ et $\mathbb{R}^2$ en associant à un nombre complexe $a + ib$ son affixe $(a, b) \in \mathbb{R}^2$.

Exemple 9 (L'espace vectoriel $\mathbb{K}[X]$).

$(\mathbb{K}[X], +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.
Les lois $+$ et $\cdot$ sont l'addition et la multiplication par un scalaire pour les polynômes.
Le zéro de cet espace est le polynôme nul.

Exemple 10 (L'espace vectoriel $M_{n,p}(\mathbb{K})$).

$(M_{n,p}(\mathbb{K}), +, \cdot)$, où $n, p \in \mathbb{N}^*$ est un $\mathbb{K}$-espace vectoriel.
Les lois $+$ et $\cdot$ sont l'addition et la multiplication par un scalaire pour les matrices de taille $n \times p$.
Le zéro de cet espace est la matrice nulle $0_{n,p}$

Exemple 11 (Espace vectoriel des applications à valeurs dans $\mathbb{K}$).

Soit Ω un ensemble non vide. L'ensemble $\mathbb{K}^\Omega$ des fonctions de Ω dans $\mathbb{K}$ peut être muni des lois $+$ et $\cdot$ définies comme suit : pour toutes fonctions f et g de Ω vers $\mathbb{K}$ et tout scalaire $\lambda \in \mathbb{K}$

$$f+g : \left\{ \begin{array}{ccc} \Omega & \to & \mathbb{K} \\ x & \mapsto & (f+g)(x) = f(x) + g(x) \end{array} \right. \qquad \text{et} \qquad \lambda \cdot f : \left\{ \begin{array}{ccc} \Omega & \to & \mathbb{K} \\ x & \mapsto & (\lambda \cdot f)(x) = \lambda \cdot f(x) \end{array} \right. .$$

$(\mathbb{K}^\Omega, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel de neutre la fonction nulle sur Ω.

Exemples :

1. Espaces de fonctions à valeurs réelles.
   Soit I un intervalle. L'ensemble $\mathbb{R}^I$, plutôt noté $\mathcal{F}(I, \mathbb{R})$, est un $\mathbb{R}$-espace vectoriel.
2. Espaces de suites.
   L'ensemble $\mathbb{K}^\mathbb{N}$ des suites à valeurs dans $\mathbb{K}$ est un $\mathbb{K}$-espace vectoriel. Son zéro est la suite nulle.

Proposition 12 (Produit d'un nombre fini de $\mathbb{K}$-espaces vectoriels).

Soit $n \in \mathbb{N}^*$ et n $\mathbb{K}$ espaces vectoriels $E_1, \dots, E_n$.
Pour tous $x = (x_1, \dots, x_n)$ et $y = (y_1, \dots, y_n)$ dans $E_1 \times \cdots \times E_n$, pour tout $\lambda \in \mathbb{K}$, on pose

$$x + y := (x_1 + y_1, \dots, x_n + y_n) \quad \text{et} \quad \lambda \cdot x := (\lambda \cdot x_1, \dots, \lambda \cdot x_n).$$

lire $x_k + y_k$ comme une somme dans l'espace E_k et $\lambda \cdot x_k$ comme une multiplication par λ dans E_k

Muni des lois $+$ et $\cdot$ définies ci-dessus, $E_1 \times \cdots \times E_n$ est un $\mathbb{K}$-espace vectoriel de zéro $(0_{E_1}, \cdots, 0_{E_n})$.

En particulier, pour E un $\mathbb{K}$-espace vectoriel et $n \in \mathbb{N}^*$, nous venons de munir E^n d'une structure de $\mathbb{K}$-espace vectoriel.

1.2 Combinaisons linéaires.

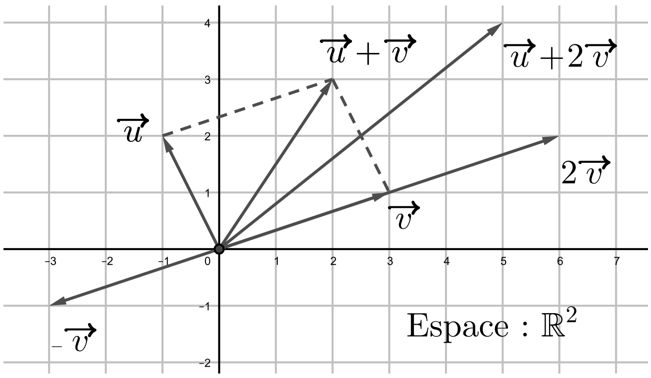
Définition 13 (Combinaison linéaire d'un nombre fini de vecteurs)**.**

Soit E un $\mathbb{K}$-espace vectoriel et $(x_1, \ldots, x_p) \in E^p$, où $p \in \mathbb{N}^*$.
On appelle **combinaison linéaire** de $x_1, \ldots x_p$ tout vecteur de la forme

$$\sum_{i=1}^{p} \lambda_i x_i = \lambda_1 x_1 + \ldots + \lambda_n x_p,$$

où $\lambda_1, \ldots, \lambda_p$ sont des scalaires de $\mathbb{K}$.

Une illustration dans $\mathbb{R}^2$: pour $\overrightarrow{u} = (-1, 2)$, $\overrightarrow{v} = (3, 1)$, on représente $-\overline{v}$, $\overrightarrow{u} + \overrightarrow{v}$ et $\overrightarrow{u} + 2\overrightarrow{v}$.



Exemple 14 (dans $\mathbb{R}^3$)**.**

Soient

$$x = (1, 1, 1) \qquad \overrightarrow{u_1} = (0, 1, 1) \qquad \overrightarrow{u_2} = (1, 0, 1) \qquad \overrightarrow{u_3} = (1, 1, 0).$$

Montrer que x est une combinaison linéaire de u_1, u_2 et u_3.

Définition 15 (Généralisation de la notion de combinaison linéaire)**.**

Soit $(x_i)_{i \in I}$ une famille de vecteurs d'un espace vectoriel E, indexée par un ensemble I non vide.
On appelle **combinaison linéaire** des vecteurs de la famille $(x_i)_{i \in I}$ tout vecteur de la forme

$$\sum_{k=1}^{n} \lambda_k x_{i_k} = \lambda_1 x_{i_1} + \cdots + \lambda_n x_{i_n},$$

avec $n \in \mathbb{N}^*$, $i_1, \ldots, i_n \in I$ et $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$.

Définition 16.

Soit I un ensemble non vide et $(\lambda_i)_{i \in I}$ une famille de scalaires de $\mathbb{K}$ indexée par I. Elle est dite **presque nulle** (ou à support fini) si λ_i n'est différent de 0 que pour un nombre fini de scalaires.

Autrement dit, $(\lambda_i)_{i\in I} \in \mathbb{K}^I$ est presque nulle si l'ensemble $J = \{i \in I : \lambda \neq 0\}$ est fini. Une telle famille est aussi dite *à support fini* et l'ensemble de ces familles peut être noté $\mathbb{K}^{(I)}$

On peut donc aussi définir une combinaison linéaire de la famille $(x_i)_{i\in I}$ comme un vecteur de la somme

$$\sum_{i\in I} \lambda_i x_i,$$

où $(\lambda_i)_{i\in I}$ est une famille presque nulle de $\mathbb{K}^I$. Même si l'ensemble d'indice est infini, la somme est à lire comme une somme finie puisque seul un nombre fini de termes sont non nuls.
La définition 15, équivalente, reste meilleure car plus concrète.

1.3 Sous-espaces vectoriels.

Soit $(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel et F une partie de E. On rappelle que F est **stable** par la loi $+$ si

$$\forall (x, y) \in F^2 \quad x + y \in F.$$

On dira que F est **stable par** $\cdot$ si

$$\forall x \in F \quad \forall \lambda \in \mathbb{K} \quad \lambda \cdot x \in F.$$

On peut alors considérer les restrictions des lois $+$ et $\cdot$ à l'ensemble F : ce sont bien respectivement une loi de composition interne et une loi de composition externe à scalaires dans $\mathbb{K}$. Notons-les encore $+$ et $\cdot$:

$$+ : \left\{ \begin{array}{ccc} F \times F & \to & F \\ (x, y) & \mapsto & x + y \end{array} \right. \qquad \text{et} \qquad \cdot : \left\{ \begin{array}{ccc} F \times \mathbb{K} & \to & F \\ (x, \lambda) & \mapsto & \lambda \cdot x \end{array} \right. .$$

On les appelle **lois induites** sur F par les lois $+$ et $\cdot$ sur E.

Définition 17.

Soit $(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel et F une partie de E.
On dit que F est un **sous-espace vectoriel** de E si
- F est stable par $+$ et $\cdot$
- $(F, +, \cdot)$ est un espace vectoriel (ou $+$ et $\cdot$ sont les lois induites sur F par celles de E).

Exemple 18 (Sous-espaces triviaux)**.**

Soit E un $\mathbb{K}$-espace vectoriel.
- E est un sous-espace vectoriel de E.
- Le singleton $\{0_E\}$ est un sous-espace vectoriel de E : clairement stable par $+$ et $\cdot$, il est, muni des lois induites, un espace vectoriel. On l'appellera **sous-espace vectoriel nul**.

Méthode.

Pour montrer qu'un ensemble $(E, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel, il suffira souvent de prouver que c'est un sous-espace vectoriel d'un espace vectoriel connu.

Et pour faire cela, on utilisera, plutôt que la définition, la caractérisation ci-après.

Proposition 19 (Caractérisation des sous-espaces vectoriels parmi les parties de E)**.**

Soit $(E, +, \cdot)$ un $\mathbb{K}$-espace vectoriel et $F \subset E$. Il y a équivalence des deux assertions suivantes.

1. F est un sous-espace vectoriel de E.
2. F satisfait les deux propriétés suivantes :
   - $0_E \in F$,
   - F est stable par combinaison linéaire de deux vecteurs, c'est à dire

$$\forall x, y \in F \quad \forall \lambda, \mu \in \mathbb{K} \quad \lambda x + \mu y \in F.$$

Proposition 20.

Un sous-espace vectoriel est stable par combinaison linéaire quelconque de vecteurs.

Exemple 21 (Des sous-espaces vectoriels de $\mathbb{K}^p$)**.**

Soit $A = (a_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} \in M_{n,p}(\mathbb{K})$. Notons S_0 l'ensemble des solutions du système linéaire homogène $AX = 0_{n,1}$, d'inconnue $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \in M_{p,1}(\mathbb{K})$ ou $(x_1, \ldots, x_p) \in \mathbb{K}^p$ (on confond $M_{p,1}(\mathbb{K})$ et $\mathbb{K}^p$). On a prouvé dans le cours sur les matrices que $\mathcal{S}_0$ est un sous-espace vectoriel de $\mathbb{K}^p$.

- **Cas particulier 1.** $n = 1, p = 2$: équation du type $ax + by = 0$.
  Dans le cas non dégénéré $(a, b) \neq (0, 0)$, l'ensemble des solutions est une droite vectorielle de $\mathbb{R}^2$. ✎
- **Cas particulier 2.** $n = 1, p = 3$: équation du type $ax + by + cz = 0$.
  Dans le cas non dégénéré $(a, b, c) \neq (0, 0, 0)$, l'ensemble des solutions est un plan vectoriel de $\mathbb{R}^3$. ✎
- **Cas particulier 3.** Le cas $n = 2, p = 3$: deux équations de plans vectoriels dans $\mathbb{R}^3$. Dans le cas non dégénéré (deux plans, non confondus) les solutions sont les vecteurs d'une droite vectorielle de $\mathbb{R}^3$. ✎

Contre-exemple. Une droite affine de $\mathbb{R}^2$ ne passant pas par $(0, 0)$ n'est pas un s.e.v. de $\mathbb{R}^2$.
Contre-exemple. Un demi-plan : $\{(x, y) \in \mathbb{R}^2 : 2x - y \geq 0\}$ n'est pas un s.e.v. de $\mathbb{R}^2$: il contient $(0, 0)$ mais n'est pas stable par combinaison linéaire. En effet, $(1, 2)$ est dans le demi-plan mais pas son opposé.

Exemple 22 (Des sous-espaces vectoriels de $\mathbb{K}[X]$)**.**

On rappelle que pour tout entier $n \in \mathbb{N}$, l'ensemble $\mathbb{K}_n[X]$ est celui des polynômes de degré inférieur à n, à coefficients dans $\mathbb{K}$. C'est un sous-espace vectoriel de $\mathbb{K}[X]$ (donc un espace vectoriel).

Pour tous entiers $n, p \in \mathbb{N}$ avec $p \leq n$, $\mathbb{K}_p[X]$ est un sous-espace vectoriel de $\mathbb{K}_n[X]$.

L'ensemble des polynômes de degré *égal* à n n'est pas un sous-espace vectoriel de $\mathbb{K}[X]$.

Exemple 23 (Un autre exemple de s.e.v. de $\mathbb{K}[X]$).

Soit $a \in \mathbb{K}$. Démontrer que l'ensemble

$$F_a = \{P \in \mathbb{K}[X] : P(a) = 0\}$$

est un sous-espace vectoriel de $\mathbb{K}[X]$.

Exemple 24 (Des sous-espaces de $M_n(\mathbb{K})$).

Les ensembles $S_n(\mathbb{K})$ et $A_n(\mathbb{K})$ sont des sous-espaces vectoriels de $M_n(\mathbb{K})$.

L'ensemble des matrice diagonales, celui des triangulaires supérieures et celui des triangulaires inférieures sont aussi des sous-espaces vectoriels de $M_n(\mathbb{K})$.

$GL_n(\mathbb{K})$ n'est pas un sous-espace vectoriel de $M_n(\mathbb{K})$.

Exemple 25 (Des sous-espaces de $\mathcal{F}(I, \mathbb{R})$).

L'ensemble $\mathcal{C}(I, \mathbb{R})$ des fonctions continues sur I est un s.e.v. de $\mathcal{F}(I, \mathbb{R})$.

L'ensemble $\mathcal{D}(I, \mathbb{R})$ des fonctions dérivables sur I est un s.e.v. de $\mathcal{F}(I, \mathbb{R})$.
C'est donc un espace vectoriel, inclus dans $\mathcal{C}(I, \mathbb{R})$: c'est un sous-espace vectoriel de $\mathcal{C}(I, \mathbb{R})$.

Pour tout $n \in \mathbb{N} \cup \{\infty\}$, $\mathcal{C}^n(I, \mathbb{R})$ est un sous-espace vectoriel de $\mathcal{F}(I, \mathbb{R})$.
Pour tous $n, p \in \mathbb{N} \cup \{\infty\}$ avec $p \geq n$, $\mathcal{C}^p(I, \mathbb{R})$ est un s.e.v. de $\mathcal{C}^n(I, \mathbb{R})$.

L'ensemble des fonctions monotones n'est pas un sous-espace vectoriel de $\mathcal{F}(I, \mathbb{R})$.

Proposition 26 (Intersection de s.e.v.).

Soit E un $\mathbb{K}$-espace vectoriel et $(F_i)_{i \in I}$ une famille de sous-espaces vectoriels de E. Alors

$$\bigcap_{i \in I} F_i \text{ est un sous-espace vectoriel de } E.$$

La réunion de deux sous-espaces vectoriels n'est pas, en général, un sous-espace vectoriel.

On peut montrer (TD) le résultat suivant pour deux sous-espaces vectoriels F et G d'un espace vectoriel E :

$$F \cup G \text{ est un sous-espace vectoriel de } E \quad \Longleftrightarrow \quad F \subset G \text{ ou } G \subset F.$$

1.4 Application linéaire entre deux espaces vectoriels.

Définition 27.

Soient $(E,+,\cdot)$ et $(F,+,\cdot)$ deux $\mathbb{K}$-espaces vectoriels.

On appelle **application linéaire** entre E et F une application $u : E \to F$ telle que

$$\forall x, y \in E \quad \forall \lambda, \mu \in \mathbb{K} \qquad u(\lambda x + \mu y) = \lambda u(x) + \mu u(y).$$

(l'image de la combinaison linéaire, c'est la combinaison linéaire des images)

Une application linéaire de E dans E est appelée **endomorphisme** de E.
Une application linéaire de E dans $\mathbb{K}$ (vu comme $\mathbb{K}$-espace vectoriel) est une **forme linéaire**.

Remarque. Il est équivalent de définir la linéarité d'une application $u : E \to F$ à l'aide des propriétés

1. $\forall x, y \in E \quad u(x+y) = u(x) + u(y)$ (propriété de morphisme de groupes additifs)
2. $\forall x \in E \ \ \forall \lambda \in \mathbb{K} \quad u(\lambda \cdot x) = \lambda \cdot u(x)$ (propriété d'homogénéité).

Exemples.

1. La transposition :
$$u : \left\{ \begin{array}{ccc} M_{n,p}(\mathbb{K}) & \to & M_{p,n}(\mathbb{K}) \\ M & \mapsto & M^\top \end{array} \right. ,$$
est une application linéaire.

2. La dérivation sur $\mathbb{K}[X]$
$$D : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K}[X] \\ P & \mapsto & P' \end{array} \right.$$
est un endomorphisme de $\mathbb{K}[X]$.

   On peut de même définir une application de dérivation définie sur $\mathcal{D}(I,\mathbb{R})$:
$$\widetilde{D} : \left\{ \begin{array}{ccc} \mathcal{D}(I,\mathbb{R}) & \to & \mathcal{F}(I,\mathbb{R}) \\ f & \mapsto & f' \end{array} \right.$$
$\widetilde{D}$ n'est pas un endomorphisme : une dérivée n'est pas toujours dérivable elle-même !

3. La trace est une forme linéaire :
$$\mathrm{tr} : \left\{ \begin{array}{ccc} M_n(\mathbb{K}) & \to & \mathbb{K} \\ M & \mapsto & \mathrm{tr}(M) \end{array} \right. .$$

4. L'évaluation des polynômes (ou des fonctions) est linéaire.
Plus précisément, Φ_a et Ψ_b, définies ci-dessous à l'aide de $a \in \mathbb{K}$ et $b \in \Omega$ fixés, sont des formes linéaires.
$$\Phi_a : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K} \\ P & \mapsto & P(a) \end{array} \right. \quad \text{et} \quad \Psi_b : \left\{ \begin{array}{ccc} \mathbb{K}^\Omega & \to & \mathbb{K} \\ f & \mapsto & f(b) \end{array} \right. .$$

5. Soit I un intervalle et $a, b \in I$. L'application $\varphi : f \mapsto \displaystyle\int_a^b f(x)\mathrm{d}x$ est une forme linéaire sur $\mathcal{C}(I,\mathbb{R})$.

6. Pour tout espace vectoriel E, Id_E est un endomorphisme de E.
7. Pour tous E et F espaces vectoriels, l'application nulle ci-dessous est linéaire.

$$N : \left\{ \begin{array}{ccc} E & \to & F \\ x & \mapsto & 0_F \end{array} \right. ,$$

Lemme 28.

Soient E et F deux $\mathbb{K}$-espaces vectoriel et $u : E \to F$ une application linéaire. On a

$$u(0_E) = 0_F.$$

Proposition 29 (Image directe/réciproque d'un s.e.v. par une application linéaire)**.**

Soient E et F deux $\mathbb{K}$-espaces vectoriels et $u : E \to F$ une application linéaire.
1. Si G est un sous-espace vectoriel de E, alors $u(G)$ est un sous-espace vectoriel de F.
2. Si H est un sous-espace vectoriel de F, alors $u^{-1}(H)$ est un sous-espace vectoriel de E.

Définition 30.

Soient E et F deux $\mathbb{K}$-espaces vectoriels et $u : E \to F$ une application linéaire.
1. On appelle **image** de u, et on note $\operatorname{Im} u$ la partie de F définie par :

$$\operatorname{Im} u = \{u(x),\ x \in E\} = \{y \in F : \exists x \in E\ y = u(x)\}.$$

2. On appelle **noyau** de u et on note $\operatorname{Ker} u$ la partie de E définie par :

$$\operatorname{Ker} u = \{x \in E : u(x) = 0_F\}.$$

Proposition 31.

Soient E et F deux $\mathbb{K}$-espaces vectoriels et $u : E \to F$ une application linéaire.
1. $\operatorname{Ker} u$ est un sous-espace vectoriel de E et

$$u \text{ est injective} \iff \operatorname{Ker} u = \{0_E\}.$$

2. $\operatorname{Im} u$ est un sous-espace vectoriel de F et

$$u \text{ est surjective} \iff \operatorname{Im} u = F.$$

Exemple 32 (Reconnaître un Ker)**.**

Soit $a \in \mathbb{K}$. À l'aide de la notion de noyau, retrouver que l'ensemble F_a est un s.e.v. de $\mathbb{K}[X]$:

$$F_a \overset{def}{=} \{P \in \mathbb{K}[X] : P(a) = 0\}$$

1.5 Sous-espace vectoriel engendré par une partie.

Proposition-Définition 33 (S.e.v. engendré par une famille finie de vecteurs)**.**

Soit E un $\mathbb{K}$-espace vectoriel, $p \in \mathbb{N}$ et $(x_1, \dots, x_p) \in E^p$.
On note $\mathrm{Vect}\,(x_1, \dots, x_p)$ l'ensemble des combinaisons linéaires de $x_1, \dots, x_p$.

$$\mathrm{Vect}(x_1, \dots, x_p) \overset{def}{=} \left\{ \sum_{k=1}^{p} \lambda_k x_k \quad \middle| \quad (\lambda_1, \dots, \lambda_p) \in \mathbb{K}^p \right\}.$$

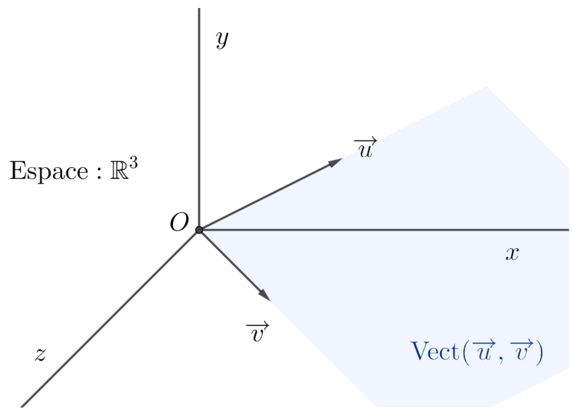
Il s'agit d'un sous-espace vectoriel de E.
On l'appelle **sous-espace vectoriel engendré** par $(x_1, \dots, x_p)$ (ou par l'ensemble $\{x_1, \dots, x_p\}$).

En particulier, pour x, y deux vecteurs d'un espace vectoriel E,

$$\boxed{\mathrm{Vect}(x) = \{\lambda x,\ \lambda \in \mathbb{K}\}}, \qquad \text{et} \qquad \boxed{\mathrm{Vect}(x, y) = \{\lambda x + \mu y,\ \lambda, \mu \in \mathbb{K}\}}.$$

Exemple 34 (et image mentale ✎)**.**

$E = \mathbb{R}^3$ et $F = \{(x, y, z) : x - 2y - z = 0\}$.
On prouve que $F = \mathrm{Vect}(\overrightarrow{u}, \overrightarrow{v})$, où $\overrightarrow{u} = (2, 1, 0)$ et $\overrightarrow{v} = (1, 0, 1)$.



Exemple 35.

Pour $n \in \mathbb{N}$,

$$\mathrm{Vect}(1, X, X^2, \cdots, X^n) = \mathbb{K}_n[X].$$

Exemple 36 (Ensemble des solutions d'une EDL2 homogène)**.**

Écrire à l'aide d'un Vect l'ensemble des solutions de $y'' + y = 0$.
On montre ainsi qu'il s'agit d'un sous-espace de l'espace des fonctions deux fois dérivables.

Proposition-Définition 37 (Sous-espace vectoriel engendré par une partie/famille quelconque)**.**

Soit E un $\mathbb{K}$-espace vectoriel et A une partie de E non vide.
On note $\mathrm{Vect}(A)$ l'ensemble des combinaisons linéaires de vecteurs de A :

$$\mathrm{Vect}(A) = \left\{ \sum_{i=1}^{n} \lambda_i x_i \mid n \in \mathbb{N}^* \ , (x_1, \dots, x_n) \in A^n, \ (\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n \right\}.$$

Il s'agit d'un sous-espace vectoriel de E. On l'appelle **sous-espace vectoriel engendré** par A.
On conviendra en outre que $\mathrm{Vect}(\emptyset) = \{0_E\}$.

En particulier, si $(x_i)_{i \in I}$ est une famille de vecteurs de E, on note $\mathrm{Vect}\,(x_i)_{i \in I}$ le sous-espace vectoriel engendré par l'ensemble $\{x_i, i \in I\}$:

$$\mathrm{Vect}\,(x_i)_{i \in I} = \left\{ \sum_{k=1}^{n} \lambda_k x_{i_k} \mid n \in \mathbb{N}^* \ , (i_1, \dots, i_n) \in I^n, \ (\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n \right\}.$$

Remarque. On insiste sur le fait que le sous-espace vectoriel engendré par une partie ou une famille, c'est toujours l'ensemble des combinaisons linéaires des vecteurs de la partie/famille. Et que même si la partie contient une infinité de vecteurs, les combinaisons linéaires sont des sommes finies !

Exemple 38.

$$\mathrm{Vect}(X^k)_{k \in \mathbb{N}} = \mathbb{K}[X].$$

Théorème 39 (Une autre vision du Vect)**.**

Soit E un $\mathbb{K}$-espace vectoriel et A une partie de E.
$\boxed{\mathrm{Vect}(A) \text{ est le plus petit sous-espace vectoriel qui contient } A}$ (plus petit au sens de l'inclusion) :

$$\forall F \in \mathcal{P}(E) \qquad \left\{ \begin{array}{c} F \ \text{ s.e.v. de } \ E \\ A \subset F \end{array} \right\} \implies \mathrm{Vect}(A) \subset F.$$

Corollaire 40.

Soit E un $\mathbb{K}$-espace vectoriel et A une partie de E.

$$\mathrm{Vect}(A) = \bigcap_{\substack{F \text{ s.e.v. de } E \\ A \subset F}} F.$$

En particulier, pour tout partie F de E, on se convaincra que

$$F \text{ est un sous-espace vectoriel de } E \quad \text{ssi} \quad F = \mathrm{Vect}(F).$$

Proposition 41 (Propriétés du Vect).

Soit E un $\mathbb{K}$-espace vectoriel, et A, A', B trois parties de E, et $x, y \in E$.

1. Croissance du Vect :
$$A \subset B \implies \mathrm{Vect}(A) \subset \mathrm{Vect}(B).$$

2. Ajout ou élimination de vecteurs superflus :
$$A' \subset \mathrm{Vect}(A) \implies \mathrm{Vect}(A \cup A') = \mathrm{Vect}(A).$$
En particulier,
$$x \in \mathrm{Vect}(A) \implies \mathrm{Vect}(A \cup \{x\}) = \mathrm{Vect}(A).$$

3. Remplacement d'un vecteur : Si $y \in \mathrm{Vect}(A \cup \{x\})$ avec un scalaire non nul sur x, alors
$$\mathrm{Vect}(A \cup \{x\}) = \mathrm{Vect}(A \cup \{y\}).$$

Corollaire 42 (Cas d'une famille finie : invariance du Vect par opérations élémentaires).

Soit E un espace vectoriel et $(x_1, \ldots, x_p) \in E^p$ une famille de vecteurs.
Les trois opérations élémentaires standard ne modifient pas le s.e.v. engendré par $(x_1, \ldots, x_p)$.

- Échange de x_i avec x_j, où $1 \leq i < j \leq p$:
$$\mathrm{Vect}(x_1, \cdots, x_i, \cdots, x_j, \cdots, x_p) = \mathrm{Vect}(x_1, \cdots, x_j, \cdots, x_i, \cdots, x_p).$$
- Dilatation : remplacement de x_i par λx_i, avec $\lambda \in \mathbb{K}^*$:
$$\mathrm{Vect}(x_1, x_2 \cdots, x_i, \cdots, x_p) = \mathrm{Vect}(x_1, x_2, \cdots, \lambda x_i, \cdots, x_p).$$
- Transvection : pour i et j distincts dans $[\![1, p]\!]$ et $\lambda \in \mathbb{K}$, remplacement de x_i par $x_i := x_i + \lambda x_j$
$$\mathrm{Vect}(x_1, x_2 \cdots, x_i, \cdots, x_p) = \mathrm{Vect}(x_1, x_2, \cdots, x_i + \lambda x_j, \cdots, x_p).$$

1.6 Somme de deux sous-espaces vectoriels.

Proposition-Définition 43 (Somme des deux s.e.v.).

Soit E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels de E.

On appelle **somme** de F et de G, et on note $F + G$ l'ensemble
$$F + G = \{x_F + x_G \mid x_F \in F, x_G \in G\} = \{x \in E \mid \exists x_F \in F\ \exists x_G \in G \quad x = x_F + x_G\},$$
Il s'agit d'un sous-espace vectoriel de E.

Proposition 44 (Évidences).

Soit E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels.

1. $F + G = G + F$.
2. $F \subset F + G$ et $G \subset F + G$.
3. $F + \{0_E\} = F$ et $\{0_E\} + G = G$.
4. $E + E = E$.

Exemple 45.

Soit E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels de E. Démontrer que

$$F + G = \mathrm{Vect}(F \cup G).$$

L'écriture d'un vecteur sur une somme n'est <u>pas unique</u> a priori. Prenons l'exemple trivial d'un espace vectoriel non réduit à $\{0_E\}$ et d'un vecteur x non nul de cet espace. Voici deux écritures distinctes d'un même vecteur x sur $E + E$:

$$x = \underbrace{x}_{\in E} + \underbrace{0_E}_{\in E} \quad \text{et} \quad x = \underbrace{\tfrac{1}{2}x}_{\in E} + \underbrace{\tfrac{1}{2}x}_{\in E}.$$

Définition 46 (Somme directe).

Soit E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels de E.

On dit que F et G sont en **somme directe** si pour tout élément de $F + G$, son écriture comme somme d'un élément de F et d'un élément de G est <u>unique</u> :

$$\forall x \in F + G \quad \exists!(x_F, x_G) \in F \times G \quad x = x_F + x_G.$$

On pourra dire que x_F est la **composante** de x sur F et x_G la composante de x sur G.

<u>Notation</u> : lorsque F et G sont en somme directe, on note $F + G = F \oplus G$.

Proposition 47 (Caractérisation d'une somme directe).

Soit E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels de E. Alors

$$F + G = F \oplus G \quad \iff \quad F \cap G = \{0_E\}.$$

Condition pour que deux droites vectorielles de $\mathbb{R}^2$ soient en somme directe ?

Deux plans vectoriels de $\mathbb{R}^3$ peuvent-ils être en somme directe ?

Définition 48 (Supplémentaires)**.**

Soit E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels de E.

On dit que F et G sont **supplémentaires** dans E, et on note $E = F \oplus G$, si tout élément de E s'écrit de manière unique comme somme d'un élément de F et d'un élément de G :

$$\forall x \in E \quad \exists!(x_F, x_G) \in F \times G \quad x = x_F + x_G.$$

Exemple 49 ($S_n(\mathbb{K})$ et $A_n(\mathbb{K})$ sont supplémentaires)**.**

Dans le cours sur les matrices, on a prouvé que toute matrice de $M_n(\mathbb{K})$ s'écrit de manière unique comme la somme d'une matrice symétrique et d'une matrice antisymétrique. On a donc

$$M_n(\mathbb{K}) = S_n(\mathbb{K}) \oplus A_n(\mathbb{K}).$$

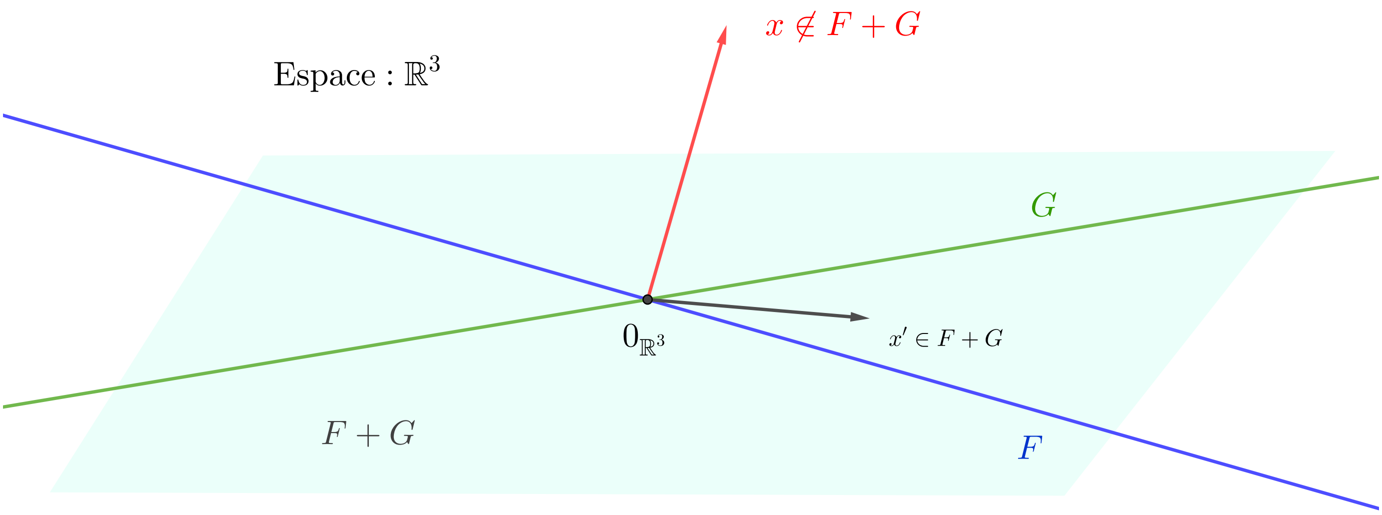
Proposition 50 (Caractérisation des supplémentaires)**.**

Soit E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels de E.

$$E = F \oplus G \quad \Longleftrightarrow \quad \begin{cases} E &= F + G \\ F \cap G &= \{0_E\}. \end{cases}$$

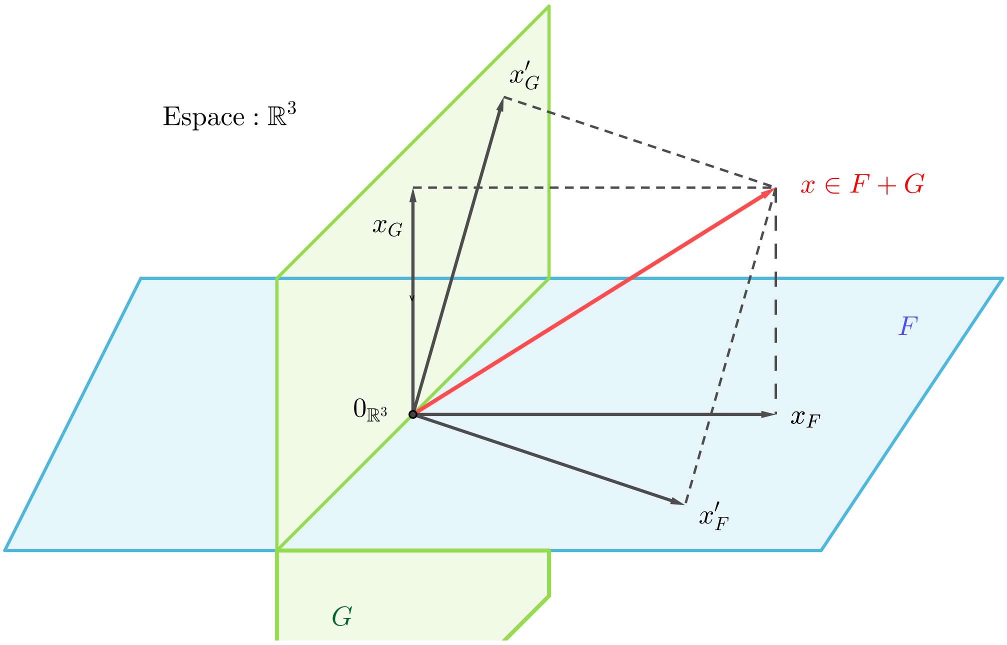
Somme, somme directe, supplémentaires... pour s'y retrouver, rien de tel que quelques ✎ dans $\mathbb{R}^3$:

Voici d'abord deux droites vectorielles F et G de $\mathbb{R}^3$ (non confondues)



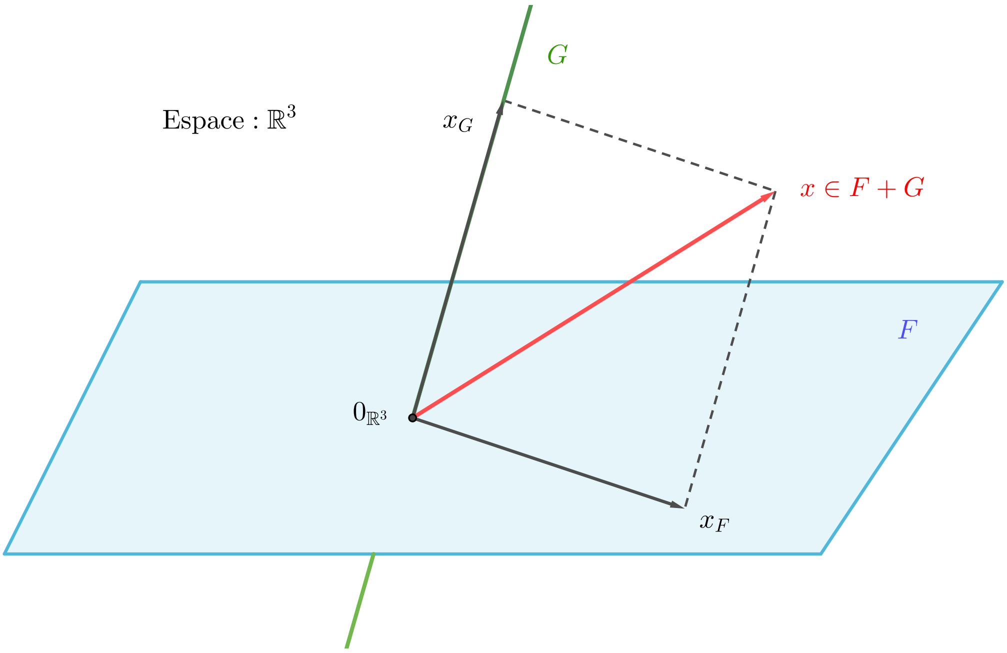
leur somme est directe mais $F + G \neq \mathbb{R}^3$.

Regardons ensuite deux plans vectoriels F et G de $\mathbb{R}^3$ (non confondus)



$\mathbb{R}^3 = F + G$ mais la somme n'est pas directe

Enfin, considérons dans $\mathbb{R}^3$ un plan vectoriel F et une droite vectorielle G <u>non incluse dans F</u> :



F et G sont supplémentaires dans $\mathbb{R}^3$: $\boxed{\mathbb{R}^3 = F \oplus G}$ (*)

(*) Cela reste à prouver ! On attendra pour ça d'avoir les outils en lien avec la dimension.

Méthode (Montrer que deux s.e.v. F et G sont supplémentaires par analyse synthèse).

- On considère un vecteur $x \in E$.
- Analyse.
  On suppose l'existence d'un couple de vecteurs $(x_F, x_G) \in F \times G$ tel que $x = x_F + x_G$.
  On tâche d'exprimer x_F et x_G à l'aide de x. On trouve un *unique* couple candidat (x_F, x_G).
  L'unicité de la décomposition est alors prouvée : on sait en fin d'analyse que F et G sont en somme directe.
- Synthèse. On définit le couple (x_F, x_G) conformément à l'analyse et on vérifie qu'il convient.
  Plus précisément, on vérifie que $x_F \in F$, que $x_G \in G$, et enfin que $x = x_F + x_G$.

Exemple 51.

Soit $E = \mathbb{K}[X]$ et $a \in \mathbb{K}$. On note $F_a = \{P \in E \mid P(a) = 0\}$. Montrer que

$$E = F_a \oplus \text{Vect}(1).$$

2 Familles de vecteurs.

2.1 Familles génératrices.

Définition 52 (Famille génératrice (cas d'une famille finie)).

On dit qu'une famille $(x_1, \ldots, x_p) \in E^p$ **engendre** $\mathbb{K}$-espace vectoriel E (ou encore qu'elle est **génératrice**) si tout vecteur de E s'écrit comme combinaison linéaire des vecteurs de la famille :

$$\forall y \in E \quad \exists (\lambda_1, \ldots, \lambda_p) \in \mathbb{K}^p \quad y = \sum_{i=1}^{p} \lambda_i x_i.$$

De façon équivalente, $(x_1, \ldots, x_p) \in E^p$ engendre E si $E = \text{Vect}(x_1, \ldots, x_p)$.

Remarque. Si F est un s.e.v. d'un espace vectoriel E, parler de famille génératrice de F, c'est bien sûr parler d'une famille de vecteurs de F qui engendre l'*espace vectoriel* F.

Exemple 53 (Écrire un Vect, c'est trouver une famille génératrice).

Donner une famille génératrice de $S_2(\mathbb{R})$. Et pour $S_n(\mathbb{R})$?

Exemple 54 (Un espace, deux familles génératrices).

Dans l'espace vectoriel $E = \mathcal{D}^2(\mathbb{R})$, on considère l'ensemble $F = \left\{y \in E \;\middle|\; y'' - y = 0.\right\}$.

1. Prouver que F est un sous-espace vectoriel de E et donner une famille génératrice de F.
2. Justifier que la famille (ch, sh) est aussi une famille génératrice de F.

Définition 55 (Partie/famille génératrice quelconque).

Soit E un $\mathbb{K}$-espace vectoriel.

1. Soit $(x_i)_{i\in I}$ une famille de vecteurs de E. Elle engendre E si $E = \text{Vect}(x_i)_{i\in I}$, c'est à dire si
$$\forall y \in E \quad \exists n \in \mathbb{N}^* \quad \exists (i_1, \dots, i_n) \in I^n \quad \exists (\lambda_1, \dots, \lambda_n) \quad y = \sum_{k=1}^{n} \lambda_k x_{i_k}.$$
2. Soit A une partie de E. Elle engendre E si $E = \text{Vect}(A)$, c'est-à-dire si
$$\forall y \in E \quad \exists n \in \mathbb{N}^* \quad \exists (x_1, \dots, x_n) \in A^n \quad \exists (\lambda_1, \dots, \lambda_n) \quad y = \sum_{k=1}^{n} \lambda_k x_k.$$

On a bien sûr que la famille $(x_i)_{i\in I}$ engendre E ssi la partie $\{x_i, i \in I\}$ engendre E.

Proposition 56 (Sur-famille d'une famille génératrice).

Toute *sur-famille* d'une famille génératrice est une famille génératrice.

Par exemple, $(\text{ch}, \text{sh}, \exp)$ est aussi une famille génératrice du sous-espace $F = \{y \in \mathcal{D}^2(\mathbb{R}) : y'' - y = 0\}$. Sur cette famille génératrice, il n'y a pas unicité de l'écriture d'un vecteur de F. Par exemple,
$$\exp = 1 \cdot \text{ch} + 1 \cdot \text{sh} + 0 \cdot \exp \quad \text{ et } \quad \exp = 0 \cdot \text{ch} + 0 \cdot \text{sh} + 1 \cdot \exp.$$
La question de l'unicité de la décomposition d'un vecteur va être au coeur du paragraphe suivant.

2.2 Familles libres, liées.

Définition 57 (Famille libre, famille liée (cas d'une famille finie)).

Soit E un $\mathbb{K}$-espace vectoriel et $p \in \mathbb{N}^*$. On dit qu'une famille $(x_1, \dots, x_p) \in E^p$ est **libre** si
$$\forall (\lambda_1, \dots, \lambda_p) \in \mathbb{K}^p \qquad \sum_{i=1}^{p} \lambda_i x_i = 0_E \quad \Longrightarrow \quad \forall i \in [\![1, p]\!] \ \lambda_i = 0.$$
Une famille qui n'est pas libre est dite **liée**.

En français : $(x_1, \dots, x_p)$ est libre si la seule combinaison linéaire nulle des vecteurs $x_1, \dots, x_p$ est celle avec scalaires nuls. On dit aussi parfois des vecteurs d'une famille libre qu'ils sont **linéairement indépendants**.

Proposition 58 (Unicité de la décomposition sur une famille libre/Identifier les coefficients).

Soit E un $\mathbb{K}$-espace vectoriel et $(x_1, \dots, x_p)$ une famille libre de E. Alors
$$\forall (\lambda_1, \dots, \lambda_p) \in \mathbb{K}^p \quad \forall (\mu_1, \dots, \mu_p) \in \mathbb{K}^p \qquad \sum_{i=1}^{p} \lambda_i x_i = \sum_{i=1}^{p} \mu_i x_i \quad \Longrightarrow \quad \begin{cases} \lambda_1 & = & \mu_1 \\ \lambda_2 & = & \mu_2 \\ & \dots & \\ \lambda_p & = & \mu_p. \end{cases}$$

Exemples 59 (Familles libres)**.**

1. Dans l'espace $E = \mathcal{D}^2(\mathbb{R})$, montrer que $(\mathrm{ch}, \mathrm{sh})$ est libre, et que $(\mathrm{ch}, \mathrm{sh}, \exp)$ est liée.
2. On considère dans $\mathbb{R}^3$ les vecteurs
$$\overrightarrow{u_1} = (0,1,1) \qquad \overrightarrow{u_2} = (1,0,1) \qquad \overrightarrow{u_3} = (1,1,0)$$
Montrer que $(\overrightarrow{u_1}, \overrightarrow{u_2}, \overrightarrow{u_3})$ est une famille libre de $\mathbb{R}^3$.
3. Soit $p \in \mathbb{N}^*$. On se donne $(a_1, \dots, a_p) \in \mathbb{R}^p$ tel que $a_1 < a_2, \dots < a_p$, et on définit p fonctions $f_1, \dots, f_p$ par
$$\forall i \in [\![1,p]\!] \quad f_i : x \mapsto e^{a_i x}.$$
Montrer que $(f_1, \dots, f_p)$ est libre dans $\mathbb{R}^{\mathbb{R}}$.

Proposition 60 (Caractérisation des familles liées)**.**

Une famille de vecteurs est liée ssi l'un des vecteurs s'écrit comme combinaison linéaire des autres.

Proposition 61 (Deux cas particuliers simples et courants)**.**

1. Une famille composée d'un seul élément non nul est toujours libre.
2. Une famille contenant le vecteur nul est toujours liée.

Proposition 62.

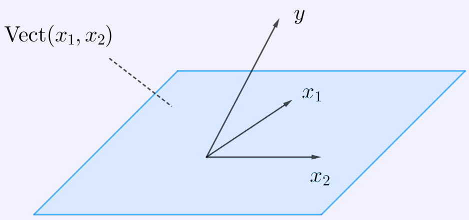
Toute *sous-famille* d'une famille libre est une famille libre.
Toute *sur-famille* d'une famille liée est liée.

En ôtant des vecteurs à une famille libre, on garde donc une famille libre. Et lorsqu'on en ajoute ?

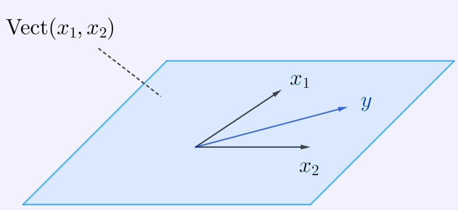
Proposition 63 (Ajout d'un vecteur à une famille libre)**.**

Soit $(x_1, \dots, x_p)$ est une famille libre dans un $\mathbb{K}$-espace vectoriel E, et y un vecteur de E.

$$(x_1, \dots, x_p, y) \text{ est liée} \iff y \in \mathrm{Vect}(x_1, \dots x_p).$$
$$(x_1, \dots, x_p, y) \text{ est libre} \iff y \notin \mathrm{Vect}(x_1, \dots x_p).$$



(x_1, x_2, y) libre

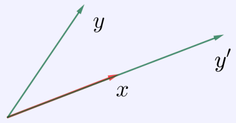


(x_1, x_2, y) liée

Corollaire 64 (Cas particulier de deux vecteurs)**.**

Dans un $\mathbb{K}$-espace vectoriel E, une famille de deux vecteurs est liée si et seulement si ces vecteurs sont *colinéaires*. Plus précisément, si $(x, y) \in E^2$,

$$(x, y) \text{ est liée} \iff (x = 0_E \text{ ou } \exists \alpha \in \mathbb{K}\ y = \alpha x).$$



Définition 65 (Famille libre, liée (cas d'une famille quelconque))**.**

Soit E un $\mathbb{K}$-espace vectoriel. On dit qu'une famille $(x_i)_{i \in I} \in E^I$ est **libre** si

$$\forall (\lambda_i)_{i \in I} \in \mathbb{K}^I \text{ presque nulle} \qquad \sum_{i \in I} \lambda_i x_i = 0_E \implies \forall i \in I \quad \lambda_i = 0.$$

Une famille qui n'est pas libre est dite **liée**. Par convention la *famille vide* est libre.

Soit A une partie de E. Il est facile de créer une famille de vecteurs où l'on met tous les vecteurs de A : c'est la famille $(x_a)_{a \in A}$, où on note $x_a = a$ pour tout $a \in A$. On dit que la partie A est **libre** si $(x_a)_{a \in A}$ l'est.

Méthode (Montrer qu'une famille de vecteurs *quelconque* est libre (rare !))**.**

Soit $(x_i)_{i \in I}$ une famille de vecteurs quelconque d'un espace vectoriel E.
Manipuler des familles de scalaires presque nulles revient à regarder des sous-familles **finies**. Ainsi, pour prouver que $(x_i)_{i \in I}$ est libre,

— on se donne n indices deux à deux distincts $i_1, \ldots, i_n$ dans I, où $n \in \mathbb{N}^*$,
— on prouve que $(x_{i_1}, \ldots, x_{i_n})$ est libre.

La proposition suivante sert d'exemple.

Proposition 66 (Condition suffisante pour qu'une famille de polynômes soit libre)**.**

Une famille de polynômes non nuls et de degrés deux à deux distincts est une famille libre.

Bien entendu, il existe des familles libres de polynômes où les degrés ne sont pas deux à deux distincts. Par exemple il est facile de voir que la famille $(X, X+1)$ est libre.

Les résultats démontrés pour les familles libres finies se généralisent à des parties/familles quelconques de vecteurs.

— On peut « identifier » les scalaires face à l'égalité de deux combinaisons linéaires, pour une famille libre quelconque.
— Toute sous-famille d'une famille libre est libre. Toute sur-famille d'une famille liée est liée.
— Si A est libre et alors $A \cup \{x\}$ est libre ssi $x \notin \mathrm{Vect}(A)$.

2.3 Bases.

Définition 67 (Base (cas d'une famille finie))**.**

Soit E un $\mathbb{K}$-espace vectoriel. On dit qu'une famille $(x_1, \dots, x_p) \in E^p$ est une **base** de E si tout vecteur de E s'écrit de manière unique comme combinaison linéaire des vecteurs de la famille :

$$\forall y \in E \quad \exists!\ (\lambda_1, \dots, \lambda_p) \in \mathbb{K}^p \quad y = \sum_{i=1}^{p} \lambda_i x_i.$$

On dit alors que $(\lambda_1, \dots, \lambda_p)$ est le p-uplet de **coordonnées** de y dans la base $(x_1, \dots, x_p)$.

Exemple 68 (Base canonique de $\mathbb{K}^n$)**.**

Pour tout $i \in [\![1, n]\!]$, on note $e_i = (0, \dots, 0, 1, 0, \dots, 0)$, où le 1 est écrit sur la $i$ème coordonnée. Tout n-uplet $(x_1, \dots, x_n)$ s'écrit

$$(x_1, \dots, x_n) = x_1(1, 0, \dots, 0) + x_2(0, 1, 0, \dots, 0) + \dots + x_n(0, \dots, 0, 1) = \sum_{i=1}^{n} x_i e_i.$$

et cette décomposition est unique. La famille $(e_1, \dots, e_n)$ est appelée **base canonique** de $\mathbb{K}^n$. Les coordonnées d'un n-uplet dans cette base sont tout simplement les coordonnées du n-uplet.

Exemple 69 (Base canonique de $\mathbb{K}_n[X]$, de $\mathbb{K}[X]$)**.**

Tout polynôme $P \in \mathbb{K}_n[X]$ s'écrit de manière unique $P = \sum_{k=0}^{n} a_k X^k$, avec $a_0, \dots, a_n \in \mathbb{K}$.

La famille de monômes $(1, X, X^2, \dots, X^n)$ est appelée **base canonique** de $\mathbb{K}_n[X]$.
Les coordonnées d'un polynôme dans cette base sont tout simplement ses coefficients.

Exemple 70 (Base canonique de $M_{n,p}(\mathbb{K})$)**.**

Pour tout couple $(i, j) \in [\![1, n]\!] \times [\![1, p]\!]$, on note $E_{i,j}$ la matrice de $M_{n,p}(\mathbb{K})$ dont tous les coefficients sont nuls sauf celui à la ligne i et à la colonne j qui vaut 1. La famille $(E_{i,j}, i \in [\![1, n]\!], j \in [\![1, p]\!])$ est une base de $M_{n,p}(\mathbb{K})$, dite **base canonique** de cet espace.
Les coordonnées d'une matrice dans cette base sont tout simplement ses coefficients.

Exemple 71.

La famille $(1, i)$ est une base du $\mathbb{R}$-espace vectoriel $\mathbb{C}$.

Quant au $\mathbb{C}$-espace vectoriel $\mathbb{C}$, la famille (1) en est une base.

Proposition 72 (Caractérisation des bases)**.**

Dans un e.v., une famille de vecteurs est une base si et seulement si elle est libre et génératrice.

Exemple 73.

On considère les sous-espaces vectoriels de $\mathcal{D}^2(\mathbb{R})$ ci-dessous :

$$F = \{y \in \mathcal{D}^2(\mathbb{R}) \mid y'' + y = 0\} \quad \text{et} \quad G = \{y \in \mathcal{D}^2(\mathbb{R}) \mid y'' - y = 0\}$$

Donner une base de F et deux bases de G.

Le lien fait ci-dessous entre bases et supplémentaires servira dans le cours sur la dimension finie.

Lemme 74 (Construction de deux supplémentaires à partir d'une base)**.**

Soit E un espace vectoriel admettant une base $(e_1, \dots, e_n)$, avec $n \in \mathbb{N}^*$. Soit $p \in [\![1, n]\!]$. Alors

$$E = \operatorname{Vect}(e_1, \dots, e_p) \oplus \operatorname{Vect}(e_{p+1}, \dots, e_n).$$

Définition 75 (Base (cas d'une famille quelconque))**.**

Soit E un $\mathbb{K}$-espace vectoriel. On dit qu'une famille $(x_i)_{i \in I} \in E^I$ est une **base** de E si

$$\forall y \in E \quad \exists!\ (\lambda_i) \in \mathbb{K}^I \text{ presque nulle} \quad y = \sum_{i \in I} \lambda_i x_i.$$

Exemple 76 (Base canonique de $\mathbb{K}[X]$)**.**

La famille $(X^k)_{k \in \mathbb{N}}$ est une base de $\mathbb{K}[X]$, appelée **base canonique**.

Exemple 77 (Base de ....)**.**

Soit $a \in \mathbb{K}$. Justifier que la famille $\big((X-a)^k\big)_{k \in \mathbb{N}}$ est une base de l'espace $\mathbb{K}[X]$.

Exemple 78 (Ceci n'est pas une base)**.**

On définit $(e^{(n)})_{n \in \mathbb{N}}$ une famille de suites réelles par

$$\forall (n, k) \in \mathbb{N}^2 \quad e_k^{(n)} = \delta_{n,k}.$$

La famille $(e^{(n)})_{n \in \mathbb{N}}$ est libre dans $\mathbb{R}^{\mathbb{N}}$ mais n'est pas une base de cet espace : par exemple, la suite constante égale à 1 ne saurait s'écrire comme combinaison linéaire de ces vecteurs.

Exercices

Espaces vectoriels, sous-espaces vectoriels.

$\boxed{\textbf{27.1}}$ **[♦◇◇]** Soit $E = \mathbb{R}^{\mathbb{N}}$ l'ensemble des suites réelles.
Notons F l'ensemble des suites bornées et G l'ensemble des suites qui tendent vers 0.

1. Démontrer que G est un sous-espace vectoriel de E.
2. Démontrer que F est un sous-espace vectoriel de E.
3. Pourquoi peut-on dire que G est un s.e.v. de F ?

$\boxed{\textbf{27.2}}$ **[♦◇◇]** Être ou ne pas être un sous-espace vectoriel.
Dans chacun des cas suivants, justifier que l'ensemble F_i donné est un s.e.v. de l'espace vectoriel E_i donné.

1. $E_1 = \mathbb{R}^3$ et $F_1 = \{(x, y, x + y), x, y \in \mathbb{R}\}$.
2. $E_2 = M_n(\mathbb{R})$ et $F_2 = \{M \in E_2 : \ \mathrm{Tr}(M) = 0\}$.
3. $E_3 = M_n(\mathbb{R})$. On fixe $A \in M_n(\mathbb{R})$ et on définit $F_3 = \{M \in M_n(\mathbb{R}) : AM = MA\}$ (l'ensemble des matrices commutant avec la matrice A).

$\boxed{\textbf{27.3}}$ **[♦♦◇]** Fonctions à variations bornées.
Soit $E = \mathcal{F}(I, \mathbb{R})$ l'ensemble des fonctions définies sur un intervalle I de $\mathbb{R}$ et

$$V = \{f - g, \quad f \ \text{ et } g \text{ croissantes sur } I\}.$$

Montrer que V est un sous-espace vectoriel de E.

$\boxed{\textbf{27.4}}$ **[♦♦◇]** Soit $j = e^{\frac{2i\pi}{3}}$. On définit les trois vecteurs de $\mathbb{C}^3$

$$u = (1, j, j^2), \qquad v = (1, j^2, j), \qquad w = (j, j^2, 1).$$

Démontrer que

$$\mathrm{Vect}(u, v, w) = \left\{(x, y, z) \in \mathbb{C}^3 \quad x + y + z = 0\right\}.$$

$\boxed{\textbf{27.5}}$ **[♦♦♦]** Soit E un $\mathbb{K}$-espace vectoriel, et F et G deux s.e.v. de E. Montrer :

$$F \cup G \text{ est un sous-espace vectoriel de } E \quad \Longleftrightarrow \quad F \subset G \text{ ou } G \subset F.$$

$\boxed{\textbf{27.6}}$ **[♦♦♦]** Soit $B \in \mathbb{K}[X]$ un polynôme non nul.
On considère $\rho : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K}[X] \\ P & \mapsto & R \end{array} \right.$, où R est le reste dans la division euclidienne de P par B.

1. Prouver que ρ est un endomorphisme de $\mathbb{K}[X]$.
2. Exprimer Im ρ à l'aide de $b = \deg B$.
3. Décrire Ker ρ.

Sommes.

$\boxed{\textbf{27.7}}$ **[♦♦◇]** Soit $E = \mathbb{R}^{\mathbb{R}}$ l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$. Notons P l'ensemble des fonctions paires sur $\mathbb{R}$ et I celui des fonctions impaires.

1. Justifier que P et I sont deux sous-espaces vectoriels de E.
2. Par analyse-synthèse, démontrer que $E = P \oplus I$.

$\boxed{\textbf{27.8}}$ **[♦♦◇]** Soit E l'ensemble des suites réelles convergentes et F celui des suites réelles de limite nulle.

1. Démontrer que E est un sous-espace vectoriel de $\mathbb{R}^{\mathbb{N}}$. On admettra que de la même façon, F est un sous-espace vectoriel de E.
2. Soit c la suite constante égale à 1. Prouver que

$$E = F \oplus \mathrm{Vect}(c).$$

27.9 **[♦♦◇]**
Soit $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}$. On note $P\mathbb{K}[X]$ l'ensemble des polynômes de $\mathbb{K}[X]$ divisibles par P.

1. Justifier que $P\mathbb{K}[X]$ est un sous-espace vectoriel de E.
2. Démontrer que $\mathbb{K}[X] = \mathbb{K}_{n-1}[X] \oplus P\mathbb{K}[X]$.

27.10 **[♦♦♦]** Soit E un $\mathbb{K}$-espace vectoriel et F, G, H trois sous-espaces vectoriels de E tels que

$$\begin{cases} F + G = F + H = F + (G \cap H) \\ F \cap G = F \cap H \end{cases}$$

Montrer que $G = H$.

Familles de vecteurs.

27.11 **[♦◇◇]** Montrer les vecteurs $(1, 0, 1, 0)$, $(0, 1, 0, 1)$ et $(1, 2, 3, 4)$ forment une famille libre de $\mathbb{R}^4$.

27.12 **[♦◇◇]** Montrer que les suites $u = (1)_{n\in\mathbb{N}}$, $v = (n)_{n\in\mathbb{N}}$, $w = (2^n)_{n\in\mathbb{N}}$ forment une famille libre de $\mathbb{R}^{\mathbb{N}}$.

27.13 **[♦♦◇]** Soit $p \in \mathbb{N}^*$ et $q_1 < q_2 \cdots < q_p$ p réels strictement positifs.
Pour $k \in [\![1, p]\!]$, on note $a^{(k)}$ la suite géométrique de raison q_k et de premier terme 1.
Montrer que $(a^{(1)}, \ldots, a^{(p)})$ est libre.

27.14 **[♦♦◇]** Soit $f \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ telle que $\mathrm{Im}(f)$ est un ensemble infini.
Démontrer que $(f^i, i \in \mathbb{N})$ est une famille libre de $\mathcal{F}(\mathbb{R}, \mathbb{R})$.

27.15 **[♦♦♦]** Déterminer les fonctions $f \in \mathbb{R}^{\mathbb{R}}$ telles que :

1. f est dérivable et (f, f') est une famille liée ;
2. f est deux fois dérivable et (f, f', f'') est une famille liée.

27.16 **[♦♦◇]** Soit $u : E \to F$ une application <u>linéaire</u> et $(e_i)_{i\in I} \in E^I$.

1. Montrer que si u est injective et si $(e_i)_{i\in I}$ est libre, la famille $(u(e_i))_{i\in I}$ est libre.
2. Montrer que si u est surjective et si $(e_i)_{i\in I}$ engendre E, la famille $(u(e_i))_{i\in I}$ engendre F.

27.17 **[♦◇◇]** Pour chacun des ensembles ci-dessous, prouver qu'il s'agit d'un espace vectoriel et en donner une base.

$$F = \{\alpha X^3 + \beta X + \alpha + \beta, \quad (\alpha, \beta) \in \mathbb{R}^2\}.$$

$$G = \{(x, y, z, t) \in \mathbb{R}^4 : x + 2y + z - t = 0 \quad \text{et} \quad 2x + 4y + z + 3t = 0\}.$$

On pourra commencer par écrire chacun des ensembles comme un Vect.

27.18 **[♦◇◇]** Soit $n \in \mathbb{N}$. On définit, pour tout $k \in [\![0, n]\!]$, $P_k = \sum\limits_{i=0}^{k} X^i$.
Démontrer que $(P_k)_{0\leq k\leq n}$ est une base de $\mathbb{R}_n[X]$.
Quelles sont les coordonnées de $1_{\mathbb{R}[X]}$ dans cette base ? et celles de X^n ?

27.19 **[♦♦◇]** Interpolation de Lagrange
Soit $(x_1, \ldots, x_n)$ un n-uplet de réels deux à deux distincts et $(L_1, \ldots, L_n)$ la famille des polynômes de Lagrange associés.
Montrer que cette famille est une base de $\mathbb{R}_{n-1}[X]$.
Donner les coordonnées d'un polynôme P sur cette base.

---

28 Espaces vectoriels de dimension finie

Dans ce cours $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$ et les lettres n et p des entiers naturels non nuls.
Sauf mention explicite du contraire, les familles de vecteurs manipulées sont finies.

Convention.

Convenons que dans un $\mathbb{K}$-espace vectoriel E la famille vide $()$ est libre et qu'elle engendre $\{0_E\}$.

1 Espaces de dimension finie.

1.1 Définition et exemples.

Définition 1.

Un espace vectoriel est dit de **dimension finie** si il est engendré par une famille finie de vecteurs.
Sinon, on dira que E est de **dimension infinie**.

Exemples.

- L'espace nul $\{0_E\}$ est de dimension finie : la famille vide () en est une base, par convention.
  Attention : (0_E) engendre l'espace nul mais n'est pas une famille libre.

- Les espaces $\mathbb{K}^n$, $\mathbb{K}_n[X]$, et $M_{n,p}(\mathbb{K})$ sont de dimension finie : on connait pour chacun au moins une base (donc une famille génératrice) :
  — pour $\mathbb{K}^n$, la base canonique $(e_1, \ldots, e_n)$;
  — pour $\mathbb{K}_n[X]$, la base canonique $(1, X, \ldots, X^n)$;
  — pour $M_{n,p}(\mathbb{K})$, la base canonique $(E_{i,j}, i \in [\![1, n]\!], j \in [\![1, p]\!])$.

- L'espace $\mathbb{K}[X]$ est de dimension infinie ; on le montre par l'absurde.

1.2 Existence de bases en dimension finie.

Lemme 2 (de la base extraite)**.**

Si $(x_i)_{1 \leqslant i \leqslant n}$ engendre un $\mathbb{K}$-ev E et si $(x_i)_{i \in I}$ est libre pour une certaine partie I de $\{1, \ldots, n\}$, alors il existe une partie J de $\{1, \ldots, n\}$ contenant I pour laquelle $(x_j)_{j \in J}$ est une base de E.

Théorème 3 (de la base extraite)**.**

De toute famille génératrice d'un espace vectoriel de dimension finie, on peut extraire une base.

Théorème 4 (de la base incomplète)**.**

Dans un espace vectoriel de dimension finie, toute famille libre peut être complétée en une base.

Corollaire 5 (Existence des bases en dimension finie)**.**

Tout espace vectoriel de dimension finie possède une base.

1.3 Cardinaux des familles de vecteurs en dimension finie

Lemme 6.

Dans un espace vectoriel engendré par n vecteurs ($n \in \mathbb{N}$), toute famille de $n+1$ vecteurs est liée.

Théorème 7.

Dans un espace vectoriel de dimension finie, toutes les bases ont même cardinal.

2 Dimension d'un espace de dimension finie.

2.1 Dimension : définition et exemples.

Nous avons prouvé dans la première partie que tout espace vectoriel de dimension finie possède une base. On sait aussi désormais que toutes les bases ont même cardinal. La définition suivante a donc un sens.

Définition 8.

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie.
On appelle **dimension** de E et on note $\dim(E)$ le cardinal commun de ses bases.

Exemple 9 (Dimensions usuelles)**.**

$\boxed{\dim\left(\mathbb{K}^n\right) = n}$ $\boxed{\dim\left(\mathbb{K}_n[X]\right) = n+1}$ $\boxed{\dim\left(M_{n,p}(\mathbb{K})\right) = np}$ $\boxed{\dim\left(M_n(\mathbb{K})\right) = n^2}$.

Exemple 10 (Un calcul de dimension)**.**

Montrer que $\left\{\begin{pmatrix} a & b \\ c & a \end{pmatrix}, a, b, c \in \mathbb{R}\right\}$ est un $\mathbb{R}$-e.v. de dimension finie et calculer sa dimension.

Proposition 11.

Soit $m \in \mathbb{N}^*$ et $E_1, \ldots, E_m$ des $\mathbb{K}$-espaces vectoriels de dimension finie.

Leur produit $E_1 \times \cdots \times E_m$ est un $\mathbb{K}$-espace vectoriel de dimension finie et

$$\dim\left(E_1 \times \cdots \times E_m\right) = \sum_{k=1}^{m} \dim E_k.$$

2.2 Familles de vecteurs et dimension.

Proposition 12 (Cardinal d'une famille et dimension de l'espace)**.**

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie ; on note $n = \dim E$.
Soit $(x_1, \ldots, x_p) \in E^p$ une famille de vecteurs de cardinal p.

1. Si $(x_1, \ldots, x_p)$ est génératrice, alors $p \geq n$.
   (le cardinal d'une famille génératrice est minoré par la dimension)
2. Si $(x_1, \ldots, x_p)$ est libre, alors $p \leq n$.
   (le cardinal d'une famille libre est majoré par la dimension)
3. Si $p > n$, alors $(x_1, \ldots, x_p)$ est liée.

Exemple 13.

Soit $M \in M_n(\mathbb{K})$.

1. Justifier que la famille $(I_n, M, M^2, \dots, M^{n^2})$ est liée.
2. « Toute matrice carrée possède un *polynôme annulateur* non trivial ». Expliquer.

Théorème 14 (Caractérisation des bases en dimension finie)**.**

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie notée n. Soit $\mathcal{B}$ une famille finie de vecteurs de E. Il y a équivalence entre :

1. $\mathcal{B}$ est une base de E ;
2. $\mathcal{B}$ est une famille libre ayant n vecteurs ;
3. $\mathcal{B}$ est une famille génératrice ayant n vecteurs.

En combinant les deux résultats précédents, on peut déclarer qu'en dimension finie,
— les bases sont exactement les familles libres de cardinal maximal ;
— les bases sont exactement les familles génératrices de cardinal minimal.

Exemple 15.

Soient $\overrightarrow{u} = (1,0,0)$, $\overrightarrow{v} = (2,1,0)$, $\overrightarrow{w} = (3,2,1)$. Démontrer que $(\overrightarrow{u}, \overrightarrow{v}, \overrightarrow{w})$ est une base de $\mathbb{R}^3$.

Proposition 16 (Condition suffisante pour avoir une base d'un espace de polynômes)**.**

Soit $n \in \mathbb{N}$ et $(P_k)_{k \in [\![0,n]\!]}$ une famille de polynômes telle que

$$\forall k \in [\![0,n]\!] \quad \deg P_k = k.$$

Alors $(P_k)_{k \in [\![0,n]\!]}$ est une base de $\mathbb{K}_n[X]$, dite de **degrés échelonnés**.

Si $(P_k)_{k \in \mathbb{N}}$ est une famille de polynômes telle que $\forall k \in \mathbb{N}\ \deg P_k = k$, alors c'est une base de $\mathbb{K}[X]$

Dans l'exemple ci-dessous, on constate que la condition sur les degrés échelonnés n'est pas *nécessaire* pour avoir une base d'un espace de polynômes.

Exemple 17 (Polynômes de Lagrange)**.**

Soit $x_1, \dots, x_n$ n scalaires de $\mathbb{K}$ deux à deux distincts et $(L_1, \dots, L_n)$ la famille définie par

$$\forall i \in [\![1,n]\!] \quad L_i = \pi_i^{-1} \prod_{\substack{k=1 \\ k \neq i}}^{n} (X - x_k) \qquad \text{où } \pi_i = \prod_{\substack{k=1 \\ k \neq i}}^{n} (x_i - x_k).$$

Démontrer que $(L_1, \dots, L_n)$ est une base de $\mathbb{K}_{n-1}[X]$.

2.3 Rang d'une famille finie de vecteurs.

Considérons un espace vectoriel E (qu'on ne suppose pas nécessairement de dimension finie) et dans cet espace vectoriel, considérons p vecteurs. Cette famille finie de vecteurs engendre (par définition !) un espace de dimension finie. La dimension de cet espace est inférieure à p, cardinal d'une famille génératrice. On va donner à cette dimension le nom de *rang*.

Définition 18.

Soit $(x_1, \ldots, x_p) \in E^p$, où E est un $\mathbb{K}$-espace vectoriel. On appelle **rang** de la famille $(x_1, \ldots, x_p)$, noté $\mathrm{rg}(x_1, \ldots, x_p)$ la dimension de l'espace vectoriel engendré par cette famille :

$$\mathrm{rg}(x_1, \ldots, x_p) = \dim\left(\mathrm{Vect}(x_1, \ldots, x_p)\right).$$

De façon cohérente avec ce qui précède, convenons que le rang de la famille vide () vaut 0.

Proposition 19 (Rang et cardinal d'une famille)**.**

Soit E un espace vectoriel et $(x_1, \ldots, x_p) \in E^p$ une famille de vecteurs. On a

$$\mathrm{rg}(x_1, \ldots, x_p) \leq p.$$

Le cas d'égalité caractérise les familles finies libres :

$$\mathrm{rg}(x_1, \ldots, x_p) = p \quad \text{ssi} \quad (x_1, \ldots, x_p) \text{ est libre.}$$

Corollaire 20 (Caractérisation des bases par le rang)**.**

Dans un espace de dimension n, les bases sont exactement les familles de n vecteurs de rang n.

Méthode (Calcul du rang d'une famille de vecteurs.)**.**

Par élimination de vecteurs superflus dans l'écriture d'un Vect (combinaisons linéaires des autres), on essaie de se ramener à une famille libre, pour laquelle nous savons que son rang est égal à son cardinal.

Exemple 21.

Calculer le rang des familles de vecteurs ci-dessous :

1. $(\overrightarrow{u}, \overrightarrow{v}, \overrightarrow{w})$, avec $\overrightarrow{u} = (1, 2, 3)$, $\overrightarrow{v} = (4, 5, 6)$, $\overrightarrow{w} = (7, 8, 9)$.
2. $(\sin, \exp, \mathrm{ch}, \mathrm{sh})$;
3. $(P_1, P_2, P_3, P_4, P_5)$, avec

$$P_1 = 1, \quad P_2 = X + 1, \quad P_3 = 2X - 3, \quad P_4 = X^2 + 3X + 4, \quad P_5 = 2X^2 + 3.$$

2.4 Le cas des dimensions 1 et 2.

Définition 22.

Un $\mathbb{K}$-espace vectoriel de dimension 1 est appelé **droite** vectorielle.
Un $\mathbb{K}$-espace vectoriel de dimension 2 est appelé **plan** vectoriel.

Remarque. Pour un $\mathbb{K}$-espace vectoriel de E, et un sous-espace vectoriel F, on dira que F est une "droite vectorielle de E" si F (en tant qu'espace vectoriel) est de dimension 1. On parlera de F comme d'un "plan vectoriel de E" si F est de dimension 2.

Proposition 23 (Description d'un plan, d'une droite vectorielle)**.**

Soit un $\mathbb{K}$-espace vectoriel E

$$E \text{ est une droite} \iff \exists x \in E \setminus \{0_E\} \ : \ E = \mathrm{Vect}(x).$$

$$E \text{ est un plan} \iff \exists (x, x') \in E^2 \ \underline{\text{libre}} \ : \ E = \mathrm{Vect}(x, x').$$

Ci-dessous, quelques exemples issus du cours d'analyse.

Exemple 24 (EDL1 homogène)**.**

Soit $a : I \to \mathbb{K}$ une fonction continue. On pose $S_0^a = \{y \in \mathcal{D}(I, \mathbb{K}) \ \mid y' + ay = 0\}$.

L'ensemble S_0^a est une <u>droite vectorielle</u> engendrée par la fonction $u : x \mapsto e^{-A(x)}$ avec A primitive de a :

$$\boxed{S_0^a = \mathrm{Vect}(u)}.$$

Exemple 25 (EDL2 homogène à coeff constants, cas complexe)**.**

Soit $(a, b) \in \mathbb{C}^2$. On pose $S_0^{a,b} = \left\{y \in \mathcal{D}^2(I, \mathbb{C}) \ \mid y'' + ay' + by = 0\right\}$.

L'ensemble $S_0^{a,b}$ est un <u>plan vectoriel</u>. On en donne ci-dessous une base.

- Si l'équation caractéristique $x^2 + ax + b = 0$ a deux solutions distinctes r_1 et r_2, alors

$$\boxed{S_0^{a,b} = \mathrm{Vect}\,(u, v)}$$

  et (u, v) est une base de $S_0^{a,b}$, où $u : x \mapsto e^{r_1 x}$ et $v : x \mapsto e^{r_2 x}$.
- Si l'équation caractéristique $x^2 + ax + b = 0$ a une racine double r, alors

$$\boxed{S_0^{a,b} = \mathrm{Vect}\,(\tilde{u}, \tilde{v})}$$

  et $(\tilde{u}, \tilde{v})$ est une base de $S_0^{a,b}$, où $\tilde{u} : x \mapsto e^{rx}$ et $\tilde{v} : x \mapsto xe^{rx}$.

Exemple 26 (SRL2 homogène à coeff constants, cas complexe).

Soit $(a,b) \in \mathbb{C}^* \times \mathbb{C}$. On pose $S_0^{a,b} = \left\{u \in \mathbb{C}^{\mathbb{N}} \ \mid \forall n \in \mathbb{N}\ u_{n+2} = au_{n+1} + bu_n\right\}$.

L'ensemble $S_0^{a,b}$ est un plan vectoriel. On en donne ci-dessous une base.

- Si l'équation caractéristique $x^2 - ax - b = 0$ a deux solutions distinctes r_1 et r_2, alors

$$\boxed{S_0^{a,b} = \text{Vect}\,(u,v)}$$

et (u,v) est une base de $S_0^{a,b}$, où $u = (r_1^n)_{n\in\mathbb{N}}$ et $v = (r_2^n)_{n\in\mathbb{N}}$ (couple de suites géométriques).
- Si l'équation caractéristique $x^2 - ax - b = 0$ a une racine double r, alors

$$\boxed{S_0^{a,b} = \text{Vect}\,(\tilde{u},\tilde{v})}$$

et $(\tilde{u},\tilde{v})$ est une base de $S_0^{a,b}$, où $\tilde{u} = (r^n)_{n\in\mathbb{N}}$ et $\tilde{v} = (nr^n)_{n\in\mathbb{N}}$.

3 Sous-espaces vectoriels et dimension finie.

3.1 Sous-espaces d'un espace vectoriel de dimension finie.

Théorème 27 (Sous-espace en dimension finie).

Soit E un $\mathbb{K}$ espace vectoriel de dimension finie et F un sous-espace vectoriel de E.

1. Le sous-espace F est un espace de dimension finie et $\dim(F) \leq \dim(E)$.
2. Il y a égalité dans l'inégalité ci-dessus si et seulement si $F = E$.

Corollaire 28 (Caractérisation en dimension finie de l'égalité de deux s.e.v.).

Soit E un $\mathbb{K}$-espace vectoriel et deux s.e.v. F et G de dimension finie.

$$F = G \quad \Longleftrightarrow \quad \begin{cases} F \subset G \\ \dim(F) = \dim(G) \end{cases}$$

Remarque. Ce résultat remplacera parfois avantageusement la caractérisation par double-inclusion !

Exemple 29 (Sous-espaces vectoriels d'un espace de dimension 2).

Soit E un $\mathbb{K}$-espace vectoriel de dimension 2.
Ses sous-espaces vectoriels sont de dimension 0, 1 ou 2. Plus précisément,

— le sous-espace vectoriel nul $\{0_E\}$ est l'unique sous-espace vectoriel de dimension 0 ;
— les sous-espaces de dimension 1 sont (par définition) les droites vectorielles de E ;
— E est l'unique sous-espace vectoriel de E de dimension 2.

Exemple 30 (Sous-espaces vectoriels d'un espace de dimension 3)**.**

Soit E un $\mathbb{K}$-espace vectoriel de dimension 3.
Ses sous-espaces vectoriels sont de dimension 0, 1, 2 ou 3. Plus précisément,
- le sous-espace vectoriel nul $\{0_E\}$ est l'unique sous-espace vectoriel de dimension 0 ;
- les sous-espaces de dimension 1 sont (par définition) les droites vectorielles de E ;
- les sous-espaces de dimension 2 sont (par définition) les plans vectoriels de E ;
- E est l'unique sous-espace vectoriel de E de dimension 3.

Théorème 31.

Dans un espace vectoriel de dimension finie, tout sous-espace vectoriel possède un supplémentaire.

3.2 Somme de sous-espaces de dimension finie.

Proposition 32.

Dans un espace vectoriel donné, si F et G sont deux sous-espaces tous deux de dimension finie, alors leur somme $F + G$ est de dimension finie.

En concaténant deux familles génératrices respectivement de F et G, on obtient une famille génératrice de $F + G$.

Proposition-Définition 33.

Dans un espace vectoriel donné, si F et G sont deux sous-espaces tous deux de dimension finie et en somme directe, alors en concaténant une base de F et une base de G, on obtient une base de $F \oplus G$.

Une telle base est appelée **base adaptée** à la somme directe $F \oplus G$.

Corollaire 34 (Dimension d'une somme directe)**.**

Dans un espace vectoriel E, si F et G sont deux sous-espaces vectoriels de dimension finie, en somme directe, alors $F \oplus G$ est de dimension finie et

$$\boxed{\dim(F \oplus G) = \dim(F) + \dim(G)}.$$

Théorème 35 (Formule de Grassmann)**.**

Soit E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels de dimension finie.
La somme $F + G$ est de dimension finie et

$$\boxed{\dim(F + G) = \dim(F) + \dim(G) - \dim(F \cap G)}.$$

3.3 Supplémentaires en dimension finie.

On a prouvé qu'en dimension finie, tout sous-espace vectoriel possède un supplémentaire. Dans les cas non dégénérés, il y a une infinité de supplémentaires distincts, mais on va voir qu'ils ont tous la même dimension.

Proposition 36 (Dimension d'un supplémentaire)**.**

Soient F et G deux sous-espaces vectoriels supplémentaires dans un même espace vectoriel E de dimension finie. Alors
$$\dim(G) = \dim(E) - \dim(F).$$

Théorème 37 (Caractérisation des supplémentaires en dimension finie)**.**

Soient E un espace vectoriel de dimension finie, et F et G deux sous-espaces de E. On a les deux caractérisations suivantes :

1. $E = F \oplus G \iff \left\{ \begin{array}{rcl} F \cap G & = & \{0_E\} \\ \dim(E) & = & \dim(F) + \dim(G). \end{array} \right.$
2. $E = F \oplus G \iff \left\{ \begin{array}{rcl} E & = & F + G \\ \dim(E) & = & \dim(F) + \dim(G). \end{array} \right.$

Exemple 38.

Soit P un plan vectoriel de $\mathbb{R}^3$ et D une droite vectorielle non incluse dans P.
Démontrer que P et D sont supplémentaires dans $\mathbb{R}^3$.

Preuve Lemme 6. L'assertion est claire pour $n=0$ (n'est-ce pas ?) On va ensuite faire une récurrence sur $\mathbb{N}^*$. Pour $n \in \mathbb{N}^*$, notons $\mathcal{P}(n)$ l'assertion du lemme.

- Initialisation ($n=1$). Soit E un espace vectoriel engendré par un vecteur x. En bref, deux vecteurs de E vont être colinéaires à x donc colinéaires tous les deux et former une famille liée. Détaillons, en considérant deux vecteurs y_1 et y_2 dans $E = \mathrm{Vect}(x)$. Il existe deux scalaires λ_1 et λ_2 tels que $y_1 = \lambda_1 x$ et $y_2 = \lambda_2 x$. On a alors
$$\lambda_2 y_1 - \lambda_1 y_2 = 0_E.$$
Dans le cas où $\lambda_1 \neq 0$, ceci prouve que (y_1, y_2) est liée.
Dans le cas où $\lambda_1 = 0$, on obtient $y_1 = \lambda_1 x = 0_E$, ce qui donne encore que (y_1, y_2) est liée. $\underline{\mathcal{P}(1) \text{ est démontrée.}}$
- Hérédité. Soit $n \in \mathbb{N}^*$. Supposons $\mathcal{P}(n)$ et montrons $\mathcal{P}(n+1)$. Pour cela, considérons un $\mathbb{K}$-espace vectoriel E engendré par $n+1$ vecteurs $(x_1, \dots, x_{n+1})$, ainsi que $n+2$ vecteurs $(y_1, \dots, y_{n+2})$ dans E. On va décomposer chaque y_i sur la famille des x_j : il existe $(\lambda_{i,j}) \in M_{n+2,n+1}(\mathbb{K})$ telle que
$$\left\{\begin{array}{ccccccccc} y_1 & = & \lambda_{1,1}\ x_1 & + & \lambda_{1,2}\ x_2 & + & \cdots & + & \lambda_{1,n+1}\ x_{n+1} \\ y_2 & = & \lambda_{2,1}\ x_1 & + & \lambda_{2,2}\ x_2 & + & \cdots & + & \lambda_{2,n+1}\ x_{n+1} \\ \vdots & & & & & & & & \\ y_{n+2} & = & \lambda_{n+2,1}\ x_1 & + & \lambda_{n+2,2}\ x_2 & + & \cdots & + & \lambda_{n+2,n+1}\ x_{n+1} \end{array}\right.$$
Pour se ramener à $n+1$ vecteurs décomposés sur n, on va faire des opérations élémentaires sur les lignes.
    - · Premier cas : $\lambda_{1,1} = \lambda_{2,1} = \cdots = \lambda_{n+2,1} = 0$.
    Alors, $(y_1, \dots, y_{n+1})$ est une famille de $n+1$ vecteurs de l'espace vectoriel $F = \mathrm{Vect}(x_2, \dots, x_{n+1})$, engendré par n vecteurs. D'après $\mathcal{P}(n)$, cette famille est liée, ce qui est vrai a fortiori pour $(y_1, \dots, y_{n+2})$.
    - · Second cas : l'un des coefficient sur la première colonne est non nul. Quitte à faire un échange, on peut supposer qu'il s'agit de $\lambda_{1,1}$, qui est alors un pivot. Pour $i \in [\![2, n+2]\!]$, l'opération $L_i \leftarrow L_i - \frac{\lambda_{i,1}}{\lambda_{1,1}} L_1$ amène
    $$\left\{\begin{array}{ccc} y_2 - \frac{\lambda_{2,1}}{\lambda_{1,1}} y_1 & = & \sum_{j=2}^{n+1} \left(\lambda_{2,j} - \frac{\lambda_{2,1}}{\lambda_{1,1}}\right) x_j \\ \vdots & & \\ y_{n+2} - \frac{\lambda_{n+2,1}}{\lambda_{1,1}} y_1 & = & \sum_{j=2}^{n+1} \left(\lambda_{n+2,j} - \frac{\lambda_{n+2,1}}{\lambda_{1,1}}\right) x_j \end{array}\right.$$
    Pour $k \in [\![2, n+2]\!]$, posons $z_k := y_k - \frac{\lambda_{k,1}}{\lambda_{1,1}} y_1$. Les vecteurs $(z_2, \dots, z_{n+2})$ sont une famille de $n+1$ vecteurs de l'espace vectoriel $F = \mathrm{Vect}(x_2, \dots, x_{n+1})$, engendré par n vecteurs. D'après $\mathcal{P}(n)$, cette famille est liée : il existe $\mu_2 \dots, \mu_{n+2}$, non tous nuls tels que $\sum_{i=2}^{n+2} \mu_i z_i = 0_E$. On a donc
    $$\sum_{i=2}^{n+2} \mu_i y_i - \sum_{i=2}^{n+2} \frac{\mu_i \lambda_{i,1}}{\lambda_{1,1}} y_1 = 0_E,$$
    avec les μ_i non tous nuls, ce qui démontre que la famille $(y_1, \dots, y_{n+2})$ est liée.

  Dans les deux cas, notre famille de $n+2$ vecteurs est liée : $\mathcal{P}(n+1)$ est liée. Le principe de récurrence s'applique, ce qui termine la preuve du lemme.

□

Exercices

$\boxed{\textbf{28.1}}$ **[♦◇◇]** Ci-dessous, se trouve un s.e.v. de $M_2(\mathbb{R})$. Le démontrer et calculer sa dimension :
$$F = \{M \in M_2(\mathbb{R}) : \mathrm{Tr}(M) = 0\}.$$

$\boxed{\textbf{28.2}}$ **[♦◇◇]** Montrer que la famille (M_1, M_2, M_3, M_4) est une base de $M_2(\mathbb{R})$, avec

$$M_1 = I_2, \quad M_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad M_3 = \begin{pmatrix} 6 & 6 \\ 6 & 0 \end{pmatrix}, \quad M_4 = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

$\boxed{\textbf{28.3}}$ **[♦◇◇]**

Montrer que l'ensemble des suites réelles 3-périodiques est de dimension finie et calculer sa dimension.

$\boxed{\textbf{28.4}}$ **[♦♦◇]** Pour $k \in [\![0, n]\!]$, on pose $P_k = X^k(1-X)^{n-k}$. Montrer que $(P_0, \dots, P_n)$ est une base de $\mathbb{K}_n[X]$.

$\boxed{\textbf{28.5}}$ **[♦♦◇]** Soient $\mathcal{B} = (e_1, \dots, e_n)$ et $\mathcal{B}' = (e'_1, \dots, e'_n)$ deux bases de E, $\mathbb{K}$-ev de dimension finie. Montrer qu'il existe $j \in [\![1, n]\!]$ tel que $(e_1, \dots, e_{n-1}, e'_j)$ est une base de E.

$\boxed{\textbf{28.6}}$ **[♦♦◇]** Soit $E = \mathcal{F}(\mathbb{R}, \mathbb{R})$ le $\mathbb{R}$-espace vectoriel des fonctions réelles de la variable réelle.

1. Pour $a \in \mathbb{R}$, on note $f_a : x \mapsto e^{ax}$. Montrer que $(f_a)_{a\in\mathbb{R}}$ est une famille libre de E.
2. Déduire de ce qui précède que E n'est pas de dimension finie.

$\boxed{\textbf{28.7}}$ **[♦♦◇]** Soient $n \in \mathbb{N}^*$ et $(\lambda_k)_{0\leq k\leq n} \in \mathbb{K}^{n+1}$ tels que $\sum_{k=0}^{n} \lambda_k (X+k)^n = 0$

1. Montrer que pour tout $p \in [\![0, n]\!]$, $\sum_{k=0}^{n} \lambda_k (X+k)^p = 0$
2. Montrer que pour tout $p \in [\![0, n]\!]$, $\sum_{k=0}^{n} \lambda_k k^p = 0$
3. Montrer que pour tout $P \in \mathbb{K}_n[X]$, $\sum_{k=0}^{n} \lambda_k P(k) = 0$
4. En déduire que $\Big((X+k)^n, k \in [\![0, n]\!]\Big)$ est une base de $\mathbb{K}_n[X]$.

$\boxed{\textbf{28.8}}$ **[♦♦◇]** Soit $n \in \mathbb{N}^*$.

1. Soit $M \in M_n(\mathbb{K})$. Justifier l'existence d'un entier p tel que $(I_n, M, M^2 \dots, M^p)$ est liée.
2. Montrer que l'inverse d'une matrice triangulaire supérieure inversible est triangulaire supérieure.

$\boxed{\textbf{28.9}}$ **[♦◇◇]** Intersection de deux plans vectoriels *(à traiter sans la formule de Grassmann)*.

1. Soient deux plans vectoriels non confondus dans un espace vectoriel de dimension 3. Montrer que leur intersection est une droite vectorielle.
2. Donner un exemple en dimension 4 de deux plans vectoriels supplémentaires.

$\boxed{\textbf{28.10}}$ **[♦♦◇]** Intersection de deux hyperplans *(à traiter avec la formule de Grassmann)*.
Soit E un espace vectoriel de dimension finie égale à n et H_1 et H_2 deux *hyperplans* de E c'est-à-dire des sous-espaces vectoriels de dimension n–1. On suppose que H_1 et H_2 sont <u>non confondus</u>. Calculer $\dim H_1 \cap H_2$.

$\boxed{\textbf{28.11}}$ **[♦♦◇]** Calculer $\dim S_n(\mathbb{R})$. En déduire $\dim A_n(\mathbb{R})$.

$\boxed{\textbf{28.12}}$ **[♦♦◇]** Soit $F = \{P \in \mathbb{R}_3[X] : P(1) = P(2)\}$.

1. Prouver que F est un sous-espace vectoriel de $\mathbb{R}_3[X]$ et justifier que $\dim F \leq 3$.
2. Trouver une base de F.

$\boxed{\textbf{28.13}}$ **[♦♦◇]** Soit $n \in \mathbb{N}$. Soit P un polynôme à coefficients réels de degré $n+1$. Démontrer que

$$\mathbb{R}_{n+1}[X] = \mathbb{R}_n[X] \oplus \mathrm{Vect}(P).$$

$\boxed{\textbf{28.14}}$ **[♦♦◇]** CNS sur λ pour que $\mathrm{Vect}((\lambda, \lambda, 1))$ et $\mathrm{Vect}((1, \lambda, 1), (2, 1, 1))$ soient supplémentaires dans $\mathbb{R}^3$.

$\boxed{\textbf{28.15}}$ **[♦♦♦]** Soient F et G deux sev d'un espace vectoriel de dimension finie. Démontrer que

$$(\dim F + G)^2 + (\dim F \cap G)^2 \geq (\dim F)^2 + (\dim G)^2 .$$

Étudier le cas d'égalité.

---

29 Applications linéaires

On a déjà défini dans le cours *Espaces vectoriels* les notions d'application linéaire, d'image et de noyau. Les énoncés correspondants sont répétés ici, afin d'obtenir un chapitre autonome.

1 Applications linéaires et opérations.

On se donne E, F et G trois $\mathbb{K}$-espaces vectoriels.

1.1 Définition et premières propriétés.

Définition 1.

On appelle **application linéaire** entre E et F une application $u : E \to F$ telle que

$$\forall x, y \in E \quad \forall \lambda, \mu \in \mathbb{K} \qquad u(\lambda x + \mu y) = \lambda u(x) + \mu u(y).$$

(l'image de la combinaison linéaire, c'est la combinaison linéaire des images)

Une application linéaire de E dans E est appelée **endomorphisme** de E.
Une application linéaire de E dans $\mathbb{K}$ (vu comme $\mathbb{K}$-espace vectoriel) est une **forme linéaire**.

Remarque. Il est équivalent de définir la linéarité d'une application $u : E \to F$ à l'aide des propriétés

1. $\forall x, y \in E \quad u(x+y) = u(x) + u(y)$ (propriété de morphisme de groupes additifs)
2. $\forall x \in E \ \ \forall \lambda \in \mathbb{K} \quad u(\lambda \cdot x) = \lambda \cdot u(x)$ (propriété d'homogénéité).

Certains auteurs préfèrent n'utiliser qu'un scalaire dans leur définition de la linéarité. Il est assez clair en effet que si $u : E \to F$ est une application entre deux $\mathbb{K}$-espaces vectoriels,

$$u : E \to F \text{ est linéaire} \quad \text{si et seulement si} \quad \forall x, y \in E \ \ \forall \lambda \in \mathbb{K} \ \ u(\lambda x + y) = \lambda u(x) + u(y).$$

Remarque. S'il nous faut justifier qu'une certaine application u définie sur E est un endomorphisme de E, on commencera par vérifier sa linéarité puis, si ce n'est pas clair, on expliquera pourquoi l'image par u d'un élément de E est bien un élément de E.

Notation.

L'ensemble des applications linéaires de E vers F est noté

$$\mathscr{L}(E, F)$$

Plutôt que $\mathscr{L}(E, E)$, l'ensemble des endomorphismes de E est noté $\mathscr{L}(E)$.

Proposition 2.

Soit $u \in \mathscr{L}(E, F)$. Alors,

1. $u(0_E) = 0_F$.
2. $\forall x \in E, \quad u(-x) = -u(x)$.
3. Pour tout entier $n \in \mathbb{N}^*$, toute famille $(x_1, \ldots, x_n) \in E^n$ et toute famille $(\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n$,

$$u\left(\sum_{i=1}^{n} \lambda_i x_i\right) = \sum_{i=1}^{n} \lambda_i u(x_i).$$

Proposition 3 (Image directe/réciproque d'un s.e.v. par une application linéaire)**.**

Soit $u \in \mathscr{L}(E,F)$.

1. Si G est un sous-espace vectoriel de E, alors $u(G)$ est un sous-espace vectoriel de F.
2. Si H est un sous-espace vectoriel de F, alors $u^{-1}(H)$ est un sous-espace vectoriel de E.

Soient deux applications $u : E \to F$ et $v : E \to F$ (non forcément linéaires). On rappelle que

$$u = v \quad \text{signifie :} \quad \forall x \in E \;\; u(x) = v(x).$$

Proposition 4 (Conditions nécessaires pour l'égalité)**.**

Soient $u, v \in \mathscr{L}(E,F)$.

1. Si u et v coïncident sur une famille génératrice de E, alors $u = v$.
2. Si u et v coïncident sur deux sous-espaces supplémentaires dans E, alors $u = v$.

Lemme 5.

La restriction d'une application linéaire à un sev est linéaire.

1.2 Exemples.

• Exemples explicites.

Dans le cours *Espaces vectoriels*, on a donné les exemples ci-dessous.

$$u : \left\{ \begin{array}{ccc} M_{n,p}(\mathbb{K}) & \to & M_{p,n}(\mathbb{K}) \\ M & \mapsto & M^\top \end{array} \right. , \qquad D : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K}[X] \\ P & \mapsto & P' \end{array} \right.$$

sont des applications linéaires (D est même un endomorphisme de $\mathbb{K}[X]$).

Voici quelques exemples de formes linéaires (a et b deux réels) :

$$\mathrm{tr} : \left\{ \begin{array}{ccc} M_n(\mathbb{K}) & \to & \mathbb{K} \\ M & \mapsto & \mathrm{tr}(M) \end{array} \right. , \qquad \varphi : \left\{ \begin{array}{ccc} \mathcal{C}([a,b],\mathbb{R}) & \to & \mathbb{R} \\ f & \mapsto & \int_a^b f(x)\mathrm{d}x \end{array} \right. , \quad \Phi_a : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K} \\ P & \mapsto & P(a) \end{array} \right. .$$

L'exemple ci-dessous sera sur le devant de la scène dans le cours consacré au lien entre les applications linéaires en dimension finie et les matrices.

Exemple 6 (Application linéaire canoniquement associée à une matrice)**.**

Soit $A \in M_{n,p}(\mathbb{K})$. On lui associe l'application ci-dessous, qui est linéaire, et qui sera appelée **application linéaire canoniquement associée à** A :

$$f : \left\{ \begin{array}{ccc} M_{p,1}(\mathbb{K}) & \to & M_{n,1}(\mathbb{K}) \\ X & \mapsto & AX \end{array} \right.$$

- Exemples plus abstraits.

Pour tout espace vectoriel E, Id_E est un endomorphisme de E.

Pour tous E et F espaces vectoriels, l'application nulle $N : \left\{ \begin{array}{ccc} E & \to & F \\ x & \mapsto & 0_F \end{array} \right.$ est linéaire

On ajoute un exemple important de forme linéaire.

Proposition 7 (Forme coordonnée)**.**

Soit $(e_i)_{i\in I}$ une base d'un $\mathbb{K}$ espace vectoriel E.
Fixons $i \in I$. Pour tout $x \in E$, on note $e_i^*(x)$ la coordonnée de x sur e_i.

L'application $e_i^* : \left\{ \begin{array}{ccc} E & \to & \mathbb{K} \\ x & \mapsto & e_i^*(x) \end{array} \right.$ est une forme linéaire, et $\forall (i,j) \in I^2 \; e_i^*(e_j) = \delta_{i,j}$.

1.3 Noyau et image d'une application linéaire.

Définition 8.

Soit $u \in \mathscr{L}(E,F)$. L'image et le noyau de u sont définis par

$$\operatorname{Im} u = \{u(x), \; x \in E\} = \{y \in F \mid \exists x \in E \; y = u(x)\}.$$

$$\operatorname{Ker} u = \{x \in E \mid u(x) = 0_F\}.$$

Proposition 9.

Soit $u \in \mathscr{L}(E,F)$.

1. $\operatorname{Ker} u$ est un sous-espace vectoriel de E et u est injective si et seulement si $\operatorname{Ker} u = \{0_E\}$.
2. $\operatorname{Im} u$ est un sous-espace vectoriel de F et u est surjective si et seulement si $\operatorname{Im} u = F$.

Proposition 10 (Image d'une famille génératrice)**.**

Soit $u \in \mathscr{L}(E,F)$, où on suppose que E est engendré par une famille $(x_i)_{i\in I}$.
La famille $(u(x_i))_{i\in I}$ est une famille génératrice de $\operatorname{Im}(u)$:

$$\operatorname{Im}(u) = \operatorname{Vect}\left(u(x_i)\right)_{i\in I}.$$

Exemple 11.

Soit $n \in \mathbb{N}$. Noyau et image de $f : P(X) \mapsto P(2X) - P(X)$, endomorphisme de $\mathbb{K}_n[X]$.

1.4 Structure de $\mathbb{K}$-espace vectoriel de $\mathscr{L}(E, F)$.

Définition 12.

Soient E et F deux $\mathbb{K}$-espaces vectoriels. Soient $u, v \in F^E$ deux applications, et $\lambda \in \mathbb{K}$. On définit la **somme** de u et v, notée $u+v$ et le **produit par un scalaire** $\lambda \cdot u$ comme les applications

$$u+v : \left\{ \begin{array}{lll} E & \to & F \\ x & \mapsto & (u+v)(x) := u(x)+v(x) \end{array} \right. \quad \text{et} \quad \lambda \cdot u : \left\{ \begin{array}{lll} E & \to & F \\ x & \mapsto & (\lambda \cdot u)(x) := \lambda u(x) \end{array} \right. .$$

Remarque. La structure d'espace vectoriel de E n'intervient nullement : on pourrait poser les mêmes définitions sur F^Ω, pour tout ensemble non vide Ω.

Théorème 13.

Muni des lois $+$ et $\cdot$ qui viennent d'être définies, F^E est un $\mathbb{K}$-espace vectoriel.

L'ensemble $\mathscr{L}(E, F)$ est un sous-espace vectoriel de F^E. C'est donc un $\mathbb{K}$-espace vectoriel.

Preuve.
On laisse au lecteur la tâche ingrate de vérifier que la structure $(F^E, +, \cdot)$ satisfait les huit axiomes de notre définition de $\mathbb{K}$-espace vectoriel. Contentons-nous de préciser que le zéro de cet espace vectoriel est l'application constante

$$0_{F^E} : \left\{ \begin{array}{lll} E & \to & F \\ x & \mapsto & 0_F \end{array} \right. .$$

Nous allons prouver soigneusement, en revanche, que $\mathscr{L}(E, F)$ est un sous-espace vectoriel de F^E.

- Le *zéro* de F^E, c'est-à-dire l'application nulle, est bien linéaire (cf exemple plus haut) : $0_{F^E} \in \mathscr{L}(E, F)$.
- Montrons que $\mathscr{L}(E, F)$ est stable par combinaison linéaire.

Pour cela, considérons deux applications linéaires $u, v \in \mathscr{L}(E, F)$ et $\alpha, \beta \in \mathbb{K}$. Montrons que $\alpha u + \beta v$ est linéaire.
Pour cela, considérons x et y dans E, λ et μ dans $\mathbb{K}$. On a

$$\begin{aligned} (\alpha u + \beta v)(\lambda x + \mu y) &= \alpha u(\lambda x + \mu y) + \beta v(\lambda x + \mu y) && (\text{def} + \text{ et } \cdot \text{ dans } F^E) \\ &= \alpha(\lambda u(x) + \mu u(y)) + \beta(\lambda v(x) + \mu v(y)) && (\text{linéarité de } u \text{ et } v) \\ &= \lambda(\alpha u(x) + \beta v(x)) + \mu(\alpha u(y) + \beta v(y)) \\ &= \lambda(\alpha u + \beta v)(x) + \mu(\alpha u + \beta v)(y). \end{aligned}$$

□

1.5 Composition des applications linéaires.

Proposition 14 (Une composée d'applications linéaires est linéaire)**.**

Si $u \in \mathscr{L}(E, F)$ et $v \in \mathscr{L}(F, G)$, alors $v \circ u \in \mathscr{L}(E, G)$.

Exemple 15 (Classique et important)**.**

Soient $f \in \mathscr{L}(E, F)$ et $g \in \mathscr{L}(F, G)$.

1. Montrer que $\mathrm{Ker} f \subset \mathrm{Ker}(g \circ f)$ et $\mathrm{Im}(g \circ f) \subset \mathrm{Im} g$.
2. Montrer que $g \circ f = 0_{\mathscr{L}(E,G)} \iff \mathrm{Im}(f) \subset \mathrm{Ker}(g)$.

Proposition 16 (Bilinéarité de la composition)**.**

La composée des applications linéaires est bilinéaire :

1. $\forall u, v \in \mathscr{L}(E, F),\ \forall w \in \mathscr{L}(F, G),\ \forall \lambda, \mu \in \mathbb{K} \quad w \circ (\lambda \cdot u + \mu \cdot v) = \lambda \cdot w \circ u + \mu \cdot w \circ v.$
2. $\forall u, v \in \mathscr{L}(F, G),\ \forall w \in \mathscr{L}(E, F),\ \forall \lambda, \mu \in \mathbb{K} \quad (\lambda \cdot u + \mu \cdot v) \circ w = \lambda \cdot u \circ w + \mu \cdot v \circ w.$

1.6 Isomorphismes.

Définition 17.

On appelle **isomorphisme** toute application linéaire et bijective entre deux espaces vectoriels. On dit de deux $\mathbb{K}$-espaces vectoriels qu'ils sont **isomorphes** s'il existe un isomorphisme entre eux.

Proposition 18 (Réciproque d'un isomorphisme)**.**

Si $u : E \to F$ est un isomorphisme, alors $u^{-1} : F \to E$ est un isomorphisme.

Proposition 19 (Composée d'isomorphismes)**.**

Si $u : E \to F$ et $v : F \to G$ sont deux isomorphismes, alors $v \circ u : E \to G$ est un isomorphisme, et

$$(v \circ u)^{-1} = u^{-1} \circ v^{-1}.$$

1.7 Deux modes de définition d'une application linéaire.

Proposition 20 (Définition d'une AL par l'image d'une base)**.**

Soient $(e_i)_{i\in I}$ une base de E et $(f_i)_{i\in I}$ une famille quelconque de vecteurs de F.

$$\exists! u \in \mathscr{L}(E,F) \quad \forall i \in I \quad u(e_i) = f_i.$$

Preuve.
Analyse. Supposons l'existence d'une application linéaire u telle que

$$\forall i \in I \quad u(e_i) = f_i.$$

Soit $x \in E$ et $(x_i)_{i\in I} \in \mathbb{K}^I$ les coordonnées de x sur la base $(e_i)_{i\in I}$ (famille de scalaires presque nulle). On a

$$u(x) = u\left(\sum_{i\in I} x_i e_i\right) = \sum_{i\in I} x_i u(e_i) = \sum_{i\in I} x_i f_i = \sum_{i\in I} e_i^*(x) f_i$$

Ainsi, u est nécessairement l'application $x \mapsto \sum_{i\in I} e_i^*(x) f_i$ (voir le paragraphe 1.2 pour la définition des e_i^*).

Synthèse. On vérifie que $u : x \mapsto \sum_{i\in I} e_i^*(x) f_i$ est linéaire et qu'elle envoie bien les e_i sur les f_i.

Conclusion. Il existe bien une unique application linéaire envoyant les e_i sur les f_i. $\square$

Proposition 21 (Définition d'une AL par les restrictions à deux supplémentaires)**.**

Soient E_1 et E_2 deux sous-espaces vectoriels de E, supplémentaires dans E ($E = E_1 \oplus E_2$).
Soient deux applications linéaires $u_1 \in \mathscr{L}(E_1, F)$, et $u_2 \in \mathscr{L}(E_2, F)$.

$$\exists! u \in \mathscr{L}(E,F) \quad u_{|E_1} = u_1 \quad \text{et} \quad u_{|E_2} = u_2.$$

Preuve. Tout vecteur x de E se décompose de manière unique comme la somme d'un vecteur $x_1 \in E_1$ et d'un vecteur $x_2 \in E_2$; notons pour ce vecteur x :

$$p_1(x) = x_2 \quad \text{et} \quad p_2(x) = x_2.$$

Ceci définit correctement deux applications

$$p_1 : E \to E_1 \quad \text{et} \quad p_2 : E \to E_2.$$

Nous étudierons ce genre d'applications dans le paragraphe consacré aux *projecteurs* où nous démontrerons notamment que p_1 et p_2 sont des applications linéaires (cela ne serait pas difficile à prouver ici).

Analyse. Supposons l'existence d'une application linéaire u telle que $u_{|E_1} = u_1$ et $u_{|E_2} = u_2$.
Soit $x \in E$ et $(x_1, x_2) \in E_1 \times E_2$ ses composantes sur E_1 et E_2.

$$\begin{aligned} u(x) &= u(x_1 + x_2) \\ &= u(x_1) + u(x_2) \qquad (u \text{ est linéaire}) \\ &= u_1(x_1) + u_2(x_2) \qquad (u_{E_1} = u_1 \quad \text{et} \quad u_{E_2} = u_2) \\ &= u_1(p_1(x)) + u_2(p_2(x)) \end{aligned}$$

On obtient donc que nécessairement, $u = u_1 \circ p_1 + u_2 \circ p_2$.

Synthèse. Posons $u = u_1 \circ p_1 + u_2 \circ p_2$. C'est une application linéaire, comme somme et composée d'applications linéaires. On vérifie facilement que pour $x_1 \in E_1$, $u(x_1) = u_1(x_1)$ et pour $x_2 \in E_2$, $u(x_2) = u_2(x_2)$.

Conclusion. Il existe bien une unique application linéaire coïncidant avec u_1 sur E_1 et avec u_2 sur E_2. $\square$

2 Endomorphismes.

Dans toute cette partie, E est un $\mathbb{K}$-espace vectoriel.

2.1 L'anneau $\mathscr{L}(E)$.

Proposition 22.

$(\mathscr{L}(E), +, \circ)$ est un anneau, non commutatif en général.
Le neutre pour $\circ$ est l'identité sur E, notée id_E.

Exemple. Les endomorphismes de $\mathbb{K}[X]$ définis par $u : P \mapsto P'$ et $v : P \mapsto XP$ ne commutent pas.

Notation.

Si u et v sont deux endomorphismes de E, leur composée $v \circ u$ pourra être notée vu.
Pour tout entier $k \in \mathbb{N}$, le $k$ème itéré de u sera noté u^k. Notamment, $u^2 = u \circ u$ et $u^0 = \mathrm{id}_E$.

On ne va pas refaire ici le cours sur les anneaux. On se contentera de rappeler que

1. Si $\boldsymbol{uv = vu}$, alors $\forall n \in \mathbb{N} \quad (u+v)^n = \sum_{k=0}^{n} \binom{n}{k} u^k v^{n-k}$.
2. Si $\boldsymbol{uv = vu}$, alors $\forall n \in \mathbb{N}^* \quad u^n - v^n = (u-v) \sum_{k=0}^{n-1} u^k v^{n-1-k}$.

   En particulier : $\forall n \in \mathbb{N}^* \quad \mathrm{id}_E - u^n = (\mathrm{id}_E - u) \sum_{k=0}^{n-1} u^k$.

Exemple 23.

Soient u et v deux endomorphismes de E qui commutent ($u \circ v = v \circ u$).
Montrer que $\mathrm{Ker}(u)$ et $\mathrm{Im}(u)$ sont stables par v.

Exemple 24.

Soit $u \in \mathscr{L}(E)$ un endomorphisme nilpotent. On note p son indice de nilpotence, c'est à dire

$$p = \min\{k \in \mathbb{N}^* \ u^k = 0\}.$$

On se donne $x \in E \setminus \mathrm{Ker}(u^{p-1})$.

1. Justifier l'existence d'un tel vecteur x.
2. Montrer que $(x, u(x), \cdots, u^{p-1}(x))$ est libre.
3. Supposons dans cette question que E est de dimension finie n. Montrer que $u^n = 0_{\mathscr{L}(E)}$.

2.2 Groupe linéaire.

Définition 25.

Un endomorphisme bijectif d'un espace vectoriel E sera appelé **automorphisme** de E.
L'ensemble des automorphismes de E sera noté $\mathrm{GL}(E)$.

Proposition 26.

$(\mathrm{GL}(E), \circ)$ est un groupe, appelé **groupe linéaire** de E.

Si E est de dimension supérieure à 2, il n'est pas abélien.

Si $u \in \mathrm{GL}(E)$, alors u^{-1} sera désigné tantôt comme la réciproque de u, tantôt comme son inverse.

Notation.

Si $u \in \mathrm{GL}(E)$ et $k \in \mathbb{Z}$, on rappelle que la notation u^k désigne le k ème itéré de u si k est positif, et dans le cas où $k \in \mathbb{Z} \setminus \mathbb{N}$, alors $u^k = \left(u^{-1}\right)^{|k|}$.

Exemple 27 (Un inverse classique)**.**

Soit $u \in \mathscr{L}(E)$ un endomorphisme nilpotent, c'est-à-dire qu'il existe $n \in \mathbb{N}^*$ tel que $u^n = 0_{\mathscr{L}(E)}$.
Montrer que $\mathrm{id}_E - u$ est un automorphisme de E.

2.3 Homothéties

Définition 28.

Soit $\lambda \in \mathbb{K}$. On appelle **homothétie** de rapport λ l'endomorphisme

$$\lambda \mathrm{id}_E : \left\{ \begin{array}{ccc} E & \to & E \\ x & \mapsto & \lambda \cdot x \end{array} \right. .$$

Exemple 29 (*Sous-espaces propres*)**.**

Soit $f \in \mathscr{L}(E)$ et $\lambda \in \mathbb{K}$.

1. Justifier que pour tout $x \in E$, $x \in \mathrm{Ker}(f - \lambda \mathrm{id}_E) \iff f(x) = \lambda x$.
2. En particulier, comment décrire les vecteurs de $\mathrm{Ker}(f - \mathrm{id}_E)$? de $\mathrm{Ker}(f + \mathrm{id}_E)$?
3. Notons $E_\lambda = \mathrm{Ker}(f - \lambda \mathrm{id}_E)$. Que dire de $f_{|E_\lambda}$?
   Supposons que $E = \mathrm{Ker}(f - \mathrm{id}) \oplus \mathrm{Ker}(f - 2\mathrm{id}_E)$. Représenter un vecteur et son image par u.

L'exercice suivant sera connu d'un étudiant de MPI⋆.

Exemple 30 (Une caractérisation classique des homothéties (*))**.**

Soit E un $\mathbb{K}$-espace vectoriel et $f \in \mathscr{L}(E)$ tel que

$$\forall x \in E \quad \exists \lambda_x \in \mathbb{K} \quad f(x) = \lambda_x \cdot x.$$

Montrer que f est une homothétie.

Solution. Commençons par remarquer que le problème consiste à échanger l'ordre des quantificateurs dans une phrase : on travaille sous l'hypothèse

$$\forall x \in E \quad \exists \lambda \in \mathbb{K} \quad f(x) = \lambda x,$$

et on doit montrer

$$\exists \lambda \in \mathbb{K} \quad \forall x \in E \quad f(x) = \lambda x.$$

Le vecteur nul est un peu à part. En effet, pour tout $\lambda \in \mathbb{K}$, $f(0_E) = 0_E = \mu \cdot 0_E$.
Ainsi, si E est réduit à ce vecteur, f est une homothétie de rapport $0, \pi$, ou 666 au choix.
En revanche, si E n'est pas réduit à $\{0_E\}$ et si x est un vecteur non nul de E, il est facile de voir que le scalaire λ_x tel que $f(x) = \lambda_x x$ est *unique*. Ainsi, pour répondre à la question, il suffit de montrer :

$$\forall x, y \in E \setminus \{0_E\} \quad \lambda_x = \lambda_y. \qquad (*)$$

Montrons $(*)$ et pour cela, considérons x et y dans E, non nuls. Il existe $(\lambda_x, \lambda_y) \in \mathbb{K}^2$ tel que $f(x) = \lambda_x x$ et $f(y) = \lambda_y y$. On a donc, par linéarité, $f(x) + f(y) = f(x+y) = \lambda_x x + \lambda_y y$. Mais le vecteur $x + y$ est dans E, donc il existe un scalaire λ_{x+y} tel que $f(x+y) = \lambda_{x+y}(x+y) = \lambda_{x+y} x + \lambda_{x+y} y$. En égalant les deux expressions de $f(x+y)$, on a

$$(\lambda_x - \lambda_{x+y})x + (\lambda_y - \lambda_{x+y})y = 0_E.$$

Deux cas se présentent.

- Dans le cas où (x, y) est libre, alors, on a $\lambda_x - \lambda_{x+y} = 0$ et $\lambda_y - \lambda_{x+y} = 0$ et donc $\underline{\lambda_x = \lambda_y}$.
- Dans le cas où (x, y) est liée, x étant non nul, il existe $\mu \in \mathbb{K}$ tel que $y = \mu x$. On a

$$f(y) = f(\mu x) = \mu f(x) = \mu(\lambda_x x) = \lambda_x(\mu x) = \lambda_x y.$$

  Or, $f(y) = \lambda_y y$. On a donc $\lambda_y y$, et, y étant non nul, $\underline{\lambda_x = \lambda_y}$.

2.4 Projecteurs.

Définition 31.

Soient F et G deux sous-espaces supplémentaires dans E ($E = F \oplus G$).
Pour tout $x \in E$, il existe un unique couple $(x_F, x_G) \in F \times G$ tel que

$$x = x_F + x_G.$$

Ceci permet de définir l'application qui à un vecteur x associe sa composante sur F :

$$p : \begin{cases} E & \to & E \\ x & \mapsto & p(x) := x_F \end{cases},$$

appelée **projection sur F parallèlement à G**. On parle aussi de p comme un **projecteur**.

Proposition 32 (Propriétés des projecteurs)**.**

Soit (F, G) un couple de s.e.v. supplémentaires dans E et p la projection sur F parallèlement à G.

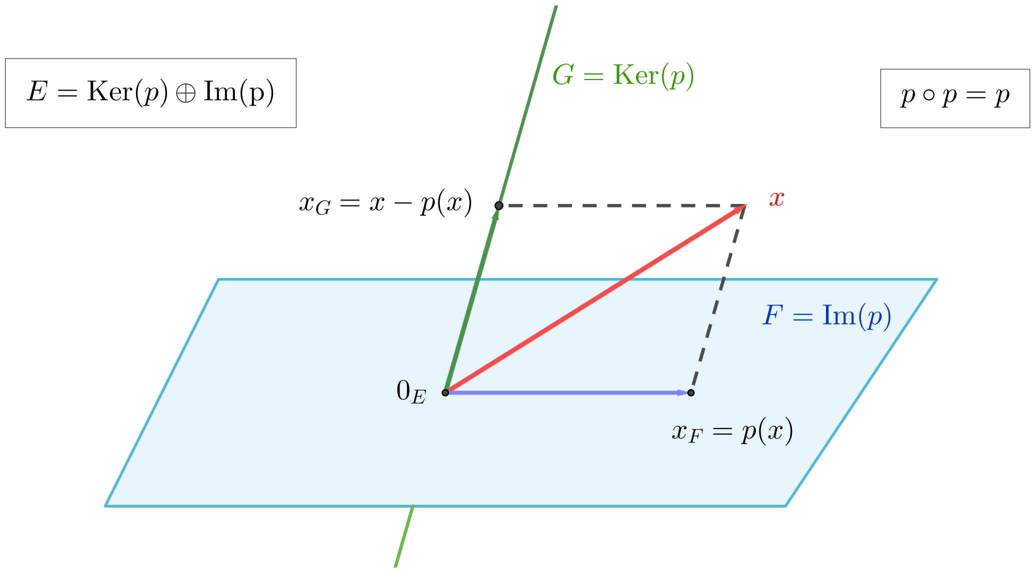
1. p est un endomorphisme de E.
2. $\boxed{p \circ p = p}$ (on dit que p est **idempotent**).
3. F est l'image de p : $F = \mathrm{Im}(p)$.
   C'est aussi l'ensemble des vecteurs invariants par p : $F = \mathrm{Im}(p) = \mathrm{Ker}(p - \mathrm{id}_E)$.
4. G est l'ensemble des vecteurs d'image nulle par p : $G = \mathrm{Ker}(p)$.
5. Ainsi, p est la projection sur $\mathrm{Im}(p)$ parallèlement à $\mathrm{Ker}(p)$. En particulier,

$$\boxed{E = \mathrm{Im}(p) \oplus \mathrm{Ker}(p)}, \qquad \text{c'est-à-dire} \qquad E = \mathrm{Ker}(p - \mathrm{id}_E) \oplus \mathrm{Ker}(p).$$

   La décomposition d'un vecteur de E s'écrit

$$\forall x \in E \qquad x = \underbrace{p(x)}_{\in \mathrm{Im}(p)} + \underbrace{x - p(x)}_{\in \mathrm{Ker}(p)}.$$

6. $\mathrm{id}_E - p$ est la projection sur G parallèlement à F.
7. p peut être vu comme l'unique endomorphisme tel que $p_{|F} = \mathrm{id}_F$ et $p_{|G} = 0_{\mathscr{L}(G)}$.



p, projection sur F, parallèlement à G

Proposition 33 (L'idempotence caractérise les projecteurs parmi les endomorphismes)**.**

Soit p un endomorphisme de E.

$$p \text{ est un projecteur} \quad \text{ssi} \quad p \circ p = p.$$

La définition d'une projection était *géométrique* ; la caractérisation qu'on vient de donner est *algébrique*

2.5 Symétries.

Définition 34.

Soient F et G deux sous-espaces supplémentaires dans E ($E = F \oplus G$).
Pour tout $x \in E$, il existe un unique couple $(x_F, x_G) \in F \times G$ tel que

$$x = x_F + x_G.$$

Ceci permet de définir l'application

$$s : \left\{ \begin{array}{ccc} E & \to & E \\ x & \mapsto & s(x) := x_F - x_G \end{array} \right. ,$$

appelée **symétrie par rapport à F parallèlement à G**.

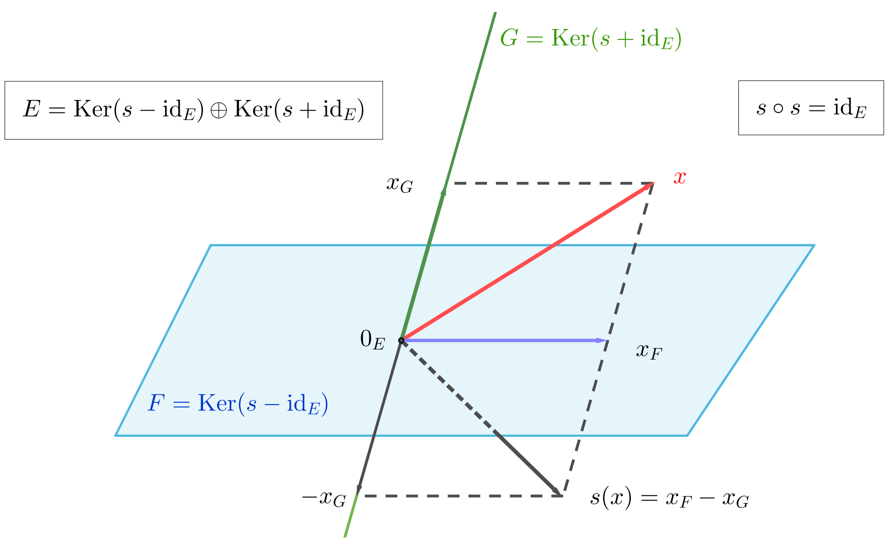
Proposition 35 (Propriétés des symétries)**.**

Soit (F, G) un couple de s.e.v. supplémentaires dans E et s la symétrie par rapport à F parallèlement à G.

1. s est un endomorphisme de E.
2. $\boxed{s \circ s = \mathrm{id}_E}$ (on dit que s est **involutive**).
3. F est l'ensemble des vecteurs invariants par s : $F = \mathrm{Ker}(s - \mathrm{id}_E)$.
4. G est l'ensemble des vecteurs transformés par s en leur opposé : $G = \mathrm{Ker}(s + \mathrm{id}_E)$.
5. Ainsi, s est la symétrie par rapport à $\mathrm{Ker}(s-\mathrm{id}_E)$ parallèlement à $\mathrm{Ker}(s+\mathrm{id}_E)$. En particulier

$$\boxed{E = \mathrm{Ker}(s - \mathrm{id}_E) \oplus \mathrm{Ker}(s + \mathrm{id}_E)}.$$

6. s peut être vue comme l'unique endomorphisme de E tel que $s_{|F} = \mathrm{id}_F$ et $s_{|G} = -\mathrm{id}_G$.



s, symétrie par rapport à F, parallèlement à G

Proposition 36 (L'involutivité caractérise les symétries parmi les endomorphismes)**.**

Soit s un endomorphisme de E.

$$s \text{ est une symétrie} \quad \text{ssi} \quad s \circ s = \mathrm{id}_E.$$

Exemple 37.

À l'aide d'une symétrie, redémontrer que $S_n(\mathbb{K})$ et $A_n(\mathbb{K})$ sont supplémentaires dans $M_n(\mathbb{K})$.

Remarque. Il n'est pas inutile de retenir la décomposition d'un vecteur sur les deux supplémentaires associés à une symétrie sur un espace E : on a

$$\forall x \in E \quad x = \underbrace{\frac{1}{2}(x + s(x))}_{\in \mathrm{Ker}(s-\mathrm{id})} + \underbrace{\frac{1}{2}(x - s(x))}_{\in \mathrm{Ker}(s+\mathrm{id})}.$$

3 Applications linéaires et dimension finie.

3.1 Image d'une base.

Théorème 38 (Caractérisation des isomorphismes par l'image d'une base)**.**

Soit $u \in \mathscr{L}(E, F)$, où E est de dimension finie n. On considère $(x_1, \ldots, x_n)$ une base de E.

1. u est surjective ssi $(u(x_1), \ldots, u(x_n))$ engendre F.
2. u est injective ssi $(u(x_1), \ldots, u(x_n))$ est libre.
3. u est bijective ssi $(u(x_1), \ldots, u(x_n))$ est une base de F.

Corollaire 39.

Une application linéaire entre deux espaces vectoriels de dimension finie est un isomorphisme si et seulement si elle transforme une base en une base.

3.2 Isomorphismes et dimension finie.

Proposition 40.

Soient deux espaces vectoriels E et F isomorphes.
Si l'un des deux est de dimension finie, alors l'autre l'est aussi et $\dim E = \dim F$.

Ce résultat donne une nouvelle méthode pour calculer la dimension d'un espace vectoriel. Il suffira d'exhiber un isomorphisme entre cet espace et un espace dont on connaît la dimension. Ci-dessous, deux applications de ce principe.

Proposition 41.

Tout $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ est isomorphe à $\mathbb{K}^n$

Corollaire 42 (Classification des espaces de dimension finie)**.**

Deux espaces vectoriels de dimension finie sont isomorphes ssi ils ont même dimension.

Proposition 43.

Soient E, F deux $\mathbb{K}$-espaces vectoriels de dimension finie. Alors $\mathscr{L}(E,F)$ est de dimension finie et

$$\dim \mathscr{L}(E,F) = \dim E \dim F.$$

Corollaire 44.

L'ensemble des formes linéaires sur E, noté $\mathscr{L}(E,\mathbb{K})$ ou parfois E^* a la même dimension que E lorsque ce dernier est de dimension finie.

E^* est appelé dual de E. L'étude de ses liens avec E est appelée dualité et est hors-programme.

On vient de voir comment un isomorphisme peut nous aider à calculer une dimension. Voyons maintenant comment la dimension finie peut nous aider à prouver qu'une application linéaire est bijective.

Théorème 45 (Caractérisation des isomorphismes entre deux e.v. de dimension finie)**.**

Soient E et F deux espaces vectoriels de dimension finie et $u \in \mathscr{L}(E,F)$. On a

$$u \text{ est bijective} \iff \begin{cases} u \text{ est injective} \\ \dim E = \dim F \end{cases} \quad \text{et} \quad u \text{ est bijective} \iff \begin{cases} u \text{ est surjective} \\ \dim E = \dim F \end{cases}$$

Corollaire 46 (Caractérisation des automorphismes en dimension finie)**.**

Soit u un endomorphisme d'un espace de dimension finie.

$$u \text{ est bijectif} \iff u \text{ est injectif} \iff u \text{ est surjectif.}$$

Corollaire 47 (L'inversibilité à gauche ou à droite suffit en dimension finie)**.**

Soit u un endomorphisme d'un espace de dimension finie.

$$u \text{ est inversible} \iff u \text{ est inversible à gauche} \iff u \text{ est inversible à droite.}$$

Si u est inversible à gauche ou à droite, l'inverse à gauche ou à droite, c'est la réciproque de u.

Exemple 48 (Retour sur l'interpolation de Lagrange)**.**

Soit $n \in \mathbb{N}^*$, $(x_1, \dots, x_n) \in \mathbb{K}^n$ (scalaires deux à deux distincts) et $(y_1, \dots, y_n) \in \mathbb{K}^n$.
À l'aide de l'application

$$\varphi : \begin{cases} \mathbb{K}_{n-1}[X] & \to & \mathbb{K}^n \\ P & \mapsto & (P(x_1), \dots, P(x_n)) \end{cases},$$

redémontrer que

$$\exists! P \in \mathbb{K}_{n-1}[X] \quad \forall i \in [\![1, n]\!] \quad P(x_i) = y_i.$$

3.3 Rang d'une application linéaire.

Définition 49.

Soit $u \in \mathscr{L}(E, F)$. On dit que u est de **rang fini** si son image $\mathrm{Im}(u)$ est de dimension finie.
On appelle alors **rang** de l'application u et on note $\mathrm{rg}(u)$ l'entier

$$\mathrm{rg}(u) = \dim\left(\mathrm{Im}(u)\right).$$

Exemple 50 (Rang nul)**.**

Soit $u \in \mathscr{L}(E, F)$. On a

$$\mathrm{rg}(u) = 0 \iff \dim \mathrm{Im}(u) = 0 \iff \mathrm{Im}(u) = \{0_F\} \iff u = 0_{\mathscr{L}(E,F)}.$$

Proposition 51 (Rang et dimension finie au départ ou à l'arrivée)**.**

Soit $u \in \mathscr{L}(E, F)$.

1. Si F est de dimension finie, alors u est de rang fini et $\mathrm{rg}(u) \leq \dim(F)$.
2. Si E est de dimension finie, alors u est de rang fini et $\mathrm{rg}(u) \leq \dim(E)$.

Remarque. Dans la preuve, on comprend que si E est de dimension finie et que $(x_1, \dots, x_n)$ est une base de E, alors u est de rang fini égal au rang de la famille $(u(x_1), \dots, u(x_n))$.

Lorsqu'on compose, le rang ne peut que diminuer, comme nous l'apprend la proposition ci-dessous.

Proposition 52.

Soient $u \in \mathscr{L}(E, F)$ et $v \in \mathscr{L}(F, G)$ deux applications linéaires.
Si u ou v est de rang fini, alors, $v \circ u$ est de rang fini et

$$\mathrm{rg}(v \circ u) \leq \min\left(\mathrm{rg}(u), \mathrm{rg}(v)\right).$$

Le rang d'une application linéaire est invariant par composition avec un isomorphisme.

Proposition 53.

Soit $u \in \mathscr{L}(E, F)$ de rang fini et soient deux isomorphismes $f \in \mathscr{L}(F, G)$ et $g \in \mathscr{L}(H, E)$. Alors $f \circ u$ et $u \circ g$ sont de rang fini et

$$\mathrm{rg}(f \circ u) = \mathrm{rg}(u) \quad \text{et} \quad \mathrm{rg}(u \circ g) = \mathrm{rg}(u).$$

3.4 Théorème du rang.

Proposition 54 (Forme géométrique du théorème du rang)**.**

Soit E et F deux espaces vectoriels et $u \in \mathscr{L}(E, F)$.
Si $\mathrm{Ker}(u)$ admet un supplémentaire S dans E, alors

$$u_{|S} : \begin{cases} S & \to & \mathrm{Im}(u) \\ x & \mapsto & u(x) \end{cases}$$

est un isomorphisme de S dans $\mathrm{Im}(u)$.

La grande idée : pour rendre une application injective, il faut *se débarrasser* de son noyau...

Théorème 55 (Théorème du rang)**.**

Soit E un espace de dimension finie, F un espace vectoriel et $u \in \mathscr{L}(E, F)$. Alors, u est de rang fini et

$$\dim E = \mathrm{rg}(u) + \dim \mathrm{Ker} u.$$

Attention, une confusion classique consiste à croire que le noyau et l'image d'une application linéaire sont sont supplémentaires... Ce n'est **pas ce que dit le théorème** ! Remarquons déjà que cela n'a aucun sens si les espaces de départ et d'arrivée E et F ne sont pas les mêmes, puisque $\mathrm{Ker} f \subset E$ et $\mathrm{Im} f \subset F$. Et même quand $E = F$, c'est faux.

4 Hyperplans.

Dans cette partie, E désigne un $\mathbb{K}$-espace vectoriel (pas nécessairement de dimension finie).

4.1 Formes linéaires et hyperplans.

On rappelle qu'une forme linéaire sur un $\mathbb{K}$-espace vectoriel E est une application linéaire d'un espace vectoriel E dans $\mathbb{K}$. On redit aussi que $\mathbb{K}$ est un $\mathbb{K}$-espace vectoriel de dimension finie égale à 1.

Définition 56.

On appelle **hyperplan** de E le noyau d'une forme linéaire non nulle sur E.

Remarque. Dire qu'une forme linéaire φ n'est pas nulle, c'est dire que φ n'est pas la fonction nulle, autrement dit qu'il existe au moins un vecteur x_0 dans E tel que $\varphi(x_0) \neq 0$.

Exemples.

- Soit $F = \{(x, y, z) \in \mathbb{R}^3 \mid x + 2y + 3z = 0\}$. C'est un plan de $\mathbb{R}^3$, on le sait. On peut aussi dire que c'est un hyperplan de $\mathbb{R}^3$ puisque c'est le noyau de la forme linéaire non nulle

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{R}^3 & \to & \mathbb{R} \\ (x, y, z) & \mapsto & x + 2y + 3z \end{array} \right. ;$$

  (la forme linéaire ϕ est non nulle car, par exemple $\varphi((1, 0, 0)) = 1 \neq 0$).

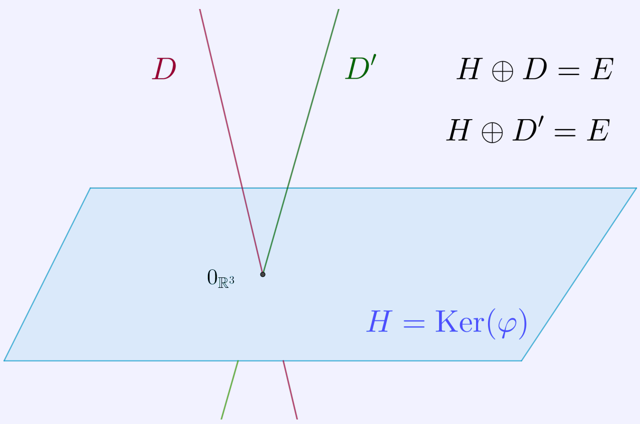
- L'ensemble $G = \{P \in \mathbb{K}[X] \mid P(2) = 0\}$ est un hyperplan de $\mathbb{K}[X]$ puisque $G = \mathrm{Ker}(\psi)$: c'est le noyau de la forme linéaire non nulle

$$\psi : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K} \\ P & \mapsto & P(2) \end{array} \right. ;$$

  (la forme linéaire ψ est non nulle car, par exemple $\psi(X) \neq 0$).

Proposition 57.

Soit H un hyperplan de E et D une droite vectorielle de E non incluse dans H. Alors $H \oplus D = E$.



Théorème 58.

Soit H un sous-espace vectoriel d'un $\mathbb{K}$-espace vectoriel E.

$$H \text{ est un hyperplan de } E \iff H \text{ est supplémentaire d'une droite de } E.$$

Si E est de dimension finie $n \geq 1$, ses hyperplans sont donc les sous-espaces de dimension $n-1$.

Les hyperplans d'un espace de dimension 3 sont ses plans vectoriels.

Les hyperplans d'un espace de dimension 2 sont ses droites vectorielles.

Exemple 59.

L'ensemble $H = \{M \in M_n(\mathbb{K}) \mid \mathrm{Tr}(M) = 0\}$ est un hyperplan de $M_n(\mathbb{K})$: c'est le noyau de la trace, forme linéaire non nulle (puisque $\mathrm{Tr}(I_n) \neq 0$ par exemple). Sa dimension est $n^2 - 1$.

Un hyperplan est le noyau d'une infinité de formes linéaires : quels sont les liens entre ces applications ?

Proposition 60 (Équations d'un hyperplan)**.**

Soit φ et ψ deux formes linéaires non nulles sur E.

$$\mathrm{Ker}\varphi = \mathrm{Ker}\psi \quad \iff \quad \exists \lambda \in \mathbb{K}^* \quad \psi = \lambda\varphi.$$

L'égalité $\varphi(x) = 0$ caractérisant l'appartenance d'un vecteur $x \in E$ à l'hyperplan $\mathrm{Ker}(\varphi)$ est appelée une **équation** de l'hyperplan.

Preuve. L'implication réciproque est facile. Supposons que $\mathrm{Ker}\varphi = \mathrm{Ker}\psi$.
Considérons un vecteur x non nul tel que $x \notin \mathrm{Ker}\varphi$. La droite $\mathrm{Vect}(x)$ est donc un supplémentaire de $\mathrm{Ker}\varphi$.
On a $\varphi(x) \neq 0$. Posons $\lambda = \frac{\psi(x)}{\varphi(x)}$, de sorte que ψ et $\lambda\varphi$ coïncident sur x puis sur $\mathrm{Vect}(x)$.
Puisqu'elles coïncident aussi sur $\mathrm{Ker}(\varphi)$ (où elles sont nulles !), les applications ψ et φ sont égales sur deux supplémentaires donc égales. $\square$

Proposition 61 (Lien entre hyperplan et équation linéaire)**.**

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie égale à n et $\mathcal{B} = (e_1, \ldots, e_n)$ une base de E.
Soit φ une forme linéaire non nulle. On a

$$x \in \mathrm{Ker}\varphi \quad \iff \quad \sum_{i=1}^{n} \varphi(e_i) e_i^*(x) = 0.$$

L'équation écrite ci-dessus est appelée une **équation** de l'hyperplan $\mathrm{Ker}(\varphi)$ dans la base $\mathcal{B}$.

Preuve. On décompose x sur la base et on applique φ... $\square$

Pour mieux comprendre la notion précédente d'équation d'un hyperplan, on peut se donner des notations plus habituelles : notons $x = \sum_{i=1}^{n} x_i e_i$ la décomposition de x sur la base $\mathcal{B}$ et, pour tout $i \in [\![1, n]\!]$, notons $a_i = \varphi(e_i)$. On a alors

$$x \in \mathrm{Ker}\varphi \iff a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0.$$

En particulier, on retrouve qu'une équation

$$ax + by = 0,$$

dans le cas où $(a, b) \neq 0$, est l'équation d'une droite vectorielle de $\mathbb{R}^2$. C'est l'équation dans la base canonique (e_1, e_2) de l'hyperplan de $\mathbb{R}^2$ associé à $\varphi : (x, y) \mapsto ax + by$. On a $a = \varphi(e_1)$ et $b = \varphi(e_2)$.

On retrouve, de la même façon, que

$$ax + by + cz = 0$$

est l'équation d'un plan vectoriel de $\mathbb{R}^3$, lorsque $(a, b, c) \neq (0, 0, 0)$: c'est l'équation dans la base canonique de l'hyperplan associé à la forme linéaire $\varphi : (x, y, z) \mapsto ax + by + cz$.

4.2 Intersection d'hyperplans.

Proposition 62.

Soient m et n deux entiers naturels non nuls, avec $m \leq n$ et E un espace vectoriel de dimension n.

1. L'intersection de m hyperplans de E est au moins de dimension $n - m$.
2. Réciproquement, tout sous-espace vectoriel de E de dimension $n - m$ est l'intersection de m hyperplans.

En particulier, considérons le système linéaire sur $\mathbb{K}^n$

$$\left\{\begin{array}{ll} a_1x_1 + a_2x_2 + \cdots + a_nx_n & = 0 \\ a'_1x_1 + a'_2x_2 + \cdots + a'_nx_n & = 0 \end{array}\right. \qquad \text{Il se récrit} \qquad \left\{\begin{array}{ll} \varphi(x_1, \cdots, x_n) & = 0 \\ \psi(x_1, \cdots, x_n) & = 0 \end{array}\right.$$

L'ensemble des solutions est donc $\mathrm{Ker}\varphi \cap \mathrm{Ker}\psi'$. Si ces deux formes linéaires sont non nulles, il s'agit d'une intersection d'hyperplans. Si (φ, φ') est libre, les deux hyperplans ne sont pas confondus. On montre alors facilement que $\mathrm{Ker}(\varphi) + \mathrm{Ker}(\psi) = \mathbb{K}^n$ puis, grâce à la formule de Grassmann, que

$$\dim \mathrm{Ker}(\varphi) \cap \mathrm{Ker}(\psi) = n - 2.$$

Dans le cas $\mathbb{K} = \mathbb{R}$ et $n = 3$, on retrouve bien sûr que l'intersection de deux plans vectoriels non confondus est une droite vectorielle.

Corollaire 63.

Un système de m équations linéaires non nulles sur $\mathbb{K}^n$, où $m \geq 1$ a pour ensemble de solutions un sous-espace vectoriel de $\mathbb{K}^n$ ayant une dimension supérieure à $n - m$.

Exercices

Images et noyau.

$\boxed{\textbf{29.1}}$ **[♦◇◇]** Soit u un endomorphisme d'un espace vectoriel E. Montrer

$$\mathrm{Ker}(u) = \mathrm{Ker}(u^2) \iff \mathrm{Ker}(u) \cap \mathrm{Im}(u) = \{0_E\}.$$

$\boxed{\textbf{29.2}}$ **[♦◇◇]** Soit u un endomorphisme d'un espace vectoriel E. Montrer

$$\mathrm{Im}(u) = \mathrm{Im}(u^2) \iff E = \mathrm{Ker}(u) + \mathrm{Im}(u).$$

$\boxed{\textbf{29.3}}$ **[♦◇◇]** Soit E un $\mathbb{K}$-espace vectoriel et F un sous-espace vectoriel de E. Notons

$$\mathcal{K}_F = \{f \in \mathscr{L}(E) : F \subset \mathrm{Ker}(f)\}.$$

1. Démontrer soigneusement que $\mathcal{K}_F$ est un sous-espace vectoriel de $\mathscr{L}(E)$.
2. Prouver que si $f \in \mathcal{K}_F$ et $g \in \mathscr{L}(E)$, alors $g \circ f \in \mathcal{K}_F$.

$\boxed{\textbf{29.4}}$ **[♦♦◇]** Noyaux itérés
Soit $u \in \mathscr{L}(E)$, où E est un espace vectoriel.

1. Montrer que pour tout $k \geq 0$, on a $\mathrm{Ker}(u^k) \subset \mathrm{Ker}(u^{k+1})$.
2. Montrer que
$$\forall k \in \mathbb{N} \quad \mathrm{Ker}(u^k) = \mathrm{Ker}(u^{k+1}) \Rightarrow \mathrm{Ker}(u^{k+1}) = \mathrm{Ker}(u^{k+2}).$$

$\boxed{\textbf{29.5}}$ **[♦♦◇]** Polynôme annulateur et applications
Soit E un $\mathbb{K}$-espace vectoriel et u un endomorphisme de E.
On suppose que $u^2 - 3u + 2\mathrm{Id}_E = 0$.

1. Montrer que u est inversible et calculer u^{-1}.
2. Soit $n \in \mathbb{N}$.
   (a) Calculer le reste dans la division euclidienne de X^n par $X^2 - 3X + 2$.
   (b) En déduire une expression de u^n.
   (c) Que dire de $\mathrm{Vect}(u^k)_{k\in\mathbb{N}}$?
3. Démontrer que $E = \mathrm{Ker}(u - \mathrm{id}_E) \oplus \mathrm{Ker}(u - 2\mathrm{id}_E)$.

$\boxed{\textbf{29.6}}$ **[♦♦♦]** Soient $u \in \mathscr{L}(E, F)$ et $v \in \mathscr{L}(F, E)$. Démontrer que

$$\mathrm{Id}_E - v \circ u \text{ injective} \iff \mathrm{Id}_F - u \circ v \text{ injective}.$$

$$\mathrm{Id}_E - v \circ u \text{ surjective} \iff \mathrm{Id}_F - u \circ v \text{ surjective}.$$

$\boxed{\textbf{29.7}}$ **[♦♦♦]** Soient E, F, G trois espaces vectoriels, E étant de dimension finie. On considère

$$f : E \to F \in \mathscr{L}(E, F) \quad \text{et} \quad g : E \to G \in \mathscr{L}(E, G).$$

Montrer l'équivalence

$$\mathrm{Ker}(f) \subset \mathrm{Ker}(g) \iff \exists \Phi \in \mathscr{L}(F, G) : g = \Phi \circ f.$$

Projecteurs, symétries.

$\boxed{\textbf{29.8}}$ **[♦◇◇]** Soit p est un projecteur et f un endomorphisme d'un espace vectoriel E.
Montrer que $p \circ f = f \circ p$ si et seulement si $\text{Ker}(p)$ et $\text{Im}(p)$ sont stables par f.

$\boxed{\textbf{29.9}}$ **[♦◇◇]** Soient f et g deux endomorphismes d'un espace vectoriel E tels que $f \circ g = \text{Id}_E$.

1. Montrer que $\text{Im}(g \circ f) = \text{Im}(g)$ et $\text{Ker}(g \circ f) = \text{Ker}(f)$.
2. Montrer que $E = \text{Ker}(f) \oplus \text{Im}(g)$.

$\boxed{\textbf{29.10}}$ **[♦♦◇]** En utilisant une symétrie, retrouver que toute fonction de $\mathbb{R}^{\mathbb{R}}$ se décompose de manière unique comme somme d'une fonction paire et d'une fonction impaire.

$\boxed{\textbf{29.11}}$ **[♦♦♦]** Soit E un $\mathbb{K}$-espace vectoriel et p et q deux projecteurs.

1. Montrer que $p + q$ est un projecteur si et seulement si $p \circ q = q \circ p = 0$.
2. Supposons que $p + q$ est un projecteur. Montrer que

$$\text{Im}(p + q) = \text{Im}(p) \oplus \text{Im}(q) \quad \text{et} \quad \text{Ker}(p + q) = \text{Ker}(p) \cap \text{Ker}(q).$$

$\boxed{\textbf{29.12}}$ **[♦◇◇]** Pour une fois, on calcule vraiment !
Soit $E = \mathbb{R}^3$, $e_1 = (1, 0, 0)$, $e_2 = (1, 1, 0)$ et $e_3 = (1, 2, 3)$, $F = \text{Vect}(e_1, e_2)$ et $G = \text{Vect}(e_3)$.

1. Montrer que F et G sont deux espaces supplémentaires de E.
2. Donner l'expression de la projection sur F parallèlement à G (calculer l'image d'un vecteur (x, y, z)).
3. Donner l'expression de la symétrie par rapport à G parallèlement à F.

Application linéaires et dimension finie.

$\boxed{\textbf{29.13}}$ **[♦◇◇]**
1. Soit $n \in \mathbb{N}$. Justifier que l'application $f_n : P \mapsto P + P'$ est un automorphisme de $\mathbb{R}_n[X]$.
2. Démontrer que $f : \left\{ \begin{array}{ccc} \mathbb{R}[X] & \to & \mathbb{R}[X] \\ P & \mapsto & P + P' \end{array} \right.$ est un automorphisme de $\mathbb{R}[X]$.

$\boxed{\textbf{29.14}}$ **[♦◇◇]** Soit $n \in \mathbb{N}$. Pour $P \in \mathbb{K}_n[X]$, on pose $f(P) = P(X + 1) - P(X)$.

1. Justifier que f est un endomorphisme de $\mathbb{K}_n[X]$.
2. Montrer que $\text{Ker}f$ est l'ensemble des polynômes constants.
3. Justifier que $\text{Im}(f) = \mathbb{K}_{n-1}[X]$.
4. Le noyau et l'image de f sont-ils supplémentaires dans $\mathbb{K}_n[X]$. ?

$\boxed{\textbf{29.15}}$ **[♦♦◇]** Soit E un espace vectoriel et u un endomorphisme de E. On dit que u est *pseudo-nilpotent* si

$$\forall x \in E \quad \exists p \in \mathbb{N} \quad u^p(x) = 0_E.$$

1. Montrer que si E est de dimension finie, tout endomorphisme pseudo-nilpotent est nilpotent.
2. Posons $E = \mathbb{K}[X]$. Proposer un endomorphisme pseudo-nilpotent qui n'est pas nilpotent.

$\boxed{\textbf{29.16}}$ **[♦♦◇]** Soit f un endomorphisme d'un espace vectoriel E de dimension n.

1. Montrer que $E = \mathrm{Ker}(f) \oplus \mathrm{Im}(f) \Longrightarrow \mathrm{Im}(f) = \mathrm{Im}(f^2)$.
2. (a) Démontrer que $\mathrm{Im}(f) = \mathrm{Im}(f^2) \Longleftrightarrow \mathrm{Ker}(f) = \mathrm{Ker}(f^2)$
   (b) Démontrer que $\mathrm{Im}(f) = \mathrm{Im}(f^2) \Longrightarrow E = \mathrm{Ker}(f) \oplus \mathrm{Im}(f)$.

$\boxed{\textbf{29.17}}$ **[♦◇◇]** Soit E un espace vectoriel de dimension n et $u \in \mathscr{L}(E)$. Démontrer :

$$\mathrm{Ker}(u) = \mathrm{Im}(u) \quad \Longleftrightarrow \quad u^2 = 0_{\mathscr{L}(E)} \text{ et } 2\mathrm{rg}(u) = n.$$

$\boxed{\textbf{29.18}}$ **[♦♦◇]** Un peu plus dur que l'exercice précédent]
Soit E un espace vectoriel de dimension finie.
Démontrer qu'il existe $u \in \mathscr{L}(E)$ tel que $\mathrm{Ker}(u) = \mathrm{Im}(u)$ si et seulement si la dimension de E est paire.

$\boxed{\textbf{29.19}}$ **[♦♦♦]** Soit E un $\mathbb{K}$-espace vectoriel et u et v deux endomorphismes de E de rang fini. Montrer que

$$\mathrm{rg}(u \circ v) = \mathrm{rg} v - \dim \mathrm{Ker} u \cap \mathrm{Im} v.$$

En vrac.

$\boxed{\textbf{29.20}}$ **[♦♦◇]** Soit E un $\mathbb{K}$-espace vectoriel de dimension n et $f \in \mathscr{L}(E)$ tel que $f^{n-1} \neq 0$ et $f^n = 0$.
On définit le *commutant* de f par $\mathcal{C}(f) = \{g \in \mathscr{L}(E) : g \circ f = f \circ g\}$.

1. Montrer qu'il existe $a \in E$ tel que $(a, f(a), \dots, f^{n-1}(a))$ soit une base de E.
2. Montrer que $(\mathrm{id}_E, f, \dots, f^{n-1})$ est une base de $\mathcal{C}(f)$. Quelle est la dimension de $\mathcal{C}(f)$?

$\boxed{\textbf{29.21}}$ **[♦♦◇]** Soit $n \in \mathbb{N}^*$. Soient $a_1, \dots, a_n$ n réels deux à deux distincts.
Soient $b_1, \dots, b_n$, $c_1, \dots, c_n$ d'autres réels. Montrer qu'il existe un unique polynôme P dans $\mathbb{R}_{2n-1}[X]$ tel que

$$\forall i \in [\![1, n]\!] \quad P(a_i) = b_i \quad \text{ et } \quad P'(a_i) = c_i.$$

$\boxed{\textbf{29.22}}$ **[♦♦♦]** Soit E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels de dimension finie.
À l'aide de l'application ci-dessous, retrouver la formule de Grassmann.

$$\varphi : \left\{ \begin{array}{ccc} F \times G & \to & F + G \\ (x, y) & \mapsto & x + y \end{array} \right. .$$

$\boxed{\textbf{29.23}}$ **[♦◇◇]** Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n.
On note E^* l'espace vectoriel des formes linéaires sur E.
Soit $(e_1, \dots, e_n)$ une base de E. Montrer que $(e_1^*, \dots, e_n^*)$ est une base de E^*.

$\boxed{\textbf{29.24}}$ **[♦♦♦]** Soient $x_1, \dots, x_n$ n réels deux à deux distincts, et

$$F = \left\{ f \in \mathbb{R}^{\mathbb{R}} \mid \forall k \in [\![1, n]\!] \ f(x_k) = 0 \right\}.$$

1. Démontrer que F est un sous-espace vectoriel de $\mathbb{R}^{\mathbb{R}}$.
2. Exhiber un supplémentaire de F dans $\mathbb{R}^{\mathbb{R}}$.

---

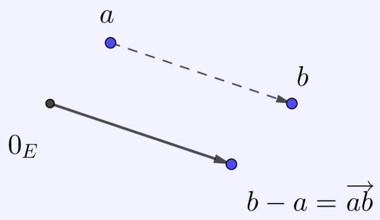
30 Sous-espaces affines d'un espace vectoriel

Dans tout ce qui suit, $(E, +, \cdot)$ désigne un $\mathbb{K}$-espace vectoriel.

Dans un contexte affine, les éléments de E peuvent être notés comme des vecteurs (on écrira alors la "flèche") mais aussi comme des **points**. Dans ce dernier cas, ils sont alors notés avec une lettre sans flèche. Le vecteur nul est noté $\overrightarrow{0}$ comme vecteur et 0_E comme point. On peut aussi noter ce point O et le voir comme un point de référence, une *origine*.

Définition 1.

Soient a et b deux points de E. On note $\overrightarrow{ab}$ le vecteur $b - a$.



Exemple 2 (Propriétés élémentaires)**.**

Soient a, b, c, d quatre points de E. On a

1. Opposé d'un vecteur.
$$\overrightarrow{ba} = -\overrightarrow{ab}.$$
2. Vecteur nul.
$$\overrightarrow{ab} = \overrightarrow{0} \iff a = b.$$
3. Relation de Chasles.
$$\overrightarrow{ac} = \overrightarrow{ab} + \overrightarrow{bc}.$$
4. Règle du parallélogramme.
$$\overrightarrow{ab} = \overrightarrow{cd} \iff \overrightarrow{ac} = \overrightarrow{bd}.$$

Proposition 3 (Deux écritures équivalentes)**.**

Soient a et b deux points de E et $\overrightarrow{u}$ un vecteur de E. On a

$$\overrightarrow{ab} = \overrightarrow{u} \iff b = a + \overrightarrow{u}.$$

En particulier, on passe facilement de la notation point à la notation vecteur en s'appuyant sur le vecteur nul : par définition, si M est un point de E et O le zéro de E, alors

$$M = \overrightarrow{OM}.$$

Définition 4.

Soit $a \in E$. On appelle **translation** de vecteur a , notée T_a l'application

$$T_a : \begin{cases} E & \to & E \\ x & \mapsto & x + a \end{cases} .$$

Proposition 5 (Propriétés des translations)**.**

1. $T_{0_E} = \mathrm{id}_E$.
2. La composée de deux translations est une translation :

$$\forall (a,b) \in E^2 \quad T_a \circ T_b = T_{a+b}$$

3. Pour tout $a \in E$, T_a est une bijection et

$$T_a^{-1} = T_{-a}$$

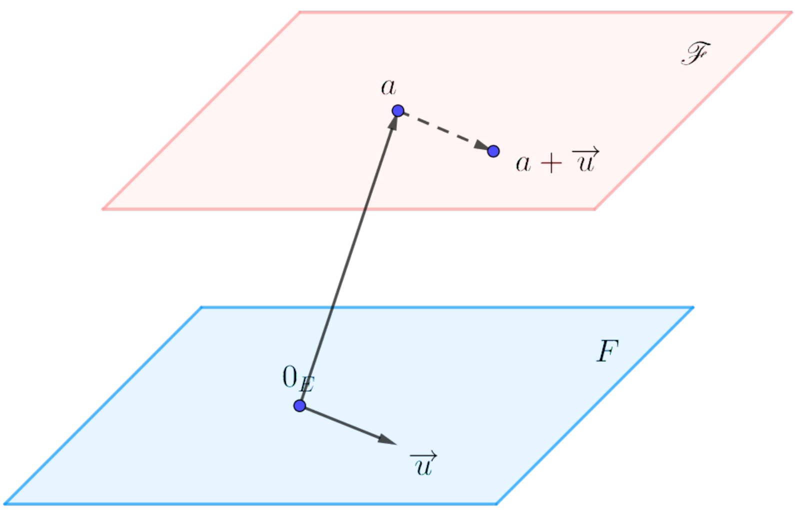
4. L'ensemble des translations sur E, noté $\mathcal{T}(E)$ est, muni de la loi $\circ$, un groupe abélien.
5. L'application $a \mapsto T_a$ est un morphisme de groupes entre $(E, +)$ et $(\mathcal{T}(E), \circ)$.

Définition 6.

D'une partie $\mathscr{F}$ de E, on dit que c'est un **sous-espace affine** de E si c'est le translaté d'un sous-espace vectoriel de E, c'est-à-dire s'il existe un point $a \in E$ un sous-espace vectoriel F de E tels que

$$\mathscr{F} = T_a(F) = a + F = \{a + \overrightarrow{u} \mid \overrightarrow{u} \in F\} .$$

On parle alors de $\mathscr{F}$ comme du sous-espace affine passant par le point a et dirigé par F.



Proposition-Définition 7.

Soit $a \in E$, F un s.e.v. de E et $\mathscr{F}$ le sous-espace affine passant par le point a et dirigé par F. Alors
$$\forall b \in \mathscr{F} \quad \mathscr{F} = b + F \quad \text{et} \quad F = \left\{ \overrightarrow{cd},\ (c,d) \in \mathscr{F}^2 \right\}.$$
Le sous-espace vectoriel F associé à $\mathscr{F}$ est donc unique et appelé **direction** du sous-espace affine $\mathscr{F}$.

Remarques.

1. Tout sous-espace vectoriel F est un sous-espace affine de E puisque $F = 0_E + F$ mais, sauf dans le cas où E est trivial, il existe des sous-espace affines de E qui ne contiennent par 0_E.
2. Un sous-espace affine est non vide par définition. Il peut être réduit à un point lorsque sa direction est le sous-espace vectoriel nul.

Preuve.

• Soit $(c,d) \in \mathscr{F}^2$. Par définition, il existe $(\overrightarrow{u}, \overrightarrow{v}) \in F^2$ tel que $c = a + \overrightarrow{u}$ et $d = a + \overrightarrow{v}$. On a bien
$$\overrightarrow{cd} = d - c = (a + \overrightarrow{v}) - (a + \overrightarrow{u}) = \overrightarrow{v} - \overrightarrow{u} \in F.$$
Réciproquement, si $\overrightarrow{u} \in F$, on peut l'écrire $\overrightarrow{u} = \overrightarrow{cd}$ avec $c = a \in \mathscr{F}$ et $d = a + \overrightarrow{u}\mathscr{F}$. Ceci achève de démontrer l'égalité
$$F = \left\{ \overrightarrow{cd},\ (c,d) \in \mathscr{F}^2 \right\}.$$
En exprimant la direction de $\mathscr{F}$ en fonction de cet espace affine, on prouve son unicité.

• Soit $b \in \mathscr{F}$. On prouve facilement l'égalité $a + F = b + F$ par double inclusion. Un élément de l'ensemble de droite s'écrit $b + \overrightarrow{u}$, avec $\overrightarrow{u} \in F$. Et s'écrit donc $a + (b - a) + \overrightarrow{u} = a + \overrightarrow{ba} + \overrightarrow{u}$. Puisque a et b sont dans $\mathscr{F}$, alors $\overrightarrow{ba}$ est dans F puis $\overrightarrow{ba} + \overrightarrow{u}$ aussi. L'autre inclusion est démontrée de la même façon. □

Définition 8.

On appelle

— **Droite affine** de E tout sous-espace affine dont la direction est une droite.

— **Plan affine** de E tout sous-espace affine dont la direction est un plan.

— **Hyperplan affine** de E tout sous-espace affine dont la direction est un hyperplan.

Un singleton de E est un sous-espace affine de E dont la direction est $\{0_E\}$.

Exemple 9 (Sous-espaces affines de $\mathbb{R}^2$).

En discutant selon la dimension de leur direction, on voit que les sous-espaces affines de $\mathbb{R}^2$ sont réduits à un point, ou une droite affine, ou $\mathbb{R}^2$.

Exemple 10 (Sous-espaces affines de $\mathbb{R}^3$).

En discutant selon la dimension de leur direction, on voit que les sous-espaces affines de $\mathbb{R}^3$ sont réduits à un point, ou une droite affine, ou un plan affine, ou $\mathbb{R}^3$.

Un exemple de droite affine de $\mathbb{R}^3$:

$$\{(1+2x, 2-x, 3+4x), x \in \mathbb{R}\} = a + \mathrm{Vect}(\overrightarrow{u}) \quad \text{avec} \quad a = (1,2,3) \ \text{ et } \ \overrightarrow{u} = (2,-1,4).$$

Un exemple de plan affine de $\mathbb{R}^3$:

$$\left\{(x,y,z) \in \mathbb{R}^3 : x+y+z=1\right\} = a + \mathrm{Vect}(\overrightarrow{u}, \overrightarrow{v})$$

$$\text{avec} \quad a = (1,0,0) \ \text{ et } \ \overrightarrow{u} = (-1,1,0), \overrightarrow{v} = (-1,0,1).$$

Ce sont des cas particuliers de solutions d'un système linéaire. On rappelle le résultat suivant.

Proposition 11 (Ensemble des solutions d'un système linéaire).

Soit $AX = B$ un système linéaire compatible et $X_{pa} \in M_{p,1}(\mathbb{K})$ une solution particulière du système. L'ensemble des solutions S s'écrit

$$S = \{X_{pa} + Y, \ Y \in S_0\},$$

où S_0 est l'ensemble des solutions de $AX = 0_{n,1}$, système homogène associé.

L'ensemble S est un sous-espace affine de $\mathbb{K}^p$ passant par X_{pa} et de direction le s.e.v. S_0.

Ci-dessous des exemples de sous-espaces affines dans des espaces vectoriels différents de $\mathbb{K}^p$.

Proposition 12 (Équations différentielles linéaires d'ordre 1).

Soient $a : I \to \mathbb{K}$ et $b : I \to \mathbb{K}$ deux fonctions continues. L'équation

$$y' + a(x)y = b(x) \quad (E)$$

a des solutions. Si z_p est une telle solution (« particulière ») et A une primitive de a sur I, alors l'ensemble des solutions de (E) est

$$\mathscr{S} = \left\{x \mapsto z_p(x) + \lambda e^{-A(x)}, \lambda \in \mathbb{K}\right\}.$$

L'ensemble $\mathscr{S}$ est une droite affine de $\mathcal{D}(I, \mathbb{K})$ passant par z_p et dirigée par la droite vectorielle $\mathrm{Vect}(e^{-A})$.

On a aussi résolu certaines équations différentielles linéaires d'ordre 2 à coefficients constants. Lorsqu'elles ont une solution, on a observé que l'ensemble des solutions a une structure de plan affine.

Proposition 13 (Suites arithmético-géométrique)**.**

Soit $(a,b) \in \mathbb{K}^2$ tel que $a \neq 1$. Notons S l'ensemble des suites u telles que

$$\forall n \in \mathbb{N} \quad u_{n+1} = au_n + b.$$

L'équation au point fixe $x = ax + b$ possède une unique solution dans $\mathbb{K}$, notons-la α. Alors,

$$\mathscr{D} = \{n \mapsto \alpha + \lambda a^n, \lambda \in \mathbb{K}\}$$

L'ensemble $\mathscr{D}$ est une droite affine de $\mathbb{R}^{\mathbb{N}}$ passant par la suite constante égale à α et dirigée par la droite vectorielle $\text{Vect}(g)$ où g est la suite géométrique de raison a et de premier terme 1.

Proposition 14 (L'ensemble des polynômes interpolateurs)**.**

Soit $n \in \mathbb{N}^*$, $(x_1, \ldots, x_n) \in \mathbb{K}^n$ (scalaires deux à deux distincts) et $(y_1, \ldots, y_n) \in \mathbb{K}^n$.
Soit P l'unique polynôme de $\mathbb{K}_{n-1}[X]$ tel que $\forall i \in [\![1, n]\!]$ $P(x_i) = y_i$.

L'ensemble $\mathscr{I}$ des polynômes $Q \in \mathbb{K}[X]$ tels que $\forall i \in [\![1, n]\!]$ $Q(x_i) = y_i$

$$\mathscr{I} = \left\{ P + A \cdot \prod_{i=1}^{n} (X - x_i), \quad \text{où } A \in \mathbb{K}[X]. \right\}$$

L'ensemble $\mathscr{I}$ est un sous-espace affine de $\mathbb{K}[X]$ passant par l'unique polynôme interpolateur de degré inférieur à $n-1$ et dirigé par le sous-espace vectoriel des multiples de $\prod_{i=1}^{n} (X - x_i)$.

Il est temps de proposer un cadre unificateur.

Théorème 15.

Soient E et F deux $\mathbb{K}$-espaces vectoriels, $f \in \mathscr{L}(E, F)$ une application linéaire et $b \in F$. L'équation

$$f(x) = b$$

d'inconnue $x \in E$ est appelée **équation linéaire**.

Supposons qu'elle possède une solution $a \in E$. Alors l'ensemble de ses solutions est

$$\{a + \overrightarrow{u} \mid \overrightarrow{u} \in \text{Ker} f\}.$$

C'est le sous-espace affine passant par a et de direction $\text{Ker} f$.

Preuve.
Soit $x \in E$. On a

$$f(x) = b \iff f(x) = f(a) \iff f(x - a) = 0_F \iff \overrightarrow{ax} \in \text{Ker} f.$$

□

Exercices

$\boxed{\textbf{30.1}}$ **[♦◇◇]** Soit $(\mathscr{F}_i)_{i\in I}$ une famille de sous-espaces affines affines de E.
Pour tout $i \in I$, on note F_i la direction de $\mathscr{F}_i$.
Montrer que si $\bigcap_{i\in I} \mathscr{F}_i \neq \emptyset$, alors $\bigcap_{i\in I} \mathscr{F}_i$ est un sous-espace affine de direction $\bigcap_{i\in I} F_i$.

$\boxed{\textbf{30.2}}$ **[♦◇◇]** Soient $\mathscr{F} = a + F$ et $\mathscr{G} = b + G$ deux sous-espaces affines de E.

1. Montrer que : $\mathscr{F} \cap \mathscr{G} \neq \emptyset \iff \overrightarrow{ab} \in F + G$.
2. On suppose que $F + G = E$. Montrer que $\mathscr{F} \cap \mathscr{G} \neq \emptyset$.
3. On suppose que $F \oplus G = E$. Montrer que $\mathscr{F} \cap \mathscr{G}$ est réduit à un point.

31

Comparaison locale

Dans ce chapitre, I est un intervalle de $\mathbb{R}$, dont a est un élément ou une borne (a peut valoir $+\infty$ ou $-\infty$). Les fonctions considérées sont définies sur I ou sur $I \setminus \{a\}$ et sont à valeurs réelles (même si des images complexes seraient possibles, après tout).

On supposera que les fonctions considérées, généralement notées f, g et h dans les définitions et propositions, ne s'annulent pas au voisinage de a sauf peut-être en a, ce qui donne un sens au quotient f/g au voisinage de a. Autoriser les fonctions à s'annuler en a permet d'écrire notamment des taux d'accroissements en a. Pour alléger les énoncés, ces hypothèses ne seront pas répétées chaque fois.

Pour ce qui concerne les suites, notées (u_n), (v_n), (w_n) dans les définitions et propositions, elles sont supposées ne plus s'annuler à partir d'un certain rang, ce qui donne un sens au quotient u/v àpdcr.

1 Trois relations de comparaison locale pour les fonctions.

1.1 Négligeabilité.

Définition 1 (Négligeabilité : fonctions)**.**

On dit que f est **négligeable** devant g **en** a si la fonction $\frac{f}{g}$ tend vers 0 en a. On note alors

$$f \underset{a}{=} o\left(g\right) \qquad \text{ou} \qquad f(x) \underset{a}{=} o\left(g(x)\right).$$

On peut dire « $f(x)$ est un petit o de $g(x)$ » en a.

Remarque. L'écriture

$$f(x) \underset{a}{=} g(x) + o(h(x))$$

s'interprète de la manière suivante : la fonction f s'écrit comme une somme de fonctions $g+\widetilde{g}$ et l'information dont on dispose sur $\widetilde{g}$, c'est que cette fonction est négligeable devant la fonction h en a.

Exemple 2.

Les exemples ci-dessous, très élémentaires pour apprivoiser la notation, sont généralisés ensuite.

$$x^2 \underset{0}{=} o(x) \qquad x \underset{+\infty}{=} o(x^2) \qquad e^x \underset{+\infty}{=} o(e^{2x}) \qquad e^{2x} \underset{-\infty}{=} o(e^x)$$

$$\ln(x) \underset{+\infty}{=} o(x) \qquad \ln(x) \underset{0_+}{=} o\left(\frac{1}{x}\right) \qquad x \underset{+\infty}{=} o(e^x) \qquad e^x \underset{-\infty}{=} o\left(\frac{1}{x}\right)$$

Proposition 3 (Puissances au voisinage de $+\infty$ et de $0+$)**.**

$$\forall(\alpha,\beta)\in\mathbb{R}^2 \qquad \alpha<\beta \quad\Longrightarrow\quad x^\alpha \underset{+\infty}{=} o(x^\beta) \quad \text{et} \quad x^\beta \underset{0+}{=} o(x^\alpha).$$

Retenons en vue des développements limités que $x^2 \underset{0}{=} o(x)$, $x^3 \underset{0}{=} o(x^2)$, $x^4 \underset{0}{=} o(x^3)$...

Proposition 4 (Fonctions exponentielles)**.**

$$\forall(a,b)\in\mathbb{R}^2 \quad a<b \quad\Longrightarrow\quad e^{ax} \underset{+\infty}{=} o(e^{bx}) \quad \text{et} \quad e^{bx} \underset{-\infty}{=} o(e^{ax}).$$

Proposition 5 (Croissances comparées)**.**

Pour tous $\alpha,\beta,\gamma\in]0,+\infty[$, on a

$$\ln^\beta(x) \underset{+\infty}{=} o(x^\alpha) \qquad x^\alpha \underset{+\infty}{=} o(e^{\gamma x}) \qquad |\ln(x)|^\beta \underset{0}{=} o(x^{-\alpha}) \qquad e^{\gamma x} \underset{-\infty}{=} o\left(|x|^{-\alpha}\right).$$

La notation $o(1)$ sera bien pratique pour désigner une quantité qui tend vers 0 :

Proposition 6 (Une nouvelle façon d'exprimer qu'une fonction tend vers 0)**.**

$$f(x) \underset{a}{=} o(1) \iff f(x) \underset{x\to a}{\longrightarrow} 0.$$

Exemple 7 (on négligera souvent des constantes)**.**

Si C est une constante et $f(x) \underset{x\to a}{\longrightarrow} +\infty$, alors $C \underset{a}{=} o\left(f(x)\right)$.

1.2 Domination.

Définition 8 (Domination : fonctions)**.**

On dit que f est **dominée** par g en a si la fonction $\frac{f}{g}$ est bornée au voisinage de a. On note alors

$$f \underset{a}{=} O\left(g\right) \qquad \text{ou} \qquad f(x) \underset{a}{=} O\left(g(x)\right).$$

On peut dire « $f(x)$ est un grand O de $g(x)$ » en a.

On se souvient qu'être bornée, c'est être majorée en valeur absolue... on a donc

$$f(x) = O(g(x)) \iff \exists C>0 \;\; \exists \eta>0 \;\; \forall x \in I\setminus\{a\} \;\; |x-a|\leq \eta \Longrightarrow |f(x)| \leq C|g(x)|.$$

Exemple 9.

$$x^2\sin(x) \underset{+\infty}{=} O(x^2) \qquad x^2 \sin\left(\frac{1}{x}\right) \underset{0}{=} O(x^2).$$

Proposition 10 (Un petit o est un grand O)**.**

$$f(x) \underset{a}{=} o(g(x)) \implies f(x) \underset{a}{=} O(g(x))$$

Proposition 11 (Une nouvelle façon d'exprimer qu'une fonction est bornée localement)**.**

$$f(x) \underset{a}{=} O(1) \iff f \text{ bornée au voisinage de } a$$

1.3 Équivalence.

Définition 12 (Équivalence de fonctions)**.**

On dit que f est **équivalente à** g **en** a si la fonction $\frac{f}{g}$ tend vers 1 en a. On note alors

$$f(x) \underset{a}{\sim} g(x).$$

Remarque. Si $f(x) \underset{a}{\sim} g(x)$, on dit que $g(x)$ est un **équivalent** de $f(x)$ au voisinage de a. Lorsqu'on cherche « un équivalent » de $f(x)$, on veut une fonction équivalente à f qui soit *plus simple* que f.

Théorème 13 (Lien entre $\sim$ et $=$)**.**

$$f(x) \underset{a}{\sim} g(x) \iff f(x) \underset{a}{=} g(x) + o(g(x))$$

Remarque. Il sera important de savoir traduire l'équivalence à l'aide d'une égalité, notamment pour travailler avec des sommes (on ne pourra pas sommer des équivalents).

Exemple 14 (Obtenir un équivalent)**.**

Donner un équivalent en $+\infty$ ainsi qu'en 0 de la fonction $x \mapsto x^2 + \ln(x) + 1$.

Donner un équivalent en $+\infty$ ainsi qu'en 0 et $-\infty$ de de la fonction $x \mapsto \dfrac{1}{x} + x + e^x + e^{2x}$.

Deux rédactions possibles :
- factoriser par le terme prépondérant et faire apparaître un facteur tendant vers 1,
- négliger le négligeable.

Exemple 15 (Équivalent de la différence)**.**

Soit f une fonction définie au voisinage de $+\infty$ et telle que

$$f(x) = \underset{+\infty}{=} x + 2\ln(x) + 3\ln(\ln(x)) + o\left(\ln(\ln(x))\right).$$

On a

$$f(x) \underset{+\infty}{\sim} x \qquad f(x) - x \underset{+\infty}{\sim} 2\ln(x) \qquad f(x) - x - 2\ln(x) \underset{+\infty}{\sim} 3\ln(\ln(x))$$

Proposition 16.

L'équivalence en a est une relation d'équivalence sur l'ensemble des fonctions ne s'annulant pas au voisinage de a sauf peut-être en a.

Proposition 17 (Limite finie non nulle).

Soit $\ell \in \mathbb{R}^*$.

$$f(x) \underset{x\to a}{\longrightarrow} \ell \quad \text{si et seulement si} \quad f(x) \underset{a}{\sim} \ell$$

Exemple 18 (Un premier tabou).

Tendre vers 0, ce n'est pas *être équivalent à zéro* : ce qui est écrit en italique n'a aucun sens.

⚠ **Pas d'équivalent à** 0**.** ⚠

Proposition 19 (Fonctions polynomiales et fractions rationnelles).

Soient $(a_0, \ldots, a_p) \in \mathbb{R}^{p+1}$ et $(b_0, \ldots, b_q) \in \mathbb{R}^{q+1}$ tels que $a_p \neq 0$ et $b_q \neq 0$.

$$a_p x^p + \ldots + a_1 x + a_0 \underset{x\to\pm\infty}{\sim} a_p x^p \quad \text{(terme de plus haut degré)}$$

$$\frac{a_p x^p + \ldots + a_1 x + a_0}{b_q x^q + \ldots + b_1 x + b_0} \underset{x\to\pm\infty}{\sim} \frac{a_p x^p}{b_q x^q} \quad \text{(termes de plus haut degré)}$$

Proposition 20 (Obtenir un équivalent à l'aide d'un encadrement).

Si on a l'encadrement $f(x) \leq g(x) \leq h(x)$ au voisinage de a et si $f(x) \underset{a}{\sim} h(x)$, alors

$$f(x) \underset{a}{\sim} g(x) \underset{a}{\sim} h(x).$$

Exemple 21.

$$\lfloor x \rfloor \underset{+\infty}{\sim} x.$$

Proposition 22 (L'équivalence préserve le signe).

Si deux fonctions sont équivalentes en a, alors elles ont le même signe au voisinage de a.

Proposition 23 (L'équivalence préserve la limite).

$$f(x) \underset{a}{\sim} g(x) \ \text{ et } \ f(x) \underset{a}{\to} L \in \overline{\mathbb{R}} \quad \Longrightarrow \quad g(x) \underset{a}{\to} L.$$

2 Règles de calcul.

2.1 Jongler avec les o et les O.

Tous les résultats ci-dessous demeurent vrais lorsque o est remplacé par O.

Proposition 24 (Multiplication d'un négligeable par une constante, une suite, une fonction)**.**

1. Les constantes multiplicatives sont absorbées et digérées par o : si $\lambda \in \mathbb{R}$,
$$\lambda \cdot o(f) \underset{a}{=} o(f).$$
2. Les fonctions sont absorbées (mais *pas* digérées) par o : si g est une fonction,
$$g \cdot o(f) \underset{a}{=} o(gf).$$

Proposition 25 (Somme de deux négligeables)**.**

$$o(f) + o(f) \underset{a}{=} o(f).$$

Proposition 26 (Transitivité de la négligeabilité)**.**

$$f \underset{a}{=} o(g) \quad \text{et} \quad g \underset{a}{=} o(h) \quad \Longrightarrow \quad f = o(h).$$

Notamment $o\left(o(f)\right) \underset{a}{=} o(f)$.

Proposition 27 (On est négligeable par rapport à toutes les fonctions équivalentes)**.**

$$f = o(g) \quad \text{et} \quad g \sim h \quad \Longrightarrow \quad f = o(h).$$

Proposition 28 (Substitution dans un négligeable)**.**

Soit $f, g : I \to \mathbb{R}$ et $u : J \to I$, ainsi que a élément ou borne de I, b élément ou borne de J.

$$\left(f(x) \underset{x \to a}{=} o(g(x)) \quad \text{et} \quad u(t) \underset{t \to b}{\to} a \right) \quad \Longrightarrow \quad f\left(u(t)\right) \underset{t \to b}{=} o\left(g\left(u(t)\right)\right).$$

Exemple 29.

$$\ln(x) \underset{x \to +\infty}{=} o(x) \quad \text{donc} \quad \ln(\ln(x)) \underset{x \to +\infty}{=} o\left(\ln(x)\right)$$

2.2 Ce qu'on peut faire avec $\sim$, et ce qu'on ne peut pas faire.

Proposition 30 (Produit d'équivalents, quotient d'équivalents)**.**

$$f(x) \underset{a}{\sim} g(x) \text{ et } f^*(x) \underset{a}{\sim} g^*(x) \implies f(x)f^*(x) \underset{a}{\sim} g(x)g^*(x) \text{ et } \frac{f(x)}{f^*(x)} \underset{a}{\sim} \frac{g(x)}{g^*(x)}.$$

Exemple 31 (Donner un exemple justifiant chaque tabou)**.**

⚠ **On ne somme pas des équivalents.** ⚠

⚠ **On ne compose pas par une fonction dans un équivalent.** ⚠

Il est possible, en revanche, de *substituer*, c'est-à-dire de composer « à droite ».

Proposition 32 (Substitution dans un équivalent)**.**

Soit $f, g : I \to \mathbb{R}$ et $u : J \to I$, ainsi que a élément ou borne de I, b élément ou borne de J.

$$\left(f(x) \underset{x \to a}{\sim} g(x) \text{ et } u(t) \underset{t \to b}{\to} a \right) \implies f(u(t)) \underset{t \to b}{\sim} g(u(t)).$$

3 Le cas des suites.

On adapte rapidement pour les suites le vocabulaire et les principes dégagés pour les fonctions. On rappelle que dans ce qui suit, u et v seront des suites qui ne s'annulent pas à partir d'un certain rang.

Définition 33 (Négligeabilité et domination : suites)**.**

On dit que (u_n) est **négligeable** devant (v_n) si $\frac{u_n}{v_n} \to 0$. On note alors $u_n = o(v_n)$

On dit que (u_n) est **dominée** par (v_n) si $\left(\frac{u_n}{v_n}\right)$ est bornée. On note alors $u_n = O(v_n)$.

On dit que (u_n) est **équivalente** à (v_n) si $\dfrac{u_n}{v_n} \to 1$. On note alors $u_n \sim v_n$.

Pour les suites, rien besoin d'écrire sous le symbole $=$ ou le symbole $\sim$: l'horizon, c'est forcément $n \to +\infty$.

Les principes établis pour les fonctions se généralisent aux suites. En particulier, les produits et quotients d'équivalents sont possibles, mais pas les sommes. Pour travailler avec ces dernières, on rappelle que

$$\boxed{u_n \sim v_n \iff u_n = v_n + o(v_n).}$$

Plutôt que de récrire les théorèmes dans le cas des suites, on va se concentrer sur une collection d'exemples.

Énonçons tout de même quelques résultats relatifs aux suites géométriques et un résultat de substitution.

Proposition 34 (Suites géométriques)**.**

$$\forall (p,q) \in \mathbb{R}\times\mathbb{R}^* \qquad |p|<|q| \quad \Longrightarrow \quad p^n = o\left(q^n\right).$$

Proposition 35 (Croissances comparées)**.**

Soient $a \in \mathbb{R}$, $p>1$ et $q \in]-1,1[$.

$$n^a = o\left(p^n\right) \quad \text{et} \quad q^n = o(n^a).$$

Proposition 36 (Substitution dans un équivalent (valable avec un o ou un O))**.**

Soit $f : I \to \mathbb{R}$ et a un élément de I ou une borne de I. Soit $(u_n) \in I^{\mathbb{N}}$.

$$\left(f(x) \underset{a}{\sim} g(x) \ \text{ et } \ u_n \to a \right) \quad \Longrightarrow \quad f\left(u_n\right) \sim g\left(u_n\right).$$

Exemple 37.

$$n+1 \sim n \qquad \text{et plus généralement } (n+1)^\alpha \sim n^\alpha \text{ pour tout réel } \alpha$$

Exemple 38.

$$\ln(n+1) \sim \ln(n) \quad \text{et} \quad e^{n+1} \not\sim e^n.$$

Exemple 39.

Donner un équivalent pour

$$\sum_{k=1}^{n} k \qquad \sum_{k=1}^{n} k^2 \qquad \sum_{k=1}^{n} k^3.$$

Exemple 40 (Négliger le négligeable)**.**

Donner un équivalent simple pour les termes généraux de suites ci-dessous :

$$\frac{1}{n^2}+\frac{1}{n} \quad 2^n+n^2 \quad \frac{\sqrt{n}}{\ln(n)}+\ln(n).$$

$$\ln(n+1)+\ln(\ln(n)), \quad 2^{-n}+3^{-n}+4^{-n}, \quad 2^n+\mathrm{ch}(n), \quad e^{\sqrt{n}}+n^6.$$

4 Techniques de calculs d'équivalents.

4.1 Approximation du premier ordre et équivalents usuels.

Dans le cours sur la dérivabilité, on a démontré que si f est une fonction dérivable en a, alors il existe une fonction ε qui tend vers 0 en a telle que

$$f(a+h) \underset{0}{=} f(a) + hf'(a) + h\varepsilon(h),$$

ce que l'on peut désormais écrire

$$f(a+h) \underset{0}{=} f(a) + hf'(a) + o(h).$$

On appelle cette écriture un développement limité au voisinage de a à l'ordre 1. Nous le récrivons

$$f(a+h) - f(a) \underset{0}{=} f'(a)h + o(h).$$

Ainsi, si $f'(a) \neq 0$, on peut écrire

$$f(a+h) - f(a) \underset{0}{\sim} f'(a)h.$$

Ceci nous permet d'écrire une petite collection de développements limités à l'ordre 1 en 0, puis la même collection exprimée à l'aide d'équivalents en 0 pour des fonctions usuelles dérivables en ce point. Pour la fonction cos, on donne exceptionnellement (et en avant-première !) le DL à l'ordre 2.

Corollaire 41 (Développements limités usuels à l'ordre 1 en 0)**.**

$$\sin x \underset{0}{=} x + o(x) \qquad \tan x \underset{0}{=} x + o(x) \qquad \cos x \underset{0}{=} 1 - \frac{x^2}{2} + o(x^2)$$

$$e^x \underset{0}{=} 1 + x + o(x) \qquad \ln(1+x) \underset{0}{=} x + o(x)$$

$$\arcsin x \underset{0}{=} x + o(x) \qquad \arctan x \underset{0}{=} x + o(x) \qquad (1+x)^\alpha \underset{0}{=} 1 + \alpha x + o(x) \quad (\alpha \in \mathbb{R})$$

Corollaire 42 (Équivalents usuels en 0)**.**

$$\sin x \underset{0}{\sim} x \qquad \tan x \underset{0}{\sim} x \qquad 1 - \cos x \underset{0}{\sim} \frac{x^2}{2}$$

$$e^x - 1 \underset{0}{\sim} x \qquad \ln(1+x) \underset{0}{\sim} x$$

$$\arcsin x \underset{0}{\sim} x \qquad \arctan x \underset{0}{\sim} x \qquad (1+x)^\alpha - 1 \underset{0}{\sim} \alpha x \quad (\alpha \in \mathbb{R})$$

Exemple 43.

Pourquoi l'écriture ci-dessous est-elle vraie et inintéressante ?

$$\sqrt{1+x} \underset{0}{\sim} 1 + \frac{1}{2}x.$$

Exemple 44.

Donner un équivalent en 0 de
$$f : x \mapsto \frac{e^{3x} - 1}{\ln(1 + x^2)}.$$

Exemple 45.

Calculer
$$\lim_{x \to 0} (1 + x)^{\frac{1}{x}}.$$

Exemple 46 (Un exemple ailleurs qu'en 0)**.**

Justifier que
$$\ln(1 + \cos(t)) \underset{\frac{\pi}{2}}{\sim} \frac{\pi}{2} - t.$$

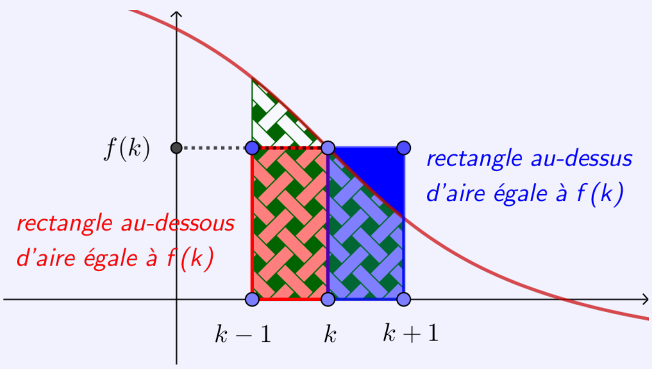
Exemple 47 (Comme un besoin de développement limité)**.**

Donner un équivalent au voisinage de 0 pour $f : x \mapsto e^x - (1 + x)^{\frac{1}{3}}$.
Pourquoi est-on incapable de faire pareil pour $g : x \mapsto e^x - (1 + x)$? De quoi avons-nous besoin ?

4.2 Comparaisons somme/intégrale.

Lemme 48 (Comparer une somme partielle à des intégrales)**.**

Soit $n_0 \in \mathbb{N}$ et $f : [n_0, +\infty[\to \mathbb{R}$ une fonction continue et décroissante. Alors,
$$\forall k \geq n_0 + 1 \qquad \int_k^{k+1} f(t)\mathrm{d}t \leq f(k) \leq \int_{k-1}^{k} f(t)\mathrm{d}t.$$



Un encadrement analogue est possible pour une fonction croissante, on saura l'écrire si besoin.

Méthode (Encadrer une somme).

Soit $f : [n_0, +\infty[\to \mathbb{R}$ décroissante. On sait que pour $k \geq n_0$:

$$\text{pour tout} k \geq n_0 : \int_k^{k+1} f(t)\mathrm{d}t \leq f(k) \qquad \text{pour tout } k \geq n_0+1 : f(k) \leq \int_{k-1}^{k} f(t)\mathrm{d}t.$$

En sommant ces inégalités on obtient pour $n \geq n_0$

$$\sum_{k=n_0}^{n} \int_k^{k+1} f(t)\mathrm{d}t \leq \sum_{k=n_0}^{n} f(k) \leq f(n_0) + \sum_{k=n_0+1}^{n} \int_{k-1}^{k} f(t)\mathrm{d}t.$$

Par la relation de Chasles :

$$\int_{n_0}^{n+1} f(t)\mathrm{d}t \leq \sum_{k=n_0}^{n} f(k) \leq f(n_0) + \int_{n_0}^{n} f(t)\mathrm{d}t.$$

Si les deux membres encadrant la somme sont équivalents, on obtient un équivalent de la somme. Cette méthode sera particulièrement utile lorsqu'on connaît une primitive de la fonction f !

Exemple 49.

Démontrer que

$$\sum_{k=1}^{n} \frac{1}{k} \sim \ln(n) \qquad \text{et} \qquad \sum_{k=1}^{n} \sqrt{k} \sim \frac{2}{3} n\sqrt{n}.$$

5 Équivalents classiques et exemples de développements asymptotiques.

On appelle **développement asymptotique** à $p+1$ termes d'une fonction f au voisinage d'un point a une écriture du type

$$f(x) \underset{a}{=} \varphi_0(x) + \varphi_1(x) + \varphi_2(x) + \cdots + \varphi_p(x) + o\left(\varphi_p(x)\right),$$

où p est un entier naturel $\varphi_0, \ldots, \varphi_p$ des fonctions telles que

$$\forall k \in [\![0, p-1]\!] \quad \varphi_k(x) \underset{x \to a}{=} o\left(\varphi_{k+1}(x)\right)$$

Les développements limités, qu'on étudiera au prochain chapitre, sont des exemples de développement asymptotique.

On appelle développement asymptotique à $p+1$ termes d'une suite (u_n) (au voisinage de l'infini nécessairement) une écriture du type

$$u_n = \varphi_n^{(0)} + \varphi_n^{(1)} + \varphi_n^{(2)} + \cdots + \varphi_n^{(p)} + o\left(\varphi_n^{(p)}\right),$$

où p est un entier naturel et $\varphi^{(0)}, \cdots, \varphi^{(p)}$ des suites telles que

$$\forall k \in [\![0, p-1]\!] \quad \varphi_n^{(k)} \underset{n \to +\infty}{=} o\left(\varphi_n^{(k+1)}\right)$$

Exemple 50 (Un développement asymptotique).

Soit $f : x \mapsto \sqrt{x^2 - 4x + 1}$. Déterminer trois réels a, b et c tels que

$$f(x) \underset{+\infty}{=} ax + b + \frac{c}{x} + o\left(\frac{1}{x}\right).$$

5.1 Somme de termes d'une suite convergente.

Le résultat ci-dessous découle directement du théorème de Cesaro, démontré dans notre cours sur les suites.

Corollaire 51 (du lemme de Cesaro).

Soit $(u_n)_{n\in\mathbb{N}^*}$ une suite qui converge vers un un nombre réel ℓ <u>non nul</u>. Alors

$$\sum_{k=1}^{n} u_k \sim n\ell.$$

Exemple 52.

Soit u la suite définie par

$$\begin{cases} u_0 = 1 \\ \forall n \in \mathbb{N} \; u_{n+1} = u_n \, e^{-u_n} \end{cases}$$

1. Montrer que u converge. Préciser la limite de u.
2. Déterminer la limite de $\frac{1}{u_{n+1}} - \frac{1}{u_n}$ puis un équivalent de u_n.

5.2 Série harmonique et constante d'Euler.

Pour $n \in \mathbb{N}^*$, notons $H_n = \sum_{k=1}^{n} \frac{1}{k}$. Nous avons démontré plus haut que

$$H_n \sim \ln(n) \qquad \text{c'est-à-dire} \qquad H_n = \ln(n) + o\left(\ln(n)\right).$$

Le résultat qui vient est plus précis.

Théorème 53 (Série harmonique et constante d'Euler).

Pour $n \in \mathbb{N}^*$, on note $H_n = \sum\limits_{k=1}^{n} \frac{1}{k}$.
Il existe une constante strictement positive appelée **constante d'Euler** et notée γ telle que

$$H_n = \ln(n) + \gamma + o(1).$$

La constante d'Euler a pour valeur approchée $0,577215$. On ignore si ce nombre est rationnel ou irrationnel.

Avec un peu plus de travail (et le cours sur les séries) on peut établir le résultat plus fin suivant (un développement asymptotique)à quatre termes :

$$H_n = \ln(n) + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + o\left(\frac{1}{n^2}\right).$$

5.3 Équivalent des intégrales de Wallis.

Exemple 54.

On définit, pour tout entier $n \in \mathbb{N}$ le nombre

$$W_n = \int_0^{\pi/2} \sin^n(x)\mathrm{d}x.$$

1. A l'aide d'une intégration par parties, montrer que

$$\forall n \in \mathbb{N} \quad W_{n+2} = \frac{n+1}{n+2} W_n.$$

2. Montrer que la suite (W_n) est décroissante, et n'a pas de terme nul.
   À l'aide d'un encadrement, montrer que $W_{n+1} \sim W_n$.
3. Démontrer les égalités suivantes pour $n \in \mathbb{N}$:

$$W_{2n} = \frac{(2n)!}{2^{2n}(n!)^2} \cdot \frac{\pi}{2} \quad \text{et} \quad W_{2n+1} = \frac{2^{2n}(n!)^2}{(2n+1)!}.$$

4. En donnant une expression explicite du quotient $\frac{W_{2n}}{W_{2n+1}}$, montrer la *formule de Wallis* :

$$\binom{2n}{n} \sim \frac{2^{2n}}{\sqrt{n\pi}}.$$

5. Montrer que la suite $(w_n)_{n\in\mathbb{N}}$, définie par $w_n = (n+1)W_{n+1}W_n$ est constante et en déduire

$$W_n \sim \sqrt{\frac{\pi}{2n}}.$$

5.4 Formule de Stirling.

Étape 1. L'équivalent sans la constante multiplicative.

Lemme 55.

Il existe une constante C dans $]0, +\infty[$ telle que

$$n! \sim C\sqrt{n}\left(\frac{n}{e}\right)^n.$$

Principales étapes de la démonstration.

• On considère la suite u définie par

$$\forall n \in \mathbb{N}^* \quad u_n = \ln\left(\frac{n^n\sqrt{n}}{e^n n!}\right).$$

• Grâce au développement limité $\ln(1+x) \underset{0}{=} x - \frac{x^2}{2} + o(x^2)$ (admis ici) on obtient

$$u_{n+1} - u_n \sim \frac{1}{12n^2},$$

ce qui donne

$$0 \leq u_{k+1} - u_k \leq \frac{1}{k(k+1)} \qquad \text{à.p.d.c.r.}$$

• Notons n_0 un rang à partir duquel l'inégalité ci-dessus est vraie. Grâce au théorème de la limite monotone, on établit la convergence de

$$\left(\sum_{k=n_0}^{n}(u_{k+1} - u_k)\right)_{n \geq n_0}$$

• Par télescopage, on en déduit que u est convergente.

• La suite de terme général e^{-u_n} converge vers une constante strictement positive, CQFD.

Étape 2. Calcul de la constante à l'aide des intégrales de Wallis.

Lemme 56.

La constante C de la proposition 55 vaut $\sqrt{2\pi}$.

Principales étapes de la démonstration.

• Pour $n \in \mathbb{N}$, rappelons que

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2}.$$

• Or, par quotient d'équivalents, en utilisant le lemme 55,

$$\binom{2n}{n} \sim \frac{\sqrt{2}}{C\sqrt{n}} 2^{2n}.$$

• En confrontant les deux équivalents obtenus pour $\binom{2n}{n}$, on obtient $\boxed{C = \sqrt{2\pi}}$.

Théorème 57 (Formule de Stirling)**.**

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

Corollaire 58 (La formule de Stirling écrite comme un développement asymptotique)**.**

$$\ln(n!) = n\ln(n) - n + \frac{1}{2}\ln(n) + \frac{1}{2}\ln(2\pi) + o(1).$$

5.5 Suites définies par récurrence.

Exemple 59.

Soit (u_n) une suite définie par $u_1 = 1$ et $u_{n+1} = \ln(n + u_n)$.

1. Montrer que $u_n \to +\infty$.
2. Montrer que $\forall n \geq 1 \ u_n \leq \ln(2n)$. En déduire que $u_n \sim \ln(n)$.
3. Donner un développement asymptotique à deux termes de (u_n).

5.6 Suites définies implicitement.

Exemple 60.

On considère, pour $n \in \mathbb{N}^*$, l'équation $x + \ln(x) - n = 0$.

1. Montrer que pour tout $n \in \mathbb{N}^*$, l'équation possède une unique solution, notée x_n.
2. Montrer que $(x_n)_{n\in\mathbb{N}^*}$ diverge
3. Donner un équivalent de x_n lorsque n tend vers $+\infty$.
4. Donner enfin un développement asymptotique à trois termes.

Exercices

31.1 **[♦◇◇]** Soient deux fonctions f et g définies au voisinage d'un point $a \in \overline{\mathbb{R}}$ et telles que

$$f(x) \underset{a}{\sim} g(x) \quad \text{et} \quad f(x) \xrightarrow[x\to a]{} +\infty.$$

Démontrer que $\ln(f(x)) \underset{a}{\sim} \ln(g(x))$.

31.2 **[♦◇◇]** On fixe un entier $p \in \mathbb{N}$. Donner un équivalent quand $n \to +\infty$ de $\binom{n}{p}$.

31.3 **[♦◇◇]** Prouver que $\sum_{k=1}^{n} \ln(k) \sim n\ln(n)$ et que $\sum_{k=1}^{n} \frac{1}{k\ln(k)} \sim \ln(\ln(n))$.

31.4 **[♦♦◇]** Prouver que $\sum_{k=1}^{n} e^{k^2} \sim e^{n^2}$.

$\boxed{\textbf{31.5}}$ **[♦♦◇]** Soit $F : x \mapsto \displaystyle\int_2^x \ln(\ln(t))\mathrm{d}t$.

1. Justifier que la fonction F est bien définie sur $]1, +\infty[$.
2. Donner un équivalent de F en $+\infty$.

$\boxed{\textbf{31.6}}$ **[♦♦◇]** Soient a et b dans $\mathbb{R}_+^*$. Calculer $\displaystyle\lim_{x\to 0}\left(\frac{a^x + b^x}{2}\right)^{\frac{1}{x}}$.

$\boxed{\textbf{31.7}}$ **[♦♦◇]** Donner un équivalent simple en $+\infty$ de $\tan\left(\frac{\pi x}{2x+1}\right)$.

$\boxed{\textbf{31.8}}$ **[♦◇◇]** Soit $f : x \mapsto \dfrac{\ln(x)}{1-x^2}$, définie sur $\mathbb{R}_+^* \setminus \{1\}$.

1. Donner un équivalent de f en 0.
2. Donner un équivalent de f en $+\infty$. Prouver que $f(x) \underset{+\infty}{=} o\left(\frac{1}{x^{3/2}}\right)$.
3. Donner un équivalent de f en 1.

$\boxed{\textbf{31.9}}$ **[♦♦◇]** Équivalent d'une suite d'intégrales

Pour $n \in \mathbb{N}$, soit $I_n = \displaystyle\int_0^{\frac{\pi}{4}} \tan^n(x)\mathrm{d}x$.

1. Calculer $I_n + I_{n+2}$ pour un entier naturel n donné.
2. Montrer que (I_n) est décroissante. En déduire l'inégalité $I_{n+2} + I_{n+2} \leq I_n + I_{n+2} \leq I_n + I_n$, valable pour tout n.
3. En déduire un équivalent de I_n.

$\boxed{\textbf{31.10}}$ **[♦♦◇]** [Développement asymptotique d'une suite définie par récurrence]

On note $(u_n)_{n\in\mathbb{N}}$ la suite définie par $u_0 = 0$ et $u_{n+1} = \sqrt{u_n + n^2}$ pour tout $n \in \mathbb{N}$.

1. Montrer que $\lim u_n = +\infty$.
2. Montrer que $n - 1 \leqslant u_n \leqslant n$ pour tout $n \in \mathbb{N}$, puis en déduire un équivalent simple de u_n lorsque n tend vers $+\infty$.
3. En déduire que $u_n = n - \frac{1}{2} + o(1)$.

$\boxed{\textbf{31.11}}$ **[♦♦♦]** Équivalent d'une suite définies implicitement]

1. Pour tout $n \in \mathbb{N}^*$, démontrer que l'équation $x - 1 - \ln(x + n) = 0$ possède une unique solution sur $\mathbb{R}_+^*$, qu'on notera x_n.
2. Démontrer que $x_n \sim \ln(n)$.

$\boxed{\textbf{31.12}}$ **[♦♦♦]** Équivalents pour deux suites définie implicitement

1. Soit $f :]0, +\infty[\to \mathbb{R}$, définie par $f(x) = x - \ln(x)$.
2. Montrer que pour tout $n \in \mathbb{N}^*$, il existe un couple unique $(u_n, v_n) \in]0, 1] \times [1, +\infty[$ tel que $f(u_n) = f(v_n) = n$.
3. Montrer que la suite $(u_n)_{n\in\mathbb{N}^*}$ converge vers 0 et que $u_n \sim e^{-n}$.
4. Montrer que la suite $(v_n)_{n\in\mathbb{N}^*}$ tend vers $+\infty$ et que $v_n \sim n$.

Développements limités

Introduction.

Soit f une fonction définie sur un intervalle I contentant a. Si f est dérivable en a, on a

$$\frac{f(x)-f(a)}{x-a} \underset{x\to a}{\longrightarrow} f'(a), \text{ ce qui se récrit } \frac{f(x)-f(a)}{x-a} \underset{a}{=} f'(a) + o(1).$$

Multiplions par x : on obtient

$$f(x) - f(a) \underset{a}{=} f'(a)(x-a) + o(x-a),$$

et enfin

$$f(x) \underset{a}{=} \underbrace{f(a) + f'(a)(x-a)}_{\text{fonction affine}} \quad + \underbrace{o(x-a)}_{\text{négligeable}},$$

ou encore

$$f(a+h) \underset{0}{=} f(a) + f'(a)h \quad + o(h),$$

On a donc obtenu une approximation de la fonction f au voisinage de a par une fonction polynomiale de degré inférieur à 1. Dans ce cours, on cherche à généraliser ce genre d'approximation : on cherchera à approximer une fonction f par une fonction polynomiale de degré quelconque.

DL (Avant-première : le développement limité du sinus en 0 à l'ordre 3)**.**

$$\sin x \underset{0}{=} x - \frac{x^3}{3!} + o(x^3).$$

Ce type de résultat va offrir de nouveaux outils pour les études locales et asymptotiques de fonctions (et donc de suites par substitution...)

Par exemple, $\dfrac{\sin x - x}{x^3} = \dfrac{-\frac{x^3}{6} + o(x^3)}{x^3} = -\dfrac{1}{6} + o(1)$, ce qui amène une convergence hors de portée jusqu'alors

$$\frac{\sin x - x}{x^3} \underset{x\to 0}{\longrightarrow} -\frac{1}{6}.$$

1 Existence de développements limités.

Dans cette partie, on considère un intervalle I non vide et non réduit à un point, et a un nombre réel, élément ou borne de I. La fonction f est définie sur I, sauf peut-être en a. Elle est en tout cas définie au voisinage de a. L'écriture $f(a+h)$ aura donc toujours un sens pour un certain h au voisinage de 0.

1.1 Notion de développement limité en a.

Définition 1.

On dit que f admet un **développement limité** à l'ordre n au voisinage de a ($\mathrm{DL}_n(a)$) s'il existe des nombres réels $a_0, a_1, \ldots, a_n$ tels que

$$f(x) \underset{a}{=} a_0 + a_1(x-a) + \ldots + a_n(x-a)^n + o\left((x-a)^n\right).$$

Proposition 2 (se ramener à 0)**.**

La fonction f admet un développement limité à l'ordre n au voisinage de a si et seulement si la fonction $h \mapsto f(a+h)$ admet un développement limité à l'ordre n au voisinage de 0, c'est-à-dire s'il existe des nombres réels $a_0, a_1, \ldots, a_n$ tels que

$$f(a+h) \underset{0}{=} a_0 + a_1 h + \ldots + a_n h^n + o\left(h^n\right).$$

Exemples. $\mathrm{DL}_1(2)$ de $\ln$; $\mathrm{DL}_n(0)$ de $x \mapsto \dfrac{1}{1-x}$.

DL.

$$\frac{1}{1-x} \underset{0}{=} \sum_{k=0}^{n} x^k + o(x^n) = 1 + x + x^2 + x^3 + \ldots + x^n + o(x^n).$$

$$\frac{1}{1+x} \underset{0}{=} \sum_{k=0}^{n} (-1)^k x^k + o(x^n) = 1 - x + x^2 - x^3 + \ldots + (-1)^n x^n + o(x^n).$$

Proposition 3 (Unicité d'un DL en a)**.**

Supposons que f admette au voisinage de a deux développements limités

$$\begin{cases} f(a+h) & \underset{0}{=} & a_0 + a_1 h + \ldots + a_n h^n + o\left(h^n\right) \\ f(a+h) & \underset{0}{=} & b_0 + b_1 h + \ldots + b_n h^n + o\left(h^n\right) \end{cases} \quad \text{Alors,} \begin{cases} a_0 & = & b_0 \\ & \ldots & \\ a_n & = & b_n. \end{cases}$$

La fonction polynomiale $x \mapsto \sum_{k=0}^{n} a_k x^k$ est appelée **partie régulière** du DL de f en a à l'ordre n.

Proposition 4 (Parité/Imparité et DL en 0).

Si une fonction paire admet un $\mathrm{DL}_n(0)$, ses coefficients d'ordre impair sont nuls.
Si une fonction impaire admet un $\mathrm{DL}_n(0)$, ses coefficients d'ordre pair sont nuls.

Proposition 5 (Troncature).

Supposons que f admet un $\mathrm{DL}_n(a)$, de partie régulière $x \mapsto \sum_{k=0}^{n} a_k x^k$.

Alors, pour tout $p \in [\![0, n]\!]$, la fonction f admet un $\mathrm{DL}_p(a)$ de partie régulière $x \mapsto \sum_{k=0}^{p} a_k x^k$.

Proposition 6 (DL à l'ordre 1 et dérivabilité).

Soit $f : I \to \mathbb{R}$ et $a \in I$. Il y a équivalence entre les deux assertions suivantes.

1. f est dérivable en a.
2. Il existe deux réels a_0, a_1 tels que

$$\forall x \in I \quad f(a+h) \underset{a}{=} a_0 + a_1 h + o(h).$$

Dans le cas où 2 est vraie, alors nécessairement, $a_0 = f(a)$ et $a_1 = f'(a)$.

L'implication (1) $\Longrightarrow$ (2) sera généralisée à un ordre plus grand par la formule de Taylor-Young, qui nous dira que si on a suffisamment de régularité en a, on y a un DL.
En revanche, l'implication (2) $\Longrightarrow$ (1) ne se généralise pas aux ordres plus grands que 2 : voir le TD pour un exemple de fonction admettant un DL à l'ordre 2 en 0 mais n'étant pas deux fois dérivable en 0.

1.2 Primitivation d'un développement limité.

Proposition 7 (Primitivation d'un DL).

Soit $f : I \to \mathbb{R}$ une fonction dérivable sur I et a un élément de I.
On suppose que f' admet un DL à l'ordre $n \in \mathbb{N}$ au voisinage de a : $\exists (a_0, a_1, \ldots, a_n) \in \mathbb{R}^{n+1}$:

$$f'(a+h) \underset{0}{=} a_0 + a_1 h + \ldots + a_n h^n + o\left(h^n\right).$$

Alors, f admet un DL à l'ordre $n+1$ au voisinage de a et

$$f(a+h) \underset{0}{=} \boxed{f(a)} + a_0 h + \frac{a_1}{2} h^2 + \ldots + \frac{a_n}{n+1} h^{n+1} + o\left(h^{n+1}\right).$$

On a encadré la « constante d'intégration » : on tâchera de ne pas l'oublier lorsqu'on primitive un DL... surtout lorsqu'elle n'est pas nulle ! ;)

Exemple 8.

En partant du DL en 0 au premier ordre de tan obtenir celui à l'ordre 3.
Utiliser le DL obtenu pour en déduire celui à l'ordre 5.

DL.

$$\ln(1-x) \underset{0}{=} -x - \frac{x^2}{2} - \frac{x^3}{3} - \cdots - \frac{x^n}{n} + o\left(x^n\right) \quad = -\sum_{k=1}^{n} \frac{x^k}{k} + o(x^n).$$

$$\ln(1+x) \underset{0}{=} x - \frac{x^2}{2} + \frac{x^3}{3} + \cdots (-1)^{n-1}\frac{x^n}{n} + o\left(x^n\right) = \sum_{k=1}^{n} (-1)^{k-1}\frac{x^k}{k} + o(x^n).$$

DL.

$$\arctan(x) = \sum_{k=1}^{n} (-1)^k \frac{x^{2k+1}}{2k+1} + o(x^{2n+1}) \underset{0}{=} x - \frac{x^3}{3} + \cdots + (-1)^n \frac{x^{2n+1}}{2n+1} + o(x^{2n+1}).$$

1.3 Formule de Taylor-Young et DL usuels.

Théorème 9 (Formule de Taylor-Young)**.**

Soient $n \in \mathbb{N}$, f une fonction de classe $\mathcal{C}^n$ sur I, et $a \in I$. Alors, f admet un développement limité à l'ordre n au voisinage de a :

$$f(a+h) \underset{0}{=} \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!} h^k + o\left(h^n\right).$$

DL.

$$\exp(x) \underset{0}{=} \sum_{k=0}^{n} \frac{x^k}{k!} + o\left(x^n\right) \underset{0}{=} 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots \frac{x^n}{n!} + o\left(x^n\right).$$

Méthode.

Il faut connaître les DL usuels à l'ordre n. On saura à la fois

— écrire la forme dépliée $e^x = {}^0{=}1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots \frac{x^n}{n!} + o\left(x^n\right)$, qui dans la pratique est généralement écrite et utilisée pour $n \in \{1, 2, 3\}$.

— écrire la somme et les coefficients sous leur forme générale : ces coefficients seront à savoir en spé dans le cours sur les séries entières, de toute façon.

DL.

$$\cos x \underset{0}{=} \sum_{k=0}^{p} \frac{(-1)^k}{(2k)!}x^{2k} + o(x^{2p+1}) = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \cdots + \frac{(-1)^p}{(2p)!}x^{2p} + o(x^{2p+1})$$

$$\sin x \underset{0}{=} \sum_{k=0}^{p} \frac{(-1)^k}{(2k+1)!}x^{2k+1} + o(x^{2p+2}) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \cdots + \frac{(-1)^p}{(2p+1)!}x^{2p+1} + o(x^{2p+2}).$$

Exemple 10.

Donner le $\mathrm{DL}_2(\pi/4)$ de cos
- en se ramenant en 0.
- en utilisant la formule de Taylor-Young,

DL (Pour un réel α fixé)**.**

$$\begin{aligned}(1+x)^\alpha &\underset{0}{=} 1 + \sum_{k=1}^{n} \frac{\alpha(\alpha-1)(\alpha-2)\dots(\alpha-(k-1))}{k!}x^k + o(x^n)\\ &\underset{0}{=} 1 + \alpha x + \frac{\alpha(\alpha-1)}{2}x^2 + \cdots + \frac{\alpha(\alpha-1)(\alpha-2)\dots(\alpha-(n-1))}{n!}x^n + o(x^n).\end{aligned}$$

Par exemple, pour $\alpha = \frac{1}{2}$, le DL de $(1+x)^\alpha$ donne

$$\boxed{\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + o(x^2).}$$

De même, pour $\alpha = -\frac{1}{2}$, on obtient

$$\boxed{\frac{1}{\sqrt{1+x}} = 1 - \frac{1}{2}x + \frac{3}{8}x^2 + o(x^2).}$$

Remarque. Pour un réel α et un entier naturel k non nul, on note parfois

$$\binom{\alpha}{k} := \frac{\alpha(\alpha-1)(\alpha-2)\dots(\alpha-k+1)}{k!}.$$

On note aussi $\binom{\alpha}{0} = 1$. Ce nombre est alors appelé "coefficient binomial généralisé". On peut ainsi écrire

$$(1+x)^\alpha \underset{0}{=} \sum_{k=0}^{n} \binom{\alpha}{k} x^k + o(x^n).$$

Lorsque α est un entier naturel, on retrouve la formule du binôme avec un négligeable nul.

⚠ On n'utilisera pas le DL de $(1+x)^\alpha$ lorsque l'exposant dépend de x ! Exemple typique : $(1+\frac{1}{n})^n$.

2 DL et opérations.

Par définition, un DL en a pour une fonction f est un DL en 0 pour $h \mapsto f(a+h)$. C'est donc au voisinage de ce point qu'on énonce tous les résultats de cette section. Dans les énoncés des propositions ci-dessous, les fonctions f et g sont supposées définies au voisinage de 0, sauf peut-être en ce point.

Somme.

Proposition 11.

Sommer un $DL_n(0)$ pour f et un $DL_p(0)$ pour g donne un $DL_q(0)$ pour $f+g$, où $q = \min(p,q)$. Les coefficients de la somme sont la somme des coefficients.

DL.

$$\operatorname{ch}(x) \underset{0}{=} \sum_{k=0}^{p} \frac{x^{2k}}{(2k)!} + o\left(x^{2p}\right) \underset{0}{=} 1 + \frac{x^2}{2!} + \dots \frac{x^{2p}}{(2p)!} + o\left(x^{2p+1}\right).$$

$$\operatorname{sh}(x) \underset{0}{=} \sum_{k=0}^{p} \frac{x^{2k+1}}{(2k+1)!} + o\left(x^{2p+2}\right) \underset{0}{=} x + \frac{x^3}{3!} + \dots \frac{x^{2p+1}}{(2p+1)!} + o\left(x^{2p+2}\right).$$

Produit.

Proposition 12.

Si f et g admettent un $\mathrm{DL}_n(0)$, alors $f \times g$ aussi.

Preuve. Supposons qu'il existe $a_0, a_1, \dots, a_n$ ainsi que $b_0, b_1, \dots, b_n$ tels que

$$f(x) = a_0 + a_1 x + \dots + a_n x^n + o(x^n) \quad \text{et} \quad g(x) = b_0 + b_1 x + \dots + b_n x^n + o(x^n).$$

Notons $P : x \mapsto \sum_{k=0}^{n} a_k x^k$ et $Q : x \mapsto \sum_{k=0}^{n} b_k x^k$ respectivement les parties régulières dans le DL à l'ordre n de f et g. On a

$$f(x) \times g(x) = (P(x) + o(x^n))(Q(x) + o(x^n)) = P(x)Q(x) + P(x)o(x^n) + Q(x)o(x^n) + o(x^{2n}).$$

On a $o(x^{2n}) = o(x^n)$. De plus, les fonctions P et Q sont continues en 0 donc y sont bornées. On a donc $P(x)o(x^n) = o(x^n)$ et $Q(x)o(x^n) = o(x^n)$. On a donc

$$f(x) \times g(x) = P(x)Q(x) + o(x^n).$$

La fonction polynomiale PQ est de degré inférieur à $2n$. Pour obtenir la partie régulière à l'ordre n de notre DL, il reste à tronquer à l'ordre n pour obtenir la fonction polynomiale R. On a alors

$$f(x) \times g(x) = R(x) + o(x^n).$$

Notons $R = \sum_{k=0}^{n} c_k x^k$. Pour $k \in [\![0, n]\!]$, c_k est le coefficient devant X^k du produit PQ : on rappelle que

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

$\square$

Exemple 13 (Première et dernière fois qu'on développe un produit de DL jusqu'au bout)**.**

Calculer naïvement le DL à l'ordre 2 en 0 de $\dfrac{e^x}{1-x}$ en écrivant tous les termes, puis souligner en rouge les termes qu'il était inutile de calculer.

Méthode (Calcul malin d'un produit de DL)**.**

Lorsqu'on développe le produit de deux développements limités d'ordre n, les termes d'ordre supérieur à $n+1$ ne sont pas écrits. On les remplace au fur et à mesure du calcul par $o(x^n)$.

Considérons le produit d'un DL de f et d'un DL de g en visant un DL final à l'ordre n.
Si le premier terme non nul de f est d'ordre $p \in [\![0, n]\!]$, il suffit d'utiliser un DL de g à l'ordre $n-p$; on rappelle en effet que $x^p \times o(x^{n-p}) = o(x^n)$.

Exemples 14.

$\mathrm{DL}_2(0)$ de $x \mapsto \sqrt{1+x}\cdot e^x$, $\qquad$ $\mathrm{DL}_3(0)$ de $x \mapsto \dfrac{\ln(1+x)}{1+x}$, $\qquad$ $\mathrm{DL}_6(0)$ de $x \mapsto (1-\cos x)\sin x$.

Quotient. Voici un quotient de DL en 0 dans lequel on a factorisé les premiers termes non nuls :

$$\frac{f(x)}{g(x)} = \frac{a_m x^m}{b_n x^n} \cdot \frac{1 + c_1 x + \ldots + c_p x^p + o(x^p)}{1 + d_1 x + \ldots + d_q x^q + o(x^q)}.$$

$\boxed{\boxed{\text{L'idée}}}$: on peut alors calculer le développement limité à l'ordre q de

$$\frac{1}{1 + d_1 x + \ldots + d_q x^q + o(x^q)} \quad \boxed{\text{à l'aide de celui de } \frac{1}{1+u}} \text{ en posant } u(x) = d_1 x + \ldots + d_q x^q + o(x^q)$$

et d'une substitution. Il restera à faire un produit de DL : on obtient alors

$$\frac{f(x)}{g(x)} = \frac{a_m}{b_n} x^{m-n} \left(1 + e_1 x + \ldots e_r x^r + o(x^r)\right), \qquad \text{où } r = \min(p, q)$$

DL.

$$\tan(x) \underset{0}{=} x + \frac{x^3}{3} + o(x^3) \qquad \text{et} \qquad \mathrm{th}(x) \underset{0}{=} x - \frac{x^3}{3} + o(x^3).$$

Exemple 15.

$$\mathrm{DL}_2(0) \text{ de } x \mapsto \frac{\sin x}{\ln(1+x)}.$$

Composée.

Exemple 16.

$$\mathrm{DL}_8(0) \text{ de } x \mapsto \cos(x^2). \qquad \mathrm{DL}_3(0) \text{ de } x \mapsto \sin\left(\ln(1+x)\right).$$

3 Applications des développements limités.

Dans les deux prochains paragraphes, la fonction f est supposée définie au voisinage de a sauf peut-être en a.

3.1 Calcul de limite, d'équivalent.

Méthode (Limite ?/ Prolongeable par continuité ?/Continue ?).

L'existence d'une limite est équivalente à celle d'un DL à l'ordre 0. Plus précisément, pour $a_0 \in \mathbb{R}$,

$$f(x) \underset{x\to a}{\longrightarrow} a_0 \qquad \Longleftrightarrow \qquad f(x) \underset{a}{=} a_0 + o(1).$$

On cherchera notamment à écrire des DL à l'ordre 0 pour prouver qu'une fonction est prolongeable par continuité en un point.
Si de surcroît f est définie en a, elle y est continue ssi elle admet en a un DL à l'ordre 0.

On pourra relire/refaire le calcul de la limite en 0 de $\left(\dfrac{a^x+b^x}{2}\right)^{\frac{1}{x}}$, fait dans le cours précédent.

Exemple 17 (Fil rouge (1/3)).

Montrer que

$$f : x \mapsto \frac{1}{\ln(1+x)} - \frac{1}{x},$$

est prolongeable par continuité en 0.

Exemple 18 (Se ramener à 0 à partir d'un point fini).

Calculer

$$\lim_{x\to 2} \frac{x^2-2^x}{x-2}.$$

Exemple 19 (Se ramener à 0 à partir de $+\infty$).

Calculer

$$\lim_{x\to+\infty} x\left[\left(1+\frac{2}{x}\right)^x - \left(1+\frac{1}{x}\right)^{2x}\right].$$

Méthode (Obtenir un équivalent à partir d'un DL).

Un DL peut nous aider à obtenir une écriture du type

$$f(a+h) \underset{0}{=} a_p h^p + o(h^p),$$

avec $p \in \mathbb{N}$ et $a_p \neq 0$ (c'est le premier coefficient non nul du DL). On sait alors que

$$f(x) \underset{a}{\sim} a_p (x-a)^p.$$

Exemples 20.

Soient a et b deux réels. On pose

$$g : x \mapsto \cos x - \frac{1+ax^2}{1+bx^2},$$

définie au voisinage de 0.

1. Calculer un développement limité de g en 0 à l'ordre 6.
2. Donner un équivalent de g en 0 de la forme $g(x) \underset{0}{\sim} cx^n$ avec c et n à préciser (on discutera selon la valeur de a et b).

3.2 Étude locale d'une fonction.

Méthode (Dérivable ? / Équation de la tangente ?).

Si f est définie en a, d'après la proposition 6, montrer la dérivabilité en a revient à montrer l'existence d'un DL à l'ordre 1 en a. L'écriture

$$f(x) \underset{a}{=} a_0 + a_1(x-a) + o(x-a),$$

implique que f est dérivable en a et que l'on a $f(a) = a_0$ et $f'(a) = a_1$.
La courbe de f admet alors la droite d'équation $y = a_0 + a_1(x-a)$ comme tangente en a.

Exemple 21 (Fil rouge (2/3)).

Reprenons

$$f : x \mapsto \frac{1}{\ln(1+x)} - \frac{1}{x}.$$

— Démontrer que f est prolongeable en 0 en une fonction dérivable en 0.
— Pour prouver que ce prolongement est de classe $\mathcal{C}^1$, que faudrait-il faire ?

Méthode (Positions relatives du graphe et de la tangente)**.**

Supposons que l'on dispose d'un DL de la forme

$$f(a+h) \underset{0}{=} a_0 + a_1 h + a_p h^p + o(h^p),$$

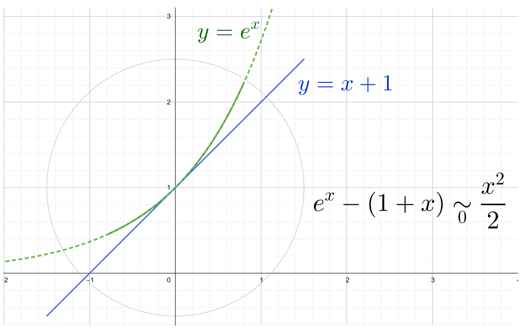
où a_p désigne le premier coefficient non nul après l'ordre 1.
Alors, le graphe de f admet au point a une tangente d'équation $y = a_0 + a_1(x-a)$, et on a

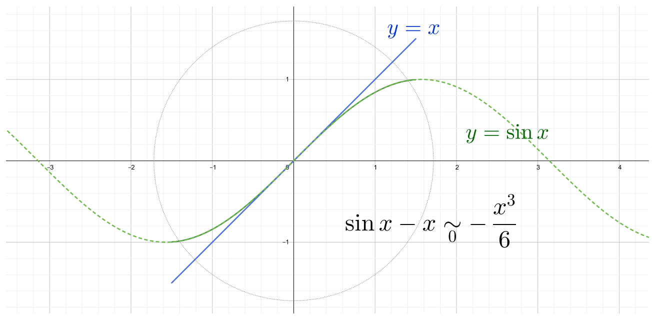
$$f(a+h) - (a_0 + a_1 h) \underset{0}{\sim} a_p h^p.$$

Au voisinage de a, la différence entre f et sa tangente est du signe de $a_p h^p$. Plus précisément,

- Si p est pair, on constate que le graphe est *au-dessus* de sa tangente au voisinage de a si $a_p > 0$, *en-dessous* si $a_p < 0$.
- Si p est impair, on constate un **point d'inflexion** : les positions relatives du graphe et de la tangente sont *opposées de part et d'autre* de a (dépend du signe de a_p).

Deux exemples immédiats pour lesquels on connaît déjà les positions relatives : exp et sin.





Exemple. Fil rouge (3/3) : Comparer $f : x \mapsto \frac{1}{\ln(1+x)} - \frac{1}{x}$ à sa tangente au voisinage de 0.

Proposition 22 (DL d'ordre 2 et extremum local)**.**

Soit $f : I \to \mathbb{R}$ et a un élément à l'*intérieur* de I ($a \in I$ n'est pas une borne de I).

- Supposons que f admet un DL à l'ordre 1 en a :

$$f(a+h) = a_0 + a_1 h + o(h).$$

  Pour que f admette un extremum local en a, il est **nécessaire** que a_1 soit nul.
  Il est équivalent de dire que si f est dérivable en un point a intérieur à son ensemble de définition, et y possède un extremum, alors a est un point critique : $f'(a) = 0$.
- Supposons que f admet un DL à l'ordre 2 en a :

$$f(a+h) = a_0 + a_1 h + a_2 h^2 + o\left(h^2\right)$$

  Pour que f admette un extremum local en a, il est **suffisant** que $a_1 = 0$ et que $a_2 \neq 0$.
  — si $a_1 = 0$ et $a_2 > 0$, f admet en a un minimum local,
  — si $a_1 = 0$ et $a_2 < 0$, f admet en a un maximum local.

Exercices

Manipuler les DL usuels

32.1 **[♦◇◇]** Donner, pour chacune des fonctions suivantes, le développement limité au point 0 à l'ordre 3.

$$a : x \mapsto \ln(1+x) + e^{-x} \quad b : x \mapsto \frac{\sin(x)}{x} \quad c : x \mapsto \frac{1-\cos(x)}{x^2} \quad d : x \mapsto \frac{1}{2+x}.$$

32.2 **[♦◇◇]** Calculer le $\mathrm{DL}_4(0)$ de $x \mapsto \exp(x)\sin(x)$ et de $x \mapsto (\ln(1-x))^2$.

32.3 **[♦♦◇]** Donner le développement limité au point 0 à l'ordre 2 de $f : x \mapsto (1+x)^{\frac{1}{x}}$.

32.4 **[♦♦◇]** Soit $f : x \mapsto \dfrac{e^x}{1+e^{2x}}$ et $g : x \mapsto \arctan(e^x)$.

1. Donner un DL de f en 0 à l'ordre 2.
2. Justifier que g est dérivable sur $\mathbb{R}$ et calculer sa dérivée.
3. En déduire un DL de g en 0 à l'ordre 3.

32.5 **[♦♦◇]** À l'aide du théorème de primitivation, donner le DL de arcsin en 0 à l'ordre 5.

32.6 **[♦♦◇]** Calculer le DL à l'ordre 10 en 0 de $f(x) = \displaystyle\int_x^{x^2} \frac{1}{\sqrt{1+t^4}}\mathrm{d}t$.

32.7 **[♦♦♦]** Donner le DL à l'ordre 100 au voisinage de 0 de $x \mapsto \ln \displaystyle\sum_{k=0}^{99} \frac{x^k}{k!}$.

Formule de Taylor-Young

32.8 **[♦◇◇]** Soit $f \in \mathcal{C}^2(I)$ et x_0 un réel de l'intervalle I. Montrer que la limite suivante existe et la calculer :

$$\lim_{h \to 0} \frac{f(x_0+h) - 2f(x_0) + f(x_0-h)}{h^2}.$$

32.9 **[♦♦◇]** Soit $f : x \mapsto \dfrac{\cos x}{1-x}$. Calculer pour k dans $[\![0,5]\!]$ la valeur de $f^{(k)}(0)$.

32.10 **[♦♦◇]** [La régularité offre des DL mais la réciproque n'est pas vraie]
Soit $f : x \mapsto x^3 \sin(\frac{1}{x})$, prolongée par continuité en 0.

1. Justifier qu'elle admet un DL à l'ordre 2 en 0.
2. Montrer que f n'est pas deux fois dérivable en 0.
3. Expliquer le titre de l'exercice.

32.11 **[♦♦♦]**

1. Donner le DL de $x \mapsto \dfrac{1}{\sqrt{1-x^2}}$ en 0 à l'ordre $2n$, où $n \in \mathbb{N}$.
   On exprimera les coefficients à l'aide des coefficients binomiaux $\binom{2k}{k}$.
2. En déduire une expression de $\arcsin^{(2n+1)}(0)$ pour tout entier $n \in \mathbb{N}$.
3. En utilisant la formule de Stirling, donner un équivalent de $\arcsin^{(2n+1)}(0)$ lorsque n tend vers $+\infty$.

32.12 **[♦♦♦]** Montrer que $f : x \mapsto xe^{x^2}$ est une bijection de $\mathbb{R}$ dans lui-même.
Justifier l'existence d'un DL à l'ordre 4 de f^{-1} en 0 et le calculer.

Applications du calcul de développements limités

32.13 [♦♦♢] Calculer le DL à l'ordre 2 en zéro de la fonction $g : x \mapsto \ln\left(\frac{\sin(x)}{x}\right)$. En déduire la limite :

$$\lim_{n\to+\infty}\left(n\sin\left(\frac{1}{n}\right)\right)^{n^2}.$$

32.14 [♦♦♢] Calculer les limites ci-dessous, si elles existent :

$$\lim_{n\to+\infty}\left(3\cdot 2^{\frac{1}{n}}-2\cdot 3^{\frac{1}{n}}\right)^n\ ;\quad \lim_{x\to 0}(1+\tan x)^{\frac{1}{\sin x}}\ ;\quad \lim_{x\to+\infty} x^{\frac{x+1}{x}}-(x-1)^{\frac{x}{x-1}}.$$

32.15 [♦♢♢] Donner un équivalent de $(1+\frac{1}{n})^{n^2}$.

32.16 [♦♢♢] Calculer un équivalent de $e^{\frac{1}{n}}-e^{\frac{1}{n+1}}$.

32.17 [♦♦♢] Donner un équivalent simple en 0 de $f(x)=x^x-\sin(x)^{\sin(x)}$.

32.18 [♦♦♢] Montrer que le graphe de $f : x \mapsto x^2\ln(1+\frac{1}{x})$ admet une asymptote en $+\infty$; on précisera l'équation de cette droite ainsi que la position du graphe par rapport à l'asymptote.

32.19 [♦♦♢] Démontrer que la fonction $f : x \mapsto \frac{\sin x}{x}$, prolongée par continuité en 0, est de classe $\mathcal{C}^1$ sur $\mathbb{R}$.

32.20 [♦♦♦] Démontrer que la fonction $f : x \mapsto \frac{1}{\tan x}-\frac{1}{x}$ se prolonge en 0 en une fonction de classe $\mathcal{C}^1$.

32.21 [♦♦♦] Soit u la suite définie par $\begin{cases} u_0 \in]0,\frac{\pi}{2}] \\ \forall n\in\mathbb{N}\quad u_{n+1}=\sin(u_n). \end{cases}$

1. Justifier que u est bien définie.
2. Démontrer que u tend vers 0.
3. Démontrer que la suite v définie par $v_n=\frac{1}{u_{n+1}^2}-\frac{1}{u_n^2}$ converge et préciser sa limite.
4. À l'aide du théorème de Cesáro, donner un équivalent de $\frac{1}{u_n^2}$, puis de u_n.

32.22 [♦♦♦]

1. Soit $n\in\mathbb{N}$. Montrer que l'équation $x+e^x=n$ admet une unique solution réelle notée x_n.
2. Établir le développement asymptotique :

$$x_n=\ln n-\frac{\ln n}{n}+o\left(\frac{\ln n}{n}\right).$$

32.23 [♦♦♦] [Recollement des solutions d'une équation différentielle]
Résoudre <u>sur $\mathbb{R}$</u> l'équation différentielle $x(x^2+1)y'+2(x^2+1)y=x$.

32.24 [♦♦♦] Soit $f : x \mapsto \left(\frac{1}{(x-1)^2}\right)^x$.
Donner un développement asymptotique au voisinage de 1 où figurent tous les termes tendant vers $+\infty$.

---

1 Séries.

1.1 Nature d'une série.

Définition 1 (Série, sommes partielles)**.**

Soit $(u_n)_{n\geq n_0}$ une suite réelle ou complexe. À partir de (u_n), on définit la suite $(S_n)_{n\geq n_0}$:

$$\forall n \geq n_0 \quad S_n = \sum_{k=n_0}^{n} u_k.$$

La suite $(S_n)_{n\geq n_0}$ est appelée **série** de terme général u_n, et notée $\sum_{n\geq n_0} u_n$ ou encore $\sum u_n$.
Pour $n \in \mathbb{N}$ le nombre S_n est appelé **somme partielle** d'indice n.

Définition 2 (Série convergente, somme)**.**

Une série $\sum u_n$ est dite **convergente** si la suite de ses sommes partielles (S_n) converge.
Dans ce cas on appelle **somme** de la série, et on note $\sum_{n=n_0}^{+\infty} u_n$ la limite de (S_n) :

$$\sum_{n=n_0}^{+\infty} u_n := \lim_{n\to+\infty} \sum_{k=n_0}^{n} u_k.$$

La série $\sum u_n$ est dite **divergente** si elle n'est pas convergente.

La convergence ou la divergence d'une suite/série sera désignée comme sa **nature**.

⚠ On prendra garde à ne pas confondre :

- $\sum u_n$ désigne une *série* (c'est à dire une suite),
- $\sum\limits_{k=n_0}^{n} u_k$, est un *nombre*, défini pour un entier $n \geq n_0$ donné,
- $\sum\limits_{n=n_0}^{+\infty} u_n$, somme de la série, est un *nombre* qui n'a de sens que si la série $\sum u_n$ est convergente.

Exemple 3 (Que savons-nous déjà sur ces séries ?)**.**

$$\sum 1, \qquad \sum (-1)^n, \qquad \sum \frac{1}{2^n}, \qquad \sum \frac{1}{n}, \qquad \sum \frac{1}{n^2}.$$

Remarque.

1. Déterminer la nature d'une série et (si elle est convergente) déterminer sa somme, sont deux problèmes distincts. Il arrivera souvent par la suite qu'on soit en mesure de prouver qu'une certaine série converge, et incapable de "calculer" sa somme, c'est-à-dire d'exprimer simplement ce nombre.
2. Une série divergente, c'est une série dont la somme partielle diverge. Cette dernière peut diverger en tendant vers $+\infty$ ou $-\infty$ mais elle peut aussi ne pas avoir de limite du tout.

Lemme 4.

Soit $(u_n)_{n\in\mathbb{N}}$ une suite et $n_0 \in \mathbb{N}$.

$$\sum u_n \text{ converge} \quad \text{ssi} \quad \sum_{n\geq n_0} u_n \text{ converge.}$$

Proposition 5 (Linéarité de la somme)**.**

Si $\sum u_n$ et $\sum v_n$ sont deux séries convergentes et $\lambda, \mu \in \mathbb{K}$, alors la série $\sum(\lambda u_n + \mu v_n)$ est convergente, et

$$\sum_{n=0}^{+\infty} (\lambda u_n + \mu v_n) = \lambda \sum_{n=0}^{+\infty} u_n + \mu \sum_{n=0}^{+\infty} v_n.$$

Proposition 6 (Séries à termes complexes)**.**

Soit $\sum u_n$ une série de terme général complexe. On a

$$\sum u_n \text{ converge} \iff \sum \mathrm{Re}(u_n) \text{ et } \sum \mathrm{Im}(u_n) \text{ convergent.}$$

S'il y a convergence,

$$\sum_{n=0}^{+\infty} u_n = \sum_{n=0}^{+\infty} \mathrm{Re}(u_n) + i \sum_{n=0}^{+\infty} \mathrm{Im}(u_n).$$

Proposition-Définition 7 (Reste).

Soit $\sum_{n\geq n_0} u_n$ une série convergente et $(S_n)_{n\geq n_0}$ la suite de ses sommes partielles.

Pour $n \geq n_0$, on appelle **reste** d'indice n et on note R_n le réel

$$R_n = \sum_{k=n+1}^{+\infty} u_k = \sum_{k=n_0}^{+\infty} u_k - \sum_{k=n_0}^{n} u_k \quad \text{de sorte que} \quad S_n + R_n = \sum_{k=n_0}^{+\infty} u_k.$$

On a

$$S_n \longrightarrow \sum_{k=n_0}^{+\infty} u_k \qquad \text{et} \qquad \boxed{R_n \longrightarrow 0}.$$

1.2 Liens entre la série et son terme général.

Proposition 8 (Terme général d'une série convergente).

Si une série $\sum u_n$ est convergente, alors son terme général u_n tend vers 0. La réciproque est fausse.

La contraposée de l'implication précédente nous dit qu'une série dont le terme général ne tend pas vers 0 n'a *aucune chance de converger*. On fixe la terminologie ci-dessous.

Définition 9.

Une série dont le terme général ne tend pas vers 0 est dite **grossièrement divergente**.

Exemple 10.

La série $\sum e^{\frac{1}{n}}$ diverge grossièrement. La série $\sum \frac{1}{n}$ diverge, mais pas grossièrement.

Le télescopage permet d'établir le résultat simple (mais utile !) ci-dessous.

Proposition 11 (Lien suite-série).

Soit $(u_n)_{n\geq n_0}$ une suite d'éléments de $\mathbb{K}$.

La suite (u_n) et la série $\sum(u_{n+1} - u_n)$ sont de même nature.

S'il y a convergence,

$$\sum_{n=n_0}^{+\infty} (u_{n+1} - u_n) = \lim u_n - u_{n_0}.$$

Exemple 12.

Montrer que la série $\sum \frac{1}{n(n+1)}$ converge et calculer sa somme.

1.3 Une famille de séries usuelles : les séries géométriques.

On appelle **série géométrique** de raison $q \in \mathbb{C}$ la série de terme général q^n.
Leurs sommes partielles étant faciles à calculer, on dispose du critère de convergence ci-dessous.

Proposition 13 (Séries géométriques)**.**

Soit $q \in \mathbb{C}$. Alors,

$$\sum q^n \text{ converge} \quad \Longleftrightarrow \quad |q| < 1.$$

Dans le cas où la série converge, on a $\displaystyle\sum_{n=0}^{+\infty} q^n = \frac{1}{1-q}$.

Exemple 14.

Soit $r \in]0,1[$ et $\theta \in \mathbb{R}$. Montrer que la série $\sum r^n \cos(n\theta)$ converge et montrer que sa somme est

$$\sum_{n=0}^{+\infty} r^n \cos(n\theta) = \frac{1 - r\cos(\theta)}{1 + r^2 - 2r\cos(\theta)}.$$

2 Outils pour les séries à termes positifs.

Soit une série réelle $\sum u_n$. Si pour tout $n \in \mathbb{N}$, $u_n \geq 0$, on dit que la série est **série à termes positifs**.

2.1 Comparaison des séries à termes positifs.

Proposition 15 (Vive la croissance !)**.**

Soit $(u_n)_{n \geq n_0}$ une suite de réels positifs et $(S_n)_{n \geq n_0}$ la suite des sommes partielles de $\sum u_n$.

1. La suite $(S_n)_{n \geq n_0}$ est croissante.
2. La série $\sum u_n$ converge si et seulement si la suite $(S_n)_{n \geq n_0}$ de ses sommes partielles est majorée.
3. Si la série $\sum u_n$ converge alors $S_n \leq \displaystyle\sum_{k=n_0}^{+\infty} u_k$ pour tout $n \geq n_0$.
4. Si la série $\sum u_n$ diverge alors $S_n \underset{n \to +\infty}{\longrightarrow} +\infty$.

Proposition 16 (Comparaison avec $\leq$)**.**

Soient $\sum u_n$ et $\sum v_n$ deux séries à termes positifs telles que $u_n \leq v_n$ à.p.d.c.r.

1. Si $\sum v_n$ converge, alors $\sum u_n$ converge.
2. Si $\sum u_n$ diverge, alors $\sum v_n$ diverge.

Proposition 17 (Comparaison avec O ou o)**.**

Soient $\sum u_n$ et $\sum v_n$ deux séries à termes strictement positifs telles que $u_n = O(v_n)$.

Si $\sum v_n$ converge, alors $\sum u_n$ converge.

C'est vrai a fortiori si $u_n = o(v_n)$.

Proposition 18 (Comparaison avec un équivalent)**.**

Soient $\sum u_n$ et $\sum v_n$ deux séries à termes strictement positifs telles que $u_n \sim v_n$. Alors,

$\sum u_n$ et $\sum v_n$ sont de même nature.

Exemple 19.

Déterminer la nature des séries ci-dessous :

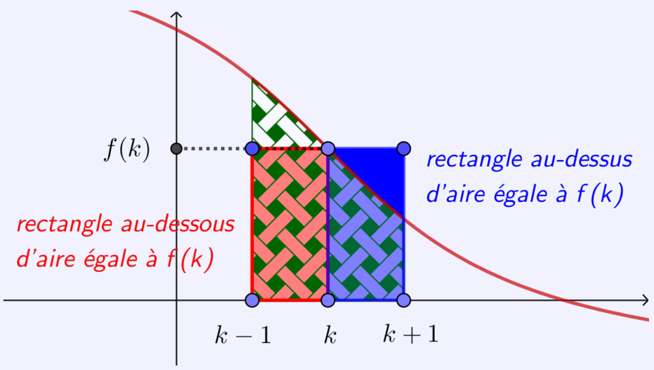
$$\sum \frac{1}{n^2 \ln(n)}, \qquad \sum \frac{\ln(n)}{n}, \qquad \sum \frac{n^2}{2^n}, \qquad \sum \sin\left(\frac{1}{n}\right), \qquad \sum \tan\left(\frac{1}{n^2}\right).$$

2.2 Comparaison série/intégrale et application aux séries de Riemann.

Lemme 20 (Comparer une somme partielle à des intégrales)**.**

Soit $n_0 \in \mathbb{N}$ et $f : [n_0, +\infty[\to \mathbb{R}$ une fonction continue et décroissante. Alors,

$$\forall k \geq n_0 + 1 \qquad \int_k^{k+1} f(t)\mathrm{d}t \leq f(k) \leq \int_{k-1}^{k} f(t)\mathrm{d}t.$$



Un encadrement analogue est possible pour une fonction croissante, on saura l'écrire si besoin.

Méthode (Encadrer une somme partielle)**.**

Soit $f : [n_0, +\infty[\to \mathbb{R}$ décroissante. On sait que pour $k \geq n_0$:

$$\int_k^{k+1} f(t)\mathrm{d}t \leq f(k)$$

et pour tout $k \geq n_0 + 1$:

$$f(k) \leq \int_{k-1}^{k} f(t)\mathrm{d}t.$$

En sommant ces inégalités on obtient pour $n \geq n_0$

$$\sum_{k=n_0}^{n} \int_k^{k+1} f(t)\mathrm{d}t \leq \sum_{k=n_0}^{n} f(k) \leq f(n_0) + \sum_{k=n_0+1}^{n} \int_{k-1}^{k} f(t)\mathrm{d}t.$$

Par la relation de Chasles :

$$\int_{n_0}^{n+1} f(t)\mathrm{d}t \leq \sum_{k=n_0}^{n} f(k) \leq f(n_0) + \int_{n_0}^{n} f(t)\mathrm{d}t.$$

Cette technique permet d'encadrer des sommes partielles, par exemple pour obtenir un équivalent. Elle s'applique aussi pour étudier des restes de séries convergentes.

Théorème 21 (Cas d'une fonction décroissante et positive)**.**

Soit $n_0 \in \mathbb{N}$ et $f : [n_0, +\infty[\to \mathbb{R}_+$ une fonction continue, décroissante et positive.

$$\text{La série } \sum_{n \geq n_0} f(n) \text{ et la suite } \left(\int_{n_0}^{n} f(t)\mathrm{d}t \right)_{n \geq n_0} \text{ sont de même nature.}$$

Les séries de la forme $\sum \frac{1}{n^\alpha}$, où $\alpha \in \mathbb{R}$ sont appelées **série de Riemann** ; et seront désormais *usuelles*.

Théorème 22 (Nature d'une série de Riemann)**.**

Soit $\alpha \in \mathbb{R}$. Alors,

$$\sum \frac{1}{n^\alpha} \text{ converge} \iff \alpha > 1.$$

Le cas $\alpha = 1$ apparaît comme un cas critique, le point où la "transition de phase" a lieu :

$$\sum \frac{1}{n} \text{ DV} \qquad \text{et} \qquad \forall \varepsilon > 0 \ \sum \frac{1}{n^{1+\varepsilon}} \text{ CV.}$$

Exemple 23 (Comparaison à une série de Riemann : un exemple important).

Démontrer que la série $\sum \frac{\ln(n)}{n^2}$ est convergente.

Exemple 24 (Généralisation de l'exemple précédent : séries de Bertrand (HP)).

Soient α et β deux réels. La série $\sum \frac{1}{n^\alpha \ln^\beta(n)}$ est appelée **série de Bertrand**.

1. si $\alpha > 1$, elle est convergente ;
2. si $\alpha < 1$, elle est divergente ;
3. si $\alpha = 1$,
   (a) elle est convergente si $\beta > 1$;
   (b) elle est divergente si $\beta \leq 1$.

Exemple 25 (Équivalent pour la somme partielle d'une série divergente).

À l'aide d'une comparaison série/intégrale, on prouve que

$$\sum_{k=2}^{n} \frac{1}{k\ln(k)} \sim \ln\left(\ln(n)\right).$$

On obtient de même des équivalents pour les sommes partielles des séries de Riemann divergentes :

$$\sum_{k=1}^{n} \frac{1}{k} \sim \ln(n) \quad \text{et} \quad \sum_{k=1}^{n} \frac{1}{k^\alpha} \sim \frac{n^{1-\alpha}}{1-\alpha} \quad (\alpha \in]0,1[).$$

3 Outils pour les séries à termes réels ou complexes.

3.1 Convergence absolue

Dans la définition suivante, $|\cdot|$ désigne, selon le contexte, la valeur absolue ou le module.

Définition 26 (Convergence absolue).

Soit (u_n) une suite à valeurs dans $\mathbb{K}$. On dit qu'il y a **convergence absolue** de la série $\sum u_n$ si la série à terme positifs $\sum |u_n|$ est convergente.

Théorème 27.

Pour une série numérique, la convergence absolue implique la convergence.

La réciproque n'est pas vraie : la série $\sum \frac{(-1)^n}{n}$ est convergente mais pas absolument convergente.

Exemples 28.

Les séries $\sum \dfrac{(-1)^n}{n\sqrt{n}}$ et $\sum \dfrac{\sin(n)}{2^n}$ convergent absolument donc convergent.

Proposition 29 (Inégalité triangulaire pour la somme d'une série absolument convergente)**.**

Soit $\sum u_n$ une série absolument convergente. Alors, pour $n_0 \in \mathbb{N}$, $\left|\sum_{n=n_0}^{+\infty} u_n\right| \leq \sum_{n=n_0}^{+\infty} |u_n|$.

Preuve. Soit $\sum u_n$ une série absolument convergente. Pour $n \geq n_0$, on sait écrire l'inégalité triangulaire pour une somme *finie* de nombres complexes :

$$\left|\sum_{k=n_0}^{n} u_k\right| \leq \sum_{k=n_0}^{n} |u_k| \quad \text{ce qui donne par passage à la limite} \quad \left|\sum_{k=n_0}^{+\infty} u_k\right| \leq \sum_{k=n_0}^{+\infty} |u_k|.$$

La série est absolument convergente, ce qui justifie l'existence de la limite à droite.
D'après le théorème 27, la série $\sum u_n$ converge, ce qui justifie l'existence de la limite à gauche. □

Proposition 30 (Comparaison avec O ou o)**.**

Soient $\sum u_n$ et $\sum v_n$ deux séries numériques telles que $u_n = O(v_n)$.

Si $\sum v_n$ converge absolument, alors $\sum u_n$ converge absolument.

C'est vrai a fortiori si $u_n = o(v_n)$.

Exemple 31 (Règle de d'Alembert (comparaison à une série géométrique))**.**

Soit $\sum u_n$ une série complexe dont les termes sont non nuls à.p.d.c.r, et ℓ un nombre réel positif.

1. Si $\left|\frac{u_{n+1}}{u_n}\right| \to \ell$ avec $\ell < 1$, alors $\sum u_n$ converge absolument (donc converge).
2. Si $\left|\frac{u_{n+1}}{u_n}\right| \to \ell$ avec $\ell > 1$, alors $\sum u_n$ diverge grossièrement.

Il ne faut pas s'exagérer l'utilité de ce résultat ! Par exemple, pour les séries de Riemann ou les séries de Bertrand, le quotient $\frac{u_{n+1}}{u_n}$ tend vers 1 et on ne peut rien conclure. Cette règle sera utile principalement en spé dans l'étude des séries entières (les séries de Taylor), dont voici ci-dessous un exemple important.

Proposition 32 (Série exponentielle)**.**

Pour tout nombre complexe $z \in \mathbb{C}$, la série $\sum \dfrac{z^n}{n!}$ est absolument convergente, donc convergente.

Admis pour le moment : $\displaystyle\sum_{n=0}^{+\infty} \frac{z^n}{n!} = e^z$.

3.2 Séries alternées.

Définition 33.

Une **série alternée** est une série de la forme $\sum(-1)^n u_n$ où (u_n) est une suite de signe constant.

Théorème 34 (Théorème des séries alternées).

Soit $(u_n)_{n\geq n_0}$ une suite de signe constant.

$$\boxed{\text{Si la suite } (|u_n|) \text{ tend vers } 0 \text{ en décroissant, alors la série } \sum(-1)^n u_n \text{ converge}}.$$

Sous l'hypothèse que $(|u_n|)$ tend vers 0 en décroissant, on a de surcroît que

- le reste $R_n = \sum\limits_{k=n+1}^{+\infty} (-1)^k u_k$ est du signe de son premier terme $(-1)^{n+1}u_{n+1}$ et $|R_n| \leq |u_{n+1}|$;
- la somme $S = \sum\limits_{n=n_0}^{+\infty} (-1)^n u_n$ est du signe de son premier terme $(-1)^{n_0}u_{n_0}$ et $|S| \leq |u_{n_0}|$.

Exemple 35.

Retrouver que $\displaystyle\sum \frac{(-1)^n}{n}$ est convergente. Démontrer que $\displaystyle\sum(-1)^n \frac{\ln(n)}{n}$ est convergente.

Exemple 36 (Comparaison à une série alternée : une erreur à éviter).

Déterminer **l'erreur** dans le raisonnement ci-dessous, puis proposer une solution satisfaisante.

— On a $\frac{(-1)^n}{n} \to 0$ et $\ln(1+x) \underset{0}{\sim} x$ donc $\ln\left(1+\frac{(-1)^n}{n}\right) \sim \frac{(-1)^n}{n}$.

— Or, la série $\sum \frac{(-1)^n}{n}$ est convergente, d'après le théorème des séries alternées, qui s'applique puisque $\left(\frac{1}{n}\right)$ tend vers 0 en décroissant.

— Par comparaison, la série $\sum \ln\left(1+\frac{(-1)^n}{n}\right)$ est convergente.

Exemple 37 (Série de Riemann alternée).

Étudier le type de convergence de $\displaystyle\sum \frac{(-1)^n}{n^\alpha}$ en discutant selon les valeurs de α.

Valeur de N pour laquelle $S_N = \sum\limits_{n=1}^{N} \frac{(-1)^n}{\sqrt{n}}$ est une approximation de $S = \sum\limits_{n=1}^{+\infty} \frac{(-1)^n}{\sqrt{n}}$ à 10^{-2} près.

Si $\alpha > 1$, exprimer $\phi(\alpha)$ à l'aide de $\zeta(\alpha)$, où

$$\zeta(\alpha) = \sum_{n=1}^{+\infty} \frac{1}{n^\alpha} \quad \text{et} \quad \phi(\alpha) = \sum_{n=1}^{+\infty} \frac{(-1)^n}{n^\alpha}.$$

Exercices

Séries à termes positifs.

$\boxed{\textbf{33.1}}$ **[♦◇◇]** Donner la nature des séries suivantes.

$$\sum \arccos\left(\frac{1}{n}\right),\quad \sum \arcsin\left(\frac{1}{n}\right),\quad \sum \frac{1}{3^n}\quad \sum \ln\left(1+\frac{1}{n^2}\right),\quad \sum \frac{\ln(n)}{\sqrt{n}},\quad \sum ne^{-n}.$$

$\boxed{\textbf{33.2}}$ **[♦◇◇]** Étudier la convergence de la série $\sum \left(n\ln\left(1+\frac{1}{n}\right) - \cos\left(\frac{1}{\sqrt{n}}\right)\right)$.

$\boxed{\textbf{33.3}}$ **[♦◇◇]** Quelle est la nature des séries $\displaystyle\sum \frac{\ln(n)}{n\sqrt{n}}$ et $\displaystyle\sum \frac{1}{\sqrt{n}\ln(n)}$?
Le résultat hors programme sur les séries de Bertrand, exemple du cours, ne sera pas utilisé ici.

$\boxed{\textbf{33.4}}$ **[♦◇◇]** Étudier la convergence de la série $\sum \ln(n)^{-\ln(n)}$.

$\boxed{\textbf{33.5}}$ **[♦◇◇]** Quelle est la nature de $\sum \left(\frac{2n+1}{3n+1}\right)^n$?

$\boxed{\textbf{33.6}}$ **[♦◇◇]** Étudier la convergence de la série $\sum e^{-n^\alpha}$, en discutant selon α (réel).

$\boxed{\textbf{33.7}}$ **[♦♦◇]** Quelle est la nature de $\sum \frac{(\lambda n)^n}{n!}$ (à discuter selon la valeur de $\lambda \in \mathbb{R}_+^*$).

$\boxed{\textbf{33.8}}$ **[♦♦◇]** Soit $a > 1$.
Nature de $\sum u_n$ où $u_n = \dfrac{1}{na^{p_n}}$, p_n étant le nombre de chiffres dans l'écriture décimale de n.

$\boxed{\textbf{33.9}}$ **[♦◇◇]** [De l'importance de la positivité dans le théorème de comparaison]
On pose

$$\forall n \geq 1 \quad u_n = \frac{(-1)^{n+1}}{\sqrt{n+1}} - \frac{(-1)^n}{\sqrt{n}} \qquad \text{et} \qquad v_n = u_n + \frac{1}{n}.$$

1. Montrer que $\sum u_n$ converge et $\sum v_n$ diverge.
2. Montrer que l'on a cependant $u_n \sim v_n$.

$\boxed{\textbf{33.10}}$ **[♦♦◇]** Soit $(u_n)_{n\geq 1}$ la suite de terme général

$$u_n = \frac{1}{n\sqrt{n+1} + (n+1)\sqrt{n}}.$$

1. Montrer que pour tout $n \geq 1$, $u_n = \frac{1}{\sqrt{n}} - \frac{1}{\sqrt{n+1}}$.
2. Démontrer que $\sum u_n$ est convergente et calculer la somme de cette série.

$\boxed{\textbf{33.11}}$ **[♦♦◇]** On considère (u_n) définie par récurrence par $u_0 \in]0,1[$ et pour tout $n \in \mathbb{N}$, $u_{n+1} = u_n - u_n^2$.

1. Montrer que la suite (u_n) converge vers une limite que l'on précisera.
2. Montrer que $\sum u_n^2$ est convergente.
3. Montrer que les séries $\sum u_n$ et $\sum \ln\left(\frac{u_{n+1}}{u_n}\right)$ sont divergentes.

$\boxed{\textbf{33.12}}$ **[♦♦◊]** Soit (u_n) décroissante telle que $\sum u_n$ converge.

1. Soit S_n la somme partielle de la série au rang n. Calculer $S_{2n} - S_n$.
2. En déduire que $nu_{2n} \to 0$.
3. Montrer que $nu_n \to 0$.
4. Réciproquement, si (u_n) est décroissante et que $nu_n \to 0$, a-t-on que $\sum u_n$ converge ?

$\boxed{\textbf{33.13}}$ **[♦♦♦]**

Soit (u_n) décroissante de limite nulle. Pour tout $n \in \mathbb{N}$, on note

$$s_n = -nu_n + \sum_{k=1}^{n} u_k.$$

On suppose que (s_n) est bornée. Montrer que $\sum u_n$ converge.

$\boxed{\textbf{33.14}}$ **[♦♦◊]**

1. Soit (u_n) une suites de réels strictement positifs.
   Montrer que si $\sqrt[n]{u_n} \to r$, où $r \in [0, 1[$, alors $\sum u_n$ est convergente.
   Note : cette implication est appelée critère de Cauchy.
2. Examiner la nature de $\sum \left(\operatorname{ch} \dfrac{a}{n}\right)^{-n^3}$ $(a \in \mathbb{R}^*)$.

$\boxed{\textbf{33.15}}$ **[♦♦◊]** Quelle est la partie entière de $\sum\limits_{k=1}^{10^9} k^{-2/3}$?

$\boxed{\textbf{33.16}}$ **[♦♦◊]** Soit (u_n) une suite <u>décroissante</u> de réels positifs. On pose $v_n = 2^n u_{2^n}$.

1. Montrer que $\sum u_n$ et $\sum v_n$ ont même nature.
2. Application : déduire le critère de convergence des séries de Riemann de celui des séries géométriques.
3. Application : Discuter, selon les valeurs de α, la convergence de la série dite de Bertrand

$$\sum \frac{1}{n(\ln(n))^\alpha}.$$

$\boxed{\textbf{33.17}}$ **[♦♦◊]** *Presque Stirling.*

Pour $n \geq 1$, on note $u_n = \ln\left(\dfrac{n!}{\sqrt{n}\left(\frac{n}{e}\right)^n}\right)$.

1. En exploitant le lien suite-série, démontrer que (u_n) converge.
   Indication : on pourra commencer par démontrer que $u_{n+1} - u_n \sim \frac{1}{12n^2}$.
2. En déduire l'existence d'une constante $C > 0$ telle que

$$n! \sim C\sqrt{n}\left(\frac{n}{e}\right)^n.$$

Comme on le sait, cette constante C vaut $\sqrt{2\pi}$. On peut le démontrer à l'aide des intégrales de Wallis.

$\boxed{\textbf{33.18}}$ **[♦♦♦]** Pour tout $n \in \mathbb{N}$, on pose $A_n = \sum\limits_{k=0}^{+\infty} \dfrac{k^n}{2^k}$.

Montrer que A_n est bien défini et l'exprimer en fonction des $(A_j, 0 \leq j \leq n-1)$.
Calculer A_0 et en déduire que A_n est un entier pair.

Séries de terme général réel ou complexe.

$\boxed{33.19}$ **[♦♦♢]** Soient les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ définies par

$$a_n = (\sqrt{2}-1)^n\pi; \quad b_n = (\sqrt{2}+1)^n\pi.$$

Examiner la nature des séries $\sum \sin(a_n)$ et $\sum \sin(b_n)$.
Indication : On pourra calculer $(1-\sqrt{2})^n + (1+\sqrt{2})^n$.

$\boxed{33.20}$ **[♦♢♢]** Soit $u_n = \cos\left(\pi n^2 \ln(1+\frac{1}{n})\right)$. Quelle est la nature de $\sum u_n$?

$\boxed{33.21}$ **[♦♦♢]** Convergence et somme de la série de terme général

$$\ln\left(1+\frac{(-1)^n}{n}\right).$$

$\boxed{33.22}$ **[♦♦♦]** Convergence et somme de

$$\sum (-1)^n \ln\left(1+\frac{1}{n}\right).$$

$\boxed{33.23}$ **[♦♦♢]** Pour tout entier $n \geq 1$, on pose

$$u_n = \ln(n) + a\ln(n+1) + b\ln(n+2).$$

1. Existe-t-il des réels a et b tels que la série de terme général u_n soit convergente ?
2. Dans l'unique cas favorable ($a=-2$, $b=1$), calculer la somme de la série.

$\boxed{33.24}$ **[♦♦♢]** Soit (a_n) une suite de $\mathbb{C}^n$ telle que $\sum |a_n|$ converge. On définit la suite $(u_n)_{n\geq 1}$ par

$$\forall n \in \mathbb{N}^* \quad u_n = \prod_{k=1}^{n}(1+a_k).$$

1. Démontrer que (u_n) est bornée.
2. Démontrer que (u_n) converge.

$\boxed{33.25}$ **[♦♦♢]** Soit (u_n) une suite réelle définie par $u_0 \in \mathbb{R}$ et pour tout $n \in \mathbb{N}$,

$$u_{n+1} = \frac{e^{-u_n}}{n+1}.$$

1. Nature de $\sum u_n$?
2. Nature de $\sum (-1)^n u_n$. *Indication :* Calculer $(-1)^{n+1}u_{n+1} - \frac{(-1)^{n+1}}{n+1}$.

$\boxed{33.26}$ **[♦♦♦]** Soit, pour $n \in \mathbb{N}^*$

$$s_n = \sum_{k=1}^{n}(-1)^k\sqrt{k} \quad \text{et} \quad t_n = s_n + s_{n+1}.$$

1. Montrer que $\sum (t_{n+1}-t_n)$ est convergente.
2. En déduire que (t_n) converge vers une limite ℓ strictement négative puis que $s_n \sim (-1)^n\frac{\sqrt{n}}{2}$.
3. Nature de $\sum \frac{1}{s_n}$.

$\boxed{33.27}$ **[♦♦♦]** Soit $j = e^{\frac{2i\pi}{3}}$. Convergence et somme de

$$\sum \frac{j^n}{n}.$$

---

34 Matrices et applications linéaires

1 Représentations matricielles.

1.1 Matrice d'un vecteur, d'une famille de vecteurs dans une base.

Définition 1 (Matrice colonne d'un vecteur dans une base).

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $\mathcal{B} = (e_1, \dots, e_n)$ une base de E.
Tout vecteur $x \in E$ se décompose de manière unique sur $\mathcal{B}$: $\exists!(x_1, \dots, x_n) \in \mathbb{K}^n : x = \sum_{i=1}^{n} x_i e_i$.
On appelle **matrice colonne** de x dans la base $\mathcal{B}$, et on note $\text{Mat}_{\mathcal{B}}(x)$ la matrice

$$\text{Mat}_{\mathcal{B}}(x) = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in M_{n,1}(\mathbb{K}).$$

Exemple 2.

Les familles $\mathcal{B} = (1, X, X^2)$ et $\mathcal{B}' = (1, X+3, (X+3)^2)$ sont deux bases de $\mathbb{R}_2[X]$. Soit $P = (X+3)^2$.

$$\text{Mat}_{\mathcal{B}}(P) = \begin{pmatrix} \quad \end{pmatrix} \qquad \text{Mat}_{\mathcal{B}'}(P) = \begin{pmatrix} \quad \end{pmatrix}$$

Le résultat simple suivant est un premier pont jeté entre l'algèbre linéaire et le calcul matriciel.

Lemme 3 (Isomorphisme d'espaces vectoriels induit par le choix d'une base)**.**

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $\mathcal{B}$ une base de E.
L'application

$$\varphi_{\mathcal{B}} : \left\{ \begin{array}{ccc} E & \to & M_{n,1}(\mathbb{K}) \\ x & \mapsto & \mathrm{Mat}_{\mathcal{B}}(x) \end{array} \right.$$

est un isomorphisme d'espaces vectoriels.
Notamment, si x et x' sont deux vecteurs de E, et λ, μ deux scalaires de $\mathbb{K}$, alors

$$\mathrm{Mat}_{\mathcal{B}}\left(\lambda x + \mu x'\right) = \lambda \mathrm{Mat}_{\mathcal{B}}(x) + \mu \mathrm{Mat}_{\mathcal{B}}(x').$$

Preuve. Notons $\mathcal{B} = (e_1, \ldots, e_n)$ et rappelons que pour $i \in [\![1, n]\!]$, l'application e_i^*, qui à un vecteur x associe sa coordonnée sur e_i, est une forme linéaire. La linéarité de $\varphi_{\mathcal{B}}$ devient assez claire lorsqu'on écrit

$$\forall x \in E \quad \varphi_{\mathcal{B}}(x) = \begin{pmatrix} e_1^*(x) \\ \vdots \\ e_n^*(x) \end{pmatrix}.$$

Les dimensions étant égales au départ et à l'arrivée, on pourrait utiliser la caractérisation des isomorphismes en dimension finie pour conclure, mais la bijectivité de $\varphi_{\mathcal{B}}$ est claire : un vecteur $\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in M_{n,1}(\mathbb{K})$ possède bien sûr un antécédent unique dans E : c'est $\sum_{i=1}^{n} y_i e_i$. □

Définition 4 (Matrice d'une famille de vecteurs dans une base)**.**

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $\mathcal{B} = (e_1, \ldots, e_n)$ une base de E.
Soit $\mathcal{F} = (v_1, \ldots, v_p)$ une famille de vecteurs de E. On appelle **matrice de la famille** $\mathcal{F}$ dans la base $\mathcal{B}$ et on note $\mathrm{Mat}_{\mathcal{B}}(\mathcal{F})$ la matrice

$$\mathrm{Mat}_{\mathcal{B}}(\mathcal{F}) = \left(C_1 \mid C_2 \mid \ldots \mid C_p\right),$$

où, pour $j \in [\![1, p]\!]$, C_j est la matrice colonne de v_j dans la base $\mathcal{B}$.

Avec les notations de la définition précédente,

$$\forall j \in [\![1, p]\!] \quad \exists!(a_{1,j}, a_{2,j}, \ldots, a_{n,j}) \in \mathbb{K}^n : v_j = \sum_{i=1}^{n} a_{i,j} e_i.$$

$$\mathrm{Mat}_{\mathcal{B}}(v_1, \ldots, v_p) = \begin{array}{c} \begin{array}{ccccc} v_1 & \cdots & v_j & \cdots & v_p \end{array} \\ \begin{pmatrix} \vdots & \vdots & a_{1,j} & \vdots & \vdots \\ \vdots & \vdots & a_{2,j} & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & a_{n,j} & \vdots & \vdots \end{pmatrix} \end{array} \begin{array}{c} \\ e_1 \\ e_2 \\ \vdots \\ e_n \end{array}$$

1.2 Matrice d'une application linéaire dans un couple de bases.

Définition 5 (Matrice d'une application linéaire dans un couple de bases)**.**

Soient E et F deux $\mathbb{K}$-e.v. de dimension finie non nulle (on note $p = \dim E$ et $n = \dim F$).
Soient $\mathcal{B} = (e_1, \ldots, e_p)$ une base de E et $\mathcal{C} = (f_1, \ldots, f_n)$ une base de F.
Soit $u \in \mathscr{L}(E, F)$. On appelle **matrice** de u **dans les bases** $\mathcal{B}$ et $\mathcal{C}$, et on note

$$\mathrm{Mat}_{\mathcal{C},\mathcal{B}}(u) \in M_{n,p}(\mathbb{K})$$

la matrice $\mathrm{Mat}_{\mathcal{C}}(u(\mathcal{B}))$, où $u(\mathcal{B})$ est la famille des images de $\mathcal{B}$ par u.
Ainsi, dans la $j$ème colonne de $\mathrm{Mat}_{\mathcal{C}}(u(\mathcal{B}))$ se trouvent les coordonnées de $u(e_j)$ dans la base $\mathcal{C}$.

Avec les notations de la définition précédente,

$$\forall j \in [\![1, p]\!] \quad \exists!(a_{1,j}, a_{2,j}, \ldots, a_{n,j}) \in \mathbb{K}^n : u(e_j) = \sum_{i=1}^{n} a_{i,j} f_i.$$

On a donc

$$\mathrm{Mat}_{\mathcal{C},\mathcal{B}}(u) = \begin{array}{c} \begin{array}{ccccc} u(e_1) & \cdots & u(e_j) & \cdots & u(e_p) \end{array} \\ \begin{pmatrix} \vdots & \vdots & a_{1,j} & \vdots & \vdots \\ \vdots & \vdots & a_{2,j} & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & a_{n,j} & \vdots & \vdots \end{pmatrix} \end{array} \begin{array}{c} \\ f_1 \\ f_2 \\ \vdots \\ f_n \end{array}$$

Définition 6 (Cas particulier d'un endomorphisme)**.**

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$, $\mathcal{B}$ une base de E et $u \in \mathscr{L}(E)$.
On appelle **matrice** de u **dans la base** $\mathcal{B}$, et on note

$$\mathrm{Mat}_{\mathcal{B}}(u) \in M_n(\mathbb{K})$$

plutôt que $\mathrm{Mat}_{\mathcal{B},\mathcal{B}}(u)$, la matrice de u dans les bases $\mathcal{B}$ et $\mathcal{B}$.

Exemple 7 (Matrice de l'endomorphisme de dérivation dans la base canonique)**.**

Soit $D : P \mapsto P'$ endomorphisme de dérivation sur $\mathbb{R}_3[X]$.
Deux écritures de la base canonique de $\mathbb{R}_3[X]$: $\mathcal{B} = (1, X, X^2, X^3)$ ou $\mathcal{B}' = (X^3, X^2, X, 1)$.
Voici la matrice de D dans la base $\mathcal{B}$ (ajouter les "bordures"). Donner celle dans $\mathcal{B}'$.

$$\mathrm{Mat}_{\mathcal{B}}(D) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad \text{et} \qquad \mathrm{Mat}_{\mathcal{B}'}(D) = \begin{pmatrix} & & & \\ & & & \\ & & & \\ & & & \end{pmatrix}$$

Exemple 8 (Matrice de l'endomorphisme de transposition dans la base canonique)**.**

Donner la matrice de $t : M \mapsto M^T$ dans la base canonique de $M_2(\mathbb{R})$.

Exemple 9 (Matrice d'une similitude directe de point fixe l'origine)**.**

Considérons le $\mathbb{R}$-espace vectoriel $\mathbb{C}$ et notons $\mathcal{B}$ la base $(1, i)$.
Fixons $(a, b) \in \mathbb{R}^2$ et considérons l'application

$$f : z \mapsto (a + ib)z.$$

Écrire la matrice de cet endomorphisme dans la base $\mathcal{B}$.
Cas particulier des rotations de centre l'origine : pour $\theta \in \mathbb{R}$, écrire la matrice dans la base $\mathcal{B}$ de

$$z \mapsto e^{i\theta} z.$$

Exemple 10 (La base canonique n'est pas toujours la meilleure)**.**

Soit $f : P \mapsto (X+1)P'$, endomorphisme de $\mathbb{R}_2[X]$. Notons $\mathcal{B} = (1, X, X^2)$ et $\mathcal{B}' = (1, X+1, (X+1)^2)$.
Écrire les quatre matrices

$$\mathrm{Mat}_{\mathcal{B}}(f), \quad \mathrm{Mat}_{\mathcal{B}'}(f), \quad \mathrm{Mat}_{\mathcal{B},\mathcal{B}'}(f), \quad \mathrm{Mat}_{\mathcal{B}',\mathcal{B}}(f).$$

Quelle est la « meilleure » représentation ? Pourquoi la dernière est-elle la moins facile à écrire ?

À *une* application linéaire, on peut donc associer *des* matrices : la matrice d'une application linéaire *dépend du couple de bases* avec lequel on travaille. La troisième partie de ce cours est consacré au **changement de bases**, on s'intéressera aux liens qui existent entre les différentes matrices qui représentent une application linéaire dans des couples de bases différentes.

Pour les homothéties, les choses sont plus simples : la matrice est toujours la même, pourvu que les bases au départ et à l'arrivée coïncident.

Proposition 11 (Matrice de l'identité, d'une homothétie)**.**

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$.

La matrice de l'identité dans *une* base de E est la matrice identité.

Plus généralement, pour tout base $\mathcal{B}$ de E et tout $\lambda \in \mathbb{K}$, $\mathrm{Mat}_{\mathcal{B}}(\lambda \mathrm{id}_E) = \lambda I_n$.

Remarque. La terminologie *matrice identité* était restée obscure mais on comprend désormais que la matrice identité est la matrice... de l'identité ! (pourvu qu'on prenne une même base au départ et à l'arrivée).

Remarque. La matrice de id_E dans un couple de bases $(\mathcal{B}, \mathcal{B}')$ avec $\mathcal{B} \neq \mathcal{B}'$ n'est pas la matrice identité ! Voir plus loin la notion de matrice de passage.

Théorème 12 (Isomorphisme d'espaces vectoriels induit par le choix d'un couple de bases).

Soient E et F deux $\mathbb{K}$-espaces vectoriels de dimensions finies non nulles p et n.
On se donne $\mathcal{B}$ une base de E et $\mathcal{C}$ une base de F.

L'application

$$\Phi_{\mathcal{C},\mathcal{B}} : \left\{ \begin{array}{ccc} \mathscr{L}(E,F) & \to & M_{n,p}(\mathbb{K}) \\ u & \mapsto & \mathrm{Mat}_{\mathcal{C},\mathcal{B}}(u) \end{array} \right.$$

est un isomorphisme d'espaces vectoriels.

Notamment, si u et v sont deux applications linéaires de $\mathscr{L}(E,F)$ linéaires et λ et μ deux scalaires,

$$\mathrm{Mat}_{\mathcal{C},\mathcal{B}}(\lambda u + \mu v) = \lambda \mathrm{Mat}_{\mathcal{C},\mathcal{B}}(u) + \mu \mathrm{Mat}_{\mathcal{C},\mathcal{B}}(v).$$

1.3 Composition des applications et produit matriciel.

Proposition 13 (Coordonnées de l'image d'un vecteur).

Soient E et F deux espaces vectoriels de dimensions (non nulles) respectives p et n.
Soient $u \in \mathscr{L}(E,F)$, $\mathcal{B}$ une base de E et $\mathcal{C}$ une base de F. Alors, pour tout $x \in E$,

$$\mathrm{Mat}_{\mathcal{C}}(u(x)) = \mathrm{Mat}_{\mathcal{C},\mathcal{B}}(u) \cdot \mathrm{Mat}_{\mathcal{B}}(x).$$

Preuve. Commençons par introduire des notations. Notons $\mathcal{B} = (e_1, \dots, e_p)$ la base de E, $\mathcal{C} = (f_1, \dots, f_n)$ celle de F. On travaille avec $u \in \mathscr{L}(E,F)$ ainsi qu'avec un vecteur x fixé dans E. On note

$$X = \mathrm{Mat}_{\mathcal{B}}(x) = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}, \quad Y = \mathrm{Mat}_{\mathcal{C}}(u(x)) = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \quad \text{et} \quad A = \mathrm{Mat}_{\mathcal{C},\mathcal{B}}(u) = (a_{i,j})_{\substack{1 \le i \le n \\ 1 \le j \le p}}.$$

On veut démontrer que $Y = AX$, c'est à dire que les coordonnées de l'image $u(x)$ s'obtiennent à l'aide d'un *produit matriciel*. Puisque $x = \sum_{j=1}^{p} x_j e_j$, on obtient par linéarité

$$u(x) = \sum_{j=1}^{p} x_j u(e_j) = \sum_{j=1}^{p} x_j \left(\sum_{i=1}^{n} a_{i,j} f_i \right) = \sum_{j=1}^{p} \sum_{i=1}^{n} a_{i,j} x_j f_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{p} a_{i,j} x_j \right) f_i$$

Fixons $i \in [\![1,n]\!]$. La coordonnée de $u(x)$ sur f_i a été noté y_i. On vient donc d'obtenir

$$y_i = \sum_{j=1}^{p} a_{i,j} x_j \quad \text{c-à-d} \quad [Y]_{i,1} = \sum_{j=1}^{p} [A]_{i,j} [X]_{j,1} = [AX]_{i,1}.$$

Ceci achève de démontrer $Y = AX$. $\square$

Remarque. Ainsi, pour $x \in E$ et $y \in F$, en notant $X = \mathrm{Mat}_{\mathcal{B}}(x) \in M_{p,1}(\mathbb{K})$, $Y = \mathrm{Mat}_{\mathcal{C}}(y) \in M_{n,1}(\mathbb{K})$, et $A = \mathrm{Mat}_{\mathcal{C},\mathcal{B}}(u)$, on a

$$\boxed{y = u(x) \iff Y = AX.}$$

Lemme 14 (de calcul matriciel)**.**

Soit $M \in M_{n,p}(\mathbb{K})$, $j \in [\![1,p]\!]$ et E_j le $j$ème vecteur de la base canonique de $M_{p,1}(\mathbb{K})$.

$$\text{Le produit } ME_j \text{ est la } j\text{ème colonne de la matrice } M.$$

Théorème 15 (*la matrice de la composée, c'est le produit des matrices*)**.**

Soient E, F et G trois $\mathbb{K}$-espaces vectoriels de dimension finie non nulle.
Soient $\mathcal{B}, \mathcal{C}, \mathcal{D}$ des bases, respectivement de E, F et G.
Soient $u \in \mathscr{L}(E,F)$ et $v \in \mathscr{L}(F,G)$. Alors,

$$\mathrm{Mat}_{\mathcal{D},\mathcal{B}}(v \circ u) = \mathrm{Mat}_{\mathcal{D},\mathcal{C}}(v) \cdot \mathrm{Mat}_{\mathcal{C},\mathcal{B}}(u).$$

Preuve. Notons

$$A = \mathrm{Mat}_{\mathcal{C},\mathcal{B}}(u), \quad B = \mathrm{Mat}_{\mathcal{D},\mathcal{C}}(v), \quad C = \mathrm{Mat}_{\mathcal{D},\mathcal{B}}(v \circ u),$$

le but étant de prouver l'égalité $C = BA$. Notons p la dimension de E, et $(e_1, \dots, e_p)$ les vecteurs de la base $\mathcal{B}$. Fixons j dans $[\![1,p]\!]$. Ainsi, la $j$ème colonne de C vaut par définition

$$\mathrm{Mat}_{\mathcal{D}}(v \circ u(e_j)) = \mathrm{Mat}_{\mathcal{D},\mathcal{B}}(v \circ u)\mathrm{Mat}_{\mathcal{B}}(e_j) = CE_j,$$

où $E_j = \mathrm{Mat}_{\mathcal{B}}(e_j)$ (c'est aussi le $j$ème vecteur de la base canonique de $M_{p,1}(\mathbb{K})$. Par ailleurs,

$$\mathrm{Mat}_{\mathcal{D}}(v \circ u(e_j)) = \mathrm{Mat}_{\mathcal{D}}(v(u(e_j))) = \underbrace{\mathrm{Mat}_{\mathcal{D},\mathcal{C}}(v)}_{B} \cdot \mathrm{Mat}_{\mathcal{C}}(u(e_j)) = B \cdot \underbrace{\mathrm{Mat}_{\mathcal{C},\mathcal{B}}(u)}_{A} \mathrm{Mat}_{\mathcal{B}}(e_j) = BAE_j.$$

Ainsi, $CE_j = BAE_j$ pour tout $1 \leq j \leq p$, ce qui montre que C et BA sont égales colonne par colonne. □

Corollaire 16 (Caractérisation matricielle des isomorphismes)**.**

Soient E et F deux $\mathbb{K}$-espaces vectoriels de même dimension finie non nulle et $u \in \mathscr{L}(E,F)$. Soient $\mathcal{B}$ et $\mathcal{C}$ des bases respectivement de E et F. Notons $A = \mathrm{Mat}_{\mathcal{C},\mathcal{B}}(u)$. Alors

$$u \text{ est bijective} \quad \text{ssi} \quad A \text{ est inversible.}$$

Dans le cas où u est un isomorphisme, $\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(u^{-1}) = A^{-1}$.

Exemple 17.

Soit un n-uplet $\lambda = (\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n$. La **matrice de Vandermonde** associée à λ, notée V_λ, est définie par

$$V_\lambda = \begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \dots & \lambda_1^{n-1} \\ 1 & \lambda_2 & \lambda_2^2 & \dots & \lambda_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \lambda_n & \lambda_n^2 & \dots & \lambda_n^{n-1} \end{pmatrix}.$$

1. On note $u_\lambda : \left\{ \begin{array}{ccc} \mathbb{K}_{n-1}[X] & \to & \mathbb{K}^n \\ P & \mapsto & (P(\lambda_1), \cdots, P(\lambda_n)) \end{array} \right.$.
   Vérifier que V_λ est la matrice de u_λ dans les bases canoniques de $\mathbb{K}_{n-1}[X]$ et $\mathbb{K}^n$.
2. Démontrer que V_λ est inversible si et seulement si les λ_i sont deux à deux distincts.

Théorème 18 (Isomorphisme d'anneaux induit par le choix d'une base)**.**

Soient E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et et $\mathcal{B}$ une base de E.
L'application

$$\Phi_{\mathcal{B}} : \begin{cases} \mathscr{L}(E) & \to & M_n(\mathbb{K}) \\ u & \mapsto & \mathrm{Mat}_{\mathcal{B}}(u) \end{cases}$$

est un isomorphisme d'anneaux. Notamment, si u et v sont deux endomorphismes de E, alors

$$\Phi_{\mathcal{B}}(v \circ u) = \Phi_{\mathcal{B}}(v) \cdot \Phi_{\mathcal{B}}(u).$$

De plus, $\Phi_{\mathcal{B}}$ induit un isomorphisme de groupes de $GL(E)$ dans $\mathrm{GL}_n(\mathbb{K})$.

Corollaire 19 (Commutativité, itérés)**.**

Soit E un espace vectoriel de dimension finie non nulle et $\mathcal{B}$ une base de E.
Soit $u, v \in \mathscr{L}(E)$, $A = \mathrm{Mat}_{\mathcal{B}}(u)$ et $B = \mathrm{Mat}_{\mathcal{B}}(v)$.

1. $u \circ v = v \circ u$ si et seulement si $AB = BA$.
2. $\forall k \in \mathbb{N} \quad \mathrm{Mat}_{\mathcal{B}}(u^k) = A^k$.
3. Si de surcroît u est un automorphisme, la ligne précédente est vraie pour tout $k \in \mathbb{Z}$.

2 Point de vue linéaire sur les matrices.

2.1 Application linéaire canoniquement associée à une matrice.

Proposition-Définition 20.

Soit $A \in M_{n,p}(\mathbb{K})$. On appelle **application linéaire canoniquement associée** à A l'application

$$f : \begin{cases} M_{p,1}(\mathbb{K}) & \to & M_{n,1}(\mathbb{K}) \\ X & \mapsto & AX \end{cases} .$$

L'application f est linéaire et sa matrice dans les bases canoniques de $M_{p,1}(\mathbb{K})$ et $M_{n,1}(\mathbb{K})$ n'est autre que A.

Lorsque A est carrée, f est appelée **endomorphisme canoniquement associé** à A.

Un léger abus fréquent consiste à identifier les colonnes à k lignes avec les k-uplets. On confondra ainsi

$$\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \in M_{3,1}(\mathbb{R}) \quad \text{et} \quad (1,2,3) \in \mathbb{R}^3.$$

L'application l'application linéaire f canoniquement associée à $A \in M_{n,p}(\mathbb{K})$ pourra donc être vue comme une application

$$f : M_{p,1}(\mathbb{K}) \to M_{n,1}(\mathbb{K}) \quad \text{ou, au prix du léger abus ci-dessus, comme} \quad \boxed{f : \mathbb{K}^p \to \mathbb{K}^n.}$$

Exemple 21.

Soit f l'application linéaire canoniquement associée à la matrice $A = \begin{pmatrix} 2 & 0 & 1 \\ 0 & -1 & 3 \end{pmatrix}$.

Donner sans calcul $f(1,0,0)$, $f(0,1,0)$ et $f(0,0,1)$. Calculer $f(1,2,3)$.

Exemple 22.

Soit N la matrice

$$N = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Notons f l'endomorphisme de $\mathbb{R}^4$ canoniquement associé à N.
Décrire l'action de f sur la base canonique de $\mathbb{R}^4$ et justifier que $N^4 = 0$.

2.2 Rang, image et noyau d'une matrice.

Dans ce paragraphe et les suivants, les espaces $\mathbb{K}^p$ et $M_{p,1}(\mathbb{K})$ sont délibérément confondus.

Définition 23.

Soit $A \in M_{n,p}(\mathbb{K})$ et $f : \mathbb{K}^p \to \mathbb{K}^n$ l'application linéaire canoniquement associée.

- Le noyau de f peut être appelé noyau de la matrice A, noté alors $\mathrm{Ker}(A)$.
- L'image de f peut être appelée image de la matrice A, noté alors $\mathrm{Im}(A)$.
- Le rang de f sera appelé **rang** de la matrice A et noté $\mathrm{rg}(A)$.

Proposition 24.

Soit $A \in M_{n,p}(\mathbb{K})$ et $f : \mathbb{K}^p \to \mathbb{K}^n$ l'application linéaire canoniquement associée.

- Par définition, $\mathrm{Ker}(A)$ est le sous-espace vectoriel de $\mathbb{K}^p$ défini par

$$\mathrm{Ker}(A) = \{X \in \mathbb{K}^p : AX = 0_{n,1}\}.$$

  On sait résoudre un tel système linéaire homogène (pivot) et donc trouver une base du noyau.

- L'image de A est engendrée par les colonnes $C_1, \dots, C_p$ de A :

$$\mathrm{Im}(A) = \mathrm{Vect}\,(C_1, \dots, C_p)\,,$$

  On saura extraire une base de cette famille génératrice, et en particulier en déduire rg(A).

- $\mathrm{rg}(A) = \mathrm{rg}(C_1, \dots, C_p)$.
  De plus, $\mathrm{rg}(A) \leq \min(n,p)$.
- $\mathrm{Ker}(A)$ est de dimension $p - \mathrm{rg}(A)$.

Remarque. Les **colonnes** engendrent l'image de A ; le rang de la matrice est celui de la famille des colonnes. En revanche, ce sont les **lignes** de A qui donnent un système d'équations du noyau.

Exemple 25 (Voici des matrices de taille n. Donner leur rang).

$$A = \begin{pmatrix} & & & n \\ & & \iddots & \\ & 2 & & \\ 1 & & & \end{pmatrix} \qquad \text{et} \qquad B = \begin{pmatrix} 1 & & & 1 \\ & \ddots & \iddots & \\ & \iddots & \ddots & \\ 1 & & & 1 \end{pmatrix}$$

Exemple 26 (Noyau de la matrice Attila).

Soit J la matrice de $M_n(\mathbb{K})$ dont tous les coefficients sont égaux à 1. Quel est son rang ?
Donner une base de $\mathrm{Ker}(J)$
— en posant le système linéaire (point de vue des lignes)
— en prenant le point de vue des colonnes et en utilisant le théorème du rang.

On formalise ci-dessous la méthode qui nous a permis ci-dessus de trouver des vecteurs du noyau en regardant les colonnes.

Méthode (Les combinaisons nulles de colonnes offrent des vecteurs dans le noyau).

Soit $A \in M_{n,p}(\mathbb{K})$, de colonnes $C_1, \ldots, C_p$ et $f : \mathbb{K}^p \to \mathbb{K}^n$ l'a.l. canoniquement associée.

Supposons qu'on ait une combinaison linéaire nulle des colonnes : $\displaystyle\sum_{j=1}^{p} \alpha_j C_j = 0_{n,1}$.

En notant $(e_1, \ldots, e_p)$ la base canonique de $\mathbb{K}^p$, on a

$$\sum_{j=1}^{p} \alpha_j f(e_j) = 0_{\mathbb{K}^n}, \quad \text{i.e.} \quad f\left(\sum_{j=1}^{p} \alpha_j e_j\right) = 0_{\mathbb{K}^n} \quad \text{soit} \quad \sum_{j=1}^{p} \alpha_j e_j \in \mathrm{Ker}(f).$$

Théorème 27 (Caractérisations de l'inversibilité d'une matrice).

Soit $A \in M_n(\mathbb{K})$. Les assertions suivantes sont équivalentes.

1. A est inversible.
2. $\mathrm{Ker}(A)$ est trivial, réduit à $\{0_{\mathbb{K}^n}\}$.
3. La famille des colonnes de A engendre $\mathbb{K}^n$.
4. $\mathrm{rg}(A) = n$.

On retiendra en particulier que

$$\boxed{\forall A \in M_n(\mathbb{K}) \quad A \in \mathrm{GL}_n(\mathbb{K}) \iff \mathrm{rg}(A) = n.}$$

Corollaire 28 (*un côté suffit*).

Pour une matrice carrée, l'existence d'un inverse à gauche (resp. à droite) suffit pour que cette matrice soit inversible. Alors, son inverse n'est autre que l'inverse à gauche (resp. à droite).

Corollaire 29 (CNS d'inversibilité d'une matrice triangulaire).

Une matrice triangulaire est inversible s.s.i. ses coefficients diagonaux sont tous non nuls.

Proposition 30 (Rang et produit matriciel).

1. Lors d'un produit matriciel, le rang ne peut que diminuer :
$$\forall A \in M_{n,p}(\mathbb{K}) \quad \forall B \in M_{p,q}(\mathbb{K}) \qquad \mathrm{rg}(AB) \leq \min\left(\mathrm{rg}(A), \mathrm{rg}(B)\right).$$
2. Le produit par une matrice inversible laisse le rang inchangé : pour $A \in M_{n,p}(\mathbb{K})$,
$$\forall P \in GL_n(\mathbb{K}) \quad \mathrm{rg}(PA) = \mathrm{rg}(A) \qquad \text{et} \qquad \forall Q \in GL_p(\mathbb{K}) \qquad \mathrm{rg}(AQ) = \mathrm{rg}(A).$$

Preuve.
1. Soient $A \in M_{n,p}(\mathbb{K})$ et $B \in M_{p,q}(\mathbb{K})$. On va tout traduire en termes d'applications linéaires. Notons
$$f : \mathbb{K}^p \to \mathbb{K}^n \qquad \text{et} \qquad g : \mathbb{K}^q \to \mathbb{K}^p,$$
les applications linéaires canoniquement associées respectivement à A et B. Notons $\mathcal{B}_q$, $\mathcal{B}_p$ et $\mathcal{B}_n$ les bases canoniques respectivement de $\mathbb{K}^q$, $\mathbb{K}^p$ et $\mathbb{K}^n$. On a alors
$$AB = \mathrm{Mat}_{\mathcal{B}_n,\mathcal{B}_p}(f)\mathrm{Mat}_{\mathcal{B}_p,\mathcal{B}_q}(g) = \mathrm{Mat}_{\mathcal{B}_n,\mathcal{B}_q}(f \circ g).$$
Ainsi, $f \circ g$ est l'application canoniquement associée à AB : on a
$$\mathrm{rg}(AB) = \mathrm{rg}(f \circ g), \quad \mathrm{rg}(A) = \mathrm{rg}(f) \quad \text{et} \quad \mathrm{rg}(B) = \mathrm{rg}(g).$$
On a démontré dans le cours sur les applications linéaires l'inégalité
$$\mathrm{rg}(f \circ g) \leq \min(\mathrm{rg}(f), \mathrm{rg}(g)).$$
On en déduit l'inégalité $\mathrm{rg}(AB) \leq \min\left(\mathrm{rg}(A), \mathrm{rg}(B)\right)$.

2. Soient $A \in M_{n,p}(\mathbb{K})$, $P \in GL_n(\mathbb{K})$ et $Q \in GL_p(\mathbb{K})$. Notons f, u et v les applications canoniquement associées à ces trois matrices. Puisque P et Q sont inversibles, u et v sont des isomorphismes. Or on a montré dans le cours sur les applications linéaires que la composition par un isomorphisme laissait le rang inchangé. On a donc
$$\mathrm{rg}(PA) = \mathrm{rg}(u \circ f) = \mathrm{rg}(f) = \mathrm{rg}(A) \quad \text{et} \quad \mathrm{rg}(AQ) = \mathrm{rg}(f \circ v) = \mathrm{rg}(f) = \mathrm{rg}(A). \quad \square$$

2.3 Rang d'une matrice et lien avec les autres notions de rang

Proposition 31 (Le rang de la famille, c'est le rang de n'importe quelle matrice associée).

Soient E un $\mathbb{K}$-e.v. de dimension finie et $\mathcal{B}$ une base de E.
Soit $\mathcal{F}$ une famille finie de vecteurs de E. et $A = \mathrm{Mat}_{\mathcal{B}}(\mathcal{F})$. On a
$$\mathrm{rg}(\mathcal{F}) = \mathrm{rg}(A).$$

Preuve. On notera n la dimension de E, $(x_1, \dots, x_p)$ les vecteurs de la famille $\mathcal{F}$ et $(C_1, \dots, C_p)$ les colonnes de A. On souhaite montrer

$$\operatorname{rg}(\mathcal{F}) = \operatorname{rg}(A)$$

$$\text{i.e.} \qquad \dim \operatorname{Vect}(x_1, \dots, x_p) = \dim \operatorname{Vect}(C_1, \dots, C_p)$$

Notons $V = \operatorname{Vect}(x_1, \dots, x_p)$ (sous-espace vectoriel de E) et $V' = \operatorname{Vect}(C_1, \dots, C_p)$ (sous-espace vectoriel de $M_{n,1}(\mathbb{K})$, noté aussi $\operatorname{Im}(A)$ plus haut). Il s'agit de prouver que $\dim V = \dim V'$, ce qu nous allons faire en prouvant que V et V' sont isomorphes.

La première proposition de ce cours énonce que, pour $\mathcal{B}$ une base de E fixée, l'application $\varphi_{\mathcal{B}} : \left\{ \begin{array}{ccc} E & \to & M_{n,1}(\mathbb{K}) \\ x & \mapsto & \operatorname{Mat}_{\mathcal{B}}(x) \end{array} \right.$ est un isomorphisme d'espaces vectoriels. Cette fonction envoie les vecteurs de $\mathcal{F}$ sur les colonnes de A :

$$\forall j \in [\![1, p]\!] \quad \varphi(x_j) = C_j,$$

$$\text{d'où} \qquad \varphi(V) = \operatorname{Im}\left(\varphi_{|V}\right) = \operatorname{Vect}\left(\varphi(x_1), \dots, \varphi(x_p)\right) = \operatorname{Vect}(C_1, \dots, C_p) = V'.$$

Or, on sait que $\varphi_{|V}$ est injective puisque φ l'est. Ceci achève de démontrer que $\varphi_{|V}$ réalise un isomorphisme entre V et V', ce qui implique que ces espaces sont de même dimension. $\square$

Proposition 32 (Le rang de l'a.l., c'est le rang de n'importe quelle matrice associée)**.**

Soient E et F deux $\mathbb{K}$-e.v. de dimension finie, $\mathcal{B}$ une base de E, $\mathcal{C}$ une base de F.
Soit $u \in \mathscr{L}(E, F)$ et $A = \operatorname{Mat}_{\mathcal{C},\mathcal{B}}(u)$. On a

$$\operatorname{rg}(u) = \operatorname{rg}(A).$$

Preuve. Notons $\mathcal{B} = (e_1, \dots, e_p)$ une base de E. On a $\operatorname{rg}(u) = \operatorname{rg}\left(u(e_1), \dots, u(e_p)\right)$. Or, d'après la proposition précédente,

$$\operatorname{rg}\left(u(e_1), \dots, u(e_p)\right) = \operatorname{rg}\left(\operatorname{Mat}_{\mathcal{C}}(u(e_1), \dots, u(e_p))\right), \qquad \text{soit} \quad \operatorname{rg}(u) = \operatorname{rg}(A)\,. \quad \square$$

2.4 Systèmes linéaires : un bilan.

Proposition 33 (Sous-espace vectoriel des solutions d'un système linéaire homogène)**.**

Soit $A \in M_{n,p}(\mathbb{K})$. L'ensemble des solutions du système linéaire homogène $AX = 0$, d'inconnue $X \in M_{p,1}(\mathbb{K})$ est $\operatorname{Ker}(A)$, le noyau de A. La dimension de cet espace de solutions est $p - \operatorname{rg}(A)$.

Proposition 34 (Sous-espace affine des solutions d'un système linéaire compatible)**.**

Soient $A \in M_{n,p}(\mathbb{K})$ et $B \in M_{n,1}(\mathbb{K})$.

Le système linéaire $AX = B$, d'inconnue $X \in M_{p,1}(\mathbb{K})$ est compatible ssi $B \in \operatorname{Im}(A)$.
Si c'est le cas et que X_{pa} est une solution particulière, l'ensemble des solutions du système est le sous-espace affine passant par X_{pa} et dirigé par $\operatorname{Ker}(A)$.

Corollaire 35.

Si A est carrée et inversible de taille n, alors tout système linéaire $AX = B$ avec $B \in M_{n,1}(\mathbb{K})$ a une unique solution. Il est alors dit **de Cramer**.

3 Changements de bases, équivalence, similitude.

3.1 Changement de bases.

Définition 36.

Soit E un espace vectoriel de dimension finie non nulle et $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E.
On appelle **matrice de passage** de $\mathcal{B}$ à $\mathcal{B}'$, et on note $P_{\mathcal{B},\mathcal{B}'}$ la matrice

$$P_{\mathcal{B},\mathcal{B}'} = \mathrm{Mat}_{\mathcal{B}}(\mathcal{B}')$$

c'est-à-dire celle des vecteurs de $\mathcal{B}'$ écrits sur la base $\mathcal{B}$. Autre notation possible : $P_{\mathcal{B}}^{\mathcal{B}'}$.

Proposition 37 (Matrice de passage et application identité)**.**

Soient $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E ; espace vectoriel de dimension finie non nulle.

- $P_{\mathcal{B},\mathcal{B}'} = \mathrm{Mat}_{\mathcal{B},\mathcal{B}'}(\mathrm{id}_E)$.
- La matrice $P_{\mathcal{B},\mathcal{B}'}$ est inversible, d'inverse

$$\left(P_{\mathcal{B},\mathcal{B}'}\right)^{-1} = \quad P_{\mathcal{B}',\mathcal{B}}.$$

- Si X et X' sont les matrices colonnes de x respectivement dans les bases $\mathcal{B}$ et $\mathcal{B}'$. Alors,

$$X' = P_{\mathcal{B}',\mathcal{B}} X.$$

Remarque. On passe donc de X (coordonnées dans $\mathcal{B}$) à X' (coordonnées dans $\mathcal{B}'$) en multipliant X par la matrice de passage de... $\mathcal{B}'$ à $\mathcal{B}$. Un mauvais point pour cette terminologie ! Pour ce qui concerne la notation, en revanche, $X' = P_{\mathcal{B}',\mathcal{B}}X$ est cohérente du point de vue de la relation de Chasles.

Une même application linéaire peut être représentée dans des couples de bases différents. Les matrices de passage permettent de passer d'une représentation à l'autre.

Théorème 38 (Effet d'un changement de bases sur la matrice d'une appli. lin.)**.**

Soient E et F deux espaces vectoriels de dimension finie non nulle.
Soient $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E, et $\mathcal{C}$ et $\mathcal{C}'$ deux bases de F. Soit $u \in \mathscr{L}(E, F)$.
On note

- $A = \mathrm{Mat}_{\mathcal{C},\mathcal{B}}(u)$ (*la matrice de u dans les anciennes bases*)
- $A' = \mathrm{Mat}_{\mathcal{C}',\mathcal{B}'}(u)$ (*celle de u dans les nouvelles bases*),
- $P = P_{\mathcal{B},\mathcal{B}'}$ et $Q = P_{\mathcal{C},\mathcal{C}'}$ (*matrices de passage d'une ancienne à une nouvelle base*)

Alors,

$$\boxed{A' = Q^{-1}AP}.$$

Lorsque deux matrices A et A' satisfont la relation encadrée, on parlera de matrices équivalentes.
Le paragraphe 3.2 est consacré à l'étude de cette relation.

Spécifions le résultat précédent dans le cas d'un endomorphisme.

Théorème 39 (Effet d'un changement de base sur la matrice d'un endomorphisme)**.**

Soit E un espace vectoriel de dimension finie non nulle, $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E, et $u \in \mathscr{L}(E)$. On note

- $A = \mathrm{Mat}_{\mathcal{B}}(u)$ (*la matrice de u dans l'ancienne base*)
- $A' = \mathrm{Mat}_{\mathcal{B}'}(u)$ (*celle de u dans la nouvelle base*),
- $P = P_{\mathcal{B},\mathcal{B}'}$ (*matrice de passage de l'ancienne à la nouvelle base*)

Alors,

$$\boxed{A' = P^{-1}AP}.$$

Lorsque deux matrices A et A' satisfont la relation encadrée, on parlera de matrices semblables.
Le paragraphe 3.3 est consacré à l'étude de cette relation.

Notations 40.

Dans la pratique, la base $\mathcal{B}$ est l'*ancienne base*, souvent la base canonique, alors que $\mathcal{B}'$ sera une *nouvelle base* que l'on souhaite adaptée à l'endomorphisme auquel on s'intéresse, de façon à ce que la matrice dans cette base soit simple (voit dans le paragraphe sur les matrices semblables la recherche d'une base de diagonalisation).

Il sera donc souvent plus facile d'exprimer $P_{\mathcal{B},\mathcal{B}'}$ (vecteurs de $\mathcal{B}'$ écrits sur $\mathcal{B}$) que $P_{\mathcal{B}',\mathcal{B}}$. C'est pour cette raison qu'on réserve la notation simple P pour la première des deux matrices.

3.2 Matrices équivalentes et rang.

Définition 41.

Soient deux matrices A et A' de $M_{n,p}(\mathbb{K})$. On dit que A est **équivalente** à A' si

$$\exists P \in GL_p(\mathbb{K}) \quad \exists Q \in GL_n(\mathbb{K}) \quad A' = Q^{-1}AP.$$

Interprétation : changement de bases pour la représentation d'une application linéaire.

Supposons que $A' = Q^{-1}AP$ avec P et Q inversibles. Soit $f \in \mathscr{L}(\mathbb{K}^p, \mathbb{K}^n)$ canoniquement associée à A, qui est donc sa matrice dans les bases canoniques. Alors A' est la matrice de f dans les bases $\mathcal{B}'$ et $\mathcal{C}'$, avec $\mathcal{B}'$ la famille des colonnes de P et $\mathcal{C}'$ celle des colonnes de Q.

Proposition 42.

L'équivalence des matrices est une relation d'équivalence sur $M_{n,p}(\mathbb{K})$.

Définition 43 (La matrice J_r).

Soit r un entier naturel non nul inférieur à n et à p. Dans $M_{n,p}(\mathbb{K})$, on note J_r la matrice ci-dessous

$$J_r = \begin{pmatrix} I_r & 0_{r,p-r} \\ 0_{n-r,r} & 0_{n-r,p-r} \end{pmatrix}.$$

Par exemple, dans $M_{3,4}(\mathbb{K})$, la matrice J_2 est celle-ci : $J_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$.

Théorème 44 (Équivalence à J_r pour une matrice de rang r).

Soit r un entier inférieur à n et à p. Toute matrice de $M_{n,p}(\mathbb{K})$ de rang r est équivalente à J_r.

Corollaire 45 (Classification des matrices équivalentes par le rang).

Deux matrices de $M_{n,p}(\mathbb{K})$ sont équivalentes si et seulement si elles ont le même rang.
Le nombre de classes d'équivalence pour l'équivalence des matrices de $M_{n,p}(\mathbb{K})$ est $\min(n,p)+1$.

Théorème 46 (Invariance du rang par transposition).

$$\forall A \in M_{n,p}(\mathbb{K}) \quad \mathrm{rg}(A^\top) = \mathrm{rg}(A).$$

Corollaire 47.

Soit $A \in M_{n,p}(\mathbb{K})$, $(C_1, \dots, C_p)$ la famille de ses colonnes et $(L_1, \dots, L_n)$ la famille de ses lignes.

$$\mathrm{rg}(A) = \mathrm{rg}(C_1, \dots, C_p) = \mathrm{rg}(L_1, \dots, L_n).$$

3.3 Matrices semblables.

Définition 48.

Soient deux matrices A et A' de $M_n(\mathbb{K})$. On dit que A est **semblable** à A' si

$$\exists P \in GL_n(\mathbb{K}) \quad A' = P^{-1}AP.$$

Interprétation : changement de base.
Supposons que $A' = P^{-1}AP$ avec P inversible. Notons f l'endomorphisme canoniquement associé à A.
La matrice A est donc celle de f dans $\mathcal{B}$ la base canonique de $\mathbb{K}^n$ et A' est la matrice de f dans la "nouvelle" base $\mathcal{B}'$ où $\mathcal{B}'$ est la famille des colonnes de P.

Proposition 49.

La similitude des matrices est une relation d'équivalence sur $M_n(\mathbb{K})$.

Exemple 50 (Semblable à l'identité)**.**

Justifier que la seule matrice semblable à I_n, c'est elle-même.
Idem pour toute matrice de forme λI_n, notamment la matrice nulle.

Exemple 51 (AB et BA)**.**

Soient $(A, B) \in (M_n(\mathbb{K}))^2$. Montrer que si A ou B est inversible, alors AB et BA sont semblables.

Exemple 52 (Équivalence et similitude)**.**

Justifier que si deux matrices sont semblables, alors elles sont équivalentes.
Exhiber un exemple simple qui montre que la réciproque est fausse.

Contrairement à ce qui a été fait pour l'équivalence des matrices, nous ne décrirons pas les différentes classes d'équivalence pour la similitude des matrices. On se contente ici de considérer des exemples où pour une matrice de départ donnée, on propose une matrice semblable *plus simple*

Exemple 53 (Réduction d'une matrice nilpotente)**.**

Soit $A \in M_n(\mathbb{K})$ telle que $A^n = 0$ et $A^{n-1} \neq 0$. Montrer que A est semblable à la matrice

$$N = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix}.$$

Exemple 54 (Une diagonalisation)**.**

Montrer que $A = \begin{pmatrix} 1 & 4 & 6 \\ 0 & 2 & 5 \\ 0 & 0 & 3 \end{pmatrix}$ est semblable à $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$.
Expliciter une matrice P telle que $A = PDP^{-1}$.
Le travail qui vient d'être fait sera généralisé (quand c'est possible !) par le cours de spé.

Un autre exemple (laissé en exercice) : prouve que $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ est semblable à $\begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}$

Définition 55 (rappel)**.**

Soit $A = (a_{i,j}) \in M_n(\mathbb{K})$. On appelle **trace** de la matrice A et on note $\mathrm{tr}(A)$ la somme de ses coefficients diagonaux :

$$\mathrm{tr}(A) = \sum_{i=1}^{n} a_{i,i}.$$

Proposition 56 (Trace et opérations, rappel)**.**

Pour toutes matrices A et B carrées d'ordre n,

- La trace est une forme linéaire sur $M_n(\mathbb{K})$.
- $\forall A \in M_n(\mathbb{K}) \quad \mathrm{tr}(A^\top) = \mathrm{tr}(A)$.
- $\forall (A, B) \in (M_n(\mathbb{K}))^2 \quad \mathrm{tr}(AB) = \mathrm{tr}(BA)$.

Proposition 57 (La trace est invariante par similitude)**.**

Si deux matrices sont semblables, alors elles ont même trace. La réciproque est fausse.

L'invariance de la trace par similitude donne un sens à la définition ci-dessous.

Définition 58.

Soient u un endomorphisme d'un espace vectoriel E de dimension finie non nulle.
On appelle **trace** de u, et on note $\mathrm{tr}(u)$ la trace de $\mathrm{Mat}_{\mathcal{B}}(u)$, où $\mathcal{B}$ est n'importe quelle base de E.

Proposition 59.

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie non nulle.

- L'application $\mathrm{tr} : u \mapsto \mathrm{tr}(u)$ est une forme linéaire sur $\mathscr{L}(E)$.
- Pour tous u et v dans $\mathscr{L}(E)$, $\mathrm{tr}(uv) = \mathrm{tr}(vu)$.

Exemple 60 (Pas possible)**.**

Soit E un espace de dimension finie non nulle.
Démontrer qu'il ne saurait exister d'endomorphismes u et v de E tels que $uv - vu = \mathrm{id}_E$.

Exemple 61 (Trace d'un projecteur)**.**

Soit p un projecteur de E, espace vectoriel de dimension finie non nulle. Montrer que

$$\mathrm{tr}(p) = \mathrm{rg}(p).$$

3.4 Deux compléments sur le rang.

Premier complément sur le rang : Rang et opérations élémentaires.

Proposition 62.

Si une matrice B est obtenue en réalisant des opérations élémentaires sur une matrice A, alors les matrices A et B sont équivalentes.
En particulier, les opérations élémentaires sur les lignes et les colonnes conservent le rang.
Plus précisément,
- Les opérations élémentaires sur les colonnes conservent l'image.
- Les opérations élémentaires sur les lignes conservent le noyau.

Lemme 63 (Rang d'une matrice échelonnée)**.**

Si les r nombres $\alpha_{i,i}$ (pour $1 \leq i \leq r$) sont non nuls, alors la matrice

$$\begin{pmatrix} \alpha_{1,1} & \dots & \alpha_{1,r} & \dots & \alpha_{1,p} \\ & \ddots & \vdots & & \vdots \\ (0) & & \alpha_{r,r} & \dots & \alpha_{r,p} \\ 0 & \dots & 0 & \dots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & \dots & 0 \end{pmatrix} \quad \text{est de rang égal à } r$$

Plus généralement, toute matrice échelonnée (en lignes) ayant r lignes non nulles est de rang r.

Méthode.

L'algorithme du pivot de Gauss permet d'échelonner en lignes (ou en colonnes si vous préférez !) une matrice donnée. Le rang a été conservé, et celui de la matrice échelonnée est facile à lire.

Exemples 64 (Calculs de rang)**.**

Soit $n \geq 2$ et a, b, c, d quatre scalaires. Calculer le rang des matrices.

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 6 \\ a & b & c & d \end{pmatrix}, \quad B = \begin{pmatrix} 1 & a & b+c \\ 1 & b & c+a \\ 1 & c & a+b \end{pmatrix}.$$

$$C = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 3 & 4 & \dots & n+1 \\ 3 & 4 & 5 & \dots & n+2 \\ \vdots & \vdots & \vdots & & \vdots \\ n & n+1 & n+2 & \dots & 2n-1 \end{pmatrix}.$$

Second complément sur le rang : Rang et matrices extraites.

Définition 65.

Soit $A = (a_{i,j}) \in M_{n,p}(\mathbb{K})$. On appelle **matrice extraite** de A toute matrice obtenue en supprimant certaines lignes et colonnes de A, plus précisément tout matrice de la forme

$$\begin{pmatrix} a_{i_1,j_1} & \cdots & a_{i_1,j_t} \\ \vdots & & \vdots \\ a_{i_s,j_1} & \cdots & a_{i_s,j_t} \end{pmatrix}, \text{ avec } 1 \leq s \leq n,\ 1 \leq t \leq p,\ 1 \leq i_1 \leq \cdots \leq i_s \leq n,\ 1 \leq j_1 \leq \cdots \leq j_t \leq p.$$

Théorème 66.

Soit $A \in M_{n,p}(\mathbb{K})$.

1. Si B est une matrice extraite de A, alors $\mathrm{rg}(B) \leq \mathrm{rg}(A)$.
2. Si A est de rang r, il existe une matrice carrée et inversible de taille r extraite de A.

Il en découle une caractérisation du rang par les matrices extraites :

Le rang est la taille maximale des matrices inversibles extraites de A.

Exemple 67 (Matrice compagnon)**.**

Pour $a_0, \ldots, a_{n-1}$, on considère la matrice

$$C = \begin{pmatrix} 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & \ldots & 0 & a_1 \\ 0 & \ddots & & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & 1 & a_{n-1} \end{pmatrix}.$$

Démontrer que pour tout $x \in \mathbb{K}$, $\mathrm{rg}(C - xI_n) \geq n - 1$.
Donner une condition nécessaire et suffisante sur les a_i pour avoir $\mathrm{rg}(C) = n$.

Exercices

Représentation matricielle des applications linéaires.

34.1 [♦◇◇] Pour $P \in \mathbb{K}_n[X]$, on pose $u(P) = P + (X-1)P'$.

1. Justifier (brièvement) que $u \in \mathscr{L}(\mathbb{K}_n[X])$.
2. Donner la matrice de u dans la base canonique.
3. À l'aide de cette matrice, justifier que u est un automorphisme de $\mathbb{K}_n[X]$.

34.2 [♦♦◇] Soit $n \in \mathbb{N}$. L'application $f : P \mapsto P(X+1)$ est un endomorphisme de $\mathbb{R}_n[X]$.

1. Donner la matrice de f dans la base canonique de $\mathbb{R}_n[X]$.
2. Justifier que cette matrice est inversible et calculer son inverse.

34.3 [♦♦◇] Soit E un espace de dimension 3 et $u \in \mathscr{L}(E)$ tel que $u^2 = 0$ et $u \neq 0$.

1. Comparer $\mathrm{Ker}(u)$ et $\mathrm{Im}(u)$ puis donner leurs dimensions.
2. Montrer qu'il existe une base de E dans laquelle la matrice de u est $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

34.4 [♦♦◇] Soit f l'endomorphisme de $\mathbb{R}^3$ canoniquement associé à $\begin{pmatrix} 1 & 1 & -1 \\ -3 & -3 & 3 \\ -2 & -2 & 2 \end{pmatrix}$.

1. Déterminer $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$.
2. Démontrer l'existence d'une base de $\mathbb{R}^3$ dans laquelle la matrice de f est
$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Changement de bases, matrices semblables, rang.

34.5 [◇◇◇] Montrer que les matrices $A = \begin{pmatrix} 1 & 2 & 7 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}$ et I_3 ont le même rang et la même trace.
Les matrices A et I_3 sont-elles semblables ? équivalentes ?

34.6 [♦◇◇] Matrice d'une symétrie
On définit les vecteurs de $\mathbb{R}^3$:

$$e'_1 = (1,-1,-3) \quad e'_2 = (1,0,3) \quad e'_3 = (2,-1,1).$$

On définit les sous-espaces vectoriels de $\mathbb{R}^3$:

$$F = \mathrm{Vect}(e'_1) \quad G = \mathrm{Vect}(e'_2, e'_3).$$

1. Déterminer une base et la dimension de F et de G. Justifier que F et G sont supplémentaires dans $\mathbb{R}^3$.
2. On note $\mathcal{B}' = (e'_1, e'_2, e'_3)$.
   Donner la matrice dans la base $\mathcal{B}'$ de la symétrie vectorielle s par rapport à F parallèlement à G.
3. Calculer la matrice de s dans la base canonique $\mathcal{B} = (e_1, e_2, e_3)$ de $\mathbb{R}^3$.

$\boxed{\textbf{34.7}}$ **[♦◇◇]**
Montrer que toute matrice triangulaire supérieure est semblable à une matrice triangulaire inférieure.

$\boxed{\textbf{34.8}}$ **[♦◇◇]**
Soit A une matrice de $M_n(\mathbb{K})$ non inversible. Prouver qu'il existe une matrice B non nulle dans $M_n(\mathbb{K})$ telle que $AB = BA = 0$.

$\boxed{\textbf{34.9}}$ **[♦◇◇]**
Soient A et B deux matrices de $M_n(\mathbb{K})$ de même rang et telles que $A^2 = A$ et $B^2 = B$. Démontrer qu'il existe deux matrices U et V de $M_n(\mathbb{K})$ telles que $A = UV$ et $B = VU$.

$\boxed{\textbf{34.10}}$ **[♦◇◇]** On suppose que $n \geq 2$. Calculer le rang de $A = (\sin(i+j))_{\substack{1\leq i\leq n \\ 1\leq j\leq n}}$.

$\boxed{\textbf{34.11}}$ **[♦♦◇]** Matrices de rang 1
Soit $H \in M_n(\mathbb{K})$ telle que $\mathrm{rg} H = 1$.

1. Montrer qu'il existe $U, V \in \mathcal{M}_{n,1}(\mathbb{K})$ telles que $H = UV^\top$.
2. Calculer $V^\top U$.
3. Montrer que $H^2 = \mathrm{tr}(H)H$.
4. Montrer que
$$\forall A \in \mathcal{M}_n(\mathbb{K}) \quad : \quad HAH = \mathrm{tr}(AH)\, H.$$

$\boxed{\textbf{34.12}}$ **[♦♦◇]** Rang de $A^\top A$
Soit $A \in M_{n,p}(\mathbb{R})$. On note u et v les applications linéaires canoniquement associées à A et $A^\top A$.

1. Soit $Y \in \mathcal{M}_{n,1}(\mathbb{R})$ tel que $Y^\top Y = 0_{1,1}$. Montrer que $Y = 0_{n,1}$.
2. Montrer que $\mathrm{Ker} u = \mathrm{Ker} v$.
3. Conclure que
$$\mathrm{rg}(A^\top A) = \mathrm{rg} A.$$

$\boxed{\textbf{34.13}}$ **[♦♦◇]** Un calcul de BA à partir de AB !
Soient $A \in \mathcal{M}_{3,2}(\mathbb{R})$, $B \in \mathcal{M}_{2,3}(\mathbb{R})$ telles que
$$AB = \begin{pmatrix} 0 & -1 & -1 \\ -1 & 0 & -1 \\ 1 & 1 & 2 \end{pmatrix}.$$

1. Montrer que AB est une matrice de projection. Calculer son rang.
2. Montrer que $BA \in GL_2(\mathbb{R})$ (on pourra calculer son rang).
3. Montrer que $BA = I_2$.

$\boxed{\textbf{34.14}}$ **[♦♦♦]** Soit $P \in M_n(\mathbb{R})$ telle que $P^2 = P$. On définit φ, endomorphisme de $M_n(\mathbb{R})$ par
$$\forall M \in M_n(\mathbb{R}) \quad \varphi(M) = PM + MP.$$
Démontrer que $\mathrm{tr}(\varphi) = 2nr$, où r est le rang de P.

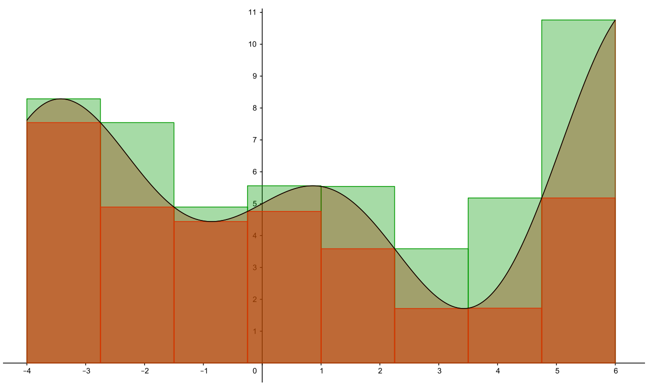
Une construction de l'intégrale de Riemann

Démarche.

La construction de l'intégrale de Riemann la plus courante repose sur une définition de l'intégrale des fonctions en escalier, ce travail étant étendu ensuite par densité à toutes les fonctions continues par morceaux via la notion d'uniforme continuité et le théorème de Heine. À cette approche par *extension*, on préfère ici une approche par *restriction* en définissant d'abord les intégrales de Darboux inférieures et supérieures d'une fonction bornée.

Le point délicat demeure l'intégrabilité au sens de Riemann des fonctions continues. Pour la démontrer, on utilise une idée de Michael Spivak [a] : le théorème fondamental de l'analyse (qui énonce que sous certaines conditions, dériver et intégrer sont deux opérations réciproques) est déjà vrai pour les intégrales de Darboux...

a. M. Spivak, *Calculus*. Fourth edition. Publish or perish, Houston, TX, 2002. 295-296.



Ceci n'est pas une aire

Les fonctions dans ce cours sont à valeurs réelles et définies sur segment $[a,b]$, avec $\boxed{a<b}$.

1 Continuité par morceaux sur un segment.

1.1 Subdivision d'un segment.

Définition 1.

On appelle **subdivision** d'un segment $[a,b]$ toute famille $\sigma = (a_0, a_1, \dots, a_n)$, où $n \in \mathbb{N}^*$, telle que

$$a = a_0 < a_1 < \dots < a_n = b.$$

L'ensemble de toutes les subdivisions d'un segment $[a,b]$ sera noté $\Sigma_{[a,b]}$.

On appelle **pas** de la subdivision σ le réel $\delta_\sigma := \min\left(a_{i+1}-a_i,\ i \in [\![0, n-1]\!]\right)$.

Soit un segment $[a,b]$ et deux subdivisions $\sigma, \sigma' \in \Sigma_{[a,b]}$.

- σ' est dite **plus fine** que σ si elle contient tous les points de σ.
  Par exemple, $(0, \frac{1}{4}, \frac{1}{2}, 1)$ est une subdivision de $[0,1]$ plus fine que $(0, \frac{1}{2}, 1)$.
- On notera $\sigma \cup \sigma'$ la subdivision obtenue en réunissant et en réordonnant les points des deux subdivisions. Par exemple, si $\sigma = (0, e^{-1}, \frac{1}{2}, 1)$ et $\sigma' = (0, \frac{1}{2}, \frac{3}{4}, 1)$, alors $\sigma \cup \sigma' = (0, e^{-1}, \frac{1}{2}, \frac{3}{4}, 1)$.

Exemple 1. Soit $n \in \mathbb{N}^*$. Pour $i \in [\![0, n]\!]$, on note

$$a_i = \frac{i}{n}.$$

La famille $\sigma_n = (a_0, \dots, a_n)$ est une subdivision de $[0,1]$ de pas $\frac{1}{n}$.

Exemple 2. Généralisons à un segment $[a,b]$. Pour $i \in [\![0, n]\!]$, on note

$$a_i = a + i\frac{b-a}{n}.$$

La famille $\sigma_n = (a_0, \dots, a_n)$ est une subdivision de $[a,b]$ dite régulière, de pas $\frac{b-a}{n}$.

Exemple 3. Pour $i \in [\![0, 2^n]\!]$, on note

$$a_i^{(n)} = a + i\frac{b-a}{2^n}.$$

La famille $\theta_n = (a_0^{(n)}, \dots, a_n^{(n)})$ est une subdivision de $[a,b]$, de pas $\frac{b-a}{2^n}$.

Les subdivisions $(\theta_n, n \in \mathbb{N})$ sont "emboîtées" : pour tout $n \in \mathbb{N}^*$, on a

$$\forall i \in [\![0, 2^n]\!] \qquad a_{2i}^{(n+1)} = a + (b-a)\frac{2i}{2^{n+1}} = a + (b-a)\frac{i}{2^n} = a_i^{(n)},$$

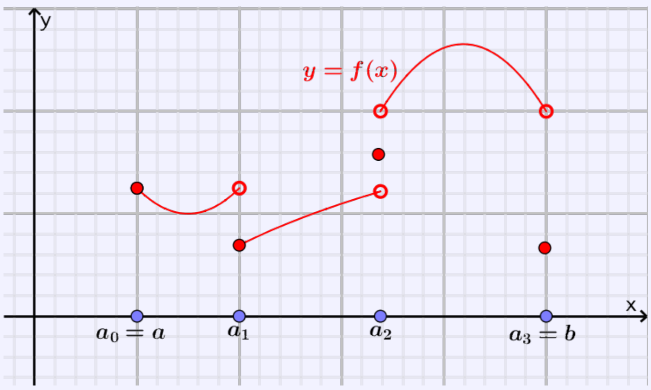
ce qui montre que θ_{n+1} est plus fine que θ_n.

1.2 Fonctions continues par morceaux sur un segment.

Définition 2.

Une fonction $f : [a, b] \to \mathbb{R}$ est dit **continue par morceaux** sur $[a, b]$ s'il existe une subdivision $\sigma = (a_0, \cdots, a_n)$ où $n \in \mathbb{N}^*$ telle que
- pour tout $i \in [\![0, n-1]\!]$, la fonction $f_{|]a_i, a_{i+1}[}$ est continue ;
- pour tout $i \in [\![0, n-1]\!]$, la fonction $f_{|]a_i, a_{i+1}[}$ prolongeable par continuité en a_i et a_{i+1}.

On dit alors que σ est une subdivision **adaptée** à f.



L'ensemble de ces fonctions sera noté $\mathcal{CM}([a, b], \mathbb{R})$ (ou plus simplement $\mathcal{CM}([a, b])$).

Si f est une fonction continue sur $[a, b]$, elle y est continue par morceaux : il suffit de prendre comme subdivision adaptée à f la famille (a, b).

Exemple 3.

Soient les trois fonctions

$$f : \left\{ \begin{array}{ccc} [0,1] & \to & \mathbb{R} \\ x & \mapsto & \left\{ \begin{array}{cc} x\ln(x) & \text{si } x \in]0,1] \\ 1 & \text{si } x = 0 \end{array} \right. \end{array} \right. \quad ; \quad g : \left\{ \begin{array}{ccc} [0,1] & \to & \mathbb{R} \\ x & \mapsto & \left\{ \begin{array}{cc} \ln(x) & \text{si } x \in]0,1] \\ 1 & \text{si } x = 0 \end{array} \right. \end{array} \right.$$

$$\mathbf{1}_{\mathbb{Q}} : \left\{ \begin{array}{ccc} [0,1] & \to & \mathbb{R} \\ x & \mapsto & \left\{ \begin{array}{cc} 1 & \text{si } x \in \mathbb{Q} \\ 0 & \text{si } x \notin \mathbb{Q} \end{array} \right. \end{array} \right.$$

Justifier que f est continue par morceaux sur $[0, 1]$ et que g et $\mathbf{1}_{\mathbb{Q}}$ ne le sont pas.

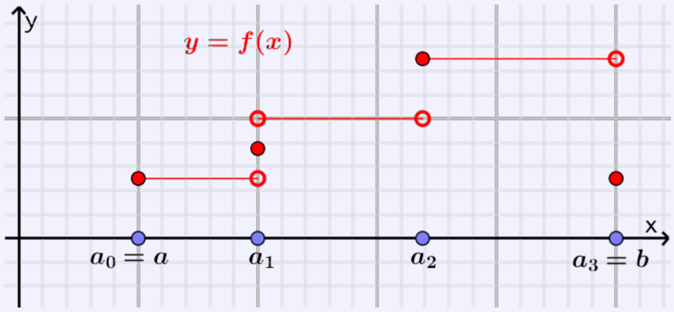
• Considérons $(0, 1)$ comme subdivision de $[0, 1]$. Puisque f a pour limite 0 en 0_+, sa restriction à $]0, 1[$ (notons-la $\widetilde{f}$) peut être prolongée par continuité en 0 en posant $\widetilde{f}(0) = 0$. La fonction f est donc continue par morceaux sur $[0, 1]$. On notera que puisque $f(0) = 1$, elle n'est pas continue sur $[0, 1]$.
• La restriction de g à $]0, 1]$ a une limite infinie en 0 : elle n'y est pas prolongeable par continuité. Ce n'est pas une fonction continue par morceaux sur $[0, 1]$.
• L'ensemble des rationnels et celui des irrationnels étant denses dans $\mathbb{R}$, la fonction $\mathbf{1}_{\mathbb{Q}}$ a une infinité de discontinuités sur $[0, 1]$ (cf cours sur la continuité). Elle ne saurait y être continue par morceaux.

Définition 4.

Une fonction $f : [a, b] \to \mathbb{K}$ est dit **en escalier** sur $[a, b]$ s'il existe une subdivision $\sigma = (a_0, \cdots, a_n)$ où $n \in \mathbb{N}^*$ telle que

$$\text{pour tout } i \in [\![0, n-1]\!], \text{ la fonction } f_{|]a_i, a_{i+1}[} \text{ est constante.}$$

On dit alors que σ est une subdivision **adaptée** à f.



Les fonctions en escalier sont donc *constantes par morceaux.* Ce sont des exemples simples de fonctions continues par morceaux. L'ensemble des fonctions en escalier est important dans la construction classique de l'intégrale de Riemann, mais pas tant que ça pour la présentation que nous avons choisie ici.

Proposition 5.

$\mathcal{CM}([a, b])$ est un sous-espace vectoriel de l'espace vectoriel des fonctions définies sur $[a, b]$.
$\mathcal{CM}([a, b])$ est un sous-anneau de l'anneau des fonctions définies sur $[a, b]$.

Preuve.
Soient f et g deux fonctions de $\mathcal{CM}([a, b])$ et σ et σ' deux subdivisions adaptées respectivement à f et g. Une combinaison linéaire de f et g, ou encore leur produit est bien une fonction continue par morceaux, avec comme subdivision adaptée la subdivision $\sigma \cup \sigma'$. $\square$

Proposition 6.

Si une fonction f est continue par morceaux sur un segment $[a, b]$, elle y est bornée.

Preuve. On considère d'abord une fonction continue par morceaux sur $[a, b]$ à valeurs réelles et une subdivision $(a_0, \ldots, a_n)$ adaptée. Pour tout $i \in [\![0, n-1]\!]$, la fonction $f_{]a_i, a_{i+1}[}$ se prolonge sur $[a_i, a_{i+1}]$ en une fonction continue $\widetilde{f_i}$. On peut alors appliquer le théorème des bornes atteintes à $\widetilde{f_i}$, fonction continue sur un segment. Notons M_i et m_i respectivement les maximum et minimum de $\widetilde{f_i}$. On peut alors poser

$$M = \max\left(\{f(a_0), f(a_1), \ldots, f(a_n)\} \cup \{M_i, i \in [\![0, n-1]\!]\}\right)$$

$$m = \min\left(\{f(a_0), f(a_1), \ldots, f(a_n)\} \cup \{m_i, i \in [\![0, n-1]\!]\}\right)$$

On vérifie alors que M et m sont respectivement un majorant et un minorant de f sur $[a, b]$.

$\square$

2 Intégrales de Darboux d'une fonction bornée.

2.1 Sommes de Darboux.

On rappelle que l'assertion suivante fait partie de nos axiomes en analyse.

Toute partie non vide et majorée A de $\mathbb{R}$ admet un plus petit majorant
que l'on appelle borne supérieure et que l'on note $\sup(A)$.

Définition 7.

Soit f une fonction <u>bornée</u> sur un intervalle $[a,b]$. Soit $\sigma = (a_0, \ldots, a_n) \in \Sigma_{[a,b]}$.
Pour tout $i \in [\![0, n-1]\!]$, on note

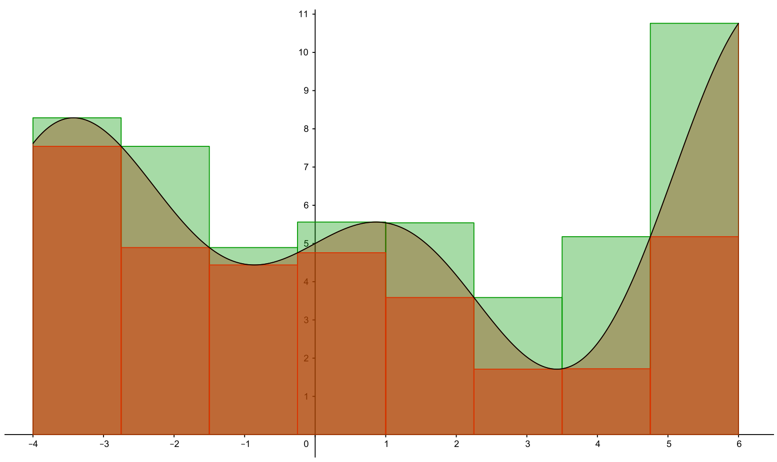
$$m_i := \inf\{f(x), x \in]a_i, a_{i+1}[\} \quad \text{et} \quad M_i := \sup\{f(x), x \in]a_i, a_{i+1}[\}.$$

On appelle **sommes de Darboux** inférieure et supérieure, associées à f et σ les nombres

$$s_{[a,b]}(f,\sigma) := \sum_{i=0}^{n-1} m_i(a_{i+1} - a_i) \quad \text{et} \quad S_{[a,b]}(f,\sigma) := \sum_{i=0}^{n-1} M_i(a_{i+1} - a_i).$$

Figure. Les réels $s_{[a,b]}(f,\sigma)$ et $S_{[a,b]}(f,\sigma)$ peuvent être vus comme des sommes d'aires de rectangles.

Voici le graphe d'une fonction positive (et continue, même si les définitions précédentes ne réclament pas cette hypothèse). Des rectangles s'appuient sur une subdivision régulière de $[a,b]$.



La somme des aires des rectangles foncés, c'est $s_{[a,b]}(f,\sigma)$, celle des rectangles clairs, c'est $S_{[a,b]}(f,\sigma)$.

On remarque que ces deux aires encadrent *l'aire sous la courbe* de f, que ce cours veut définir rigoureusement.

Exemple 0. Les fonctions constantes.
Soit f une fonction constante égale à C sur $[a,b]$. On vérifie facilement que pour toute subdivision $\sigma \in \Sigma_{[a,b]}$, on a

$$s_{[a,b]}(f,\sigma) = S_{[a,b]}(f,\sigma) = C(b-a).$$

Exemple 1. Sommes de Darboux d'une fonction croissante.
Soit f une fonction croissante sur $[a,b]$. Soit $\sigma = (a_0,\dots,a_n)$ une subdivision de $[a,b]$. En reprenant les notations m_i et M_i de la définition précédente, par croissance de f,

$$\forall i \in [\![0,n-1]\!] \qquad m_i = f(a_i^+) \quad \text{et } M_i = f(a_{i+1}^-),$$

où on note $f(a_i^+)$ et $f(a_{i+1}^-)$ respectivement les limites à droite et à gauche en a_i et a_{i+1} (ces limites existent par monotonie de f, on laisse se convaincre que ce sont bien les bornes de la fonction croissante f sur $]a_i,a_{i+1}[$). On a

$$s_{[a,b]}(f,\sigma) = \sum_{i=0}^{n-1} f(a_i^+)(a_{i+1}-a_i) \quad \text{et} \quad S_{[a,b]}(f,\sigma) = \sum_{i=0}^{n-1} f(a_{i+1}^-)(a_{i+1}-a_i).$$

Exemple 2. Sommes de Darboux pour l'indicatrice de $\mathbb{Q}$.
Soit $\sigma_n = (a_0,\dots,a_n)$ une subdivision de $[0,1]$. Soit $i \in [\![0,n-1]\!]$; dans le segment $]a_i,a_{i+1}[$ se trouve au moins un rationnel (densité de $\mathbb{Q}$ dans $\mathbb{R}$), de sorte que le supremum de $\mathbf{1}_{\mathbb{Q}}$ sur $]a_i,a_{i+1}[$ est atteint et vaut $M_i = 1$. De la même façon, $]a_i,a_{i+1}[$ contient au moins un irrationnel, d'où $m_i = 0$. On a donc

$$s_{[0,1]}(\mathbf{1}_{\mathbb{Q}},\sigma) = \sum_{i=0}^{n-1} 0\cdot(a_{i+1}-a_i) = 0 \qquad \text{et} \qquad S_{[0,1]}(\mathbf{1}_{\mathbb{Q}},\sigma) = \sum_{i=0}^{n-1} 1\cdot(a_{i+1}-a_i) = a_n - a_0 = 1.$$

et ceci est valable pour toute subdivision σ de $[0,1]$.

Les bornes de f servent à encadrer les sommes de Darboux.

Proposition 8.

Soit f une fonction minorée sur $[a,b]$ par un réel m et majorée par un réel M. Alors,

$$\forall \sigma \in \Sigma_{[a,b]} \qquad m(b-a) \le s_{[a,b]}(f,\sigma) \le S_{[a,b]}(f,\sigma) \le M(b-a).$$

Preuve.
Notons $\sigma = (a_0,\dots,a_n)$, ainsi que m_i et M_i respectivement l'infimum et le supremum de f sur $]a_i,a_{i+1}[$, où $i \in [\![0,n-1]\!]$. Si m et M sont respectivement un minorant et un majorant de f sur $[a,b]$, on a clairement

$$\forall i \in [\![0,n-1]\!] \quad m \le m_i \le M_i \le M.$$

En effet, m est un minorant de f sur $]a_i,a_{i+1}[$, et m_i le plus grand des minorants sur ce segment.
On a donc, en sommant,

$$\underbrace{m\sum_{i=0}^{n-1}(a_{i+1}-a_i)}_{m(b-a)} \le \underbrace{\sum_{i=0}^{n-1} m_i(a_{i+1}-a_i)}_{s_{[a,b]}(f,\sigma)} \le \underbrace{\sum_{i=0}^{n-1} M_i(a_{i+1}-a_i)}_{S_{[a,b]}(f,\sigma)} \le \underbrace{M\sum_{i=0}^{n-1}(a_{i+1}-a_i)}_{M(b-a)}.$$

$\square$

Proposition 9.

Soit f une fonction bornée sur $[a,b]$. Soient σ et σ' dans $\Sigma_{[a,b]}$. Si σ' est plus fine que σ, alors,

$$s_{[a,b]}(f,\sigma) \le s_{[a,b]}(f,\sigma') \quad \text{et} \quad S_{[a,b]}(f,\sigma) \ge S_{[a,b]}(f,\sigma').$$

Preuve. Il suffit, quitte à itérer ensuite, de montrer que cette chose est vraie si σ' possède *un* point de plus que σ. On note donc $\sigma = (a_0, \ldots, a_n)$ et on considère le cas où $\sigma' = \sigma \cup \{c\}$, où $c \notin \sigma$.

$$\exists k \in [\![0, n-1]\!] \qquad a_k < c < a_{k+1},$$

d'où $\sigma' = (a_0, \ldots, a_k, c, a_{k+1}, \ldots, a_n)$. Notons, pour $i \in [\![0, n-1]\!]$, $m_i = \inf\{f(x), x \in]a_i, a_{i+1}[\}$. On calcule :

$$\begin{aligned} s_{[a,b]}(f,\sigma) = \sum_{i=0}^{n-1} m_i(a_{i+1}-a_i) &= \sum_{\substack{i=0\\ i\neq k}}^{n-1} m_i(a_{i+1}-a_i) + m_k(a_{k+1}-a_k) \\ &= \sum_{\substack{i=0\\ i\neq k}}^{n-1} m_i(a_{i+1}-a_i) + m_k(c-a_k) + m_k(a_{k+1}-c). \end{aligned}$$

Notons $m_k' = \inf\{f(x), x \in]a_k, c[\}$ et $m_k'' = \inf\{f(x), x \in]c, a_{k+1}[\}$. Or, m_k étant *un* minorant de f sur $]a_k, c[$, on a $m_k \leq m_k'$. Pour les mêmes raisons, $m_k \leq m_k''$. On en déduit la majoration

$$s_{[a,b]}(f,\sigma) \leq \sum_{\substack{i=0\\ i\neq k}}^{n-1} m_i(a_{i+1}-a_i) + m_k'(c-a_k) + m_k''(a_{k+1}-c) = s_{[a,b]}(f,\sigma').$$

On montrerait de même, cette fois en manipulant des bornes supérieures, que $S_{[a,b]}(f,\sigma) \geq S_{[a,b]}(f,\sigma')$. $\square$

2.2 Intégrales de Darboux.

Définition 10.

Soit f une fonction bornée sur un segment $[a,b]$. On appelle **intégrales de Darboux** inférieure et supérieure de f sur $[a,b]$ les réels

$$\underline{\int}_{[a,b]} f := \sup\left\{s_{[a,b]}(f,\sigma),\ \sigma \in \Sigma_{[a,b]}\right\} \quad \text{et} \quad \overline{\int}_{[a,b]} f := \inf\left\{S_{[a,b]}(f,\sigma),\ \sigma \in \Sigma_{[a,b]}\right\}.$$

Remarque. D'après la proposition 8, si f est majorée par M sur $[a,b]$ l'ensemble $\left\{s_{[a,b]}(f,\sigma),\ \sigma \in \Sigma_{[a,b]}\right\}$ est majoré par $M(b-a)$. Clairement non vide, il admet bien une borne supérieure. De même, l'ensemble $\left\{S_{[a,b]}(f,\sigma),\ \sigma \in \Sigma_{[a,b]}\right\}$ est non vide et minoré par $m(b-a)$.

Exemple. Fonctions constantes.
Pour une fonction f constante sur $[a,b]$ égale à C, les sommes de Darboux inférieures et supérieures ne dépendent pas de la subdivision choisie et valent $C(b-a)$. On a donc

$$\underline{\int}_{[a,b]} f = \overline{\int}_{[a,b]} f = C(b-a).$$

Exemple. Indicatrice de $\mathbb{Q}$.
On a a montré que

$$\forall \sigma \in \Sigma_{[0,1]} \qquad s_{[0,1]}(\mathbf{1}_{\mathbb{Q}},\sigma) = 0 \quad \text{et} \quad S_{[0,1]}(\mathbf{1}_{\mathbb{Q}},\sigma) = 1.$$

En passant à la borne supérieure sur toutes les subdivisions pour s (inférieure pour S), on obtient

$$\underline{\int}_{[0,1]} \mathbf{1}_{\mathbb{Q}} = 0 \quad \text{et} \quad \overline{\int}_{[0,1]} \mathbf{1}_{\mathbb{Q}} = 1.$$

Proposition 11 (Inégalité de la moyenne pour les intégrales de Darboux)**.**

Soit f une fonction définie sur un segment $[a,b]$, minorée par un réel m et majorée par un réel M. On a

$$m(b-a) \leq \underline{\int}_{[a,b]} f \leq \overline{\int}_{[a,b]} f \leq M(b-a).$$

Preuve. Soit σ une subdivision de $[a,b]$. D'après la proposition 8, on a

$$m(b-a) \leq s_{[a,b]}(f,\sigma) \leq S_{[a,b]}(f,\sigma) \leq M(b-a)$$

Le réel $m(b-a)$ est un minorant de l'ensemble $\left\{s_{[a,b]}(f,\sigma),\ \sigma \in \Sigma_{[a,b]}\right\}$ et l'intégrale de Darboux inférieure est le plus grand des minorants de cet ensemble. On peut écrire le même genre d'argument pour les sommes supérieures et obtenir :

$$m(b-a) \ \leq \ \underline{\int}_{[a,b]} f \qquad \text{et} \qquad \overline{\int}_{[a,b]} f \ \leq \ M(b-a).$$

Reste à comparer les deux intégrales de Darboux. Pour cela on introduit σ_1 et σ_2 deux subdivisions de $[a,b]$. Puisque $\sigma_1 \cup \sigma_2$ est plus fine que σ_1 et que σ_2, on a

$$s_{[a,b]}(f,\sigma_1) \leq s_{[a,b]}(f,\sigma_1 \cup \sigma_2) \leq S_{[a,b]}(f,\sigma_1 \cup \sigma_2) \leq S_{[a,b]}(f,\sigma_2) \quad \text{en particulier } s_{[a,b]}(f,\sigma_1) \leq S_{[a,b]}(f,\sigma_2).$$

On passe d'abord passage au sup (en σ_1) : $\underline{\int}_{[a,b]} f \leq S_{[a,b]}(f,\sigma_2)$. Puis à l'inf (en σ_2) : $\underline{\int}_{[a,b]} f \leq \overline{\int}_{[a,b]} f$. □

On retrouve le résultat montré plus haut pour les fonctions constantes.

Corollaire 12 (Intégrales de Darboux d'une fonction constante)**.**

Si f est une fonction constante, égale à $C \in \mathbb{R}$ entre deux points a et b, alors

$$\underline{\int}_{[a,b]} f = \overline{\int}_{[a,b]} f = C(b-a).$$

Preuve. On applique la proposition 11 avec $m = C = M$. □

Proposition 13 (Relation de Chasles pour les intégrales de Darboux)**.**

Soit f une fonction bornée sur un intervalle $[a,b]$ non réduit à un point, et $c \in]a,b[$. Alors,

$$\underline{\int}_{[a,b]} f = \underline{\int}_{[a,c]} f + \underline{\int}_{[c,b]} f.$$

La relation est aussi vraie pour les intégrales de Darboux supérieures.

Preuve. • Soient deux subdivisions $\sigma_1 \in \Sigma_{[a,c]}$ et $\sigma_2 \in \Sigma_{[c,b]}$. On note σ la subdivision de $[a,b]$ obtenue en concaténant σ_1 et σ_2. Plus précisément, si $\sigma_1 = (a_0, \ldots, a_{n-1}, c)$ et $\sigma_2 = (c, a'_1, \ldots, a'_p)$, alors $\sigma = (a_0, \ldots, a_{n-1}, c, a'_1, \ldots, a'_p)$. On peut alors écrire

$$s_{[a,c]}(f, \sigma_1) \ + \ s_{[c,b]}(f, \sigma_2) \ = \ s_{[a,b]}(f, \sigma) \ \leq \ \underline{\int}_{[a,b]} f$$

(l'égalité ci-dessus est immédiate en revenant aux définitions, et l'inégalité vient de ce que $\underline{\int}_{[a,b]} f$ est une borne supérieure sur toutes les subdivisions). *Fixons* σ_2. On a

$$s_{[a,c]}(f, \sigma_1) \leq \underline{\int}_{[a,b]} f \ - \ s_{[c,b]}(f, \sigma_2) \qquad \text{soit en passant au sup sur } \sigma_1 \qquad \underline{\int}_{[a,c]} f \leq \underline{\int}_{[a,b]} f \ - \ s_{[c,b]}(f, \sigma_2).$$

$$\text{soit} \qquad s_{[c,b]}(f, \sigma_2) \leq \underline{\int}_{[a,b]} f - \underline{\int}_{[a,c]} f.$$

En passant au sup sur σ_2, on obtient

$$\underline{\int}_{[c,b]} f \leq \underline{\int}_{[a,b]} f - \underline{\int}_{[a,c]} f \qquad \text{soit} \qquad \underline{\int}_{[a,c]} f + \underline{\int}_{[c,b]} f \leq \underline{\int}_{[a,b]} f.$$

• Soit une subdivision $\sigma \in \Sigma_{[a,b]}$. Il existe $k \in [\![0, n-1]\!]$ tel que $c \in [a_k, a_{k+1}]$. Notons $\sigma_1 = (a_0, \ldots, a_k, c)$ (en confondant a_k et c s'ils sont égaux) puis $\sigma_2 = (c, a_{k+1}, \ldots, a_n)$ (en confondant c et a_{k+1} s'ils sont égaux). On note σ' la concaténation de σ_1 et de σ_2 (voir-ci-dessus). La subdivision σ' est plus fine que σ, ce qui entraîne d'après la Proposition 9 la première des inégalités suivantes :

$$s_{[a,b]}(f, \sigma) \leq s_{[a,b]}(f, \sigma') = s_{[a,c]}(f, \sigma_1) + s_{[c,b]}(f, \sigma_2) \leq \underline{\int}_{[a,c]} f + \underline{\int}_{[c,b]} f.$$

Il reste à passer à la borne supérieure (sur σ) pour obtenir $\underline{\int}_{[a,b]} f \leq \underline{\int}_{[a,c]} f + \underline{\int}_{[c,b]} f.$

On conclut en combinant les deux inégalités obtenues. □

Voici le résultat sur lequel repose la preuve de l'intégrabilité des fonctions continues dans ce cours.
C'est ici qu'intervient l'idée de Spivak (voir première page).

Théorème 14 (Théorème fondamental de l'analyse pour les intégrales de Darboux)**.**

Soit un segment $[a,b]$ avec $a < b$ et f une fonction *bornée* sur $[a,b]$. Alors, la fonction

$$F : \left\{ \begin{array}{ccc}]a,b] & \to & \mathbb{R} \\ x & \mapsto & \displaystyle\underline{\int}_{[a,x]} f \end{array} \right.$$

est une fonction <u>continue</u> sur $]a,b]$ et telle que $F(x) \underset{x \to a+}{\longrightarrow} 0$.

De surcroît, la fonction F est <u>dérivable</u> en tout point $x_0 \in]a,b]$ où f est continue, de dérivée

$$F'(x_0) = f(x_0).$$

Le résultat reste vrai avec une intégrale de Darboux supérieure.

Preuve. On se concentre sur la continuité puis la dérivabilité à droite, sans vraie perte de généralité.

Soit $x_0 \in]a,b[$ et $x \in]x_0,b]$. En appliquant la relation de Chasles (Prop. 13) sur $[a,x]$ avec $x_0 \in]a,x[$, on obtient

$$F(x) - F(x_0) = \underline{\int}_{[a,x]} f - \underline{\int}_{[a,x_0]} f = \underline{\int}_{[x_0,x]} f.$$

Notons m un minorant et M un majorant de f sur $[a,b]$. Appliquons l'inégalité de la moyenne (proposition 11) sur $[x_0,x]$: on obtient

$$m(x-x_0) \leq F(x) - F(x_0) \leq M(x-x_0).$$

Par encadrement, on obtient que F est continue à droite en x_0. On montrerait de façon analogue que F est continue à gauche. Pour la limite nulle en a_+, il suffit à nouveau d'écrire, pour $x \in]a,b]$, l'encadrement

$$m(x-a) \leq \underline{\int}_{[a,x]} f \leq M(x-a).$$

Supposons dorénavant que x_0 est un point où f est continue. Pour un réel $\varepsilon > 0$ fixé, on a l'existence d'un réel $\eta > 0$ tel que

$$\forall x \in [x_0, x_0+\eta[\quad f(x_0) - \varepsilon \leq f(x) \leq f(x_0) + \varepsilon.$$

Supposons que $x \in [x_0, x_0+\eta[$. en appliquant nouveau 11 sur $[x_0,x]$, on obtient

$$(f(x_0)-\varepsilon)\cdot(x-x_0) \leq \underline{\int}_{[x_0,x]} f \leq (f(x_0)+\varepsilon)\cdot(x-x_0)$$

$$\text{soit} \quad f(x_0) - \varepsilon \leq \frac{F(x)-F(x_0)}{x-x_0} \leq f(x_0)+\varepsilon.$$

Ceci montre que F est dérivable à droite en x_0, de dérivée $f(x_0)$.
On montrerait de façon analogue que F est dérivable à gauche, de dérivée $f(x_0)$. □

On pourrait croire que le travail est fini et que l'intégrale de Darboux, inférieure ou supérieure, est une "bonne" définition de l'intégrale. Comme on va le voir ci-dessous, elles ont un défaut...

Exemple 15 (Défaut de linéarité des intégrales de Darboux)**.**

Considérons les fonctions $\mathbf{1}_{\mathbb{Q}}$ et $\mathbf{1}_{\mathbb{R}\setminus\mathbb{Q}}$. En remarquant que $\mathbf{1}_{\mathbb{Q}} + \mathbf{1}_{\mathbb{R}\setminus\mathbb{Q}} = \mathbf{1}_{\mathbb{R}}$, on peut écrire

$$\underbrace{\underline{\int}_{[0,1]} \mathbf{1}_{\mathbb{Q}}}_{0} + \underbrace{\underline{\int}_{[0,1]} \mathbf{1}_{\mathbb{R}\setminus\mathbb{Q}}}_{0} < \underbrace{\underline{\int}_{[0,1]} (\mathbf{1}_{\mathbb{Q}} + \mathbf{1}_{\mathbb{R}\setminus\mathbb{Q}})}_{1},$$

$$\underbrace{\overline{\int}_{[0,1]} (\mathbf{1}_{\mathbb{Q}} + \mathbf{1}_{\mathbb{R}\setminus\mathbb{Q}})}_{1} < \underbrace{\overline{\int}_{[0,1]} \mathbf{1}_{\mathbb{Q}}}_{1} + \underbrace{\overline{\int}_{[0,1]} \mathbf{1}_{\mathbb{R}\setminus\mathbb{Q}}}_{1}.$$

On a cependant des inégalités, données dans les deux lemmes ci-dessous.

Lemme 16 (Presque linéarité des intégrales de Darboux (1))**.**

Soient f et g deux fonctions bornées sur $[a,b]$. Alors

$$\underline{\int}_{[a,b]}(f+g) \ \geq \ \underline{\int}_{[a,b]} f + \underline{\int}_{[a,b]} g \quad \text{ et } \quad \overline{\int}_{[a,b]}(f+g) \ \leq \ \overline{\int}_{[a,b]} f + \overline{\int}_{[a,b]} g.$$

Preuve.

On prouve l'inégalité pour les intégrales de Darboux supérieures. On va d'abord montrer pour toute subdivision θ de $[a,b]$ l'inégalité

$$S_{[a,b]}(f+g,\theta) \leq S_{[a,b]}(f,\theta) + S_{[a,b]}(g,\theta) \qquad (*).$$

Pour cela considérons $\theta = (a_0, \dots, a_n) \in \Sigma_{[a,b]}$. Notons, pour $i \in [\![0, n-1]\!]$

$$M_i = \sup\{f(x)+g(x), x \in]a_i, a_{i+1}[\}, \quad M_i' = \sup\{f(x), x \in]a_i, a_{i+1}[\}, \quad M_i'' = \sup\{g(x), x \in]a_i, a_{i+1}[\}.$$

Le nombre $M_i' + M_i''$ est un majorant de $f+g$ sur $]a_i, a_{i+1}[$; m_i étant le plus petit des majorants, on a $M_i \leq M_i' + M_i''$. On a donc bien

$$S_{[a,b]}(f+g,\theta) = \sum_{i=0}^{n-1} M_i(a_{i+1}-a_i) \leq \sum_{i=0}^{n-1} M_i'(a_{i+1}-a_i) + \sum_{i=0}^{n-1} M_i''(a_{i+1}-a_i) = S_{[a,b]}(f,\theta) + S_{[a,b]}(g,\theta),$$

ce qui montre $(*)$.

Soient σ et σ' deux subdivisions de $[a,b]$. On peut écrire

$$\begin{aligned} S_{[a,b]}(f,\sigma) + S_{[a,b]}(g,\sigma') &\geq S_{[a,b]}(f,\sigma\cup\sigma') + S_{[a,b]}(g,\sigma\cup\sigma') \\ &\geq S_{[a,b]}(f+g,\sigma\cup\sigma') \\ &\geq \overline{\int}_{[a,b]}(f+g). \end{aligned}$$

La première inégalité est obtenue en utilisant la proposition 9, $\sigma\cup\sigma'$ étant plus fine que σ et plus fine que σ'. La seconde est obtenue en écrivant $(*)$ pour $\theta = \sigma\cup\sigma'$, et la dernière en utilisant que l'intégrale est une borne inférieure et donc minore les sommes de Darboux pour toute subdivision.

Fixons σ'. En passant à l'inf en σ, on obtient

$$\overline{\int}_{[a,b]} f + S_{[a,b]}(g,\sigma') \geq \overline{\int}_{[a,b]}(f+g).$$

Il reste à prendre la borne inférieure sur toutes les subdivisions σ' pour obtenir

$$\overline{\int}_{[a,b]} f + \overline{\int}_{[a,b]} f \geq \overline{\int}_{[a,b]}(f+g).$$

□

Lemme 17 (Presque linéarité des intégrales de Darboux (2))**.**

Soit f une fonction bornée sur $[a,b]$ et $\lambda \in \mathbb{R}$,

1. Si $\lambda \geq 0$,
$$\underline{\int}_{[a,b]}(\lambda f) = \lambda \underline{\int}_{[a,b]} f \quad \text{et} \quad \overline{\int}_{[a,b]}(\lambda f) = \lambda \overline{\int}_{[a,b]} f.$$
2. Si $\lambda < 0$,
$$\underline{\int}_{[a,b]}(\lambda f) = \lambda \overline{\int}_{[a,b]} f \quad \text{et} \quad \overline{\int}_{[a,b]}(\lambda f) = \lambda \underline{\int}_{[a,b]} f.$$

Preuve.

Soit $[\alpha,\beta] \subset [a,b]$ et $\lambda \in \mathbb{R}$. En revenant aux définitions on montre facilement que

- Si $\lambda \geq 0$, $\quad \inf\limits_{x\in[\alpha,\beta]}(\lambda f(x)) = \lambda \inf\limits_{x\in[\alpha,\beta]}(f(x))$ et $\sup\limits_{x\in[\alpha,\beta]}(\lambda f(x)) = \lambda \sup\limits_{x\in[\alpha,\beta]}(f(x))$.
- Si $\lambda < 0$, $\quad \inf\limits_{x\in[\alpha,\beta]}(\lambda f(x)) = \lambda \sup\limits_{x\in[\alpha,\beta]}(f(x))$ et $\sup\limits_{x\in[\alpha,\beta]}(\lambda f(x)) = \lambda \inf\limits_{x\in[\alpha,\beta]}(f(x))$.

Détaillons la preuve dans le cas $\lambda < 0$, pour l'intégrale de Darboux inférieure (les autres cas se traitent de façon analogue). Soit $\sigma = (a_0, \ldots, a_n)$ une subdivision de $[a,b]$.

$$s_{[a,b]}(\lambda f, \sigma) = \sum_{i=0}^{n-1}(a_{i+1}-a_i)\cdot \inf_{x\in]a_i,a_{i+1}[}(\lambda f(x)) = \lambda \sum_{i=0}^{n-1}(a_{i+1}-a_i)\cdot \sup_{x\in]a_i,a_{i+1}[}(f(x)) = \lambda S_{[a,b]}(f,\sigma).$$

Par définition de l'intégrale de Darboux supérieure, $S_{[a,b]}(f,\sigma) \geq \overline{\int}_{[a,b]} f$, soit ($\lambda$ étant négatif)

$$s_{[a,b]}(\lambda f, \sigma) = \lambda S_{[a,b]}(f,\sigma) \leq \lambda \overline{\int}_{[a,b]} f.$$

En passant au sup sur toutes les subdivisions σ, on obtient

$$\underline{\int}_{[a,b]}(\lambda f) \leq \lambda \overline{\int}_{[a,b]} f \qquad (1)$$

De plus, par définition de l'intégrale de Darboux inférieure, $s_{[a,b]}(\lambda f,\sigma) \leq \underline{\int}_{[a,b]}\lambda f$, soit ($\lambda$ étant strictement négatif),

$$S_{[a,b]}(f,\sigma) = \frac{1}{\lambda} s_{[a,b]}(\lambda f,\sigma) \geq \frac{1}{\lambda}\underline{\int}_{[a,b]}(\lambda f).$$

En passant à l'inf sur toutes les subdivisions σ, on obtient

$$\overline{\int}_{[a,b]} f \geq \frac{1}{\lambda}\underline{\int}_{[a,b]}(\lambda f), \quad \text{soit} \quad \lambda \overline{\int}_{[a,b]} f \leq \underline{\int}_{[a,b]}(\lambda f) \qquad (2)$$

En combinant (1) et (2), on achève de prouver que

$$\lambda \overline{\int}_{[a,b]} f = \underline{\int}_{[a,b]}(\lambda f).$$

$\square$

3 Intégrale d'une fonction continue par morceaux sur un segment.

3.1 Fonctions intégrables au sens de Riemann.

Définition 18.

On dira d'une fonction f bornée sur un segment $[a,b]$ qu'elle est **Riemann-intégrable** sur $[a,b]$ si ses intégrales de Darboux inférieures et supérieures sont égales.

On appelle alors **intégrale** de f sur $[a,b]$ leur valeur commune, notée

$$\int_{[a,b]} f.$$

Exemple. Les fonctions constantes sont Riemann-intégrables. En effet, si f est constante sur $[a,b]$, égale à $C \in \mathbb{R}$, alors, d'après le corollaire 12, les intégrales de Darboux inférieures et supérieures valent toutes deux $C(b-a)$. La fonction f est donc bien intégrable et

$$\int_{[a,b]} f = C(b-a).$$

Exemple. La fonction $\mathbf{1}_{\mathbb{Q}}$ n'est *pas* Riemann-intégrable sur $[0,1]$: on a vu que ses intégrales de Darboux inférieures et supérieures valent respectivement 0 et 1.

Proposition 19 (HP).

Une fonction croissante sur un segment y est Riemann-intégrable.

Preuve.
Considérons f, croissante sur $[a,b]$. On considère $\sigma_n = (a_0, \ldots, a_n)$ la subdivision régulière de $[a,b]$: on note $\delta_n = \frac{b-a}{n}$; pour tout $i \in [\![0,n]\!]$, $a_i = a + i\delta_n$. On a, pour tout $n \in \mathbb{N}^*$,

$$s_{[a,b]}(f,\sigma_n) \leq \underline{\int}_{[a,b]} f \leq \overline{\int}_{[a,b]} f \leq S_{[a,b]}(f,\sigma_n) \qquad (*).$$

On a déjà examiné les sommes de Darboux dans le cas particulier d'une fonction croissante :

$$s_{[a,b]}(f,\sigma_n) = \sum_{i=0}^{n-1} f(a_i^+)(a_{i+1}-a_i) = \delta_n \sum_{i=0}^{n-1} f(a_i^+) \ \text{ et } \ S_{[a,b]}(f,\sigma_n) = \sum_{i=0}^{n-1} f(a_{i+1}^-)(a_{i+1}-a_i) = \delta_n \sum_{i=0}^{n-1} f(a_{i+1}^-).$$

On a donc

$$S_{[a,b]}(f,\sigma_n) - s_{[a,b]} = \delta_n \sum_{i=0}^{n-1} \left(f(a_{i+1}^-) - f(a_i^+) \right).$$

Or, par croissance de f, pour tout $i \in [\![0,n-1]\!]$, on a $f(a_{i+1}^-) - f(a_i^+) \leq f(a_{i+1}) - f(a_i)$.
On peut donc majorer par une somme qui télescope *vraiment* :

$$S_{[a,b]}(f,\sigma_n) - s_{[a,b]}(f,\sigma_n) \leq \delta_n \sum_{i=0}^{n-1} (f(a_{i+1}) - f(a_i)) \leq \delta_n (f(b) - f(a)) \underset{n\to+\infty}{\longrightarrow} 0.$$

L'encadrement $(*)$ donne alors l'égalité $\underline{\int}_{[a,b]} f = \overline{\int}_{[a,b]} f$, ce qu'il fallait démontrer. □

3.2 Continuité et intégrabilité au sens de Riemann.

Théorème 20.

Les fonctions continues par morceaux sur un segment y sont Riemann-intégrables.

Preuve. Soit $f \in \mathcal{CM}([a,b])$ et $\sigma = (a_0, \dots, a_n)$ une subdivision adaptée. La fonction f étant continue par morceaux sur $[a,b]$, elle y est bornée, ce qui donne un sens aux fonctions

$$I : \begin{cases}]a,b] & \to & \mathbb{R} \\ x & \mapsto & \displaystyle\underline{\int}_{[a,x]} f \end{cases} \quad \text{et} \quad S : \begin{cases}]a,b] & \to & \mathbb{R} \\ x & \mapsto & \displaystyle\overline{\int}_{[a,x]} f \end{cases}$$

D'après le théorème 14, puisque f est continue sur les intervalles $]a_i, a_{i+1}[$, les fonctions I et S y sont dérivables et chacune a pour dérivée f. La différence $S - I$ est donc dérivable en tout point de $[a,b] \setminus \{a_0, \dots, a_n\}$ et sa dérivée y est nulle. La fonction $S - I$ est donc constante sur tout intervalle de la forme $]a_i, a_{i+1}[$ (cela vient des accroissements finis...) De plus, le théorème 14 donne que $S - I$ est continue sur $]a,b]$, ce qui amène qu'elle est constante sur $]a,b]$. Puisqu'elle a pour limite 0 en a_+, la fonction $S - I$ est nulle sur $]a,b]$. En particulier,

$$I(b) = S(b) \qquad \text{i.e.} \qquad \underline{\int}_{[a,b]} f = \overline{\int}_{[a,b]} f.$$

Les deux intégrales de Darboux coïncident pour la fonction f, qui est donc bien intégrable au sens de Riemann sur le segment $[a,b]$. □

Proposition 21 (Nombre fini de différences)**.**

Si f et $\widetilde{f}$ sont deux fonctions continues par morceaux sur $[a,b]$ et qu'elles ne diffèrent qu'en un nombre <u>fini</u> de points, alors

$$\int_{[a,b]} f = \int_{[a,b]} \widetilde{f}.$$

Preuve. Soit f et $\widetilde{f}$ deux fonctions de $\mathcal{CM}([a,b])$ et σ et $\widetilde{\sigma}$ deux subdivisions adaptées respectivement à f à $\widetilde{f}$. On suppose que l'ensemble des points $x \in [a,b]$ tels que $f(x) \neq \widetilde{f}(x)$ est fini et on l'insère dans la subdivision $\sigma \cup \widetilde{\sigma}$ pour créer une subdivision de $[a,b]$ qu'on notera $s = (s_0, \cdots, s_n)$. Notons

$$F : x \mapsto \int_{[a,x]} f \quad \text{et} \quad \widetilde{F} : x \mapsto \int_{[a,x]} \widetilde{f}.$$

Le théorème précédent donne que les fonctions F et $\widetilde{F}$ sont continues sur $]a,b]$ et dérivables sur $[a,b] \setminus \{s_0, \cdots, s_n\}$ (puisque les points de discontinuité se trouvent dans s). De plus,

$$\forall x \in [a,b] \setminus \{s_0, \cdots, s_n\} \quad F'(x) - \widetilde{F}'(x) = f(x) - \widetilde{f}(x) = 0,$$

(puisque les points où f et $\widetilde{f}$ diffèrent se trouvent dans s). Ceci prouve que $F - \widetilde{F}$ est constante par morceaux (ou en escalier) ; plus précisément elle est constante sur chaque intervalle $]s_i, s_{i+1}[$. Puisque $F - \widetilde{F}$ est continue, elle est constante sur $]a,b]$, et donc nulle puisque sa limite en a_+ est nulle (toujours le thoérème précédent). En particulier, $F(b) = \widetilde{F}(b)$, soit

$$\int_{[a,b]} f = \int_{[a,b]} \widetilde{f}.$$

□

3.3 Propriétés de l'intégrale d'une fonction c.p.m. sur un segment.

Commençons par la propriété qui faisait défaut pour les intégrales de Darboux d'une fonction bornée.

Proposition 22 (Linéarité de l'intégrale)**.**

Soient f et g dans $\mathcal{CM}([a,b])$ et deux réels λ, μ. On a

$$\int_{[a,b]} (\lambda f + \mu g) = \lambda \int_{[a,b]} f + \mu \int_{[a,b]} g.$$

Remarque. On peut écrire alternativement que l'application $f \mapsto \int_{[a,b]} f$, définie sur l'espace vectoriel des fonctions c.p.m sur $[a,b]$, est une forme linéaire.

Preuve. La fonction f, continue par morceaux sur $[a,b]$, y est Riemann-intégrable, d'après le théorème 20 ce qui signifie que

$$\int_{[a,b]} f = \underline{\int}_{[a,b]} f = \overline{\int}_{[a,b]} f.$$

Ceci est bien sûr vrai pour les fonctions c.p.m. g et $f+g$. D'après le Lemme 16, on a :

$$\underline{\int}_{[a,b]} f + \underline{\int}_{[a,b]} g \leq \underline{\int}_{[a,b]} (f+g) \leq \overline{\int}_{[a,b]} (f+g) \ \leq \overline{\int}_{[a,b]} f + \overline{\int}_{[a,b]} g.$$

Or, aux deux extrémités de l'inégalité, les membres valent tous deux $\int_{[a,b]} f + \int_{[a,b]} g$, quand ceux du milieu valent $\int_{[a,b]}(f+g)$. Ceci montre l'égalité

$$\int_{[a,b]} (f+g) = \int_{[a,b]} f + \int_{[a,b]} g \qquad (1).$$

De plus, dans le Lemme 17, la Riemann-intégrabilité de f et de λf permet de remplacer les intégrales de Darboux supérieures et inférieures par de « vraies » intégrales. On obtient alors

$$\forall \lambda \in \mathbb{R} \qquad \int_{[a,b]} (\lambda f) = \lambda \int_{[a,b]} f \qquad (2).$$

La linéarité cherchée est obtenue en combinant (1) et (2). □

Proposition 23 (Positivité de l'intégrale)**.**

Soit $f \in \mathcal{CM}([a,b])$ une fonction telle que $\forall x \in [a,b], f(x) \geq 0$. Alors,

$$\int_{[a,b]} f \geq 0.$$

Preuve. La fonction f, c.p.m. sur $[a,b]$, y est Riemann-intégrable. On a donc $\int_{[a,b]} f = \underline{\int}_{[a,b]} f$. Il suffit alors d'appliquer l'inégalité de la moyenne pour les intégrales de Darboux inférieures (Prop. 11 avec $m=0$) pour obtenir $\int_{[a,b]} f \geq 0$. □

Proposition 24 (Croissance de l'intégrale).

Soient f et g deux fonctions de $\mathcal{CM}([a,b])$ telle que $\forall x \in [a,b], f(x) \leq g(x)$. Alors,

$$\int_{[a,b]} f \leq \int_{[a,b]} g.$$

Preuve. Sous les hypothèses de la proposition, la différence $g - f$ est une fonction c.p.m. et positive. D'après la proposition 23, on a $\int_{[a,b]}(g-f) \geq 0$. Par linéarité (proposition 22),

$$\int_{[a,b]} g - \int_{[a,b]} f \geq 0. \qquad \square$$

Proposition 25 (Inégalité triangulaire pour les intégrales).

Pour toute fonction $f \in \mathcal{CM}([a,b])$,

$$\left| \int_{[a,b]} f \right| \leq \int_{[a,b]} |f|.$$

Preuve. On a $\forall x \in [a,b],\ f(x) \leq |f(x)|$ et $-f(x) \leq |f(x)|$. D'après la proposition 24

$$\int_{[a,b]} f \leq \int_{[a,b]} |f| \qquad \text{et} \qquad \int_{[a,b]} (-f) \leq \int_{[a,b]} |f|, \text{ i.e. } -\int_{[a,b]} f \leq \int_{[a,b]} |f|.$$

En rappelant que $\forall x \in \mathbb{R}\ |x| = \max(x, -x)$, on obtient bien l'inégalité voulue. $\square$

Proposition 26 (Stricte positivité de l'intégrale).

Soit f une fonction <u>continue</u> sur $[a,b]$ telle que $\forall x \in [a,b]\ f(x) \geq 0$.
Si l'intégrale de f est nulle, alors, f est la fonction nulle sur $[a,b]$, i.e.

$$\int_{[a,b]} f = 0 \quad \Longrightarrow \quad f = 0.$$

Preuve. Montrons la contraposée et supposons que f n'est pas la fonction nulle sur $[a,b]$. Cela signifie qu'il existe dans $[a,b]$ un élément x_0 tel que $f(x_0) > 0$. On peut supposer de plus que $x_0 \in]a,b[$ car si f est nulle sur $]a,b[$, elle l'est aux extrémités par continuité. Posons $\varepsilon = \frac{1}{2} f(x_0)$. La fonction f étant continue en x_0, il existe $\eta > 0$ tel que

$$\forall x \in]x_0 - \eta, x_0 + \eta[\quad |f(x) - f(x_0)| \leq \varepsilon, \text{ i.e. } f(x) \in [\tfrac{1}{2} f(x_0), \tfrac{3}{2} f(x_0)].$$

Comme $x_0 \in]a,b[$, quitte à réduire η, on peut supposer que $]x_0 - \eta, x_0 + \eta[\subset]a,b[$. Posons alors

$$a_0 = a, \quad a_1 = x_0 - \eta \quad , a_2 = x_0 + \eta, \quad a_3 = b \qquad \text{et} \qquad \sigma = (a_0, a_1, a_2, a_3).$$

Sur $[a_1, a_2]$, f est minorée par $\frac{1}{2} f(x_0)$, ce qui amène

$$\int_{[a,b]} f \ \geq\ s_{[a,b]}(f, \sigma) \ \geq\ \frac{1}{2} f(x_0)(a_2 - a_1) = f(x_0)\eta > 0.$$

On a donc que $\int_{[a,b]} f \neq 0$, ce qui achève la preuve de la contraposée. $\square$

36 Intégrales sur un segment

Dans le chapitre précédent, nous avons *construit* l'intégrale de Riemann pour les fonctions continues par morceaux sur un segment $[a, b]$ (avec $a < b$) et à valeurs réelles. Ainsi, lorsque $f \in \mathcal{CM}([a, b], \mathbb{R})$, son intégrale sur $[a, b]$ a été notée

$$\int_{[a,b]} f.$$

Ce chapitre-ci se donne des objectifs plus pratiques. On s'appuie sur les calculs de primitive déjà faits au premier semestre, en cherchant cette fois à mettre en valeur les applications des propriétés théoriques de l'intégrale de Riemann.

Dans la partie 1 de ce cours, nous nous débarrassons de la contrainte sur l'ordre des bornes pour la définition, que nous étendons aux fonctions à valeurs complexes. Nous (re)donnons les **propriétés de l'intégrale** montrées dans le chapitre de construction et appliquons ces propriétés dans une selection d'exercices de cours.

La partie 2 du cours est consacrée au **théorème fondamental de l'analyse**. Une preuve de ce théorème est donnée, même si elle se trouve déjà, en réalité, dans notre construction (et au coeur de celle-ci). Parmi les conséquences du théorème se trouvent la formule de calcul d'une intégrale à l'aide d'une primitive, et celles d'**intégration par parties** et de **changement de variable**, dont on redonne les énoncés.

Les parties 3 et 4 sont consacrées à des nouveautés : la **formule de Taylor avec reste intégral**, et les **sommes de Riemann**. Ces dernières permettent un calcul approché d'une intégrale : c'est la *méthode des rectangles* et c'est l'occasion de parler un peu d'analyse numérique.

1 Intégrale d'une fonction continue par morceaux sur un segment.

1.1 Ensemble $\mathcal{CM}(I, \mathbb{K})$.

Pour une fonction $f : [a, b] \to \mathbb{C}$, la définition de « f est continue par morceaux sur $[a, b]$ » peut être reprise du chapitre précédent, sans modification.

Définition 1 (Fonction c.p.m sur un intervalle)**.**

Soit I un intervalle et $f : I \to \mathbb{K}$. On dit que f est **continue par morceaux** sur I si pour tout segment $[a, b]$ inclus dans I, la restriction $f_{|[a,b]}$ est continue par morceaux sur $[a, b]$.
On note $\mathcal{CM}(I, \mathbb{K})$ l'ensemble des fonctions continues par morceaux sur I.

On se convaincra que $\mathcal{CM}(I, \mathbb{K})$ est un sous-espace vectoriel de $(\mathcal{F}(I, \mathbb{K}), +, \cdot)$ et un sous-anneau de $(\mathcal{F}(I, \mathbb{K}), +, \times)$.
Il est clair que $\mathcal{C}(I, \mathbb{K}) \subset \mathcal{CM}(I, \mathbb{K})$.

Exemple 2.

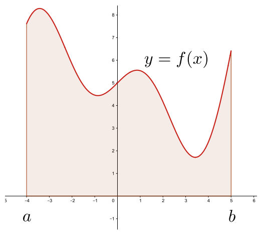
La fonction $x \mapsto \lfloor \frac{1}{x} \rfloor$ est continue par morceaux sur $\mathbb{R}_+^*$. Expliquer.

1.2 Intégrale d'une fonction continue par morceaux entre deux bornes.

Dans le chapitre de construction, nous avons démontré que les fonctions continues par morceaux sur un segment (et à valeurs réelles) y sont intégrables au sens de Riemann. Plus concrètement, si $f \in \mathcal{CM}([a, b], \mathbb{R})$ (où $a < b$), on a donné un sens au nombre

$$\int_{[a,b]} f.$$

Lorsque f prend des valeurs positives, on a interprété le nombre ci-dessus comme *l'aire sous la courbe* de f :



Un cas particulier : si f est constante égale à C sur $[a, b]$, nous avons vu que $\displaystyle\int_{[a,b]} f = C(b - a)$.

Définition 3.

Soit $f \in \mathcal{CM}(I, \mathbb{R})$ et $a, b \in I$. On note $\int_a^b f(x)\mathrm{d}x$, ou plus simplement $\int_a^b f$ le nombre réel défini par

$$\int_a^b f(x)\mathrm{d}x := \int_{[a,b]} f \text{ si } a < b, \qquad \int_a^a f(x)\mathrm{d}x := 0, \quad \text{et} \quad \int_a^b f(x)\mathrm{d}x := -\int_{[b,a]} f \text{ si } a > b.$$

Proposition-Définition 4.

Soit $f \in \mathcal{CM}(I, \mathbb{C})$.
Les fonctions $x \mapsto \mathrm{Re}(f(x))$ et $x \mapsto \mathrm{Im}(f(x))$ sont continues par morceaux sur I.
Pour $a, b \in I$, on pose

$$\int_a^b f(x)\mathrm{d}x := \int_a^b \mathrm{Re}\,(f(x))\,\mathrm{d}x + i \int_a^b \mathrm{Im}\,(f(x))\,\mathrm{d}x.$$

Ainsi, la partie réelle de l'intégrale est l'intégrale de la partie réelle, idem pour la partie imaginaire.

Preuve. Pour prouver la continuité par morceaux de $\mathrm{Re}(f)$ et $\mathrm{Im}(f)$ à partir de celle de f, on introduit une subdivision adaptée à f $\sigma = (a_0, \dots, a_n)$ et on prouve qu'elle est adaptée à sa partie réelle et à sa partie imaginaire. On peut utiliser pour cela les relations

$$\forall x \in I \quad \mathrm{Re}(f(x)) = \frac{1}{2}\left(f(x) + \overline{f(x)}\right) \qquad \text{et} \qquad \mathrm{Im}(f(x)) = \frac{1}{2i}\left(f(x) - \overline{f(x)}\right).$$

En effet, ces relations donnent que pour un i fixé dans $[\![0, n-1]\!]$, les restrictions de $\mathrm{Re}(f)$ et $\mathrm{Im}(f)$ à $]a_i, a_{i+1}[$ y sont continues, et prolongeables par continuité sur les bords. $\square$

1.3 Relation de Chasles.

Proposition 5 (Relation de Chasles)**.**

Soient $f \in \mathcal{CM}(I, \mathbb{K})$, et $(a, b, c) \in I^3$.

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

Preuve. La relation a été établie dans le cours de construction pour une fonction à valeurs réelles dans le cas où $a < c < b$. On laisse au lecteur le soin de prouver que la relation demeure vraie pour une fonction à valeur complexes, et surtout qu'elle est vraie quel que soit l'ordre sur a, b, c en utilisant la définition 3. $\square$

1.4 Linéarité.

Proposition 6 (Linéarité de l'intégrale)**.**

Soient $f, g \in \mathcal{CM}(I, \mathbb{K})$, et $(a, b) \in I^2$. Pour tous scalaires $\lambda, \mu \in \mathbb{K}$,

$$\int_a^b (\lambda f + \mu g) = \lambda \int_a^b f + \mu \int_a^b g.$$

Preuve. La relation a été établie dans le cours de construction pour une fonction à valeurs réelles et des scalaires réels. On laisse au lecteur le soin de prouver que la relation demeure vraie pour une fonction à valeur complexes, en utilisant la définition 4. $\square$

1.5 Intégrales et inégalités.

Évidemment, puisque nous parlons ici d'inégalités, les fonctions considérées seront seulement à valeurs **réelles**, sauf pour l'inégalité triangulaire. Nous soulignons aussi que les propriétés qui suivent réclament toujours que les intégrales examinées soient écrites avec des bornes « bien rangées ». Cette hypothèse essentielle a été encadrée à chaque fois.

Proposition 7 (Positivité)**.**

Soit $f \in \mathcal{CM}([a,b],\mathbb{R})$ où le segment $[a,b]$ est tel que $\boxed{a \leq b}$.

Si f est positive sur $[a,b]$, alors l'intégrale $\displaystyle\int_a^b f(x)\mathrm{d}x$ est un nombre positif.
Si f est négative sur $[a,b]$, cette intégrale est un nombre négatif.

Proposition 8 (Intégrale nulle d'une fonction positive et continue)**.**

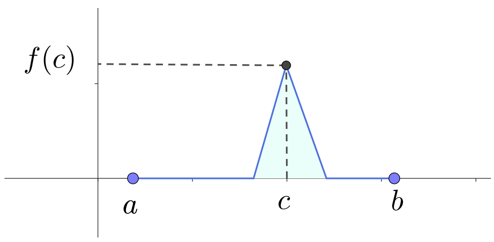
Soit $f : [a,b] \to \mathbb{R}$, avec $\boxed{a < b}$.

$$\text{Si } \left\{ \begin{array}{c} f \text{ est } \underline{\text{continue}} \text{ sur}[a,b] \\ f \text{ est } \underline{\text{positive}} \text{ sur}[a,b] \\ \displaystyle\int_a^b f(x)\mathrm{d}x = 0 \end{array} \right\} \quad \text{alors } f \text{ est nulle sur } [a,b].$$

On a aussi par contraposée la propriété de *stricte positivité de l'intégrale*

$$\text{Si } \left\{ \begin{array}{c} f \text{ est } \underline{\text{continue}} \text{ sur}[a,b] \\ f \text{ est } \underline{\text{positive}} \text{ sur}[a,b] \\ \exists c \in [a,b] \ f(c) > 0 \end{array} \right\} \quad \text{alors } \int_a^b f(x)\mathrm{d}x > 0.$$

Remarque. Dans la première implication, *positive* peut être remplacé par *de signe constant.*



Proposition 9 (Croissance)**.**

Soient $f, g \in \mathcal{CM}([a,b],\mathbb{R})$, avec $\boxed{a \leq b}$.

$$f \leq g \quad \Longrightarrow \quad \int_a^b f(x)\mathrm{d}x \leq \int_a^b g(x)\mathrm{d}x.$$

Proposition 10 (Inégalité de la moyenne)**.**

Soit $f \in \mathcal{CM}([a,b],\mathbb{R})$, avec $\boxed{a \leq b}$.

Si f est minorée par un réel m et majorée par un réel M sur $[a,b]$, alors,

$$m(b-a) \leq \int_a^b f(x)\mathrm{d}x \leq M(b-a), \quad \text{Lorsque } a<b, \text{ on a } \ m \leq \tfrac{1}{b-a}\int_a^b f(x)\mathrm{d}x \leq M.$$

Notamment, si f est constante, égale à C sur $[a,b]$, $\displaystyle\int_a^b f(x)\mathrm{d}x = C(b-a)$.

Remarque. Lorsque $a<b$, le nombre $\displaystyle\frac{1}{b-a}\int_a^b f(x)\mathrm{d}x$ représente la *valeur moyenne* prise par f sur $[a,b]$.

Proposition 11 (Inégalité triangulaire)**.**

Soit $f \in \mathcal{CM}([a,b],\mathbb{K})$, avec $\boxed{a \leq b}$.

$$\left|\int_a^b f(x)\mathrm{d}x\right| \leq \int_a^b |f(x)|\mathrm{d}x.$$

Preuve.
L'inégalité se prouve facilement pour une fonction f continue par morceaux et à valeurs <u>réelles</u> sur $[a,b]$: pour une telle fonction f, les fonctions $|f|-f$ et $|f|+f$ sont c.p.m et positives sur $[a,b]$. Par positivité, $\int_a^b (|f|-f) \geq 0$ et $\int_a^b (|f|+f) \geq 0$. Par linéarité, on obtient

$$\int_a^b f \leq \int_a^b |f| \quad \text{et} \quad -\int_a^b f \leq \int_a^b |f|.$$

Le passage au maximum donne l'inégalité voulue.

Pour une preuve dans le cas complexe, il faut un peu ruser. Considérons $f \in \mathcal{CM}([a,b],\mathbb{C})$. Écrivons l'intégrale de f sous forme exponentielle :

$$\exists \theta \in \mathbb{R} \quad \int_a^b f(t)\mathrm{d}t = re^{i\theta}, \quad \text{avec } \ r = \left|\int_a^b f(t)\mathrm{d}t\right|.$$

Isolons r :

$$r = e^{-i\theta}\int_a^b f(t)\mathrm{d}t = \int_a^b e^{-i\theta} f(t)\mathrm{d}t.$$

La fonction $t \mapsto e^{-i\theta}f(t)$ n'a aucune raison d'être à valeurs réelles mais r, lui, l'est donc

$$r = \mathrm{Re}(r) = \mathrm{Re}\left[e^{-i\theta}\int_a^b f(t)\mathrm{d}t\right] = \int_a^b \mathrm{Re}\left(e^{-i\theta}f(t)\right)\mathrm{d}t \leq \int_a^b \left|\mathrm{Re}\left(e^{-i\theta}f(t)\right)\right|\mathrm{d}t \leq \int_a^b |f(t)|\mathrm{d}t,$$

où on a utilisée l'inégalité $\mathrm{Re}(z) \leq |\mathrm{Re}(z)| \leq |z|$ vraie pour tout nombre complexe z, ainsi que la croissance de l'intégrale. On a bien obtenu

$$\left|\int_a^b f(t)\mathrm{d}t\right| \leq \int_a^b |f(t)|\mathrm{d}t.$$

□

2 Intégration et dérivation.

2.1 Théorème fondamental de l'analyse.

Théorème 12 (Théorème fondamental de l'analyse)**.**

Soit I un intervalle et $f : I \to \mathbb{K}$ une fonction continue sur I. Soit $a \in I$. La fonction

$$F : \begin{cases} I & \to & \mathbb{K} \\ x & \mapsto & F(x) = \int_a^x f(t)\mathrm{d}t \end{cases}$$

est de classe $\mathcal{C}^1$ sur I et de dérivée $F' = f$.

Corollaire 13.

Toute fonction continue sur un intervalle y admet des primitives.
Sur un intervalle, deux primitives d'une même fonction diffèrent d'une constante.

Une conséquence : la primitive donnée par le TFA est l'*unique* primitive de f sur I qui s'annule en a.

Proposition 14.

Soit $f \in \mathcal{C}(I, \mathbb{K})$ et F une primitive de f sur I. Alors, pour tous $a, b \in I$,

$$\int_a^b f(t)\mathrm{d}t = F(b) - F(a).$$

Proposition 15.

Soit $f \in \mathcal{C}^1(I, \mathbb{K})$. Alors, pour tous $a, b \in I$,

$$\int_a^b f'(t)\mathrm{d}t = f(b) - f(a).$$

2.2 Outils de calcul intégral.

Théorème 16 (Formule d'intégration par parties)**.**

Soient $u, v \in \mathcal{C}^1(I, \mathbb{K})$ et $a, b \in I$. Alors,

$$\int_a^b u'(t)v(t)\mathrm{d}t = [uv]_a^b - \int_a^b u(t)v'(t)\mathrm{d}t.$$

Méthode (Suites dont le terme général est une intégrale).

Soit $(f_n)_{n\in\mathbb{N}}$ une suite de fonctions continues sur $[a,b]$ et la suite numérique $(I_n)_{n\in\mathbb{N}}$ définie par

$$\forall n \in \mathbb{N} \quad I_n := \int_a^b f_n(x)\mathrm{d}x.$$

Expliciter directement le nombre I_n à l'aide d'un calcul de primitive n'est parfois pas possible mais dans certains cas, une IPP permettra d'obtenir une **relation de récurrence** sur la suite (I_n).

Exemple à connaître : la suite des intégrales de Wallis.

Théorème 17 (Formule de changement de variable).

Soit $\varphi \in \mathcal{C}^1(I,J)$, $f \in \mathcal{C}(J,\mathbb{K})$ et $(a,b) \in I^2$. On a

$$\int_{\varphi(a)}^{\varphi(b)} f(x)\mathrm{d}x = \int_a^b f(\varphi(t))\,\varphi'(t)\mathrm{d}t.$$

Le moyen mnémotechnique pour se souvenir de la formule : on pose $x = \varphi(t)$ et on écrit « $\mathrm{d}x = \varphi'(t)\mathrm{d}t$ ».

Corollaire 18 (Intégrale d'une fonction paire, d'une fonction impaire).

Soit $f \in \mathcal{CM}([-a,a],\mathbb{K})$.

$$\text{Si } f \text{ est paire, } \int_{-a}^{a} f(t)\mathrm{d}t = 2\int_0^a f(t)\mathrm{d}t. \qquad \text{Si } f \text{ est impaire, } \int_{-a}^{a} f(t)\mathrm{d}t = 0.$$

Preuve. La preuve avait été écrite en début d'année pour une fonction continue et l'idée reste la même : le changement de variable $x = -t$. Considérons une subdivision σ de $[-a,a]$ et créons à partir de σ une nouvelle subdivision de ce segment cette fois *symétrique* par rapport à 0. Il suffit pour cela d'y mettre 0, tous les points de σ, et tous lesurs opposés. On obtient

$$\sigma' = (-b_p, \dots, -b_1, b_0, b_1, \dots, b_p), \quad \text{avec } b_0 = 0.$$

On a alors

$$\int_0^a f(t)\mathrm{d}t = \sum_{i=0}^{p-1} \int_{b_i}^{b_{i+1}} f(t)\mathrm{d}t = \sum_{i=0}^{p-1} \int_{b_i}^{b_{i+1}} \widetilde{f}_i(t)\mathrm{d}t,$$

où pour i fixé $\widetilde{f}_i$ désigne la restriction de f à $]b_i, b_{i+1}[$, prolongée par continuité (de sorte que $f_{|[b_i,b_{i+1}]}$) et $\widetilde{f}_i$ ne diffèrent qu'en b_i et en b_{i+1} éventuellement. Pour $i \in [\![0, p-1]\!]$, on obtient par changement de variable $t = -x$,

$$\int_{b_i}^{b_{i+1}} \widetilde{f}_i(t)\mathrm{d}t = -\int_{-b_i}^{-b_{i+1}} \widetilde{f}_i(-x)\mathrm{d}x = \int_{-b_{i+1}}^{-b_i} \widetilde{f}_i(-x)\mathrm{d}x.$$

En sommant, on obtient

$$\int_0^a f(t)\mathrm{d}t = \sum_{i=0}^{p-1} \int_{b_i}^{b_{i+1}} \widetilde{f}_i(t)\mathrm{d}t = \sum_{i=0}^{p-1} \int_{-b_{i+1}}^{-b_i} \widetilde{f}_i(-x)\mathrm{d}x = \int_{-b_p}^{b_0} f(-x)\mathrm{d}x = \int_{-a}^{0} f(-t)\mathrm{d}t.$$

On obtient bien que
- si f est paire, alors $\int_0^a f(t)\mathrm{d}t = \int_{-a}^0 f(t)\mathrm{d}t$;
- si f est impaire, $\int_0^a f(t)\mathrm{d}t = \int_{-a}^0 (-1)f(t)\mathrm{d}t = -\int_{-a}^0 f(t)\mathrm{d}t$.

□

Corollaire 19.

Soit $f \in \mathcal{CM}(\mathbb{R}, \mathbb{K})$, une fonction T périodique, où T est un réel strictement positif.

$$\forall a \in \mathbb{R} \quad \int_a^{a+T} f(t)\mathrm{d}t = \int_0^T f(t)\mathrm{d}t.$$

Preuve. On laisse au lecteur le soin d'adapter la preuve donnée en début d'année pour une fonction continue, et ceci en utilisant la même idée : prouver que

$$\varphi : a \mapsto \int_a^{a+T} f(t)\mathrm{d}t$$

est constante en la dérivant. Cette fois, la fonction φ n'est plus dérivable sur $\mathbb{R}$ tout entier mais seulement en tout point où f est continue... □

2.3 Quelques exercices de cours.

Exemple 20.

Pour $a \in \mathbb{R}_+^*$, on pose $I_a = \displaystyle\int_a^{a^2} \ln^3(x)\mathrm{d}x$. Existence et signe de I_a.

Exemple 21 (La fonction s'annule)**.**

Soit $f : [a, b] \to \mathbb{R}$ une fonction continue telle que $\displaystyle\int_a^b f(t)\mathrm{d}t = 0$.
Justifier que f s'annule au moins une fois sur $[a, b]$:
1. Solution 1 : en utilisant la stricte positivité de l'intégrale ;
2. Solution 2 : en utilisant le théorème fondamental de l'analyse.

Exemple 22 (Un exercice : suite définie par une intégrale)**.**

Soit, pour $n \in \mathbb{N}$, $I_n := \displaystyle\int_1^e (\ln(x))^n \,\mathrm{d}x$.
1. Prouver que (I_n) est convergente.
2. Prouver que la limite vaut 0.
3. Donner un équivalent de I_n.

Exemple 23 (Lemme de Riemann-Lebesgue, sous l'hypothèse $\mathcal{C}^1$).

Soit $f \in \mathcal{C}^1([a,b],\mathbb{C})$. Montrer que

$$\int_a^b f(t)e^{int}\mathrm{d}t \underset{n\to+\infty}{\longrightarrow} 0.$$

Exemple 24.

Soit la fonction

$$F : x \mapsto \int_x^{x^2} \frac{1}{\ln(t)}\mathrm{d}t.$$

1. Donner le domaine de définition de F.
2. Montrer que F est dérivable sur D et calculer sa dérivée. Donner les variations de f.
3. (*) Calculer les limites intéressantes.

Exemple 25 (Un changement de variable).

Démontrer que $\displaystyle\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \frac{\mathrm{d}x}{4+\sin x} = \frac{\pi}{\sqrt{15}}$ en posant le changement de variable $t = \tan\frac{x}{2}$.

3 Formule de Taylor avec reste intégral.

Théorème 26 (Formule de Taylor avec reste intégral).

Soit I un intervalle et $a \in I$. Soit $n \in \mathbb{N}$ et $f \in \mathcal{C}^{n+1}(I,\mathbb{K})$. Alors, pour tout $x \in I$,

$$f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k + \int_a^x \frac{(x-t)^n}{n!} f^{(n+1)}(t)\mathrm{d}t.$$

- Dans le second membre de l'égalité ci-dessus, la première moitié est la fonction polynomiale
$$x \mapsto \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k,$$
parfois appelée polynôme de Taylor à l'ordre n de f. On l'a déjà vu apparaître dans la formule de Taylor-Young : c'est la partie régulière du DL en a à l'ordre n. Pour les fonctions usuelles, et $a = 0$, on connait ses coefficients, car on connait nos développements limités sur le bout des doigts...

- La seconde moitié
$$\int_a^x \frac{(x-t)^n}{n!} f^{(n+1)}(t)\mathrm{d}t,$$
est appelée **reste intégral** à l'ordre n. C'est une expression semi-explicite de l'erreur d'approximation d'une fonction par son polynôme de Taylor à l'ordre n.

Exemple 27 (Comparer une fonction et son polynôme de Taylor).

Montrer l'inégalité :

$$\forall x \in \left[0, \frac{\pi}{2}\right] \qquad \cos x \geq 1 - \frac{x^2}{2!}.$$

Un corollaire : l'inégalité ci-dessous, qui généralise l'inégalité des accroissements finis.

Proposition 28 (Inégalité de Taylor Lagrange).

Soit I un intervalle, $a \in I$, $n \in \mathbb{N}$ et $f \in \mathcal{C}^{n+1}(I, \mathbb{K})$.
On suppose que la fonction $|f^{(n+1)}|$ est majorée par une constante M_{n+1} sur I. Alors,

$$\forall x \in I \qquad \left| f(x) - f(a) - \sum_{k=1}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k \right| \leq M_{n+1} \frac{(x-a)^{n+1}}{(n+1)!}.$$

Exemple 29 (Une fonction qui est somme de sa série de Taylor).

Prouver que

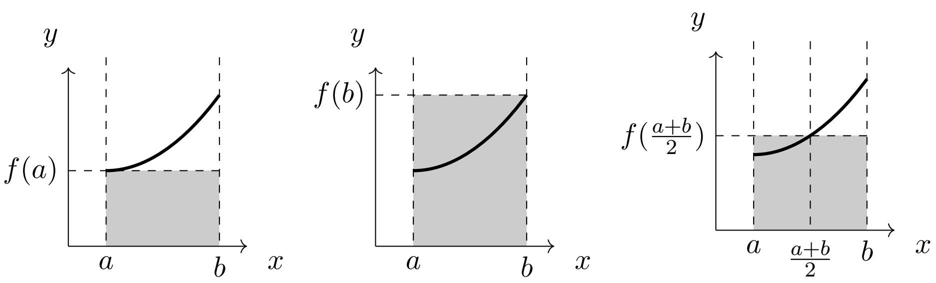
$$\forall x \in [0, 1] \qquad \lim_{n \to +\infty} \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k} x^k = \ln(1+x).$$

4 Sommes de Riemann.

Dans cette partie du cours, les théorèmes sont établis pour des fonctions c.p.m. à valeurs complexes. Dès que l'on interprète les choses en termes d'« aire sous la courbe », ou d'« aire de rectangle », il faudra considérer que la fonction dont on parle à ce moment là est à valeurs *réelles positives*.

4.1 Convergence des sommes de Riemann.

Une première approximation du nombre $\int_a^b f(x)\mathrm{d}x$ est celle donnée par l'aire d'un rectangle de base $b-a$ et de hauteur $f(c)$ où c est un point de $[a, b]$. On fait donc l'approximation $\int_a^b f(x)\mathrm{d}x \approx (b-a)f(c)$.
Trois choix naturels pour le point c : $c = a$ ("rectangle à gauche"), $c = b$ (à droite), $c = \frac{a+b}{2}$ (point milieu).



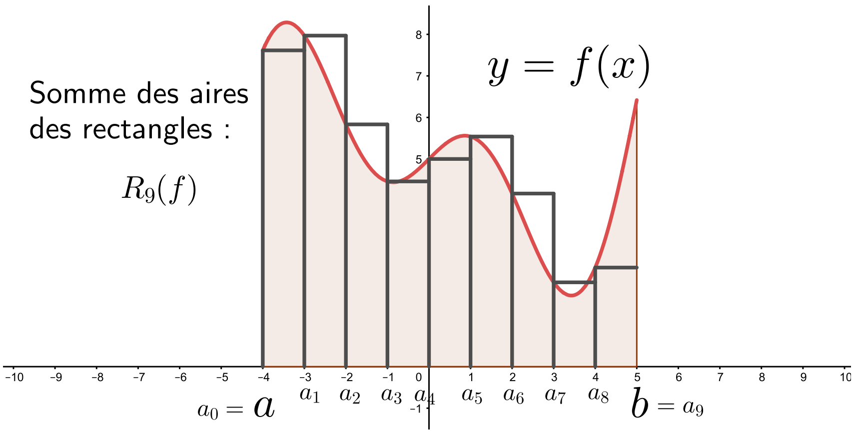
Définition 30.

Soit un segment $[a, b]$ avec $a < b$. Pour $n \in \mathbb{N}^*$ et $k \in [\![0, n]\!]$, on note $a_k = a + k\frac{b-a}{n}$.

La famille $(a_0, \ldots, a_n)$ est appelée **subdivision régulière** de $[a, b]$ à n segments. Chaque segment de la subdivision est de longueur $\frac{b-a}{n}$, et ce nombre est appelé **pas** de la subdivision.

Soit $f \in \mathcal{CM}([a, b], \mathbb{K})$. On appelle $n$ème **somme de Riemann** de f le nombre

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



Théorème 31 (Convergence des sommes de Riemann)**.**

Soit $f \in \mathcal{CM}([a, b], \mathbb{K})$.

Pour $n \in \mathbb{N}^*$ et $k \in [\![0, n]\!]$, on note $a_k = a + k\frac{b-a}{n}$ et $R_n(f) = \frac{b-a}{n} \sum\limits_{k=0}^{n-1} f(a_k)$. Alors,

$$R_n(f) \underset{n\to+\infty}{\longrightarrow} \int_a^b f(t)\mathrm{d}t.$$

Remarques.

- Ajouter ou retrancher un nombre fini de rectangles ne change rien puisque, lorsque le pas de la subdivision tend vers 0, la contribution du rectangle en question aussi. Par exemple,

$$\frac{b-a}{n} \sum_{k=1}^{n} f\left(a + k\frac{b-a}{n}\right) = R_n(f) + \frac{b-a}{n}(f(b) - f(a)) \underset{n\to+\infty}{\longrightarrow} \int_a^b f(t)\mathrm{d}t \;+\; 0.$$

- Le programme officiel n'exige la preuve du résultat que dans le cas d'une fonction f lipschitzienne sur $[a, b]$. Nous écrivons cette preuve, qui démontre la proposition 35. L'hypothèse lipschitz permet de préciser la vitesse de convergence de la "méthode des rectangles".
- Nous prouvons aussi le résultat sous l'hypothèse que f est continue, c'est l'occasion d'utiliser la notion de *continuité uniforme*.

Corollaire 32 (Cas particulier important : $a = 0$ et $b = 1$)**.**

Soit $f \in \mathcal{CM}([0,1], \mathbb{K})$.

$$\frac{1}{n}\sum_{k=0}^{n-1} f\left(\frac{k}{n}\right) \underset{n\to+\infty}{\longrightarrow} \int_0^1 f(t)\mathrm{d}t.$$

Exemple 33 (Calculer)**.**

$$\lim \frac{1}{n}\sum_{k=1}^{n} \frac{\sqrt{k}}{\sqrt{n}}; \qquad \text{et} \qquad \lim \sum_{k=0}^{n-1} \frac{1}{n+k}.$$

Exemple 34 (Inégalité de Jensen pour les intégrales)**.**

Soit $f : [a,b] \to \mathbb{R}$ une fonction continue par morceaux à valeurs dans un intervalle I et φ une fonction convexe *et continue* sur I. Démontrer l'inégalité de Jensen pour les intégrales :

$$\varphi\left(\frac{1}{b-a}\int_a^b f(t)\mathrm{d}t\right) \leq \frac{1}{b-a}\int_a^b \varphi\left(f(t)\right)\mathrm{d}t.$$

4.2 Comparaison de la méthode des rectangles avec celle des trapèzes.

On rappelle que si M est un réel positif et $f : I \to \mathbb{K}$ est une fonction définie sur un intervalle I, on dit que f est M-lispschitzienne sur I, si

$$\forall (x,y) \in I \quad |f(x) - f(y)| \leq M|x-y|$$

Cette hypothèse est plus forte que la continuité de f (l'une implique l'autre).

Proposition 35 (Erreur d'approximation avec la méthode des rectangles)**.**

Soit $f : [a,b] \to \mathbb{K}$ une fonction M-lipschitzienne, (avec $M \in \mathbb{R}_+^*$).

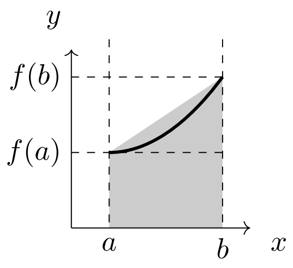
Notons $R_n(f) = \frac{b-a}{n}\sum\limits_{k=0}^{n-1} f\left(a + k\frac{b-a}{n}\right)$, ceci pour tout $n \in \mathbb{N}^*$.

Ce nombre est une valeur approchée de l'intégrale $\int_a^b f(x)\mathrm{d}x$.

$$\text{Voici une majoration de l'erreur d'approximation} \quad \left|R_n(f) - \int_a^b f(t)\mathrm{d}t\right| \leq \frac{M(b-a)^2}{2n}.$$

$$\text{On a donc } \left|R_n(f) - \int_a^b f(t)\mathrm{d}t\right| = O\left(\frac{1}{n}\right).$$

Peut-on faire mieux qu'une erreur d'approximation en $O(\frac{1}{n})$? La réponse est <u>oui</u> : en remplaçant le **rectangle** par un **trapèze** dans l'approximation élémentaire.



$$\int_a^b f(x)\mathrm{d}x \;\approx\; \frac{1}{2}(b-a)\left(f(a)+f(b)\right).$$

On peut préciser la qualité de l'approximation ci-dessus : si f est de classe $\mathcal{C}^2$, on a

$$(*)\qquad \left|\int_a^b f(x)\mathrm{d}x \;-\; \frac{1}{2}(b-a)\left(f(a)+f(b)\right)\right| \leq \frac{(b-a)^3}{12}M_2 \quad \text{où} \quad M_2=\sup_{t\in[a,b]}|f''(t)|.$$

On propose ci-dessous une preuve à l'aide d'une double intégration par parties. Signalons qu'une autre démarche souvent rencontrée repose sur des arguments de type Rolle. On a (première IPP)

$$\int_a^b f(x)\mathrm{d}x = \Big[(x-\tfrac{a+b}{2})f(x)\Big]_a^b - \int_a^b (x-\tfrac{a+b}{2})f'(x)\mathrm{d}x = \frac{b-a}{2}(f(a)+f(b)) - \int_a^b (x-\tfrac{a+b}{2})f'(x)\mathrm{d}x.$$

Pour la seconde IPP, nous dérivons f' et primitivons la fonction affine en $g : x \mapsto \frac{1}{2}(x-\frac{a+b}{2})+C$, où C est une constante choisie de sorte que notre trinôme g s'annule en a et en b. C'est possible car l'axe de symétrie de la parabole est la médiatrice de $[a,b]$! La valeur de C (poser l'équation) est $-\frac{(b-a)^2}{8}$. Ceci procure un crochet nul et amène

$$\int_a^b f(x)\mathrm{d}x - \frac{1}{2}(b-a)\left(f(a)+f(b)\right) = 0 + \int_a^b g(t)f''(x)\mathrm{d}x$$

L'inégalité triangulaire amène

$$\left|\int_a^b f(x)\mathrm{d}x \;-\; \frac{1}{2}(b-a)\left(f(a)+f(b)\right)\right| \leq \int_a^b |g(x)|\cdot|f''(x)|\mathrm{d}x \leq M_2\int_a^b |g(x)|\mathrm{d}x$$

Reste à calculer

$$\begin{aligned}
\int_a^b |g(x)|\mathrm{d}x &= \int_a^b \left|\frac{1}{2}(x-\tfrac{a+b}{2})^2 - \frac{(b-a)^2}{8}\right|\mathrm{d}x \\
&= \int_{-\frac{b-a}{2}}^{\frac{b-a}{2}} \left|\frac{1}{2}u^2 - \frac{(b-a)^2}{8}\right|\mathrm{d}u \qquad \left(u = x-\tfrac{a+b}{2};\ \mathrm{d}u=\mathrm{d}x\right) \\
&= \int_{-1}^{1} \frac{(b-a)^2}{8}|v^2-1|\frac{b-a}{2}\mathrm{d}v \qquad \left(v=\frac{2}{b-a}u;\ \mathrm{d}v = \frac{2}{b-a}\mathrm{d}u\right) \\
&= \frac{(b-a)^3}{16}\int_{-1}^{1}(1-u^2)\mathrm{d}u
\end{aligned}$$

L'essentiel pour la suite est là : c'est le $(b-a)^3$. Il reste à calculer l'intégrale qui vaut $\frac{4}{3}$.
On obtient bien une intégrale égale à $\frac{(b-a)^3}{12}$, ce qui achève de prouver $(*)$.

Passons maintenant au découpage. Notons toujours $a_k = a + k\frac{b-a}{n}$, et sommons, pour définir $T_n(f)$, la somme des aires des n trapèzes associés à la subdivision régulière $(a_k)_{0\leq k\leq n}$.

$$T_n(f) = \sum_{k=0}^{n-1} \frac{1}{2}\frac{b-a}{n}\left(f(a_k)+f(a_{k+1})\right)$$

Proposition 36 (Erreur d'approximation avec la méthode des trapèzes)**.**

Soit $f \in \mathcal{C}^2([a,b],\mathbb{K})$. Pour $n \in \mathbb{N}^*$, on définit $T_n(f)$ comme ci-dessus. On a

$$\left| T_n(f) - \int_a^b f(t)\mathrm{d}t \right| = O\left(\frac{1}{n^2}\right).$$

Preuve.

Comme dans la preuve de la proposition 35, on obtient, grâce à la relation de Chasles, que

$$\left| \int_a^b f(t)\mathrm{d}t - T_n(f) \right| \leq \sum_{k=0}^{n-1} \left| \int_{a_k}^{a_{k+1}} f(t)\mathrm{d}t - \frac{1}{2}\frac{b-a}{n}\left(f(a_k)+f(a_{k+1})\right) \right|.$$

Or, en utilisant l'inégalité (*) énoncée plus haut entre a_k et a_{k+1}, puis en sommant, on a

$$\left| \int_a^b f(t)\mathrm{d}t - T_n(f) \right| \leq \sum_{k=0}^{n-1} \frac{(a_{k+1}-a_k)^3}{12} \cdot M_2 = \frac{M_2(b-a)^3}{12} \times \frac{1}{n^3} \times \qquad \square$$

L'approximation par les trapèzes est donc meilleure. Le calcul de $R_n(f)$ et de $T_n(f)$ « coûte » la même chose : $O(n)$ opérations mais la deuxième suite converge plus vite vers l'intégrale. Terminons en remarquant qu'il existe une relation simple entre les deux quantités :

$$T_n(f) = \sum_{k=0}^{n-1} \frac{1}{2}\frac{b-a}{n}\left(f(a_k)+f(a_{k+1})\right) = \frac{1}{2}\frac{b-a}{n}\sum_{k=0}^{n-1} f(a_k) + \frac{1}{2}\frac{b-a}{n}\sum_{k=0}^{n} f(a_k) + \frac{1}{2}\frac{b-a}{n}\left(f(a_n)-f(a_0)\right)$$

On obtient

$$T_n(f) = R_n(f) + \frac{b-a}{n} \cdot \frac{f(b)-f(a)}{2}.$$

Exercices

Propriétés générales des intégrales.

$\boxed{\textbf{36.1}}$ **[♦♦◇]** Trouver toutes les fonctions f de $\mathcal{C}([a,b],\mathbb{R})$ telles que

$$\int_a^b f(t)\mathrm{d}t = (b-a)\max_{t\in[a,b]}|f(t)|.$$

$\boxed{\textbf{36.2}}$ **[♦♦♦]** Soit $f : [0,1] \to \mathbb{R}$ une fonction continue telle que

$$\int_0^1 f(t)\mathrm{d}t = \int_0^1 tf(t)\mathrm{d}t = 0.$$

Justifier que f s'annule au moins deux fois sur $[0,1]$.

$\boxed{\textbf{36.3}}$ **[♦♦♦]** Démontrer que $\lim\limits_{n\to+\infty} \displaystyle\int_0^1 |\sin nx|\mathrm{d}x$ existe et la calculer

---

Suites définies par des intégrales

$\boxed{\textbf{36.4}}$ **[♦◇◇]** Pour $n \in \mathbb{N}$, on pose $I_n = \displaystyle\int_0^1 \frac{x^n}{1+x^n}\mathrm{d}x$. Déterminer $\displaystyle\lim_{n\to+\infty} I_n$ et $\displaystyle\lim_{n\to+\infty} nI_n$.

$\boxed{\textbf{36.5}}$ **[♦◇◇]** Soit (u_n) la suite dont le terme général est défini pour tout entier naturel n par

$$u_n = \int_0^1 \sqrt{1+x^n}\mathrm{d}x.$$

Conjecturer que (u_n) tend vers un nombre réel à préciser. Démontrer votre conjecture.

$\boxed{\textbf{36.6}}$ **[♦♦◇]** Soit (I_n) la suite dont le terme général est défini pour tout entier naturel n par

$$I_n = \int_0^1 x^n \ln(1+x^2)\mathrm{d}x.$$

1. Démontrer que $I_n \to 0$.
2. Calculer un équivalent de I_n.

Intégration par parties et changement de variable.

$\boxed{\textbf{36.7}}$ **[♦◇◇]** Soit f une fonction continue et strictement positive sur $[0,1]$. Calculer

$$\int_0^1 \frac{f(x)}{f(x)+f(1-x)}\mathrm{d}x.$$

$\boxed{\textbf{36.8}}$ **[♦♦◇]**

1. À l'aide d'une décomposition en éléments simples, calculer l'intégrale $I_1 = \displaystyle\int_0^1 \frac{1}{1+x^3}\mathrm{d}x$.
2. Calculer par récurrence l'intégrale $I_n = \displaystyle\int_0^1 \frac{1}{(1+x^3)^n}\mathrm{d}x$.

$\boxed{\textbf{36.9}}$ **[♦♦◇]** Calculer, pour tout entier naturel n le nombre $I_n = \displaystyle\int_0^1 x^n\sqrt{1-x}\mathrm{d}x$.

$\boxed{\textbf{36.10}}$ **[♦♦◇]** Soit $\alpha \in \mathbb{R}\setminus\pi\mathbb{Z}$. En vous aidant du changement de variable $u = \tan\frac{x}{2}$, démontrer que

$$\int_0^{2\pi} \frac{\mathrm{d}x}{1+\cos\alpha\cos x}\mathrm{d}x = \frac{2\pi}{|\sin\alpha|}.$$

Théorème fondamental de l'analyse et applications.

$\boxed{\textbf{36.11}}$ **[♦♦◇]** Soit f une fonction continue sur $\mathbb{R}$ et $g : x \mapsto f(x)\int_0^x f(t)\mathrm{d}t$.
Montrer que si g est décroissante sur $\mathbb{R}$, alors f est la fonction nulle.

$\boxed{\textbf{36.12}}$ **[♦♦♦]** Déterminer les fonctions continues sur $\mathbb{R}$ vérifiant

$$\forall\, x\in\mathbb{R}, \qquad f(2x) = 1 + \int_0^x (x-t)f(2t)\,dt$$

$\boxed{\textbf{36.13}}$ **[♦♦◇]** Soit $f \in \mathcal{C}^1(\mathbb{R}_+,\mathbb{R}_+)$. On suppose $f(0)=0$ et que f est strictement croissante sur $\mathbb{R}_+$ (f est donc une bijection de $\mathbb{R}_+$ dans $f(\mathbb{R}_+)$).

1. Montrer que pour tout $x \geq 0$, on a $\displaystyle\int_0^x f(t)\,dt + \int_0^{f(x)} f^{-1}(t)\,dt = x\,f(x)$
2. Montrer que pour tout $a\in\mathbb{R}_+$ et $b \in f(\mathbb{R}_+)$, on a $\displaystyle\int_0^a f(t)\,dt + \int_0^b f^{-1}(t)\,dt \geq ab$

Formule de Taylor avec reste intégral.

$\boxed{\textbf{36.14}}$ **[♦♦◇]** Soit $f \in \mathcal{C}^1([a,b],\mathbb{R})$. On suppose que $f(a)=0$.

1. Montrer que
$$\left|\int_a^b f(t)\mathrm{d}t\right| \leq \frac{(b-a)^2}{2} \times \sup_{t\in[a,b]} |f'(t)|$$
2. Étudier le cas d'égalité.

$\boxed{\textbf{36.15}}$ **[♦♦♦]** [Inégalité de Kolmogorov]
Soit f de classe $\mathcal{C}^2$ sur $\mathbb{R}$ et à valeurs dans $\mathbb{R}$ telle que f et f'' sont bornées.
On note $M_0 = \sup_{x\in\mathbb{R}}|f(x)|$ et $M_2 = \sup_{x\in\mathbb{R}}|f''(x)|$.
Nous allons prouver que f' est bornée et majorer $x \mapsto |f(x)|$.

1. Soient $a \in \mathbb{R}$ et $h > 0$. Montrer que
$$\left|f(a+h) - f(a-h) - 2hf'(a)\right| \leq M_2 h^2.$$
puis que $|f'(a)| \leq \frac{1}{h}M_0 + \frac{h}{2}M_2$.
2. Justifier l'existence de $M_1 = \sup_{x\in\mathbb{R}}|f'(x)|$. Montrer que $M_1 \leq \sqrt{2M_0M_2}$.

Sommes de Riemann.

$\boxed{\textbf{36.16}}$ **[♦◇◇]** Montrer la convergence des suites u, v, w dont le terme général est donné ci-dessous, en précisant la limite :
$$u_n = \sum_{k=0}^{n-1} \frac{n}{n^2+k^2}, \qquad v_n \frac{1}{n\sqrt{n}} \sum_{k=1}^{n} \lfloor\sqrt{k}\rfloor, \qquad w_n = \prod_{k=0}^{n-1}\left(1+\frac{k^2}{n^2}\right)^{1/n}.$$

$\boxed{\textbf{36.17}}$ **[♦♦◇]** Prouver l'existence du nombre suivant et le calculer :
$$\lim_{n\to+\infty} \frac{1}{n}\left(\frac{(2n)!}{n!}\right)^{1/n}.$$

$\boxed{\textbf{36.18}}$ **[♦♦♦]** Soit $f \in \mathcal{C}([0,1],\mathbb{R})$. Limite de la suite de terme général $u_n = \prod_{k=1}^{n}\left(1+\frac{1}{n}f(\frac{k}{n})\right)$.

$\boxed{\textbf{36.19}}$ **[♦♦♦]** Pour $n \in \mathbb{N}^*$, on note
$$u_n = \left(2^2 3^3 \cdots n^n\right)^{\frac{1}{n^2}}.$$
Démontrer que $u_n \sim c\sqrt{n}$ où vous expliciterez la constante c.

$\boxed{\textbf{36.20}}$ **[♦♦♦]** Soit $\lambda \in \mathbb{R} \setminus \{1,-1\}$. Justifier que l'intégrale ci-dessous existe et la calculer :
$$I_\lambda = \int_0^\pi \ln(1-2\lambda\cos t + \lambda^2)\mathrm{d}t.$$

Dans tout ce chapitre, n sera un entier naturel non nul.

1 Permutations.

Définition 1.

Une bijection de $[\![1, n]\!]$ dans lui même est appelée une **permutation** de $[\![1, n]\!]$.
L'ensemble des permutations de $[\![1, n]\!]$ sera noté S_n.

On peut représenter une permutation $\sigma \in S_n$ à l'aide du tableau

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Exemple 2.

Soient
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \quad \text{et} \quad \sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}.$$
Calculer $\sigma \circ \sigma'$, $\sigma' \circ \sigma$, σ^2 et σ^{-1}.

Proposition 3.

1. $(S_n, \circ)$ est un groupe, appelé **groupe symétrique**.
2. S_n est fini et son cardinal vaut $n!$
3. Ce groupe n'est pas abélien dès que $n \geq 3$.

Notation multiplicative : pour $\sigma, \sigma' \in S_n$, on pourra noter $\sigma\sigma'$ la permutation $\sigma \circ \sigma'$.

Définition 4 (Un peu de vocabulaire sur les permutations)**.**

Soit $\sigma \in S_n$.

1. On dit que x est un **point fixe** de σ si $\sigma(x) = x$.
2. On appelle **support** de σ l'ensemble des éléments de $[\![1, n]\!]$ qui ne sont pas un point fixe. Notation (locale) pour le support de γ : $\text{supp}(\gamma)$.
3. Deux permutations σ et σ' sont dites **conjuguées** s'il existe $\alpha \in S_n$ tel que $\sigma' = \alpha\sigma\alpha^{-1}$.

Proposition 5.

Deux permutations dont les supports sont disjoints commutent.

Preuve. Notons A et A' les supports. On peut faire un dessin patate ici, ça permet de visualiser les trois cas à traiter.

— Le cas où x n'est ni dans A ni dans A' est très simple : x est alors un point fixe pour σ <u>et</u> pour σ', et on a $\sigma\sigma'(x) = x = \sigma'\sigma(x)$.

— Traitons le cas où $x \in A$ et $x \notin A'$. Alors x est fixé par σ'. On a donc $\sigma\sigma'(x) = \sigma(x)$. Pour conclure, il suffit de prouver que $\sigma'(\sigma(x)) = \sigma(x)$, c'est-à-dire que $\sigma(x) \notin A'$. On prouve cela en raisonnant par l'absurde. Supposons que $\sigma(x) \in A'$. Alors $\sigma(x) \notin A$ (hypothèse) puis $\sigma(x)$ est fixe par σ, d'où $\sigma(\sigma(x)) = \sigma(x)$ puis $\sigma(x) = x$ par injectivité de σ. Ceci contredit le fait que x appartient à A.

— Le cas où $x \in A'$ et $x \notin A$ est symétrique du précédent.

$\square$

2 Cycles.

Définition 6.

Soit p un entier supérieur à 2.
Une permutation γ est appelée un p-**cycle** s'il existe p éléments distincts $a_1, \ldots, a_p$ de $[\![1, n]\!]$ tels que

$$a_1 \overset{\gamma}{\mapsto} a_2 \overset{\gamma}{\mapsto} a_3 \cdots \overset{\gamma}{\mapsto} a_p \overset{\gamma}{\mapsto} a_1$$

$$\text{et} \quad \forall b \in [\![1, n]\!] \setminus \{a_1, \cdots, a_p\} \quad \gamma(b) = b.$$

On note alors $\gamma = (a_1\ a_2\ \cdots\ a_p)$. Il est clair que $\text{supp}(\gamma) = \{a_1, \ldots, a_p\}$.

Notation.

Soit $\gamma = (a_1\ a_2\ \ldots\ a_p)$ un p-cycle. Il y a p façons de décrire γ comme un p-cycle :

$$\gamma = (a_1\ a_2\ \ldots\ a_p) = (a_2\ \ldots\ a_p\ a_1) = (a_3\ \ldots\ a_p\ a_1\ a_2) = \cdots = (a_p\ a_1\ \ldots\ a_{p-1}).$$

On peut aussi écrire les choses ainsi : pour tout entier a dans le support de γ,

$$\gamma = \left(a\ \gamma(a)\ \gamma^2(a)\ \cdots\ \gamma^{p-1}(a)\right).$$

Exemple 7 (Calculs sur un cycle)**.**

Soit $\gamma = (a_1 \ \dots \ a_p)$ un p-cycle. Déterminer γ^{-1} et γ^p.

Preuve.

— On démontre tranquillement que $\gamma^{-1} = (a_p \cdots a_1)$.

— Ici l'écriture de γ sous la forme $(a\gamma(a) \cdots \gamma^{p-1}(a))$, va être commode pour vérifier que $\gamma^p = \mathrm{id}$.

 — Si b est fixe pour γ, il l'est pour γ^p.

 — $\gamma^p(a) = \gamma(\gamma^{p-1}(a)) = a$.

 — Soit $j \in [\![0, p-1]\!]$. On a
$$\gamma^p(\gamma^j(a)) = \gamma^j(\gamma^p(a)) = \gamma^j(a).$$

□

Exemple 8 (Conjugué d'un cycle)**.**

Soit $\gamma = (a_1 \ \dots \ a_p)$ un cycle et $\sigma \in S_n$. Montrer que $\sigma\gamma\sigma^{-1} = (\sigma(a_1) \ \sigma(a_2) \ \dots \ \sigma(a_p))$.
Une conséquence de ce calcul : tous les p-cycles sont conjugués.

Preuve. Notons $\gamma' = (\sigma(a_1) \ \dots \ \sigma(a_p))$. Son support est $\mathrm{supp}(\gamma') = \{\sigma(a_1), \dots, \sigma(a_p)\}$.

— Soit $b \in [\![1, n]\!] \setminus \mathrm{supp}(\gamma')$. Alors $\sigma^{-1}(b) \notin \mathrm{supp}(\gamma)$: c'est un point fixe de γ. Ainsi,
$$\sigma\gamma\sigma^{-1}(b) = \sigma\left(\gamma(\sigma^{-1}(b))\right) = \sigma\left(\sigma^{-1}(b)\right) = b.$$

— Considérons maintenant un élément du support de γ' : $\sigma(a_j)$ avec $j \in [\![1, p]\!]$. On a
$$\sigma\gamma\sigma^{-1}(\sigma(a_j)) = \sigma\gamma(a_j) = \sigma(a_{j+1}),$$
avec la convention naturelle $a_{p+1} = a_1$.

On a bien prouvé ci-dessus que
$$\forall x \in [\![1, n]\!] \quad \sigma\gamma\sigma^{-1}(x) = \gamma'(x).$$

Pour la conséquence, on prend deux p-cycles $(a_1 \cdots a_p)$ et $(b_1 \cdots b_p)$, et on crée une bijection σ de $[\![1, n]\!]$ dans lui-même en lui demandant d'envoyer les a_i sur les b_i. □

3 Transpositions.

Définition 9.

Une permutation τ qui est un 2-cycle sera appelée une **transposition**.
Une transposition est donc une permutation de la forme (a, b) où $\{a, b\}$ est une paire de $[\![1, n]\!]$.

Proposition 10 (Involutivité)**.**

Si τ est une transposition, alors
$$\tau^2 = \mathrm{id} \quad \text{et } \tau^{-1} = \tau.$$

Lemme 11 (Décomposition d'un cycle en produit de transpositions).

Soit $\gamma = (a_1 \ \dots \ a_p)$ un p-cycle. Alors

$$\gamma = (a_1 \ a_2)(a_2 \ a_3)\dots(a_{p-1} \ a_p) \quad \text{ou} \quad \gamma = (a_1 \ a_p)(a_1 \ a_{p-1})\dots(a_1 \ a_2)$$

On retrouve ici l'exemple minimal qui nous a servi à démontrer que S_3 n'est pas abélien :

$$(1\ 2)(2\ 3) = (1\ 2\ 3) \quad \text{et} \quad (2\ 3)(1\ 2) = (3\ 2)(2\ 1) = (3\ 2\ 1) = (1\ 3\ 2).$$

4 Théorèmes de décomposition.

Théorème 12 (Décomposition en produit de cycles à supports disjoints).

Soit $\sigma \in S_n$. Il existe $\gamma_1, \dots, \gamma_r$ r cycles à supports disjoints tels que

$$\sigma = \gamma_1\gamma_2\cdots\gamma_r.$$

Les γ_i commutent. Cette décomposition est unique à l'ordre des facteurs près.

Preuve. Il va falloir partitionner $\{1, \cdots, n\}$ et prouver que sur chaque cluster, σ agit comme un cycle.
• Une relation d'équivalence sur $\{1, \cdots, n\}$.
Pour i et j dans cet ensemble, on note $i \sim j$ s'il existe $k \in \mathbb{Z}$ tel que $j = \sigma^k(i)$. On prouve facilement que ceci est une relation d'équivalence.
• On a donc une partition de $\{1, \cdots, n\}$ en classes d'équivalences pour $\sim$. Soit $x \in \{1, \cdots, n\}$. On va prouver qu'il existe un entier p tel que

$$[x] = \left\{x, \sigma(x), \dots, \sigma^{p-1}(x)\right\}.$$

L'application $k \mapsto \sigma^k(x)$ nous y aide : c'est une application de $\mathbb{Z}$ dans $[x]$ qui ne saurait être injective : il existe $q < q'$ tels que $\sigma^q(x) = \sigma^{q'}(x)$, soit $\sigma^{q'-q}(x) = x$. On peut poser

$$p = \min\{k \in \mathbb{N}^* \mid \sigma^k(x) = x\},$$

bien défini comme partie non vide et minorée. Reste à prouver l'égalité d'ensemble : pour l'inclusion non triviale, faire la division euclidienne par p.
• Créer les cycles. On note r le nombre de classes d'équivalences non réduite à un singleton. Sur une classe d'équivalence de cardinal p, le point précédent montre que σ agit comme un p-cycle : il n'y a plus qu'à poser les choses. Les supports des cycles sont disjoints deux à deux car ce sont les classes d'équivalence. □

Exemple 13 (Une décomposition).

On considère la permutation de S_8

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 1 & 7 & 8 & 6 & 2 & 3 \end{pmatrix}.$$

1. Décomposer σ en produit de cycles à supports disjoints.
2. Déterminer σ^4, σ^{12} et σ^{666}

Corollaire 14.

Toute permutation est un produit de transpositions.
La décomposition n'est pas unique et les transpositions ne commutent pas nécessairement.

Exemple 15 (une décomposition).

Décomposer en produit de transpositions la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 1 & 2 & 4 & 6 & 3 \end{pmatrix}.$$

5 Signature.

Définition 16.

Soit $\sigma \in S_n$.

1. Une paire $\{i, j\}$ de $[\![1, n]\!]$ est une **inversion** pour σ si $i - j$ et $\sigma(i) - \sigma(j)$ sont de signe opposé.
2. Le nombre d'inversions de σ est noté $\mathrm{Inv}(\sigma)$.
3. On appelle **signature** de σ le nombre $\varepsilon(\sigma) = (-1)^{\mathrm{Inv}(\sigma)}$.

Exemple 17.

Après avoir calculé son nombre d'inversions, donner la signature de

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}.$$

Proposition 18.

1. L'identité a pour signature 1.
2. Les transpositions ont pour signature -1.

Preuve. Contrairement à ce que l'on pourrait dire trop vite, le nombre d'inversions d'une transposition $\tau = (ab)$ avec $a < b$ n'est pas 1...

- Si $\{i, j\}$ est une paire d'indices, et que $\{i, j\} \cap \{a, b\} = \emptyset$, alors $\{i, j\}$ n'est pas une inversion.
- Une paire $\{a, j\}$ avec $j \notin \{a, b\}$ est une inversion ssi $(\tau(j) - \tau(a))(j - a) < 0$, c'est-à-dire ssi $(j - b)(j - a) < 0$ soit $j \in [\![a + 1, b - 1]\!]$.
- C'est pareil pour les paires $\{i, b\}$ avec $i \notin \{a, b\}$.
- Reste enfin à considérer la paire $\{a, b\}$ qui est une inversion.

Ainsi, le nombre d'inversions d'une transposition est

$$\mathrm{Inv}(\tau) = 2|[\![a+1, b-1]\!]| + 1 = 2(b-a-1) + 1 = 2(b-a) - 1.$$

On a bien un nombre d'inversions impair : $\varepsilon(\tau) = -1$.

$\square$

Proposition 19 (La signature écrite comme un produit)**.**

$$\forall \sigma \in S_n \quad \varepsilon(\sigma) = \prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i - j},$$

le produit étant indexé par l'ensemble de toutes les paires $\{i, j\}$ (donc $i \neq j$) de $[\![1, n]\!]$.

Preuve. Pour une paire $\{i, j\}$ on écrit

$$\frac{\sigma(i) - \sigma(j)}{i - j} = (-1)^{x_{\{i,j\}}} \left| \frac{\sigma(i) - \sigma(j)}{i - j} \right|.$$

Le produit donne

$$\prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i - j} = (-1)^{\sum\limits_{\{i,j\}} x_{\{i,j\}}} \times \frac{\prod\limits_{\{i,j\}} |\sigma(i) - \sigma(j)|}{\prod\limits_{\{i,j\}} |i - j|}$$

D'une part, $\sum\limits_{\{i,j\}} x_{\{i,j\}} = \mathrm{Inv}(\sigma)$. D'autre part, en remarquant que

$$f_\sigma : \left\{ \begin{array}{ccc} \mathcal{P}_2(\{1, ..., n\}) & \to & \mathcal{P}_2(\{1, ..., n\}) \\ \{i, j\} & \mapsto & \{\sigma(i), \sigma(j)\} \end{array} \right.$$

est une bijection, on peut poser le changement d'indices $\{u, v\} = \{\sigma(i), \sigma(j)\}$ et ceci prouve que le quotient de valeurs absolues vaut 1. $\square$

Théorème 20.

La signature est un morphisme de groupes de $(S_n, \circ)$ dans $(\mathbb{C}^*, \times)$:

$$\forall \sigma, \sigma' \in S_n \quad \varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$$

Preuve. Découle de la propriété précédente. $\square$

Corollaire 21 (un peu plus précis mais pas au programme)**.**

Pour $n \geq 2$, la signature est l'unique morphisme de groupes non trivial de $(S_n, \circ)$ dans $(\mathbb{C}^*, \times)$.

Preuve. Soit $f : S_n \to \mathbb{C}^*$ un morphisme de groupes. On va prouver que $f = \mathbf{1}$ ou que $f = \varepsilon$. On va fixer une transposition τ dans S_n et organiser la discussion autour de $f(\tau)$.
• $\tau^2 = \mathrm{id}$ donc $f(\tau^2) = f(\tau)^2 = 1$, ce qui donne $f(\tau) \in \{-1, 1\}$.

• Si $f(\tau) = 1$, alors f prend la valeur 1 sur toutes les transpositions. En effet, on a vu que toutes les transpositions sont conjuguées ! Si τ' est une autre transposition, il existe $\sigma \in S_n$ telle que $\tau' = \sigma\tau\sigma^{-1}$ ce qui conduit à $f(\tau') = f(\tau)$ par propriété de morphisme. Puisque toute permutation s'écrit comme un produit de transpositions, la propriété de morphisme conduite à $f = \mathbf{1}$.
• Si $f(\tau) = -1$ alors f prend la valeur -1 sur toutes les transpositions, et par théorème, c'est forcément la signature. □

Exemple 22.

Soit $p \geq 2$. Que vaut la signature d'un p-cycle ?

Exercices

37.1 **[♦◇◇]** Écrire explicitement S_1, S_2 et S_3.

37.2 **[♦◇◇]** Soit n et p deux entiers naturels supérieurs à 2 tels que $p \leq n$.
Combien S_n contient-il de p-cycles ?

37.3 **[♦♦◇]** Sous-groupe alterné
Notons A_n l'ensemble des permutations de signature égale à 1.
Justifier qu'il s'agit là d'un sous-groupe de S_n et que si $n \geq 2$, $|A_n| = \frac{n!}{2}$.

37.4 **[♦♦◇]** Calculer $\varepsilon(\sigma)$, signature de σ, où

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix}.$$

37.5 **[♦♦♦]** (*) Théorème de Cayley
Soit G un groupe fini de cardinal n.

1. Pour $a \in G$, on pose
$$\tau_a : \left\{ \begin{array}{ccc} G & \to & G \\ x & \mapsto & ax \end{array} \right. .$$
l'opérateur de translation à gauche associé à a. Vérifier que pour tout a dans G, τ_a est un automorphisme de G.
2. Vérifier que
$$\Phi : \left\{ \begin{array}{ccc} G & \to & S_G \\ a & \mapsto & \tau_a \end{array} \right.$$
est un morphisme de groupes injectif.
3. En déduire que G est isomorphe à un sous-groupe de S_n.

37.6 **[♦♦♦]** Centre de S_n
On note $Z(S_n)$ le centre de S_n, c'est-à-dire l'ensemble des permutations qui commutent avec toutes les autres.

1. Que vaut $Z(S_2)$?
2. Montrer que $Z(S_n)$ est trivial dès que $n \geq 3$.

Déterminants

1 La théorie.

Dans toute cette partie, n est un entier naturel non nul et E un $\mathbb{K}$-espace vectoriel de dimension n.

1.1 Formes n-linéaires alternées.

Définition 1.

On appelle **forme n-linéaire** sur E toute application $f : E^n \to \mathbb{K}$ vérifiant

$$\forall j \in [\![1,n]\!] \ \forall (a_1,\dots,a_{j-1},a_{j+1},\dots,a_n) \in E^{n-1} \quad x \mapsto f(a_1,\dots,a_{j-1},x,a_{j+1},\dots,a_n) \text{ est linéaire.}$$

On dira aussi que f est linéaire « par rapport à chacune de ses variables ».
Autrement dit, pour $j \in [\![1,n]\!]$ et $(a_1,\dots,a_{j-1},a_{j+1},\dots,a_n)$ fixé, l'application $f(a_1,\dots,a_{j-1},\bullet,a_{j+1},\dots,a_n)$ est une forme linéaire.

Proposition 2.

Soit $f : E^n \to \mathbb{K}$ une forme n-linéaire.

1. $\forall \lambda \in \mathbb{K} \quad \forall (x_1,\dots,x_n) \in E^n \quad f(\lambda x_1,\dots,\lambda x_n) = \lambda^n f(x_1,\dots,x_n)$.
2. Soit $(x_1,\dots,x_n) \in E^n$. Si l'un des x_i vaut 0_E, alors $f(x_1,\dots,x_n) = 0_{\mathbb{K}}$.

Définition 3.

Soit $f : E^n \to \mathbb{K}$ une forme n-linéaire ($n \geq 2$). Elle est dite **alternée** si et seulement si $f(x_1,\dots,x_n) = 0$ pour tout n-uplet $(x_1,\dots,x_n) \in E^n$ dont au moins deux vecteurs sont égaux.

Proposition 4.

Soit $f : E^n \to \mathbb{K}$ une forme n-linéaire alternée ($n \geq 2$) et $(x_1, \ldots, x_n) \in E^n$.

1. On ne change pas la valeur prise par f sur $(x_1, \ldots, x_n)$ en ajoutant à l'un des vecteurs de la famille une combinaison linéaire des autres.
2. Si $(x_1, \ldots, x_n)$ est liée, alors $f(x_1, \ldots, x_n) = 0$.
3. <u>Effet d'une transposition</u>. Soit une paire d'indices $\{i, j\}$ avec $i < j$.

$$f\left(\ldots, x_{i-1}, \boxed{x_j}, x_{i+1}, \ldots, x_{j-1}, \boxed{x_i}, x_{j+1}, \ldots\right) = -f\left(\ldots, x_{i-1}, \boxed{x_i}, x_{i+1}, \ldots, x_{j-1}, \boxed{x_j}, x_{j+1}, \ldots\right).$$

   Cette dernière propriété est aussi appelée propriété d'**antisymétrie**.

4. <u>Effet d'une permutation</u>. Pour tout $\sigma \in S_n$,

$$f\left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right) = \varepsilon(\sigma) f(x_1, \ldots, x_n).$$

1.2 Déterminant d'une famille de vecteurs dans une base.

Théorème 5 (fondamental)**.**

L'ensemble des formes n-linéaires alternées sur E est une droite vectorielle.

Si $\mathcal{B} = (e_1, \ldots, e_n)$ est une base de E, il existe une unique forme n-linéaire alternée qui prend la valeur 1 sur $\mathcal{B}$. On l'appelle **déterminant dans la base** $\mathcal{B}$ et on la note $\det_{\mathcal{B}}$. On a

$$\forall (x_1, \ldots, x_n) \in E^n \quad \det_{\mathcal{B}}(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{j=1}^{n} e^*_{\sigma(j)}(x_j).$$

Corollaire 6 (c'est ça, une droite vectorielle)**.**

Si f est une forme n-linéaire alternée sur E et $\mathcal{B}$ une base de E, il existe $\lambda \in \mathbb{K}$ tel que $f = \lambda \det_{\mathcal{B}}$.

Définition 7.

Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base de E et $(x_1, \ldots, x_n) \in E^n$.
Le nombre $\det_{\mathcal{B}}(x_1, \ldots, x_n)$ est appelé **déterminant dans la base** $\mathcal{B}$ de $(x_1, \ldots, x_n)$.

Théorème 8 (Caractérisation des bases)**.**

Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base de E et $(x_1, \ldots, x_n) \in E^n$.

$$(x_1, \ldots, x_n) \text{ est une base de } E \quad \Longleftrightarrow \quad \det_{\mathcal{B}}(x_1, \ldots, x_n) \neq 0.$$

Exemple 9 (Interprétation géométrique).

• Si $E = \mathbb{R}^2$ et $\mathcal{B}$ est la base canonique de $\mathbb{R}^2$, pour $(\overrightarrow{u_1}, \overrightarrow{u_2})$ un couple de vecteurs, le nombre $\det_{\mathcal{B}}(\overrightarrow{u_1}, \overrightarrow{u_2})$ peut être vu comme *l'aire orientée* du parallélogramme engendré par $(\overrightarrow{u_1}, \overrightarrow{u_2})$.

• Si $E = \mathbb{R}^3$ et $\mathcal{B}$ est la base canonique de $\mathbb{R}^3$, pour $(\overrightarrow{u_1}, \overrightarrow{u_2}, \overrightarrow{u_3})$ un triplet de vecteurs, le nombre $\det_{\mathcal{B}}(\overrightarrow{u_1}, \overrightarrow{u_2}, \overrightarrow{u_3})$ peut être vu comme *le volume orienté* du parallélépipède engendré par $(\overrightarrow{u_1}, \overrightarrow{u_2}, \overrightarrow{u_3})$.

1.3 Déterminant d'un endomorphisme en dimension finie.

On rappelle que E est dans toute cette première partie un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$.

Lemme 10 (*).

Soit $u \in \mathscr{L}(E)$.
Le nombre $\det_{\mathcal{B}}(u(e_1), \dots, u(e_n))$ ne dépend pas de la base $\mathcal{B} = (e_1 \dots, e_n)$ considérée.

Définition 11.

Soit $u \in \mathscr{L}(E)$. On appelle **déterminant** de u et on note $\det(u)$ le nombre

$$\det(u) = \det_{\mathcal{B}}(u(e_1), \dots, u(e_n)),$$

où $\mathcal{B} = (e_1, \dots, e_n)$ est une base quelconque de E.

Proposition 12.

Soit $u \in \mathscr{L}(E)$, $\mathcal{B}$ une base de E et $(x_1, \dots, x_n) \in E^n$. On a

$$\det_{\mathcal{B}}(u(x_1), \dots, u(x_n)) = \det(u) \times \det_{\mathcal{B}}(x_1, \dots, x_n).$$

Proposition 13.

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \geq 1$.

1. $\det(\mathrm{id}_E) = 1$.
2. $\forall u \in \mathscr{L}(E)\ \forall \lambda \in \mathbb{K}\ \ \det(\lambda u) = \lambda^n \det(u)$.
3. $\forall (u, v) \in \mathscr{L}(E)^2 \quad \det(u \circ v) = \det(u) \det(v)$.
4. Pour tout $u \in \mathscr{L}(E)$, u est un automorphisme si et seulement si $\det(u) \neq 0$.
   Si c'est le cas,
$$\det(u^{-1}) = (\det(u))^{-1}.$$

Attention, on n'a aucune relation intéressante à proposer concernant $\det(u + v)$.

Corollaire 14.

Si E est de dimension finie, det induit un morphisme de groupes entre $GL(E)$ et $\mathbb{K}^*$.

Exemple 15 (Déterminant d'une symétrie vectorielle)**.**

Que dire de $\det(s)$ si s est une symétrie vectorielle de E ?

1.4 Déterminant d'une matrice carrée.

Définition 16.

Soit $A \in M_n(\mathbb{K})$. On appelle **déterminant** de A, et on note $\det(A)$ le nombre

$$\det(A) = \det_{\mathcal{B}_c}(C_1, \ldots, C_n),$$

où $\mathcal{B}_c$ est la base canonique de $M_{n,1}(\mathbb{K})$ et $C_1, \ldots, C_n$ les n colonnes de la matrice A.

Autrement dit, $\det(A)$ est le déterminant de l'endomorphisme canoniquement associé à A.

Notation.

Si $A = (a_{i,j})_{1 \leq i,j \leq n}$ le déterminant de A est aussi noté

$$\begin{vmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \ldots & a_{n,n} \end{vmatrix}.$$

Théorème 17.

1. $\det(I_n) = 1$.
2. $\forall A \in M_n(\mathbb{K})\ \forall \lambda \in \mathbb{K}\ \ \det(\lambda A) = \lambda^n \det(A)$.
3. $\boxed{\forall (A, B) \in M_n(\mathbb{K})^2\ \ \det(AB) = \det(A)\det(B)}$.
4. Pour tout $A \in M_n(\mathbb{K})$, A est inversible si et seulement si $\det(A) \neq 0$.
   Si c'est le cas,
   $$\det(A^{-1}) = (\det(A))^{-1}.$$

Corollaire 18.

L'application det induit un morphisme de groupes entre $GL_n(\mathbb{K})$ et $\mathbb{K}^*$.

Proposition 19.

Soit $A = (a_{i,j})$ une matrice carrée d'ordre $n \geq 1$.

$$\det(A) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n}.$$

Exemple 20 (Cohérence avec la définition en taille 2)**.**

Retrouver à l'aide de la formule précédente l'expression connue pour le déterminant d'une matrice de taille 2 :

$$\begin{vmatrix} a & c \\ b & d \end{vmatrix} = ad - bc.$$

Exemple 21 (Une application simple)**.**

On peut noter $\mathcal{M}_n(\mathbb{Z})$ l'ensemble des matrices carrées à coefficients entiers relatifs.
Montrer que si $A \in M_n(\mathbb{Z})$, alors $\det A \in \mathbb{Z}$.

Théorème 22.

$$\forall A \in M_n(\mathbb{K}) \quad \det(A^T) = \det(A).$$

Corollaire 23.

Soit $A \in M_n(\mathbb{K})$ de lignes $L_1, \dots, L_n$.

$$\det(A) = \det_{\mathcal{B}_c}(L_1, \dots, L_n),$$

où $\mathcal{B}_c$ est la base canonique de $M_{1,n}(\mathbb{K})$.

Proposition 24 (peu importe la base, à nouveau)**.**

Soit $u \in \mathscr{L}(E)$ et $\mathcal{B}$ une base de E. On a

$$\det(\mathrm{Mat}_{\mathcal{B}}(u)) = \det(u).$$

Corollaire 25.

Deux matrices semblables ont même déterminant.

2 La pratique.

2.1 Échelonner.

Proposition 26 (Effet des opérations de pivot sur les colonnes).

Soit $A \in M_n(\mathbb{K})$. On note $(C_j, j \in [\![1, n]\!])$ ses colonnes. Soit $\mathcal{O}$ une opération élémentaire sur les colonnes, transformant A en B :

$$A \underset{\mathcal{O}}{\sim} B.$$

1. Si $\mathcal{O}$ est du type $C_i \leftrightarrow C_j$, alors $\det(B) = -\det(A)$,
2. Si $\mathcal{O}$ est du type $C_j \leftarrow \lambda C_j$, avec $\lambda \in \mathbb{K}^*$, alors $\det(B) = \lambda \det(A)$,
3. Si $\mathcal{O}$ est du type $C_j \leftarrow C_j + \lambda C_i$, avec $\lambda \in \mathbb{K}$, alors $\det(B) = \det(A)$.

Le déterminant étant invariant par transposition, tout reste vrai pour des opérations élémentaires sur les lignes.

Proposition 27 (Déterminant d'une matrice triangulaire).

Le déterminant d'une matrice triangulaire est le produit de ses coefficients diagonaux.
Par exemple, pour une matrice triangulaire supérieure,

$$\begin{vmatrix} \alpha_1 & * & \dots & * \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & \alpha_n \end{vmatrix} = \prod_{j=1}^{n} \alpha_j.$$

Exemples 28.

Calculer $\begin{vmatrix} 5 & 6 & -2 \\ 10 & 6 & -4 \\ 15 & 6 & -2 \end{vmatrix}$ et $\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix}$.

Exemple 29.

Soit $a \in \mathbb{C}$. Calculer le déterminant de taille n ci-dessous.

$$\begin{vmatrix} a & 1 & & (1) \\ 1 & \ddots & \ddots & \\ & \ddots & \ddots & 1 \\ (1) & & 1 & a \end{vmatrix}.$$

<u>Indication</u> : la somme des éléments de chaque colonne (ou de chaque ligne) est toujours la même...

2.2 Développer selon une colonne ou une ligne.

Remarque. Puisque la nullité d'un déterminant caractérise l'inversibilité de la matrice, c'est sous forme factorisée que l'on cherche à écrire les déterminants. Mais comme on va le voir dans les quelques exemples donnés plus bas, *développer* est parfois nécessaire pour mettre en évidence certaines propriétés.

Soit $A = (a_{k,l})_{1\leq k,l\leq n} \in M_n(\mathbb{K})$ et $(i,j) \in [\![1,n]\!]^2$. Dans le théorème qui suit, on notera $\Delta_{i,j}$ déterminant de la matrice $(a_{k,l})_{\substack{k\neq i\\ l\neq j}}$ extraite de A en ôtant la $i$ème ligne et la $j$ème colonne. On parle parfois de ce déterminant comme du *mineur* à la position (i,j).

Exemple : $A = \begin{pmatrix} 2 & 3 & 1 \\ 5 & 9 & 1 \\ 0 & -1 & 2 \end{pmatrix}$ Son mineur de position $(1,2)$: $\Delta_{1,2} = \begin{vmatrix} 5 & 1 \\ 0 & 2 \end{vmatrix}$.

Lemme 30.

Soit $n \in \mathbb{N} \setminus \{0,1\}$ et $a_2, \dots, a_n$ dans $\mathbb{K}$ Alors,

$$\forall A \in M_{n-1}(\mathbb{K}) \qquad \begin{vmatrix} 1 & 0 & \dots & 0 \\ a_2 & & & \\ \vdots & & A & \\ a_n & & & \end{vmatrix}_n = \begin{vmatrix} & A & \end{vmatrix}_{n-1}$$

Preuve. Posons

$$\Psi : \left\{ \begin{array}{ccc} M_{n-1}(\mathbb{K}) & \to & \mathbb{K} \\ A & \mapsto & \begin{vmatrix} 1 & 0 & \dots & 0 \\ a_2 & & & \\ \vdots & & A & \\ a_n & & & \end{vmatrix}_n \end{array} \right. .$$

Notons $E = M_{n-1,1}(\mathbb{K})$; Ψ peut être vue comme une application définie sur E^{n-1} et à valeurs dans $\mathbb{K}$.

• Multilinéarité. Soit $A \in M_{n-1}(\mathbb{K})$. Supposons que pour j fixé dans $[\![1, n-1]\!]$, la $j$ème colonne de A soit égale à $\lambda X + \mu Y$, avec $X, Y \in E$ et $\lambda, \mu \in \mathbb{K}$.

$$\begin{vmatrix} 1 & 0 & \cdots & \lambda 0 + \mu 0 & \cdots & 0 \\ a_2 & & & & & \\ \vdots & & & \lambda X + \mu Y & & \\ a_n & & & & & \end{vmatrix}_n = \lambda \begin{vmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 \\ a_2 & & & & & \\ \vdots & & & X & & \\ a_n & & & & & \end{vmatrix}_n + \mu \begin{vmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 \\ a_2 & & & & & \\ \vdots & & & Y & & \\ a_n & & & & & \end{vmatrix}_n$$

en utilisant la linéarité du déterminant sur $M_n(\mathbb{K})$ par rapport à la $(j+1)$ème colonne. Ceci prouve que Ψ est une forme $(n-1)$-linéaire sur E^{n-1}.

• Soit $A \in M_{n-1}(\mathbb{K})$ une matrice ayant deux colonnes égales. Alors $\Psi(A)$ est le déterminant d'une matrice ayant deux colonnes égales : il est nul. Ceci montre que Ψ est une forme $(n-1)$-linéaire alternée.

• Image de la base canonique de E. Cela revient à calculer $\Psi(I_{n-1}) = \begin{vmatrix} 1 & 0 & \dots & 0 \\ a_2 & 1 & & \\ \vdots & & \ddots & \\ a_n & & & 1 \end{vmatrix}_n = 1.$

En remplissant les trois conditions plus haut, l'application Ψ doit être le déterminant sur la base canonique de E^{n-1}, ce qui achève de prouver le résultat. □

Théorème 31 (Développement selon une ligne ou une colonne)**.**

Soit $A = (a_{i,j}) \in M_n(\mathbb{K})$. Pour $(i,j) \in [\![1,n]\!]^2$, on note $\Delta_{i,j}$ le déterminant de la matrice extraite de a en supprimant la ligne i et la colonne j. On a les développements suivants :

Développement selon la $i$ème ligne
$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{i,j} \Delta_{i,j}.$$

Développement selon la $j$ème colonne
$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{i,j} \Delta_{i,j}.$$

Remarque. On remarque l'alternance de signe. Lorsque le développement commence en haut à gauche, le premier signe est $+$ à cause du facteur $(-1)^{1+1}$.

$\boxed{\textbf{Application 1}}$ Le développement de déterminants de taille 3.

Selon C_1 :
$$\begin{vmatrix} a & d & g \\ b & e & h \\ c & f & i \end{vmatrix} = a \begin{vmatrix} e & h \\ f & i \end{vmatrix} - b \begin{vmatrix} d & g \\ f & i \end{vmatrix} + c \begin{vmatrix} d & g \\ e & h \end{vmatrix}$$

Selon L_2 :
$$\begin{vmatrix} a & d & g \\ b & e & h \\ c & f & i \end{vmatrix} = -b \begin{vmatrix} d & g \\ f & i \end{vmatrix} + e \begin{vmatrix} a & g \\ c & i \end{vmatrix} - h \begin{vmatrix} a & d \\ c & f \end{vmatrix}.$$

$\boxed{\textbf{Application 2}}$ Tirer parti des propriétés particulières d'une ligne/colonne.

Exemple 32.

Soit x un réel. On note $D(x) = \begin{vmatrix} (1+x)^2 & (2+x)^2 & (3+x)^2 & (4+x)^2 \\ 2^2 & 3^2 & 4^2 & 5^2 \\ 3^2 & 4^2 & 5^2 & 6^2 \\ 4^2 & 5^2 & 6^2 & 7^2 \end{vmatrix}$

a) Justifier que $D : x \mapsto D(x)$ est une fonction polynomiale de degré au plus 2.

b) En déduire la valeur de $D(x)$ pour tout x.

$\boxed{\textbf{Application 3}}$ Obtenir une relation de récurrence.

Exemple 33.

Soit $n \in \mathbb{N}^*$ et a et b deux nombre complexes. Soit la matrice "bidiagonale"

$$\begin{pmatrix} a & & & b \\ & \ddots & ⋰ & \\ & ⋰ & \ddots & \\ b & & & a \end{pmatrix} \in M_{2n}(\mathbb{C}).$$

Calculer son déterminant D_n en établissant une relation de récurrence satisfaite par (D_n).

Théorème 34 (Déterminant de Vandermonde)**.**

Soient $a_1, \ldots, a_n$ n nombres réels ou complexes.

$$\begin{vmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \ldots & a_2^{n-1} \\ 1 & a_3 & a_3^2 & \ldots & a_3^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n & a_n^2 & \ldots & a_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (a_j - a_i) \,.$$

Exemple 35.

Deux exemples de problèmes se ramenant à des systèmes linéaires de Vandermonde :

1. L'interpolation de Lagrange.
2. Le problème des moments pour des variables aléatoires d'image finie.

2.3 Complément théorique : la comatrice.

Définition 36.

Soit $A = (a_{i,j}) \in M_n(\mathbb{K})$ et $(i,j) \in [\![1,n]\!]^2$.
On note $\Delta_{i,j}$ le déterminant de la matrice extraite de A en supprimant la ligne i et la colonne j.
Le réel $A_{i,j} = (-1)^{i+j}\Delta_{i,j}$ est alors appelé **cofacteur** de $a_{i,j}$ dans A.
La matrice $(A_{i,j})_{1 \leq i,j \leq n}$ est appelée **comatrice** de A et notée $\mathrm{Com}(A)$.

Proposition 37.

$$\forall A \in M_n(\mathbb{K}) \quad A \cdot (\mathrm{Com}(A))^T = (\mathrm{Com}(A))^T \cdot A = \det(A) I_n.$$

En particulier, si A est inversible, alors $A^{-1} = \dfrac{1}{\det(A)}(\mathrm{Com}(A))^T$.

Exemple 38.

Si $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, on retrouve que $A^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$

Exemple 39 (Inverse à coefficients entiers)**.**

Soit $A \in GL_n(\mathbb{R}) \cap M_n(\mathbb{Z})$. Montrer que

$$A^{-1} \in M_n(\mathbb{Z}) \iff \det A = \pm 1.$$

Annexe : Preuves.

Preuve de la proposition 10.
On note $\Lambda_n(E)$ l'ensemble des formes n-linéaires alternées qui est, rappelons-le, une droite.
Pour f une telle forme, considérons la fonction

$$(x_1, \dots, x_n) \mapsto f(u(x_1), \dots, u(x_n)).$$

Grâce à la n-linéarité de f et à la linéarité de u, on se convainc facilement qu'elle est n-linéaire. Elle est aussi alternée : cela découle du caractère alterné de f. Notons $\varphi_u(f)$ cette fonction de $\Lambda_n(E)$, ceci définit l'application

$$\varphi_u : \left\{ \begin{array}{ccc} \Lambda_n(E) & \to & \Lambda_n(E) \\ f & \mapsto & \varphi_u(f) \end{array} \right. .$$

Que dire, maintenant, de l'application φ_u ? Elle est linéaire, c'est assez clair ! Et une application linéaire définie sur une droite... est une homothétie ! Laissons cet exercice facile au lecteur et terminons cette preuve.

Nous venons de prouver l'existence d'une constante $\lambda_u \in \mathbb{K}$, dépendant seulement de u, telle que

$$\forall f \in \Lambda_n(E) \quad \varphi_u(f) = \lambda_u f.$$

Considérons maintenant une base de E notée $\mathcal{B} = (e_1, \dots, e_n)$. Puisque $\det_{\mathcal{B}}$ est un élément de $\Lambda_n(E)$, on a

$$\varphi_u(\det_{\mathcal{B}}) = \lambda_u \det_{\mathcal{B}}.$$

Évaluons l'égalité précédente en $(e_1 \dots, e_n)$: on obtient

$$\det_{\mathcal{B}}(u(e_1), \dots, u(e_n)) = \lambda_u \det_{\mathcal{B}}(e_1, \dots, e_n) = \lambda_u.$$

Ceci démontre que le nombre $\det_{\mathcal{B}}(u(e_1), \dots, u(e_n))$ ne dépend pas de $\mathcal{B}$. □

Exercices

38.1 **[♦◇◇]** Soit $n \geq 2$. Calculer le déterminant de taille n suivant.

$$\begin{vmatrix} 1 & n & n & \cdots & n \\ n & 2 & n & \cdots & n \\ n & n & 3 & \cdots & n \\ \vdots & \vdots & \vdots & \ddots & \\ n & n & n & \cdots & n \end{vmatrix}.$$

38.2 **[♦◇◇]** Soit $n \geq 2$. Pour tout $k \in [\![1, n]\!]$, on note $S_k = \sum\limits_{i=k}^{n} i$. Calculer

$$\begin{vmatrix} S_1 & S_1 & S_1 & \cdots & S_1 \\ S_1 & S_2 & S_2 & \cdots & S_2 \\ S_1 & S_2 & S_3 & \cdots & S_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ S_1 & S_2 & S_3 & \cdots & S_n \end{vmatrix}.$$

$\boxed{\textbf{38.3}}$ **[♦◇◇]** Soient a et b deux nombres complexes. Calculer le déterminant de la matrice ci-dessous sous forme factorisée. La réponse s'écrit en huit signes.

$$\begin{pmatrix} a^2 & ab & ab & b^2 \\ ab & a^2 & b^2 & ab \\ ab & b^2 & a^2 & ab \\ b^2 & ab & ab & a^2 \end{pmatrix},$$

$\boxed{\textbf{38.4}}$ **[♦◇◇]** Soit $(a, b, c) \in \mathbb{R}^3$. Factoriser $\begin{vmatrix} 1 & 1 & 1 \\ \sin a & \sin b & \sin c \\ \cos a & \cos b & \cos c \end{vmatrix}$.

$\boxed{\textbf{38.5}}$ **[♦◇◇]** Calculer $\begin{vmatrix} & & & a_n \\ & & & \\ & a_2 & & \\ a_1 & & & \end{vmatrix}$

$\boxed{\textbf{38.6}}$ **[♦♦◇]** Soit $(a, b) \in \mathbb{C}^2$. Calculer pour $n \in \mathbb{N}^*$ le déterminant ci-dessous :

$$D_n = \begin{vmatrix} a+b & a & 0 & \cdots & 0 \\ b & a+b & a & \ddots & \vdots \\ 0 & b & a+b & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & a \\ 0 & \cdots & 0 & b & a+b \end{vmatrix}.$$

$\boxed{\textbf{38.7}}$ **[♦♦◇]** Pour $n \in \mathbb{N}$ avec $n \geq 2$, on note

$$D_n = \begin{vmatrix} 1 & & & & n \\ & 1 & & & n-1 \\ & & \ddots & & \vdots \\ & & & \ddots & 2 \\ n & n-1 & \dots & 2 & 1 \end{vmatrix}_{[n]}$$

1. Calculer D_2 et D_3.
2. Pour $n \geq 2$, déterminer une relation entre D_{n+1} et D_n.
3. En déduire D_n pour $n \geq 2$.

$\boxed{\textbf{38.8}}$ **[♦♦◇]** Soit, pour $a, b, c \in \mathbb{R}$ le déterminant D et la fonction f :

$$D = \begin{vmatrix} a & c & \cdots & c \\ b & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & c \\ b & \cdots & b & a \end{vmatrix}, \qquad f : x \mapsto \begin{vmatrix} a+x & c+x & \cdots & c+x \\ b+x & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & c+x \\ b+x & \cdots & b+x & a+x \end{vmatrix}.$$

1. Justifier que f est une fonction polynomiale. de degré inférieur à 1.
2. Calculer D dans le cas $b \neq c$.
3. Calculer D dans le cas $b = c$.

$\boxed{\textbf{38.9}}$ **[♦♦♢]** Le retour du Vandermonde
On note

$$V(a_1,\dots,a_n)=\begin{vmatrix}1 & a_1 & a_1^2 & \dots & a_1^{n-1}\\ 1 & a_2 & a_2^2 & \dots & a_2^{n-1}\\ 1 & a_3 & a_3^2 & \dots & a_3^{n-1}\\ \vdots & \vdots & \vdots & & \vdots\\ 1 & a_n & a_n^2 & \dots & a_n^{n-1}\end{vmatrix}\quad \text{et}\quad f : x\mapsto \begin{vmatrix}1 & x & x^2 & \dots & x^{n-1}\\ 1 & a_2 & a_2^2 & \dots & a_2^{n-1}\\ 1 & a_3 & a_3^2 & \dots & a_3^{n-1}\\ \vdots & \vdots & \vdots & & \vdots\\ 1 & a_n & a_n^2 & \dots & a_n^{n-1}\end{vmatrix}.$$

1. Justifier que f est une fonction polynomiale, de degré inférieur à $n-1$.
2. En considérant ses racines, prouver sans calcul que
$$V(a_1,a_2\dots,a_n)=\left(\prod_{j=2}^{n}(a_j-a_1)\right)V(a_2,\dots,a_n).$$
3. En déduire une expression de $V(a_1,\dots,a_n)$ sous forme factorisée.

$\boxed{\textbf{38.10}}$ **[♦♦♢]** [Matrice compagnon d'un polynôme] Soit $P=X^n-\sum\limits_{k=0}^{n-1}a_kX^k\in\mathbb{C}[X]$. Soit la matrice

$$C=\begin{pmatrix}0 & 0 & \dots & 0 & a_0\\ 1 & 0 & \dots & 0 & a_1\\ 0 & \ddots & & \vdots & \vdots\\ \vdots & \ddots & \ddots & 0 & \vdots\\ 0 & \dots & 0 & 1 & a_{n-1}\end{pmatrix}$$

Montrer que pour tout $\lambda\in\mathbb{C}$, $\det(\lambda I_n-C)=P(\lambda)$.
Application : donner le rang de λI_n-C (on discutera selon les valeurs de λ).

$\boxed{\textbf{38.11}}$ **[♦♦♢]** Soient $a,b,c,d\in\mathbb{R}$.

On veut calculer $D=\begin{vmatrix}1 & a & a^2 & a^4\\ 1 & b & b^2 & b^4\\ 1 & c & c^2 & c^4\\ 1 & d & d^2 & d^4\end{vmatrix}$. On introduit, pour $x\in\mathbb{R}$, $P(x)=\begin{vmatrix}1 & a & a^2 & a^3 & a^4\\ 1 & b & b^2 & b^3 & b^4\\ 1 & c & c^2 & c^3 & c^4\\ 1 & d & d^2 & d^3 & d^4\\ 1 & x & x^2 & x^3 & x^4\end{vmatrix}$.

On note $\alpha=(b-a)(c-a)(d-a)(c-b)(d-b)(d-c)$.

1. Montrer que $P\in\mathbb{R}[X]$.
2. À quelle condition nécessaire et suffisante sur les coefficients a,b,c,d le polynôme P est-il de degré 4 ?
3. Trouver une relation entre P et D, puis en déduire une expression factorisée de D à l'aide de α.

$\boxed{\textbf{38.12}}$ **[♦♦♦]** Sur un espace probabilisé (Ω,P), on se donne n^2 variables de Rademacher indépendantes

$$(X_{i,j},1\le i,j\le n)\quad \text{telles que } \forall(i,j)\in[\![1,n]\!]^2\ P(X_{1,1}=1)=P(X_{1,1}=-1)=\frac{1}{2}.$$

et on note M la matrice de coefficients $X_{i,j}$.

1. Calculer l'espérance de $\det(M)$.
2. Montrer que sa variance vaut $n!$

$\boxed{\textbf{38.13}}$ **[♦♦♦]** Soit n un entier supérieur à 2 et $A\in M_n(\mathbb{K})$ telle que

$$\forall M\in M_n(\mathbb{K})\quad \det(A+M)=\det(A)+\det(M).$$

Démontrer que A est nulle.

39

Espaces probabilisés finis et variables aléatoires

Lançons une pièce de monnaie. Cela constitue une **expérience**. Il y a deux **issues** possibles à celle-ci : on va obtenir Pile ou Face. Le **résultat** effectivement obtenu dépend de bien des facteurs : position initiale de la pièce, force imprimée par le pouce, conditions météo... Le processus mécanique mis en jeu dans l'expérience est si complexe que l'on abandonne bien vite l'idée de le mettre en équations pour déterminer son résultat. La situation est inconfortable : on a besoin, au moins du point de vue du langage, que le résultat de l'expérience dépende de *quelque-chose*. On résout ce problème en disant que ce résultat dépend du *hasard*. Un même mot va servir pour des expériences bien différentes : le tirage du Loto du soir, le nombre de clients se présentant à un guichet un jour donné, ou encore le sexe d'un enfant à naître. Une expérience dépendant du hasard est qualifiée d'**aléatoire**, alea signifiant jeu de dés en latin.

Si notre pièce est équilibrée et qu'elle est lancée sans tricher, on entend souvent qu'on a « une chance sur deux » d'obtenir Pile. Le lien entre le nombre $\frac{1}{2}$, et l'expérience est un peu flou. Le résultat est binaire : Pile ou bien Face, alors que signifie cette fraction ? On peut chercher une réponse dans la notion de **fréquence empirique**. Cette pièce de monnaie, lançons-la 50 fois. On obtient 28 fois Pile (et donc 22 fois Face). Lançons-la 1000 fois : on obtient 493 fois Pile. Lançons-la 50000 fois , on obtient 25062 fois Pile. Les fréquences empiriques obtenues pour Pile sont donc tour à tour

$$\frac{28}{50} = 0,56 \qquad \frac{493}{1000} = 0,493 \qquad \frac{25062}{50000} = 0,50124.$$

Il semble donc, au moins sur cet exemple, que plus on répète l'expérience, plus la fréquence empirique de l'issue Pile se rapproche de $\frac{1}{2}$. C'est une façon de retrouver le « une chance sur deux », qui est une **fréquence théorique** (ou a priori) à laquelle on donnera bientôt le nom de probabilité.

La convergence de la fréquence empirique d'un événement est un phénomène physique appelé Loi des grands nombres. On pourra estimer que la théorie que l'on va construire ici est un bon **modèle** de la réalité si elle permet de retrouver mathématiquement (de *modéliser*) le phénomène de la Loi des grands nombres.

Signalons que critiquer, comparer et améliorer des modèles probabilistes en les confrontant à l'expérience est le travail d'une branche des mathématiques appelée **statistique**. Aucun résultat de statistiques n'est au programme des CPGE mais nombreux sont ceux parmi vous qui les découvriront dans leur poursuite d'études.

1 Univers fini et variables aléatoires.

1.1 Univers et événements.

Rien de nouveau ici : seulement un nouveau vocabulaire sur les ensembles finis, ainsi que des notations spécifiques aux probabilités.

Notation.

On appelle **univers** un ensemble non vide. Dans ce cours et conformément au programme de première année, tous les univers considérés seront supposés <u>finis</u>.
L'idée : un univers modélise l'ensemble des issues (ou résultats possibles) d'une expérience.
Cet ensemble est noté traditionnellement Ω en probabilités.

On appelle **événement** toute partie A d'un univers Ω (on note $A \subset \Omega$ ou $A \in \mathcal{P}(\Omega)$).

Les singletons de Ω sont parfois appelés *événements élémentaires.*

Si Ω est un univers, Ω en est un événement, qui pourra être appelé *événement certain.*
$\emptyset$ est aussi un événement, qui pourra être appelé *événement impossible.*

Se restreindre en première année à des univers finis implique qu'on ne pourra modéliser que des expériences ayant un nombre fini d'issues. On sait déjà que sur un univers Ω de n éléments, le nombre total d'événements pouvant être considérés est fini et vaut $|\mathcal{P}(\Omega)| = 2^n$. En seconde année, on définira un cadre moins contraignant, mais certains résultats, faciles à démontrer dans le contexte d'un univers fini, devront alors être admis.

Exemples 1 (Événements : de la phrase à l'ensemble)**.**

1. On jette une fois un dé.
   — Proposer un univers modélisant cette expérience.
   — Donner alors l'événement A : « le résultat obtenu est pair ».
2. On lance deux fois de suite une pièce de monnaie.
   — Proposer un univers modélisant cette expérience.
   — Donner alors l'événement B : « on obtient deux fois la même chose. ».

Notation.

Soit Ω un univers, et deux événements $A, B \in \mathcal{P}(\Omega)$.

- Le complémentaire de A, noté $\overline{A}$ est parfois appelé **événement contraire** de A.
- L'intersection $A \cap B$ est parfois notée « A **et** B ».
- La réunion $A \cup B$ est parfois notée « A **ou** B ».
- Si A et B sont disjoints ($A \cap B = \emptyset$), ils sont dits **incompatibles**.

Deux événements incompatibles n'ont pas d'éléments (issues) en commun : ils ne peuvent *pas être réalisés en même temps*.

Exemple 2.

Soit $n \in \mathbb{N}^*$. On joue n parties d'un jeu auquel on peut gagner ou perdre. On suppose la situation correctement modélisée par un univers qu'on ne cherchera pas à déterminer.

Notons , pour $i \in [\![1, n]\!]$ $\quad A_i$ l'événement « on gagne la partie i ».

Écrire à l'aide des A_i les événements suivants :

B : « on gagne toutes les parties » $\qquad$ C : « on perd toutes les parties »
D : « on gagne au moins une partie » $\qquad$ E : « on gagne exactement une partie »

Définition 3.

En probabilités, un recouvrement disjoint de l'univers est appelé **système complet d'événements**.

Plus précisément, si Ω est un univers (fini), un système complet d'événements est une famille d'événements $(A_i)_{i \in [\![1,n]\!]}$, deux à deux incompatibles, et dont la réunion vaut Ω :

$$\forall i, j \in [\![1, n]\!] \quad i \neq j \Longrightarrow A_i \cap A_j = \emptyset \qquad \text{et} \qquad \bigcup_{i=1}^{n} A_i = \Omega.$$

Proposition 4 (Un s.c.e. souvent utilisé)**.**

Si A est un événement d'un univers Ω, alors la famille $(A, \overline{A})$ est un système complet d'événements.

Exemple 5.

Dessiner un univers et un système complet d'événements

La famille $(A_i)_{i \in [\![1,n]\!]}$ de l'exemple 2 est-elle un système complet d'événements ?

1.2 Variables aléatoires.

Notation.

Soit un univers Ω et un ensemble E. On appelle **variable aléatoire** à valeurs dans E une application de Ω vers E. Plutôt que f, la lettre traditionnellement utilisée en probabilités est X.

Notations 6.

Soit $X : \Omega \to E$ une variable aléatoire sur un univers fini Ω.

1. On note $X(\Omega)$ l'image (directe) de Ω par X, c'est-à-dire
$$X(\Omega) = \{X(\omega),\ \omega \in \Omega\}.$$
C'est l'ensemble des valeurs que peut prendre la variable aléatoire X. $\Big(\underline{X(\Omega) \subset E}\Big)$.
2. Soit A une partie de E. On note $\{X \in A\}$ ou $(X \in A)$ l'image réciproque de A par X :
$$\{X \in A\} = \{\omega \in \Omega : X(\omega) \in A\}.$$
Cet ensemble, noté $X^{-1}(A)$ dans un contexte non probabiliste, est <u>une partie de Ω</u> : c'est un événement.

Pour une variable aléatoire $X : \Omega \to E$, si $x \in E$, on note
$$(X = x) = \{\omega \in \Omega : X(\omega) = x\}.$$
Si X est une variable aléatoire <u>à valeurs réelles</u>, on pourra aussi noter
$$(X \leq x) = \{\omega \in \Omega : X(\omega) \leq x\}.$$

Exemple 7.

Représenter une variable aléatoire X entre deux ensembles Ω et E, une partie A de E, et enfin représenter l'événement $(X \in A)$.

Remarque. Rien d'*aléatoire* dans la définition de variable aléatoire c'est simplement une fonction.
Le mot variable vient du fait que dans la pratique, l'univers Ω ne nous intéresse pas vraiment ou bien est hors de portée : la fonction X n'est connue qu'à travers la manière dont ses images *varient* dans E.

Proposition 8 (Le s.c.e. associé à une variable aléatoire)**.**

Si X est une variable aléatoire définie sur un univers fini Ω, alors la famille
$$(X = x)_{x \in X(\Omega)}$$
est un système complet d'événements.

2 Probabilités sur un univers fini.

2.1 Définition et propriétés additives.

On répète une expérience N fois. On note Ω l'ensemble des issues de l'expérience et pour A un événement, on note N_A le nombre de fois que A s'est produit lors des N expériences. L'événement A a pour **fréquence**

$$f(A) := \frac{N_A}{N}.$$

- La fréquence d'un événement est clairement un nombre de $[0,1]$.
- La fréquence de Ω, événement certain, est bien sûr $f(\Omega) = \frac{N}{N} = 1$.
- Si A et B sont deux événements $\boxed{\text{incompatibles}}$, le nombre de fois que « A ou B » se produit est $N_{A\cup B} = N_A + N_B$. La fréquence de $A \cup B$ est donc

$$f(A\cup B) = \frac{N_{A\cup B}}{N} = \frac{N_A + N_B}{N} = \frac{N_A}{N} + \frac{N_B}{N} = f(A) + f(B).$$

Les propriétés observées ci-dessus sur les fréquences *a posteriori* inspirent la définition ci-dessous ; la probabilité d'un événement pourra être vue comme sa fréquence *a priori*.

Définition 9.

On appelle **probabilité** sur un univers fini Ω une application $P : \left\{ \begin{array}{ccc} \mathcal{P}(\Omega) & \to & \mathbb{R} \\ A & \mapsto & P(A) \end{array} \right.$, telle que

- $\forall A \in \mathcal{P}(\Omega) \quad P(A) \in [0,1]$,
- $P(\Omega) = 1$,
- $\forall A, B \in \mathcal{P}(\Omega), \quad A \cap B = \emptyset \implies P(A \cup B) = P(A) + P(B)$.

Le couple (Ω, P) est alors appelé **espace probabilisé** fini.

Proposition 10.

Soit (Ω, P) un espace probabilisé et A et B deux événements. On a

1. $P(A \setminus B) = P(A) - P(A \cap B)$. En particulier $P(\overline{A}) = 1 - P(A)$ et $P(\emptyset) = 0$.
2. Si $B \subset A$ alors $P(B) \leq P(A)$ (croissance).
3. $P(A \cup B) = P(A) + P(B) - P(A \cap B)$ (probabilité d'une union quelconque).

Proposition 11 (Additivité pour n événements deux à deux disjoints)**.**

Soit (Ω, P) un espace probabilisé et $A_1, \ldots, A_n$ n événements <u>deux à deux incompatibles</u>. Alors,

$$P\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} P(A_i).$$

En particulier, si $(A_1, \ldots, A_n)$ un système complet d'événements, alors $\sum_{i=1}^{n} P(A_i) = 1$.

Proposition 12 (Sous-additivité dans le cas général)**.**

Soit (Ω, P) un espace probabilisé et $A_1, \ldots, A_n$ n événements. Alors,

$$P\left(\bigcup_{i=1}^{n} A_i\right) \leq \sum_{i=1}^{n} P(A_i).$$

Ci-dessous, un exemple de probabilité. Elle sera très souvent utilisée en modélisation.

Proposition-Définition 13.

Soit Ω un univers fini et non vide. L'application

$$P : \left\{ \begin{array}{ccc} \mathcal{P}(\Omega) & \to & \mathbb{R} \\ A & \mapsto & \dfrac{|A|}{|\Omega|} \end{array} \right. .$$

est une probabilité sur Ω. On l'appelle **equiprobabilité** sur Ω.

2.2 Distribution de probabilités sur un ensemble fini.

Définition 14.

Soit E un ensemble fini et non vide. Une famille de nombres $(p_x, x \in E)$ est appelée **distribution de probabilités** sur E si elle est constituée de réels positifs tels que $\sum\limits_{x \in E} p_x = 1$.

Exemple élémentaire. Soit p_1, p_2, p_3 des nombres définis par

i	1	2	3
p_i	2/6	1/6	3/6

.

La famille (p_1, p_2, p_3) est une distribution de probabilités sur $\{1, 2, 3\}$.

Les singletons de Ω forment clairement un système complet d'événements. D'après la proposition 11, on a $\sum_{\omega \in \Omega} P(\{\omega\}) = 1$, et les termes de la somme sont tous positifs. La famille $(P(\{\omega\}))_{\omega \in \Omega}$ est donc une distribution de probabilités sur Ω. On va prouver que réciproquement, une distribution de probabilités sur un univers fini permet de définir une (unique) probabilité sur cet univers.

Proposition 15 (Probabilité définie par une distribution de probabilités)**.**

Soit Ω un univers fini et $(p_\omega, \omega \in \Omega)$ une distribution de probabilités sur Ω.
Il existe une unique probabilité P sur Ω telle que $\forall \omega \in \Omega \; P(\{\omega\}) = p_\omega$; cette probabilité vérifie

$$\forall A \in \mathcal{P}(\Omega) \quad P(A) = \sum_{\omega \in A} p_\omega.$$

La preuve de la proposition 15 est donnée en annexe. On vient d'énoncer un résultat important d'un point de vue théorique : pour définir une probabilité sur un univers fini, il est suffisant de se donner une distribution de probabilités sur cet univers. Signalons que définir rigoureusement une probabilité sur un univers infini est une autre paire de manches ! (le problème sera évoqué en seconde année).

Exemple 16 (Un autre regard sur l'équiprobabilité)**.**

Si Ω est un univers de cardinal $n \in \mathbb{N}^*$, la famille $(p_\omega, \omega \in \Omega)$ où tous les p_ω valent $\frac{1}{n}$ est une distribution de probabilités sur Ω. L'unique probabilité qu'elle définit est l'équiprobabilité sur Ω.

Exemple 17 (Une expérience, deux modèles)**.**

On lance un dé équilibré. On se donne l'univers $\Omega = [\![1, 6]\!]$.
Proposer deux espaces probabilisés (Ω, P) et $(\Omega, \widetilde{P})$ modélisant l'expérience.
On souhaite que (Ω, P) soit *bon* et $(\Omega, \widetilde{P})$ *mauvais* du point de vue du statisticien (ou du physicien).

3 Loi d'une variable aléatoire.

3.1 Loi d'une variable aléatoire.

Proposition-Définition 18.

Soit (Ω, P) un espace probabilisé fini et X une variable aléatoire définie Ω. L'application

$$P_X : \begin{cases} \mathcal{P}(X(\Omega)) & \to & \mathbb{R} \\ A & \mapsto & P(X \in A) \end{cases}.$$

est une probabilité sur l'univers fini $X(\Omega)$. On l'appelle **loi** de la variable aléatoire X.

Méthode.

Soit (Ω, P) un espace probabilisé et X une variable aléatoire définie sur Ω. La loi de X est entièrement déterminée par la distribution de probabilités

$$(P(X = x))_{x \in X(\Omega)}.$$

Pour décrire la loi de X, on va donc

1. Préciser $X(\Omega)$, l'ensemble des valeurs que peut prendre X,
2. Pour chaque valeur $x \in X(\Omega)$, calculer $P(X = x)$. On peut éventuellement rassembler ces nombres dans un tableau

x
$P(X = x)$

Possible aussi : un diagramme en bâtons : le bâton centré sur x est de hauteur $P(X = x)$.

Exemple 19 (Un chouette jeu)**.**

On jette un dé équilibré. Si le résultat est $1, 2$ ou 3, on ne gagne rien. Si le résultat est 4 ou 5, on gagne dix euros. Si le résultat est 6, on empoche 100 euros.
On note X le gain à ce jeu. Proposer un espace probabilisé sur lequel X est une variable aléatoire. Donner alors la loi de X.
On représentera cette loi par un tableau, ainsi que par un diagramme en bâtons.

Notation.

Soient deux variables aléatoires X et Y, à valeurs dans un même ensemble E (mais pas forcément définies sur le même univers). Si elles ont même loi, on écrira $X \sim Y$.

3.2 Lois usuelles.

Dans les trois définitions de ce paragraphe, X désigne une variable aléatoire définie sur un univers Ω, sur lequel est définie une probabilité P.

Définition 20.

Soit E un ensemble fini non vide. On dit que X suit la loi **uniforme** sur E si la loi de X est l'équiprobabilité sur E ; on note alors $X \sim \mathscr{U}(E)$.

$$X(\Omega) = E \quad \text{et} \quad \forall x \in E \quad P(X = x) = \frac{1}{|E|}.$$

Interprétation.

Une variable X uniforme sur E modélise le tirage "au hasard" d'un élément de E avec, pour tous les éléments de E, une même chance d'être choisi.

Définition 21.

Soit $p \in [0, 1]$. On dit que X suit la loi de **Bernoulli** de paramètre p (on peut noter $X \sim \mathscr{B}(p)$) si sa loi est associée à la distribution de probabilités donnée par

$$X(\Omega) = \{0, 1\} \quad \text{et} \quad P(X = 1) = p \quad P(X = 0) = 1 - p.$$

Interprétation.

On appelle expérience de Bernoulli une épreuve aléatoire dont l'issue est un succès (avec probabilité p) ou un échec (avec probabilité $1 - p$).
Si X est une v.a. qui vaut 1 lorsque l'expérience est un succès, et 0 sinon, alors $X \sim \mathscr{B}(p)$.

Par exemple, le lancer d'une pièce équilibrée peut être modélisé par une variable aléatoire de loi $\mathcal{B}(\frac{1}{2})$, en convenant par exemple que 1 correspond à Pile, et 0 à Face. C'est aussi la loi uniforme sur $\{0,1\}$.

Proposition 22.

Soit (Ω, P) un espace probabilisé et un événement $A \in \mathcal{P}(\Omega)$.
La fonction indicatrice de A, que l'on note $\mathbf{1}_A$, suit la loi de Bernoulli $\mathscr{B}(p)$, où $p = P(A)$

Définition 23.

Soit $n \in \mathbb{N}^*$ et $p \in [0,1]$. On dit que X suit la loi **binomiale** de paramètres n et p (on peut noter $X \sim \mathscr{B}(n,p)$) si sa loi est associée à la distribution de probabilités donnée par

$$X(\Omega) = [\![0,n]\!] \quad \text{et} \quad \forall k \in [\![0,n]\!] \quad P(X=k) = \binom{n}{k} p^k (1-p)^{n-k}.$$

Remarques.

— On remarque que la loi binomiale $\mathscr{B}(1,p)$ est identique à la loi de Bernoulli $\mathscr{B}(p)$.
— On vérifie grâce au binôme que la famille $\left(\binom{n}{k}p^k(1-p)^{n-k}, k \in [\![0,n]\!]\right)$ est bien une distribution de probabilités : ces nombres sont positifs et leur somme vaut $(p+1-p)^n = 1$.

Interprétation.

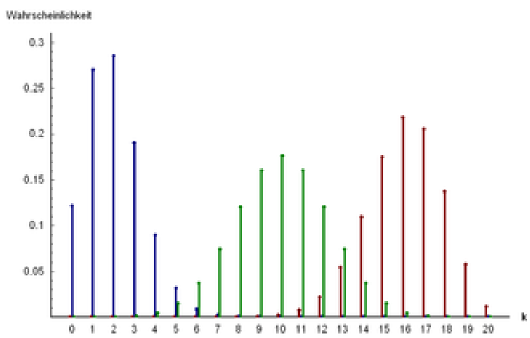
On réalise n expériences de Bernoulli aléatoires *indépendantes*. L'issue de chacune est donc un succès (avec probabilité p) ou un échec (avec probabilité $1-p$). On prouvera dans la proposition 57 que si X est le **nombre total de succès** obtenus dans ce contexte, alors $X \sim \mathscr{B}(n,p)$

Exemple 24.

Mes voisins ont cinq enfants. Quelle est la probabilité qu'ils aient trois filles ?

Les diagrammes en bâtons ci-dessous (pris sur la page Wikipedia consacrée à la loi binomiale) représentent

· en bleu, les probabilités associées à la loi $\mathscr{B}(20, \frac{1}{10})$,
· en vert, les probabilités associées à la loi $\mathscr{B}(20, \frac{1}{2})$,
· en rouge, les probabilités associées à la loi $\mathscr{B}(20, \frac{8}{10})$.



On remarque qu'une variable binomiale a "plus de chances" d'être proche de sa *moyenne* que de prendre des valeurs extrêmes. Ce n'est pas le cas pour une loi uniforme : par exemple pour $\mathscr{U}([\![0,20]\!])$, tous les bâtons auraient même hauteur $(\frac{1}{21})$.

3.3 Loi de l'image.

Si X est une variable aléatoire sur Ω à valeurs dans E, et $f : E \to F$ une application, alors on note $f(X)$ la variable aléatoire :

$$f(X) : \left\{ \begin{array}{lcl} \Omega & \to & F \\ \omega & \mapsto & f(X(\omega)) \end{array} \right. .$$

Exemple 25 (L'exemple avant le résultat général)**.**

Soit X une variable aléatoire à valeurs dans $\{-1, 0, 1, 2\}$ dont la loi est donnée par

x	-1	0	1	2
$P(X = x)$	$\frac{1}{4}$	$\frac{1}{6}$	$\frac{1}{4}$	$\frac{1}{3}$

Donner la loi de $Y = X^2$.

Proposition 26 (Loi de l'image d'une v.a.)**.**

Soit (Ω, P) un espace probabilisé fini.
Soit $X : \Omega \to E$ une variable aléatoire et $f : E \to F$ une application. On note $Y = f(X)$. Alors,

$$Y(\Omega) = \{f(x), x \in X(\Omega)\} \qquad \text{et} \qquad \forall y \in Y(\Omega) \quad P(Y = y) = \sum_{x \in X(\Omega) : f(x) = y} P(X = x).$$

Exemple 27.

Soit $n \in \mathbb{N}^*$ et X une variable aléatoire qui suit la loi uniforme sur $[\![1, 2n]\!]$. Soit $Y = \dfrac{1 + (-1)^X}{2}$.
Déterminer la loi de Y.

Proposition 28.

Soit deux espaces probabilisés (Ω, P) et (Ω', P'), et deux ensembles E et F.
Soient $X : \Omega \to E$ et $X' : \Omega' \to E$ deux variables aléatoires, et $f : E \to F$ une application.
Si X et X' ont même loi, alors $f(X)$ et $f(X')$ aussi. Ce qui s'écrit

$$X \sim X' \quad \Longrightarrow \quad f(X) \sim f(X').$$

3.4 Loi d'un couple, loi d'une famille.

Considérons $X : \Omega \to E$ et $Y : \Omega \to F$, deux variables aléatoires sur un même univers fini Ω.
Le couple de variables aléatoires (X, Y) peut être vu comme une variable aléatoire

$$(X,Y) : \left\{ \begin{array}{lll} \Omega & \to & E \times F \\ \omega & \mapsto & (X(\omega), Y(\omega)) \end{array} \right. .$$

Notation.

Si (X, Y) est un couple de variables aléatoires défini sur un espace probabilisé (Ω, P), alors pour tous $x \in X(\Omega)$ et $y \in Y(\Omega)$,

$$P(X = x, Y = y) \quad \text{plutôt que} \quad P((X,Y) = (x,y)).$$

Définition 29.

Soit (Ω, P) un espace probabilisé fini et $(X, Y) : \Omega \to E \times F$ un couple de variables aléatoires.
On appelle **loi conjointe** de X et Y la loi du couple (X, Y). Cette loi est déterminée par la distribution de probabilités

$$(P(X = x, Y = y))_{(x,y) \in X(\Omega) \times Y(\Omega)}.$$

Les lois de X et Y sont dans ce contexte appelées **lois marginales**.

Exemple. Soit $(X, Y) : \Omega \to \{0, 1\}^2$ un couple de variables sur Ω, dont la loi conjointe est donnée à travers les nombres $P(X = x, Y = y)$ du tableau

$P(X = x, Y = y)$:

$x \backslash y$	0	1
0	$\frac{1}{3}$	$\frac{1}{3}$
1	$\frac{1}{4}$	$\frac{1}{12}$

Donner les lois marginales de X et Y :

x	0	1
$P(X = x)$		

et

y	0	1
$P(Y = y)$		

Proposition 30.

Soit (X, Y) un couple de variables aléatoires défini sur (Ω, P). La loi de X, première loi marginale, est donnée par

$$\forall x \in X(\Omega) \quad P(X = x) = \sum_{y \in Y(\Omega)} P(X = x, Y = y).$$

Remarque. La proposition précédente montre que si on a la loi (conjointe) du couple (X, Y), on peut en déduire les lois (marginales) de X et de Y. La réciproque est fausse en général, comme on le prouve dans l'exemple ci-dessous.

Exemple 31 (Les lois conjointes sont différentes mais les lois marginales sont les mêmes)**.**

Soit $(X, Y) : \Omega \to \{0, 1\}^2$ un couple de variables sur Ω, dont la loi conjointe est donnée à travers les nombres $P(X = x, Y = y)$ du tableau

$P(X = x, Y = y)$:

$x\backslash y$	0	1
0	$\frac{1}{4}$	$\frac{1}{4}$
1	$\frac{1}{4}$	$\frac{1}{4}$

Vérifier que (X, Y) et (X, X) ont les mêmes lois marginales, puis justifier que les deux couples n'ont pas la même loi conjointe.

Somme de deux variables aléatoires. Soit (X, Y) un couple de variables aléatoires à valeurs réelles, définies sur un univers Ω. On note $X + Y$ la variable aléatoire

$$X + Y : \begin{cases} \Omega & \to & \mathbb{R} \\ \omega & \mapsto & X(\omega) + Y(\omega) \end{cases} .$$

La variable $X + Y$ peut être vue comme l'image par $f : (x, y) \mapsto x + y$ du couple (X, Y). La proposition 26 permet alors de déduire calculer la loi de la somme $X + Y$ à l'aide de la loi conjointe de (X, Y).

Proposition 32 (Loi d'une somme)**.**

Soit (X, Y) un couple de variables aléatoires à valeurs réelles défini sur (Ω, P).

$$\forall z \in (X + Y)(\Omega) \quad P(X + Y = z) = \sum_{x \in X(\Omega)} P\left(X = x, Y = z - x\right).$$

Exemple 33 (Les lois conjointes sont différentes mais les lois marginales sont les mêmes)**.**

Calculer la loi de la somme pour les couples (X, Y) puis (X, X) de l'exemple 31

On généralise à des n-uplets de variables aléatoires.

Définition 34.

Soit (Ω, P) un espace probabilisé. Soit $n \in \mathbb{N}^*$ et $X_1, \ldots, X_n$ des variables aléatoires définies sur Ω et à valeurs respectivement dans des ensembles $E_1, \ldots, E_n$.
Le n-uplet $(X_1, \ldots, X_n)$ est une variable aléatoire définie sur Ω et à valeurs dans le produit cartésien $E_1 \times \cdots \times E_n$. Sa loi est appelée **loi conjointe** du n-uplet.

Cette loi est déterminée par la distribution de probabilités

$$\left(P(X_1 = x_1, \ldots, X_n = x_n), \quad x_1 \in X_1(\Omega), \ldots, x_n \in X_n(\Omega)\right).$$

4 Conditionnement.

4.1 Probabilités conditionnelles.

Considérons une expérience aléatoire, modélisée par un espace probabilisé (Ω, P) et un événement A. La probabilité $P(A)$ est la fréquence théorique de réalisation de l'événement A. Supposons que l'on réalise un grand nombre de fois (noté N) l'expérience, les réalisations étant indépendantes entre elles. On note N_A le nombre de fois où A a été réalisé. Si notre espace probabilisé modélise bien la situation, on s'attend à ce que la fréquence de l'événement soit proche de sa probabilité (sa *fréquence a priori*).

$$\frac{N_A}{N} \approx P(A).$$

Considérons maintenant un événement B et notons $N_{A\cap B}$ le nombre de fois que les événements A et B ont été réalisés *en même temps*, lors des N réalisations de l'expérience. Diviser ce nombre par N_B revient à examiner la fréquence de l'événement A *sachant que B est réalisé*. On a

$$\frac{N_{A\cap B}}{N_B} = \frac{N_{A\cap B}/N}{N_B/N} \approx \frac{P(A\cap B)}{P(B)}.$$

Ceci motive la définition suivante.

Pour une approche fréquentiste de la question des probabilités conditionnelles, il sera plus clair, en classe, de considérer un *exemple*.
Tous les matins, il est possible que se réalise l'événement A : « le professeur est en retard ».
Approche probabiliste : on suppose que la situation est correctement modélisée par un espace probabilisé (Ω, P) et que $A \subset \Omega$. On attribue alors à l'événement A sa probabilité $P(A)$.
Approche fréquentiste. On observe le phénomène sur un nombre N de matins consécutifs et on note N_A le nombre de fois où le professeur a été en retard. La fréquence du retard est N_A/N.

Si ce qui se passe un matin donné n'a pas trop d'influence sur les autres retards (le professeur n'a pas trop honte d'être en retard), que N est assez grand, N_A pas trop petit, et le modèle (Ω, P) pas trop mauvais, on s'attend à ce que

$$\frac{N_A}{N} \approx P(A).$$

Soit maintenant l'événement B « il pleut ce matin ». On veut calculer la fréquence des retards *sachant* qu'il pleut. Notons $N_{A\cap B}$ le nombre de matins où le professeur était en retard et où il pleuvait i.e. A et B réalisés *en même temps*, lors des N réalisations de l'expérience. Diviser ce nombre par N_B, nombre de jours de pluie revient bien à examiner fréquence du retard *sachant qu'il pleut*. On a

$$\frac{N_{A\cap B}}{N_B} = \frac{N_{A\cap B}/N}{N_B/N} \approx \frac{P(A\cap B)}{P(B)}.$$

Ceci motive la définition suivante.

Proposition-Définition 35.

Soit (Ω, P) un espace probabilisé, et un événement B tel que $P(B) > 0$. L'application

$$P_B : \begin{cases} \mathcal{P}(\Omega) & \to & \mathbb{R} \\ A & \mapsto & \dfrac{P(A \cap B)}{P(B)} \end{cases}$$

est une probabilité sur Ω.
Pour A un événement, $P_B(A)$ est appelé **probabilité conditionnelle de A sachant B**.
Ce nombre peut aussi être noté $P(A \mid B)$.

Remarques.

1. La définition de $P_B(A)$ n'a de sens que si B n'est pas de probabilité nulle : on dira alors que B est **non négligeable**. En toute rigueur, il faudrait écrire que B est « non P-négligeable ».
2. Si A et B sont deux événements non négligeables d'un espace probabilisé, on peut écrire les deux égalités
$$P(A \cap B) = P_B(A)P(B) \quad \text{et} \quad P(A \cap B) = P_A(B)P(A).$$

Définition 36.

Soit (Ω, P) un espace probabilisé et B un événement tel que $P(B) > 0$. Soit X une variable aléatoire définie sur Ω et à valeurs dans un ensemble E. La distribution de probabilités

$$(P_B(X = x))_{x \in X(\Omega)}$$

définit une unique probabilité sur $X(\Omega)$ appelée **loi de X conditionnellement à B**.

4.2 Trois formules de décomposition.

Convention. Dans les formules suivantes interviennent des quantités de la forme $P(B \mid A)P(A)$. Cette écriture n'a de sens, normalement, que si $P(A) > 0$. Pour ne pas avoir à discuter ce point, on conviendra que

$$P(A \cap B) = P(B \mid A)P(A) \text{ lorsque } P(A) = 0.$$

Proposition 37 (Formule des probabilités composées)**.**

Soit (Ω, P) un espace probabilisé et $A_1, \dots A_n \in \mathcal{P}(\Omega)$. Alors,

$$\boxed{P\left(A_1 \cap \ldots \cap A_n\right) = P(A_1)P_{A_1}\left(A_2\right) P_{A_1 \cap A_2}\left(A_3\right) \cdots P_{A_1 \cap \ldots \cap A_{n-1}}\left(A_n\right)}$$

Exemple 38 (Tirages sans remise)**.**

Une urne contient n boules noires et n boules blanches. On tire successivement, et sans remise n boules dans l'urne. Calculer la probabilité de ne tirer que des boules blanches :

1. à l'aide de la formule des probabilités composées ;
2. en modélisant rigoureusement la situation.

Proposition 39 (Formule des probabilités totales)**.**

Soit (Ω, P) un espace probabilisé et $(A_i)_{i\in[\![1,n]\!]}$ un système complet d'événements.
Pour tout $B \in \mathcal{P}(\Omega)$,

$$\boxed{P(B) = \sum_{i=1}^{n} P\left(B \cap A_i\right)} \quad \text{ou encore} \quad P(B) = \sum_{i=1}^{n} P_{A_i}(B)\, P(A_i).$$

Corollaire 40 (Cas particulier d'un s.c.e. à deux événements)**.**

Soit (Ω, P) un espace probabilisé et A un événement. Pour tout $B \in \mathcal{P}(\Omega)$,

$$P(B) = P(B \cap A) + P(B \cap \overline{A}) = P_A(B)P(A) + P_{\overline{A}}(B)P(\overline{A}).$$

Exemple 41 (Urne de Polya)**.**

On considère une urne contenant initialement une boule blanche et une boule noire.
On répète l'expérience suivante : on tire une boule dans l'urne et on remet cette boule dans l'urne en ajoutant aussi une boule de la même couleur.
Notons, pour $n \geq 1$, X_n le nombre de boules blanches dans l'urne après n tirages.
Montrer que pour tout $n \in \mathbb{N}^*$, X_n suit la loi uniforme sur $\{1, \ldots, n+1\}$.

Proposition 42 (Formules de Bayes)**.**

Soit (Ω, P) un espace probabilisé. Si A et B sont deux événements non négligeables, alors

$$\boxed{P\left(A \mid B\right) = \frac{P\left(B \mid A\right) P(A)}{P(B)}}$$

Exemple 43 (Un test positif)**.**

Un virus est porté par une personne sur mille dans la population. Un test permet de le dépister. Fiable à 99% sur les personnes porteuses du virus, il rend un faux positif dans $0,2\%$ des cas.
On choisit une personne au hasard dans la population et on lui fait faire un test, qui s'avère positif.
Quelle est la probabilité que cette personne soit effectivement porteuse du virus ?

5 Indépendance.

5.1 Événements indépendants.

Commençons par définir l'indépendance de deux événements.

Définition 44.

Soit (Ω, P) un espace probabilisé. On dit que deux événements A et B sont **indépendants** si

$$P(A \cap B) = P(A)P(B).$$

Proposition 45 (Triviale, mais elle permet de comprendre le concept)**.**

Soit (Ω, P) un espace probabilisé et (A, B) un couple d'événements tel que B est non négligeable.

$$A \text{ et } B \text{ sont indépendants} \quad \text{si et seulement si} \quad P_B(A) = P(A).$$

Savoir que B est réalisé ne modifie pas la "fréquence a priori" de A.

Proposition 46.

Soit (Ω, P) un espace probabilisé et deux événements A et B indépendants. Alors,

1. A et $\overline{B}$ sont indépendants.
2. $\overline{A}$ et B sont indépendants.
3. $\overline{A}$ et $\overline{B}$ sont indépendants.

Exemple 47 (Un exemple explicite)**.**

Lançons deux dés équilibrés (un rouge, un vert). Modéliser à l'aide d'un espace probabilisé (Ω, P).
On considère les événements

A : « le résultat rouge est pair », B : « le résultat vert est pair »,

C : « la somme des deux résultats est impaire » D : « la somme des deux résultats vaut 8 ».

Vérifier que A et B sont indépendants. Pourquoi était-ce attendu ?
Vérifier que A et C sont indépendants. Est-ce aussi intuitif que précédemment ?
Vérifier que A et D ne sont pas indépendants. Comparer $P(D)$ et $P_A(D)$.

Définition 48.

Soit (Ω, P) un espace probabilisé, et $(A_i)_{i\in I}$ une famille finie d'événements.
Les événements de cette famille sont dits **indépendants** si

$$\forall J \in \mathcal{P}(I) \setminus \{\emptyset\} \qquad P\left(\bigcap_{j\in J} A_j\right) = \prod_{j\in J} P(A_j).$$

Soit n un entier supérieur à 2 et $(A_1, \ldots, A_n)$ une famille finie d'événements indépendants (l'ensemble d'indices de la définition précédente est ici $I = [\![1, n]\!]$). En prenant $J = I$ dans la définition précédente, on obtient

$$P\left(\bigcap_{i=1}^{n} A_i\right) = \prod_{i=1}^{n} P(A_i).$$

On peut aussi choisir $J = \{k, l\}$ où k et l sont deux entiers distincts de $[\![1, n]\!]$. On obtient alors que

$$P(A_k \cap A_l) = P(A_k)P(A_l).$$

Proposition 49.

Si des événements sont indépendants, ils le sont deux à deux.
La réciproque est fausse : l'indépendance deux à deux n'implique pas l'indépendance.

Proposition 50.

Soit (Ω, P) un espace probabilisé. On considère $(A_i)_{i\in[\![1,n]\!]}$ et $(B_i)_{i\in[\![1,n]\!]}$ deux familles d'événements telles que

$$\forall i \in [\![1, n]\!] \quad B_i \in \{A_i, \overline{A_i}\}.$$

Si les événements de la famille $(A_i)_{i\in[\![1,n]\!]}$ sont indépendants, alors ceux de la famille $(B_i)_{i\in[\![1,n]\!]}$ le sont aussi.

En particulier, $\overline{A_1}, \ldots, \overline{A_n}$ sont indépendants.

5.2 Variables aléatoires indépendantes.

Définition 51.

Soit (Ω, P) un espace probabilisé et X et Y deux variables aléatoires définies sur Ω.
On dit que les variables X et Y sont **indépendantes** (et on note $X \perp\!\!\!\perp Y$) si

$$\forall A \in \mathcal{P}(X(\Omega)) \quad \forall B \in \mathcal{P}(Y(\Omega)) \qquad (X \in A) \text{ et } (Y \in B) \text{ sont indépendants.}$$

Proposition 52.

Soit (Ω, P) un espace probabilisé et X et Y deux variables aléatoires définies sur Ω.
Elles sont indépendantes si et seulement si

$$\forall x \in X(\Omega) \;\; \forall y \in Y(\Omega) \qquad P\left(X = x, Y = y\right) = P(X = x)P(Y = y).$$

Preuve. Voir celle de la proposition 55, qui généralise ce résultat.

Remarque. Pour un couple de variables aléatoires indépendantes, les lois marginales suffisent à calculer la loi conjointe.

Proposition 53 (Images de v.a. indépendantes)**.**

Soit (Ω, P) un espace probabilisé et quatre ensembles $E, \widetilde{E}, F$ et $\widetilde{F}$.
Soient $X : \Omega \to E$ et $Y : \Omega \to \widetilde{E}$ deux variables aléatoires et $f : E \to F$ et $g : \widetilde{E} \to \widetilde{F}$ deux applications.

Si X et Y sont indépendantes, alors $f(X)$ et $g(Y)$ le sont aussi.

Définition 54 (extension à n variables)**.**

Soit (Ω, P) un espace probabilisé et $X_1, \ldots, X_n$ des variables aléatoires toutes définies sur Ω (chacune avec son propre ensemble d'arrivée). Elles sont dites **indépendantes** si pour toute famille d'ensembles $(A_i)_{i\in[\![1,n]\!]} \in \prod_{i=1}^n \mathcal{P}\left(X_i(\Omega)\right)$, les événements de $(X_i \in A_i)_{i\in[\![1,n]\!]}$ sont indépendants.

Proposition 55.

Soit (Ω, P) un espace probabilisé et $X_1, \ldots, X_n$ des variables aléatoires toutes définies sur Ω (chacune avant son propre ensemble d'arrivée). Elles sont indépendantes si et seulement si

$$\forall (x_i)_{i\in[\![1,n]\!]} \in \prod_{i=1}^n X_i(\Omega) \qquad P\left(\bigcap_{i=1}^n (X_i = x_i)\right) = \prod_{i=1}^n P(X_i = x_i).$$

La preuve de la proposition 55 est donnée en annexe.

Remarque. Pour vérifier que des variables aléatoires sont indépendantes, on passera toujours par la caractérisation donnée par la proposition 55. En, effet, travailler avec la définition 54 nous obligerait à manipuler la définition 48 de l'indépendance d'une famille d'événements, peu commode à cause du « $\forall J \in \mathcal{P}([\![1, n]\!]) \backslash \{\emptyset\}$ ».

Exemple 56.

Soit (Ω, P) un espace probabilisé et X et Y deux variables aléatoires indépendantes, toutes deux suivant la loi de Bernoulli de paramètre $1/2$. On pose $Z = |X - Y|$. Loi de Z ?
Vérifier que X, Y et Z sont indépendantes deux à deux mais ne sont pas indépendantes.

Proposition 57 (Somme de variables de Bernoulli indépendantes).

Soient $n \in \mathbb{N}^*$ et $p \in [0,1]$.
Si $X_1, \dots, X_n$ sont des variables aléatoires indépendantes, toutes de loi $\mathscr{B}(p)$, alors la variable $X_1 + \cdots X_n$ suit la loi binomiale $\mathscr{B}(n,p)$.

Proposition 58 (Lemme des coalitions).

Soit (Ω, P) un espace probabilisé et $X_1, \dots, X_n$ des variables aléatoires définies sur Ω et respectivement à valeurs dans des ensembles $E_1, \dots, E_n$. Soit un entier $m \in [\![1, n]\!]$.
Soient deux applications f_1, définie sur $E_1 \times \cdots \times E_m$, et f_2, définie sur $E_{m+1} \times \cdots E_n$. On pose

$$Y_1 = f_1(X_1, \dots, X_m) \quad \text{et} \quad Y_2 = f_2(X_{m+1}, \dots, X_n).$$

$$\boxed{\text{Si les } n \text{ variables } X_1, \dots, X_n \text{ sont indépendantes, alors les deux variables } Y_1 \text{ et } Y_2 \text{ aussi.}}$$

Proposition 59 (extension à p coalitions).

Soit (Ω, P) un espace probabilisé et $(X_i)_{i \in I}$ une famille de variables aléatoires indexée par un ensemble fini et non vide I. Soit $p \in \mathbb{N}^*$ et $(J_k)_{k \in [\![1,p]\!]}$ une partition de l'ensemble I. On pose

$$\forall k \in [\![1, p]\!] \quad Y_k = f_k\left((X_j)_{j \in J_k}\right),$$

où les p fonctions f_k sont définies telles que les composées aient un sens.

Si les n variables $X_1, \dots, X_n$ sont indépendantes, alors les p variables $Y_1, \dots, Y_p$ le sont aussi.

Pour terminer, un résultat d'existence, prouvé en annexe .

Théorème 60 (Existence de n variables aléatoires indépendantes, de lois prescrites).

Soient $n \in \mathbb{N}^*$ et $(\Omega_1, P_1), \dots, (\Omega_n, P_n)$ des espaces probabilisés finis. Alors, il existe un espace probabilisé fini (Ω, P) et $X_1, \dots, X_n$ des variables aléatoires définies sur Ω telles que

$$X_1, \dots, X_n \text{ sont indépendantes} \quad \text{et} \quad \text{pour tout } i \in [\![1, n]\!] \ X_i \text{ est de loi } P_i.$$

Annexe : quelques preuves.

Preuve de la proposition 15. Soit Ω un univers fini et $(p_\omega, \omega \in \Omega)$ une distribution de probabilités sur Ω.

<u>Analyse</u>. Supposons qu'il existe une probabilité P définie sur Ω telle que $\forall \omega \in \Omega \quad P(\{\omega\}) = p_\omega$.
Soit A un événement. On peut l'écrire comme la réunion de ses singletons :

$$A = \bigcup_{\omega \in A} \{\omega\}.$$

Passons aux probabilités :

$$P(A) = P\left(\bigcup_{\omega \in A} \{\omega\}\right) = \sum_{\omega \in A} P(\{\omega\}) = \sum_{\omega \in A} p_\omega.$$

Ceci implique l'unicité de la probabilité P si elle existe.

Synthèse. Posons $P : \left\{ \begin{array}{ccc} \mathcal{P}(\Omega) & \to & [0,1] \\ A & \mapsto & \sum\limits_{\omega \in A} p_\omega \end{array} \right.$, et vérifions que P est une probabilité.

- Vérifions d'abord que P prend ses valeurs dans $[0,1]$.
  Si $A \in \mathcal{P}(\Omega)$, on a, pour tout $\omega \in \Omega$, $0 \leq \mathbf{1}_A(\omega) \leq 1$, donc $0 \leq p_\omega \mathbf{1}_A(\omega) \leq p_\omega$. Sommons :

$$\underbrace{\sum_{\omega \in \Omega} p_k \cdot 0}_{0} \;\leq\; \underbrace{\sum_{\omega \in \Omega} p_\omega \mathbf{1}_A(\omega)}_{P(A)} \;\leq\; \underbrace{\sum_{\omega \in \Omega} p_\omega \cdot 1}_{1}.$$

- $P(\Omega) = \sum\limits_{\omega \in \Omega} p_\omega = 1.$
- Soient A et B deux événements incompatibles : $A, B \in \mathcal{P}(\Omega) : A \cap B = \emptyset$.

$$P(A \cup B) = \sum_{\omega \in A \cup B} p_\omega \underset{A \cap B = \emptyset}{=} \sum_{\omega \in A} p_\omega + \sum_{\omega \in B} p_\omega = P(A) + P(B).$$

Conclusion. Il existe bien une unique probabilité P sur Ω telle que $\forall \omega \in \Omega\ P(\{\omega\}) = p_\omega$. $\square$

Preuve de la proposition 55.

Soient $X_1, \dots, X_n$ des variables aléatoires définies sur un même espace probabilisé (Ω, P).

• Supposons que $X_1, \dots, X_n$ sont indépendantes. Soit $(x_i)_{i \in [\![1,n]\!]} \in \prod_{i=1}^n X_i(\Omega)$. De la définition, il vient que les événements $(X_1 = x_1), \dots, (X_n = x_n)$ sont indépendants, de sorte qu'on a bien

$$P\left(\bigcap_{i=1}^n (X_i = x_i)\right) = \prod_{i=1}^n P(X_i = x_i).$$

• Réciproquement, supposons l'égalité précédente vraie pour toute famille $(x_i)_{i \in [\![1,n]\!]} \in \prod_{i=1}^n X_i(\Omega)$.
Soit J une partie de $[\![1, n]\!]$, non vide, et une famille d'événements $A_j \in \prod_{j \in J} \mathcal{P}(X_j(\Omega))$.
On va vérifier que $P\left(\bigcap\limits_{i \in J} (X_j \in A_j)\right) = \prod\limits_{j \in J} P(X_j \in A_j)$. Commençons par "compléter" l'intersection :

$$\bigcap_{i \in J} (X_j \in A_j) = \bigcap_{i=1}^n (X_i \in A_i^*) \qquad \text{où} \quad \forall i \in [\![1, n]\!] \ \ A_i^* = \begin{cases} A_i & \text{si } i \in J \\ X_i(\Omega) & \text{si } i \notin J \end{cases}$$

Ainsi,

$$\bigcap_{i \in J} (X_j \in A_j) = \bigcap_{i=1}^n \bigcup_{x_i \in A_i^*} (X_i = x_i) = \bigcup_{x_1 \in A_1^*} \bigcup_{x_2 \in A_2^*} \cdots \bigcup_{x_n \in A_n^*} \bigcap_{i=1}^n (X_i = x_i).$$

On a donc

$$\begin{aligned} P\left(\bigcap_{i \in J} (X_j \in A_j)\right) &\underset{union\ disjointe}{=} \sum_{x_1 \in A_1^*} \sum_{x_2 \in A_2^*} \cdots \sum_{x_n \in A_n^*} P\left(\bigcap_{i=1}^n P(X_i = x_i)\right) \\ &\underset{hypotèse}{=} \sum_{x_1 \in A_1^*} \sum_{x_2 \in A_2^*} \cdots \sum_{x_n \in A_n^*} \prod_{i=1}^n P(X_i = x_i) \\ &= \left(\sum_{x_1 \in A_1^*} P(X_1 = x_1)\right) \cdots \left(\sum_{x_n \in A_n^*} P(X_n = x_n)\right) \end{aligned}$$

Or, pour tout $i \in [\![1, n]\!]$,

$$\sum_{x_i \in A_i^*} P(X_i = x_i) = \begin{cases} \sum\limits_{x_i \in A_i} P(X_i = x_i) = P(A_i) & \text{si } i \in J \\ \sum\limits_{x_i \in X_i(\Omega)} P(X_i = x_i) = 1 & \text{si } i \notin J \end{cases}$$

On a bien

$$P\left(\bigcap_{i \in J} (X_j \in A_j)\right) = \prod_{j \in J} P(X_j \in A_j).$$

Les variables $X_1, \dots, X_n$ sont bien indépendantes. $\square$

Preuve du théorème 60.

Soient $n \in \mathbb{N}^*$ et $(\Omega_1, P_1), \dots, (\Omega_n, P_n)$ des espaces probabilisés finis. Posons $\Omega = \Omega_1 \times \cdots \times \Omega_n$. On définit alors $X_1, \dots, X_n$ par

$$\forall i \in [\![1, n]\!] \quad X_i : \left\{ \begin{array}{ccc} \Omega & \to & \Omega_i \\ (\omega_1, \dots, \omega_n) & \mapsto & \omega_i \end{array} \right. .$$

On va définir sur Ω une probabilité qui fait de $X_1, \dots, X_n$ des variables aléatoires indépendantes de lois respectives $P_1, \dots, P_n$. Pour cela, posons

$$\forall \omega = (\omega_1, \dots, \omega_n) \in \Omega \qquad p_\omega := \prod_{i=1}^n P_i\left(\{\omega_i\}\right).$$

La famille $(p_\omega)_{\omega \in \Omega}$ est une distribution de probabilités. En effet, il s'agit d'une famille de réels positifs tels que

$$\sum_{\omega \in \Omega} p_\omega = \sum_{\omega_1 \in \Omega_1} \cdots \sum_{\omega_n \in \Omega_n} \prod_{i=1}^n P_i\left(\{\omega_i\}\right) = \prod_{i=1}^n \underbrace{\left(\sum_{\omega_i \in \Omega_i} P_i\left(\{\omega_i\}\right) \right)}_{=1} = 1.$$

Notons P l'unique probabilité « sur Ω » (en fait sur $\mathcal{P}(\Omega)$) déterminée par cette distribution de probabilités.

• Fixons d'abord un entier $i \in [\![1, n]\!]$ et un élément $x \in \Omega_i$. On a

$$(X_i = x) = \Omega_1 \times \cdots \Omega_{i-1} \times \{x\} \times \Omega_i \cdots \times \Omega_n$$

D'autre part, $(X_i = x) = \bigcup\limits_{\omega \in (X_i = x)} \{\omega\}$. D'où

$$\begin{aligned}
P(X_i = x) &= \sum_{\omega \in (X_i = x)} \underbrace{P\left(\{\omega\}\right)}_{=p_\omega} \\
&= \sum_{(\omega_1, \dots, \omega_n) \in (X_i = x)} P_1\left(\{\omega_1\}\right) \cdots P_i\left(\{x\}\right) \cdots P_n\left(\{\omega_n\}\right) \\
&= \left(\sum_{\omega_1 \in \Omega_1} P(\{\omega_1\}) \right) \cdots \left(\sum_{\omega_{i-1} \in \Omega_{i-1}} P(\{\omega_{i-1}\}) \right) \cdot P_i(\{x\}) \cdot \left(\sum_{\omega_{i+1} \in \Omega_{i+1}} P(\{\omega_{i+1}\}) \right) \cdots \left(\sum_{\omega_n \in \Omega_n} P(\{\omega_n\}) \right) \\
&= P_i(\{x\}), \quad \text{les autres facteurs étant des sommes égales à 1.}
\end{aligned}$$

On a donc vérifié que X_i avait pour loi P_i.

• Soit $(x_i)_{i \in [\![1,n]\!]}$. La définition de Ω et des X_i étant ce qu'elle est, l'événement $\bigcap\limits_{i=1}^n (X_i = x_i)$ est simplement le singleton $\{(x_1, \dots, x_n)\}$. Ainsi,

$$P\left(\bigcap_{i=1}^n (X_i = x_i) \right) = P\left(\{(x_1, \dots, x_n)\}\right) = \prod_{i=1}^n P_i\left(\{x_i\}\right) = \prod_{i=1}^n P(X_i = x_i).$$

Ceci démontre que les variables $X_1, \dots, X_n$ sont indépendantes, ce qui achève la preuve du théorème. $\square$

Exercices.

Expériences aléatoires et leur modélisation.
Dans les exercices de ce paragraphe, une *modélisation* de la situation est attendue : à nous de proposer un espace probabilisé (Ω, P) adéquat.

$\boxed{\textbf{39.1}}$ **[♦◇◇]** (Facile !) Une urne contient cinq boules blanches et cinq boules noires.
On tire simultanément trois boules dans l'urne. Quelle est la probabilité de tirer trois boules noires ?

$\boxed{\textbf{39.2}}$ **[♦♦◇]** Soit n un entier supérieur à 3. On place aléatoirement n boules dans n urnes.
Quelle est la probabilité qu'une urne exactement demeure vide ?

$\boxed{\textbf{39.3}}$ **[♦♦◇]** On mélange un jeu de $2n$ cartes numérotées de 1 à $2n$.
Quelle est la probabilité pour que les cartes de numéro impair soient correctement ordonnées ?

$\boxed{\textbf{39.4}}$ **[♦♦◇]** Paradoxe des anniversaires.
48 MP2I jeunes et fringants arriveront à PV en septembre 2025. Quelle est la probabilité pour que deux d'entre eux aient la même date d'anniversaire ?

$\boxed{\textbf{39.5}}$ **[♦♦♦]** Inspirons.
Démontrer qu'il y a plus d'une chance sur cent que dans la bouffée d'air qui entre dans nos poumons, se trouve une des molécules de dioxygène expirée par Jules César en disant « *Tu quoque fili* ».
Données physiques : l'atmosphère contient environ 10^{44} molécules de dioxygène et chacune de nos inspirations en contient $2 \cdot 10^{22}$.

Calculs de probabilités
Dans les exercices ci-dessous, on travaille avec un espace probabilisé (Ω, P) qu'on n'aura pas besoin d'expliciter. Lorsqu'il est question de situation concrète, on considèrera que la modélisation de l'expérience aléatoire a été faite correctement.

$\boxed{\textbf{39.6}}$ **[♦◇◇]** (Facile !) Soit (Ω, P) un espace probabilisé et X une variable aléatoire définie sur Ω, telle que $X(\Omega) = \{0, 1, 2, 3\}$ telle que $P(X = 0) = P(X = 1)$, $P(X \leq 1) = \frac{1}{4}$ et $P(X \leq 2) = \frac{2}{3}$. Donner la loi de X.

$\boxed{\textbf{39.7}}$ **[♦◇◇]** Soit X une variable aléatoire de loi uniforme sur $\{-1, 0, 1\}$ et soit M la *matrice aléatoire*

$$M = \begin{pmatrix} 1 & 1 \\ 1 & X \end{pmatrix}$$

Donner la loi du rang de X.

$\boxed{\textbf{39.8}}$ **[♦♦◇]** Une urne contient n boules noires et n boules blanches. On tire les boules de l'urne deux par deux. Calculer p_n, la probabilité d'avoir à chaque tirage une boule blanche et une boule noire.
Calculer un équivalent de p_n.

39.9 **[♦◇◇]** Soient $(n+1)$ urnes $U_0, U_1, \ldots, U_n$. L'urne U_k contient k boules rouges et $n-k$ noires. On choisit une urne au hasard et on tire une boule de l'urne. On suppose la situation correctement modélisée par un espace probabilisé (Ω, P) qu'on ne cherchera pas à connaître.

1. Quelle est la probabilité que la boule tirée soit rouge ? Commenter.
2. Soit $k \in [\![0, n]\!]$. Quelle est la probabilité d'avoir choisi l'urne U_k sachant que la boule tirée est rouge ?

39.10 **[♦◇◇]** On considère un dé pipé, truqué de manière à ce que la fréquence d'apparition de chaque face soit proportionnelle au numéro de la face. Plus précisément, il existe un réel α telle que la fréquence d'apparition de $k \in \{1, \ldots, 6\}$ vaut $\alpha \cdot k$.

1. Que vaut α ?
2. On lance ce dé plusieurs fois. Pour $n \in \mathbb{N}^*$, on s'intéresse à l'événement

   A_n l'événement « la somme des n premiers lancers est paire ».

   Supposons que la situation est correctement modélisée par un espace probabilisé (Ω, P) que l'on ne cherchera pas à connaître. On note $p_n = P(A_n)$.
   (a) Soit $n \in \mathbb{N}^*$. Exprimer p_{n+1} à l'aide de p_n.
   (b) Donner le terme général de la suite (p_n) ainsi que sa limite si elle existe.

39.11 **[♦♦◇]** À Gotham City, il y a 80% de taxis jaunes, les autres sont verts. Il y a trois mois un homme est mort, renversé par un taxi qui a pris la fuite (Batman télétravaillait). Un témoin déclare avoir vu un taxi vert. Mais c'était la nuit, et le témoin a pu se tromper sur la couleur. Des tests visuels sont organisés et on découvre que le témoin se trompe sur la couleur du taxi dans 20% des cas.
Un chauffeur de taxi vert est sur le banc des accusés, et vous êtes son avocat.
Écrire une plaidoirie dont le but sera d'écarter le témoignage gênant.

Probabilité sur un univers fini

39.12 Soit $(A_i)_{1 \leq i \leq n}$ une famille d'événements d'un espace probabilisé (Ω, P). Démontrer que

$$P\left(\bigcup_{k=1}^{n} A_k\right) \leq \sum_{k=1}^{n} P(A_k) \leq P\left(\bigcap_{k=1}^{n} A_k\right) + n - 1.$$

Indépendance

39.13 **[♦◇◇]** Soit (Ω, P) un espace probabilisé et $A_1, \ldots, A_n$ des événements indépendants. Montrer que

$$A_1 \cup \ldots \cup A_n = \Omega \implies (\exists i \in [\![1, n]\!] \; P(A_i) = 1)$$

39.14 **[♦◇◇]** Soient X et Y deux variables aléatoires définies sur un même espace probabilisé (Ω, P). On suppose qu'elles sont indépendantes et suivent toutes deux la loi uniforme sur $[\![-n, n]\!]$.

1. Calculer $P(X = Y)$.
2. Calculer $P(X^2 = Y^2)$.

39.15 **[♦♦◇]** Soit n un entier supérieur à 3. Sur un même espace probabilisé (Ω, P), on considère A et B deux variables indépendantes et de loi uniforme sur $[\![1, n]\!]$. Calculer $P\left(A^B \leq B^A\right)$.

39.16 **[♦♦◇]** Soient $X_1, \ldots, X_n$ n variables aléatoires indépendantes de loi de Bernoulli $\mathcal{B}(1/2)$.
Pour $k \in [\![1, n-1]\!]$, on note $A_k = \{X_k \neq X_{k+1}\}$.

1. Montrer que les événements (A_k) sont deux à deux indépendants.
2. *Plus difficile* : montrer que les événements (A_k) sont indépendants.

39.17 **[♦♦◊]** Somme de binomiales indépendantes
Soient $n, n' \in \mathbb{N}^*$ et $p \in [0,1]$.
On considère X et Y deux variables aléatoires définies sur un espace probabilisé (Ω, P) telles que $X \sim \mathscr{B}(n,p)$, que $Y \sim \mathscr{B}(n',p)$ et telles que X et Y sont indépendantes. Montrer que $X+Y \sim \mathscr{B}(n+n',p)$.

39.18 **[♦♦◊]** Soient X et Y deux variables aléatoires définies sur un même espace probabilisé (Ω, P), indépendantes et suivant toutes deux la loi uniforme sur $[\![1,n]\!]$.

1. Calculer la loi de $U = \min(X,Y)$ et de $V = \max(X,Y)$.
   Idée à retenir : commencer par le calcul des probabilités de la forme $P(V \leq k)$.
2. Justifier que U et V ne sont pas indépendantes.

39.19 **[♦♦◊]** Soit (Ω, P) un espace probabilisé fini et X et Y deux variables aléatoires indépendantes et de même loi. Justifier que $X-Y$ et $Y-X$ ont même loi.

39.20 **[♦♦♦]** Dans cet exercice, n est un entier naturel supérieur à 2.
Soit (Ω, P) un espace probabilisé et n variables aléatoires $X_1, \ldots, X_n$ indépendantes, toutes de loi uniforme sur $[\![1,n]\!]$. On note

$$\forall i \in [\![1,n]\!], \quad Y_i = \mathrm{Card}\{j \in [\![1,n]\!] \ / \ X_j = i\}$$

1. Soit $i \in [\![1,n]\!]$. Quelle est la loi de Y_i ?
   idée (à retenir) : écrire Y_i comme une somme de variables aléatoires.
2. Soient $(i,j,k) \in [\![1,n]\!]^3$ tel que $i \neq j$.
   Déterminer la loi de Y_j conditionnellement à $(Y_i = k)$.

39.21 **[♦♦♦]** Oral Mines-Ponts MP 2023
Soit (J_n) une suite de joueurs. Le joueur J_0 affronte le joueur J_1 ; le gagnant affronte J_2, puis le gagnant de ce nouveau match affronte J_3 et ainsi de suite.
Lors d'un match, le joueur entrant a une probabilité $p \in]0,1[$ de remporter le match. Le jeu termine lorsqu'un même joueur remporte trois victoires.
Pour $n \in \mathbb{N}^*$, on note A_n l'événement « le n-ième match est joué ».
Déterminer la limite de $P(A_n)$ quand $n \to +\infty$.
On admettra l'existence d'un espace probabilisé (Ω, P) sur lequel sont bien définis tous les événements de l'exercice. Cet espace ne saurait être fini, mais on fait comme si (en attendant le cours de spé).

Espaces préhilbertiens

Dans ce chapitre, E désignera un $\mathbb{R}$-espace vectoriel et on insiste sur le fait que les scalaires sont réels. Les notions de produit scalaire ou d'orthogonalité sur les $\mathbb{C}$-espaces vectoriels sont hors-programme.

1 Produits scalaires

Définition 1 (Produit scalaire)**.**

On appelle **produit scalaire** sur E toute application

$$\langle\cdot,\cdot\rangle : \left\{\begin{array}{ccc} E\times E & \to & \mathbb{R} \\ (x,y) & \mapsto & \langle x,y\rangle \end{array}\right. ,$$

- bilinéaire : $\forall (x,x',y,y')\in E^4 \quad \forall(\lambda,\mu)\in\mathbb{R}^2 \quad \left\{\begin{array}{ccc} \langle \lambda x+\mu x', y\rangle & = & \lambda\langle x,y\rangle+\mu\langle x',y\rangle \\ \langle x, \lambda y+\mu y'\rangle & = & \lambda\langle x,y\rangle+\mu\langle x,y'\rangle. \end{array}\right.$
- symétrique : $\forall x,y\in E \quad \langle x,y\rangle=\langle y,x\rangle$.
- définie : $\forall x\in E \quad \langle x,x\rangle=0 \Longrightarrow x=0_E$.
- positive : $\forall x\in E \quad \langle x,x\rangle\geq 0$.

Pour x et y deux vecteurs de E, $\langle x,y\rangle$ est un nombre réel, appelé produit scalaire de x et y.

Autres notations utilisées pour définir des produits scalaires : $(x,y)\mapsto(x\mid y)$ ou encore $(x,y)\mapsto x\cdot y$.

Définition 2 (Espaces préhilbertiens, euclidiens)**.**

Si $\langle\cdot,\cdot\rangle$ est un produit scalaire sur E, le couple $(E,\langle\cdot,\cdot\rangle)$ est appelé **espace préhilbertien**.
Un espace préhilbertien de dimension finie est appelé **espace euclidien**.

Sur $\mathbb{R}^n/M_{n,1}(\mathbb{R})$.

Cet exemple est fondamental car tous les $\mathbb{R}$-espaces vectoriels de dimension n peuvent être « identifiés » à $\mathbb{R}^n$ (il suffit de travailler avec les coordonnées sur une base).

Proposition 3.

L'application $\langle \cdot, \cdot \rangle$ qui à $x = (x_1, \dots, x_n)$ et $y = (y_1, \dots, y_n)$ associe

$$\langle x, y \rangle := \sum_{i=1}^{n} x_i y_i,$$

est un produit scalaire sur $\mathbb{R}^n$, dit **produit scalaire canonique**.

Quitte à identifier $\mathbb{R}^n$ et $M_{n,1}(\mathbb{R})$ (on écrit les n-uplets comme des matrices colonnes), on peut calculer le produit scalaire canonique à l'aide d'un produit matriciel :

$$\forall X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad \forall Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \qquad \boxed{\langle X, Y \rangle = X^\top Y}.$$

Lorsqu'on parlera de « l'espace euclidien $\mathbb{R}^n$ » sans expliciter le produit scalaire, c'est au produit scalaire canonique que l'on fait référence. Il y en a d'autres !

On retrouve pour $n = 2$ le produit scalaire sur $\mathbb{R}^2$ avec lequel on travaillait en terminale :

$$(x, y) \cdot (x', y') = xx' + yy'.$$

et pour $n = 3$ celui sur $\mathbb{R}^3$ que l'on connaissait aussi et que l'on utilise en physique :

$$(x, y, z) \cdot (x', y', z') = xx' + yy' + zz'.$$

Sur $M_{n,p}(\mathbb{R})$.

Proposition 4.

L'application $\langle \cdot, \cdot \rangle$ qui à deux matrices $A = (a_{i,j})$ et $B = (b_{i,j})$ de matrices de $M_{n,p}(\mathbb{R})$ associe

$$\langle A, B \rangle = \sum_{i=1}^{n} \sum_{j=1}^{p} a_{i,j} b_{i,j}.$$

est un produit scalaire sur $M_{n,p}(\mathbb{R})$, dit **produit scalaire canonique**.

On peut exprimer le produit scalaire de A et B ainsi :

$$\boxed{\langle A, B \rangle = \operatorname{tr}(A^\top B)}.$$

Sur $\mathcal{C}([a,b],\mathbb{R})$.

Proposition 5.

Soient deux réels a et b tels que $\boxed{a < b}$.
L'application $\langle \cdot, \cdot \rangle$ qui à un couple (f,g) de fonctions de $\mathcal{C}([a,b],\mathbb{R})$ associe

$$\langle f, g \rangle = \int_a^b f(t)g(t)\mathrm{d}t,$$

est un produit scalaire sur $\mathcal{C}([a,b],\mathbb{R})$.

Muni de ce produit scalaire, $\mathcal{C}([a,b],\mathbb{R})$ est un espace préhilbertien.

Sur $\mathbb{R}[X]$.

L'application qui à un couple de polynômes $(P,Q) \in \mathbb{R}[X]^2$ tels que $P = \sum a_n X^n$ et $Q = \sum b_n X^n$ associe

$$\langle P, Q \rangle = \sum_{n=0}^{+\infty} a_n b_n$$

est un produit scalaire sur $\mathbb{R}[X]$, assez analogue au produit scalaire canonique sur $\mathbb{R}^n$ (on fait le produit des coordonnées et on somme...) On rappelle que la somme ci-dessus compte un nombre fini de termes non nuls.

Exemple 6 (Un produit scalaire intégral sur l'espace des polynômes)**.**

Pour P et Q deux polynômes de $\mathbb{R}[X]$, on note

$$\langle P, Q \rangle = \int_0^1 P(t)Q(t)\mathrm{d}t.$$

Vérifier que l'application $\langle \cdot, \cdot \rangle$ est un produit scalaire sur $\mathbb{R}[X]$.

2 Norme associée à un produit scalaire.

On considère dans cette partie un produit scalaire $\langle \cdot, \cdot \rangle$ sur E.

Définition 7.

On appelle **norme associée au produit scalaire** $\langle \cdot, \cdot \rangle$ l'application

$$\|\cdot\| : \left\{ \begin{array}{ccl} E & \to & \mathbb{R}_+ \\ x & \mapsto & \|x\| := \sqrt{\langle x, x \rangle} \end{array} \right. .$$

L'an prochain, dans le cours Espaces vectoriels normés, vous travaillerez avec des normes non forcément définies à partir d'un produit scalaire.

Exemple 8.

Pour tout $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, la norme (associée au produit scalaire canonique) de x vaut

$$\|x\| = \sqrt{\sum_{i=1}^{n} x_i^2}.$$

Cette norme est souvent écrite en physique dans les cas $n = 2$ et $n = 3$:

$$\text{Pour } \overrightarrow{u}(x,y) \quad \|\overrightarrow{u}\| = \sqrt{x^2+y^2} \qquad \text{et pour } \overrightarrow{v}(x,y,z) \quad \|\overrightarrow{v}\| = \sqrt{x^2+y^2+z^2}.$$

Autres exemples : la norme d'une fonction $f \in \mathcal{C}([a,b], \mathbb{R})$ lorsque cette norme est associée au produit scalaire défini plus haut :

$$\|f\| = \sqrt{\int_a^b f^2(t)\mathrm{d}t},$$

ou encore pour une matrice $A \in M_{n,p}(\mathbb{R})$ sa norme associée au produit scalaire canonique :

$$\|A\| = \sqrt{\mathrm{tr}(A^\top A)}.$$

Proposition 9 (Faits élémentaires)**.**

Soit $\|\cdot\|$ la norme associée au produit scalaire $\langle \cdot, \cdot \rangle$ sur E.

1. Le vecteur nul a pour norme 0 et c'est le seul vecteur dans ce cas (propriété de *séparation*) :
$$\|0_E\| = 0 \qquad \text{et} \qquad \forall x \in E \quad \|x\| = 0 \Longrightarrow x = 0_E.$$
2. Pour tout $x \in E$, pour tout λ réel, on a $\|\lambda x\| = |\lambda| \cdot \|x\|$ (propriété d'*homogénéité*).
3. Si x est un vecteur non nul, le vecteur $\dfrac{1}{\|x\|}x$ est de norme 1. On le note aussi $\dfrac{x}{\|x\|}$

Proposition 10 (Identités remarquables)**.**

Soit $\|\cdot\|$ la norme associée au produit scalaire $\langle \cdot, \cdot \rangle$ sur E. Soient deux vecteurs x et y.

1. <u>Identités remarquables</u> :
$$\|x+y\|^2 = \|x\|^2 + 2\langle x, y\rangle + \|y\|^2 \qquad \text{et} \qquad \|x-y\|^2 = \|x\|^2 - 2\langle x, y\rangle + \|y\|^2$$
2. <u>Identité du parallélogramme</u> :
$$\|x+y\|^2 + \|x-y\|^2 = 2\left(\|x\|^2 + \|y\|^2\right).$$
3. <u>Identité de polarisation</u> :
$$\langle x, y\rangle = \frac{1}{4}\left(\|x+y\|^2 - \|x-y\|^2\right).$$
utile si on a un renseignement sur les normes et que l'on veut parler de produit scalaire.

Exemple 11 (avec n vecteurs)**.**

Développer $\left\|\sum_{k=1}^{n} x_k\right\|^2$, pour n vecteurs $x_1, \dots x_n$ d'un espace préhilbertien $(E, \langle\cdot,\cdot\rangle)$.

Théorème 12 (Inégalité de Cauchy-Schwarz)**.**

Soit $\|\cdot\|$ la norme associée au produit scalaire $\langle\cdot,\cdot\rangle$ sur E. Alors,

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

Cette inégalité est une égalité ssi (x,y) est liée, c'est-à-dire ssi $y = 0_E$ ou $\exists \alpha \in \mathbb{R} : x = \alpha y$.

Exemple 13 (Des inégalités de Cauchy-Schwarz écrites au carré)**.**

- Soient $(a_1, \dots, a_n) \in \mathbb{R}^n$ et $(b_1, \dots, b_n) \in \mathbb{R}^n$. En utilisant le produit scalaire canonique,

$$\left(\sum_{i=1}^{n} a_i bi\right)^2 \leq \left(\sum_{i=1}^{n} a_i^2\right)\left(\sum_{i=1}^{n} b_i^2\right).$$

- Soient f et g dans $\mathcal{C}([a,b],\mathbb{R})$. En utilisant le produit scalaire de la proposition 5,

$$\left(\int_a^b f(t)g(t)\mathrm{d}t\right)^2 \leq \left(\int_a^b f(t)^2\mathrm{d}t\right)\left(\int_a^b g(t)^2\mathrm{d}t\right).$$

Proposition 14 (Inégalité triangulaire)**.**

Soit $\|\cdot\|$ la norme associée au produit scalaire $\langle\cdot,\cdot\rangle$ sur E. Alors,

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

Il s'agit d'une égalité ssi x et y sont positivement liés, c'est-à-dire ssi $y = 0_E$ ou $\exists \alpha \in \mathbb{R}_+ : x = \alpha y$.

Corollaire 15.

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

Définition 16.

Soit $\|\cdot\|$ la norme associée au produit scalaire $\langle\cdot,\cdot\rangle$ sur E.
On appelle **distance euclidienne** entre deux vecteurs x et y de E le nombre positif

$$d(x,y) = \|x - y\|.$$

3 Orthogonalité.

On considère toujours dans cette partie un produit scalaire $\langle \cdot, \cdot \rangle$ sur E et on note $\|\cdot\|$ la norme associée.

3.1 Vecteurs orthogonaux, familles orthogonales.

Définition 17.

Deux vecteurs d'un espace préhilbertien sont dits **orthogonaux** si leur produit scalaire est nul.

Exemples 18.

- Couples de vecteurs orthogonaux de $\mathbb{R}^2$ pour le produit scalaire canonique.
- Dans l'espace préhilbertien $\mathcal{C}([0, 2\pi], \mathbb{R})$ muni du produit scalaire de la proposition 5, les vecteurs cos et sin sont orthogonaux.
- Diagonales d'un losange, dans un espace préhilbertien quelconque : si x et y ont même norme, alors $x + y$ et $x - y$ sont orthogonaux.

Proposition 19.

Le vecteur nul est orthogonal à tous les vecteurs d'un espace préhilbertien, et seul dans ce cas.

Définition 20.

Soit $(x_1, \ldots, x_n) \in E^n$ une famille de vecteurs de l'espace préhilbertien E.

On dit que c'est une **famille orthogonale** si les vecteurs de cette famille sont orthogonaux deux à deux :

$$\forall 1 \leq i, j \leq n \quad i \neq j \Longrightarrow \langle x_i, x_j \rangle = 0.$$

On parle de **famille orthonormée** (ou orthonormale) si en plus, tous les vecteurs de la famille sont de norme 1, i.e.

$$\forall 1 \leq i \leq n \quad \|x_i\| = 1.$$

Proposition 21.

Soit $(x_1, \ldots, x_n) \in E^n$.

$$(x_1, \ldots, x_n) \text{ est orthonormée} \quad \Longleftrightarrow \quad \forall i, j \in [\![1, n]\!] \quad \langle x_i, x_j \rangle = \delta_{i,j}.$$

Exemples. La base canonique de $\mathbb{R}^n$ est orthonormée pour le produit scalaire canonique $(X, Y) \mapsto X^\top Y$.

La base canonique de $M_{n,p}(\mathbb{R})$ est orthonormée pour le produit scalaire canonique $(A, B) \mapsto \operatorname{Tr}(A^\top B)$.

Proposition 22 (Renormalisation).

Si $(x_1, \dots, x_n)$ est une famille orthogonale de E, constituée de vecteurs non nuls, on peut poser

$$\forall i \in [\![1, n]\!] \quad e_i := \frac{x_i}{\|x_i\|}.$$

Alors, la famille $(e_1, \dots, e_n)$ est une famille orthonormée.

Proposition 23.

Une famille orthogonale formée de vecteurs non nuls est libre.

Notamment, les familles orthonormées sont libres.

Proposition 24 (Théorème de Pythagore).

Soit $(x_1, \dots, x_n)$ une famille orthogonale d'un espace préhilbertien pour lequel on note $\|\cdot\|$ la norme associée au produit scalaire. Alors,

$$\left\| \sum_{i=1}^{n} x_i \right\|^2 = \sum_{i=1}^{n} \|x_i\|^2.$$

3.2 Orthogonal d'une partie.

Définition 25.

Soit X une partie de E. On appelle **orthogonal** de X, et on note $X^\perp$ l'ensemble des vecteurs orthogonaux à tous les éléments de X, c'est-à-dire

$$X^\perp = \{y \in E : \quad \forall x \in X, \quad \langle x, y \rangle = 0\}.$$

On a clairement $\{0_E\}^\perp = E$. La proposition 19 donne que si E est un espace préhilbertien, alors $E^\perp = \{0_E\}$.

Exemple 26 (Conséquences immédiates de la définition).

Si X et Y sont deux parties de E,

1. $X \subset Y \implies Y^\perp \subset X^\perp$.
2. $X \subset (X^\perp)^\perp$.

Exemple 27 (se ramener à un sous-espace vectoriel).

$$\forall X \in \mathcal{P}(E) \quad X^\perp = (\mathrm{Vect}(X))^\perp.$$

Proposition 28.

Si X est une partie de $(E, \langle\cdot,\cdot\rangle)$, alors $X^\perp$ est un sous-espace vectoriel de E.

Si F est un sous-espace vectoriel de E, alors $F^\perp$ est un s.e.v. de E en somme directe avec F.

Exemple 29 (Reconnaître un « vecteur normal » à un hyperplan)**.**

• Soit $(a,b,c) \neq (0,0,0)$. On considère le plan de $\mathbb{R}^3$

$$F = \left\{(x,y,z) \in \mathbb{R}^3 \ \mid \ ax+by+cz=0\right\}.$$

Écrire F sous la forme $\text{Vect}(u)^\perp$ où u est un vecteur de $\mathbb{R}^3$ à expliciter
Sait-on prouver que $F^\perp = \text{Vect}(u)$?

• On considère le sous-espace vectoriel de $M_n(\mathbb{R})$ défini par

$$G = \{M \in M_n(\mathbb{R}) \quad \text{tr}(M) = 0\}.$$

Écrire G sous la forme $\text{Vect}(U)^\perp$ où U est une matrice de $M_n(\mathbb{R})$ à expliciter.
Sait-on prouver que $G^\perp = \text{Vect}(U)$?

3.3 Bases orthonormées d'un espace euclidien.

La terminologie est transparente : on parlera d'une **base orthonormée** (b.o.n.) d'un espace euclidien à propos d'une base de cet espace constituée de vecteurs deux à deux orthogonaux et tous de norme 1.

Théorème 30.

Dans un espace euclidien de dimension non nulle, il existe des bases orthonormées.

Proposition 31 (Les coordonnées dans une b.o.n. se calculent facilement)**.**

Si E est de dimension finie et que $(e_1,\dots,e_n)$ en est une base orthonormée, alors

$$\forall x \in E \quad x = \sum_{i=1}^n \langle x, e_i\rangle e_i.$$

Corollaire 32.

Si E est de dimension finie et que $(e_1,\dots,e_n)$ en est une base orthonormée, alors, pour $(x,y) \in E^2$,

$$\langle x,y\rangle = \sum_{i=1}^n \langle x,e_i\rangle\langle y,e_i\rangle \quad \text{et} \quad \|x\|^2 = \sum_{i=1}^n \langle x,e_i\rangle^2.$$

Exemple 33.

Soit $E = \mathcal{C}^2([0,\pi],\mathbb{R})$ muni du produit scalaire $(f,g) \mapsto \langle f,g\rangle = \int_0^\pi fg$.
On considère $F = \{f \in E \mid f'' + f = 0\}$, muni de la restriction du produit scalaire à F^2.

a) Justifier que $(\cos,\sin)$ est une base de F et qu'elle est orthogonale.

b) En déduire une base orthonormée de F.

c) Prouver enfin que pour toute fonction $f \in F$, on a

$$\frac{\pi}{2}\int_0^\pi f^2(t)\mathrm{d}t = \left(\int_0^\pi f(t)\cos(t)\mathrm{d}t\right)^2 + \left(\int_0^\pi f(t)\sin(t)\mathrm{d}t\right)^2.$$

4 Projection orthogonale sur un sous-espace de dimension finie.

4.1 Projeté orthogonal.

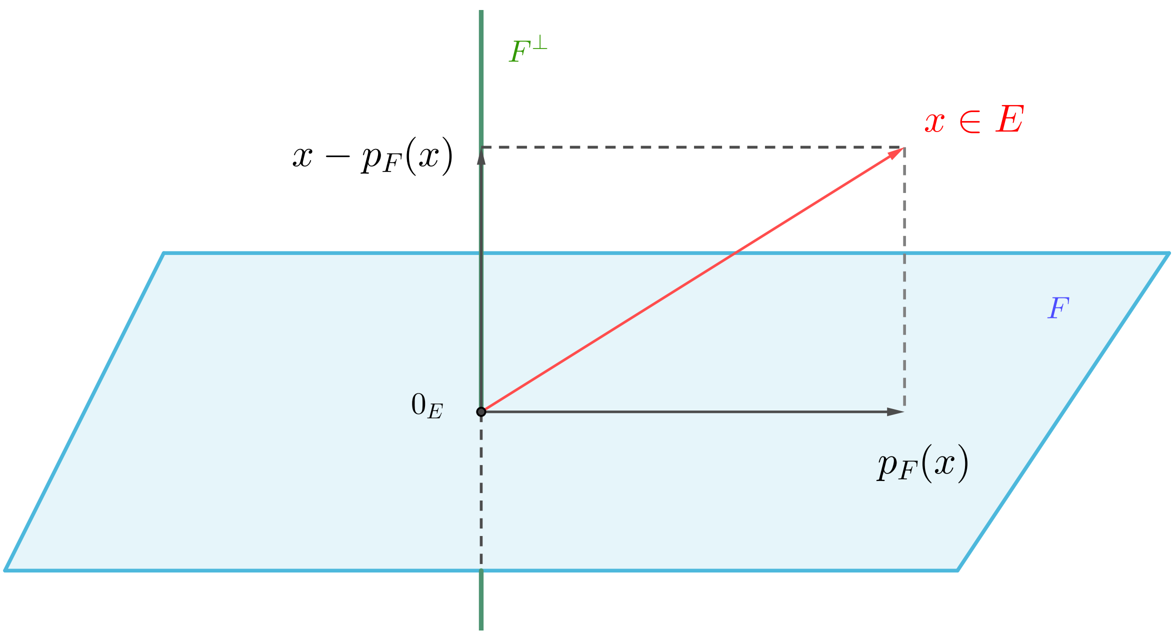
Proposition-Définition 34 (Supplémentaire orthogonal d'un sous-espace de dimension finie)**.**

Soit $(E,\langle\cdot,\cdot\rangle)$ un espace préhilbertien et F un sous-espace vectoriel <u>de dimension finie</u>.
Alors, $F^\perp$ est un supplémentaire de F dans E :

$$\boxed{E = F \oplus F^\perp}$$

La projection sur F parallèlement à $F^\perp$ est notée ici p_F et appelée **projecteur orthogonal** sur F.

Si $(e_1,\dots,e_p)$ est une base orthonormée de F, alors $\qquad p_F(x) = \sum_{i=1}^{p}\langle x,e_i\rangle e_i.$



Corollaire 35 (Inégalité de Bessel).

Soit $(E, \langle\cdot,\cdot\rangle)$ un espace préhilbertien et F un sous-espace de dimension finie. Alors,

$$\forall x \in E \qquad \|p_F(x)\| \leq \|x\|.$$

Corollaire 36 (Cas où E est aussi de dimension finie).

Soit E un espace <u>euclidien</u> et F un sous-espace vectoriel de E. Alors,

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

Lorsque la dimension de $F^\perp$ est nettement inférieure à celle de F est avantageux de projeter sur $F^\perp$ plutôt que sur F. Ce sera très net au paragraphe suivant lorsqu'il s'agira de calculer la distance à un hyperplan.

Proposition 37 (Hors-programme ? La question du bi-orthogonal).

Soit $(E, \langle\cdot,\cdot\rangle)$ un espace préhilbertien et F un sous-espace vectoriel de E tel que $F \oplus F^\perp = E$. On a

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

Le projecteur orthogonal sur $F^\perp$ est le projecteur sur $F^\perp$ parallèlement à F, de sorte que

$$\forall x \in E \quad x = p_F(x) + p_{F^\perp}(x).$$

Tout ceci est vrai en particulier lorsque F est de dimension finie, et donc en particulier dans le cas où E est euclidien.

Preuve. L'inclusion $F \subset (F^\perp)^\perp$ est connue.

Soit $x \in (F^\perp)^\perp$. Il se décompose sur $F \oplus F^\perp$ et s'écrit $x = x_F + x_{F^\perp}$. Par linéarité,

$$\langle x, x_{F^\perp}\rangle = \langle x_F + x_{F^\perp}, x_{F^\perp}\rangle = \langle x_F, x_{F^\perp}\rangle + \langle x_{F^\perp}, x_{F^\perp}\rangle = 0 + \|x_{F^\perp}\|^2.$$

Puisque $x \in (F^\perp)^\perp$ et $x_{F^\perp} \in F^\perp$, le produit scalaire que l'on vient de calculer vaut 0.
Ainsi, $\|x_{F^\perp}\| = 0$ puis $x_{F^\perp} = 0_E$. On a démontré que $x = x_F$, soit $x \in F$.

$\square$

Remarque. *à réserver pour une seconde lecture*
Le programme officiel ne parle que de projection orthogonale sur un sous-espace de dimension finie. Or, nous venons de prouve que si F est de dimension finie, alors $F^\perp$ est supplémentaire à son orthogonal (qui est F !) Cela a donc un sens de définir $p_{F^\perp}$... même si $F^\perp$ n'est pas de dimension finie.
Tout cela est un peu subtil car, comme on l'aperçoit dans le TD, il existe des espaces préhilbertiens E et dans ces espaces des sous-espaces F de dimension infinie tels que $F \oplus F^\perp \neq E$. On peut alors avoir $\left(F^\perp\right)^\perp \neq F$!

4.2 Distance à un sous-espace de dimension finie.

Définition 38.

Soit $(E, \langle \cdot, \cdot \rangle)$ un espace préhilbertien, F un sous-espace de E et $x \in E$ un vecteur.
On appelle **distance** de x à F, que l'on pourra noter $d(x, F)$ le réel positif

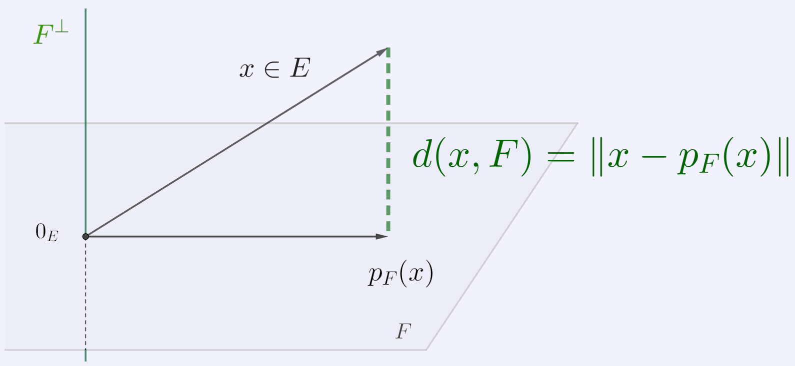
$$d(x, F) = \inf_{y \in F} \|x - y\|.$$

Le nombre ci-dessus est bien défini, comme borne inférieure d'un ensemble de réels non vide et minoré (par 0).

Proposition 39 (Distance à un sous-espace.)**.**

Soit $(E, \langle \cdot, \cdot \rangle)$ un espace préhilbertien. Soit F un sous-espace de dimension finie. On a

$$\boxed{d(x, F) = \|x - p_F(x)\|.}$$



La distance au sous-espace est donc *atteinte* : $\|x - p_F(x)\| = \min_{y \in F} \|x - y\|$, et le projeté orthogonal $p_F(x)$ est l'unique vecteur de F qui réalise le minimum.

Preuve. Notons $y_0 = p_F(x)$ (existe car F est de dimension finie) et considérons $y \in F$. Puisque $x - y_0$ appartient à $F^\perp$ et que $y - y_0$ appartient à F, le théorème de Pythagore donne

$$\|x - y\|^2 = \|x - y_0 + y_0 - y\|^2 = \|x - y_0\|^2 + \|y_0 - y\|^2.$$

Puisque $\|y_0 - y\|^2 \geq 0$, on a

$$\|x - y\|^2 \geq \|x - y_0\|^2$$

avec égalité si et seulement si $\|y_0 - y\| = 0$.
On a donc bien prouvé que $\|x - y\| \geq \|x - y_0\|$ avec égalité si et seulement si $y = y_0$.

□

Corollaire 40 (Distance à un sous-espace, dans un espace de dimension finie)**.**

Soit $(E, \langle \cdot, \cdot \rangle)$ un espace euclidien et F un sous-espace vectoriel de E.
Pour tout vecteur x de E, on a

$$d(x, F) = \|p_{F^\perp}(x)\|.$$

4.3 Projeté orthogonal et calcul de distance : la pratique.

Méthode (En pratique : projeter un vecteur sur F lorsqu'on a une b.o.n. de F)**.**

Soit F un sous-espace vectoriel de dimension finie d'un espace préhilbertien E et $x \in E$.
Pour calculer $p_F(x)$, projeté orthogonal de x sur F, on peut

1. se donner une b.o.n. $(e_1, \ldots, e_p)$ de F
   (voir paragraphe suivant pour un algorithme de construction),
2. utiliser la formule $p_F(x) = \sum\limits_{i=1}^{p} \langle x, e_i \rangle e_i$.

Méthode (En pratique : projeter un vecteur sur F lorsqu'on a une base quelconque de F)**.**

Soit F un sous-espace vectoriel de dimension finie d'un espace préhilbertien E et $x \in E$.
Pour calculer $p_F(x)$, projeté orthogonal de x sur F, on peut

1. se donner une base $(u_1, \ldots, u_p)$ de F
2. Introduire $(\lambda_1, \ldots, \lambda_p)$, p-uplet des coordonnées de $p_F(x)$ sur $(u_1, \ldots, u_p)$.
3. Écrire le système linéaire sur les λ_i correspondant à l'orthogonalité de $x - p_F(x)$ avec les u_i.
4. Résoudre le système linéaire !

Exemple 41 (Distance à un hyperplan en dimension finie)**.**

Soit H un hyperplan de E, $u \in H^\perp \setminus \{0_E\}$ et x un vecteur de E.

1. Que dire de $H^\perp$? Dessiner.
   Lequel de $p_H(x)$ ou de $p_{H^\perp}(x)$ est le plus facile à calculer ?
   Justifier que la distance de x à H est $d(x, H) = \dfrac{|\langle x, u \rangle|}{\|u\|}$.
2. Application : montrer que la distance d'un vecteur $x = (x_0, y_0, z_0) \in \mathbb{R}^3$ à un plan vectoriel P d'équation $ax + by + cz = 0$ (où $(a, b, c) \neq (0, 0, 0)$) vaut

$$d(x, P) = \frac{|ax_0 + by_0 + cz_0|}{\sqrt{a^2 + b^2 + c^2}}.$$

Exemple 42.

Calculer le nombre

$$\inf_{(a,b) \in \mathbb{R}^2} \int_0^1 \left(t^2 - ax - b\right)^2 \mathrm{d}x.$$

4.4 Construction de b.o.n. : algorithme d'orthonormalisation de Gram-Schmidt.

Exemple 43 (Comprendre d'abord pour deux vecteurs.)**.**

On orthonormalise une famille libre (u_1, u_2), en illustrant.

Proposition 44 (Algorithme d'orthonormalisation de Gram-Schmidt)**.**

Soit E un espace préhilbertien. Soit $(u_1, \ldots, u_n)$ une famille libre de vecteurs de E ($n \geq 2$).
Il est possible de définir des vecteurs $e_1, e_2, \ldots, e_n$ tels que

$$\forall k \in [\![1, n]\!] \quad (e_1, \ldots, e_k) \text{ est une b.o.n. de } \mathrm{Vect}(u_1, \ldots, u_k) := F_k.$$

Le procédé de construction est le suivant : on commence par poser

$$e_1 := \frac{u_1}{\|u_1\|}.$$

Pour $k \in [\![1, n-1]\!]$, si $e_1, \ldots, e_k$ sont construits, on pose $e_{k+1} := \dfrac{v_{k+1}}{\|v_{k+1}\|}$, où

$$v_{k+1} := u_{k+1} - p_{F_k}(u_{k+1}) = u_{k+1} - \sum_{i=1}^{k} \langle u_{k+1}, e_i \rangle e_i.$$

Le procédé mis en œuvre pour passer de $(u_1, \ldots, u_n)$ à $(e_1, \ldots, e_n)$ est appelé **algorithme d'orthonormalisation de Gram-Schmidt** et on dit que l'on a orthonormalisé la famille $(u_1, \ldots, u_n)$.

Exemple 45.

Orthonormaliser la famille (u_1, u_2, u_3) où $u_1 = (2, -1, 1)$, $u_2 = (-1, 1, 1)$, $u_3 = (1, 1, 1)$.
Solution : l'algorithme de Gram-Schmidt renvoie (e_1, e_2, e_3) *avec*

$$e_1 = \frac{1}{\sqrt{6}}(2, -1, 1), \quad e_2 = \frac{1}{\sqrt{21}}(-1, 2, 4), \quad e_3 = \frac{1}{\sqrt{14}}(2, 3, -1).$$

Exemple 46 (Matrice de passage)**.**

Soit $(u_1 \ldots, u_n)$ une base d'un espace euclidien et $(e_1, \ldots, e_n)$ la b.o.n. obtenue en appliquant l'algorithme de Gram-Schmidt. Expliquer pourquoi la matrice de passage de la première à la seconde est triangulaire supérieure.

Proposition 47 (Théorème de la b.o.n. incomplète)**.**

Dans un espace euclidien, toute famille orthonormée peut être complétée en une b.o.n.

Exercices

Calculs de distances.

$\boxed{\textbf{40.1}}$ **[♦♦♢]** Soient $a_0, a_1, \dots, a_n$, $n+1$ réels deux à deux distincts. Soit l'application

$$\langle \cdot,\cdot \rangle : \begin{cases} \mathbb{R}_n[X]^2 & \to & \mathbb{R} \\ (P,Q) & \mapsto & \sum\limits_{k=0}^{n} P(a_k)Q(a_k) \end{cases}.$$

1. Montrer que $\langle \cdot,\cdot \rangle$ est un produit scalaire sur $\mathbb{R}_n[X]$.
2. Déterminer une base de $\mathbb{R}_n[X]$ orthonormée pour ce produit scalaire.
3. On note $H = \left\{ P \in \mathbb{R}_n[X] : \sum\limits_{i=0}^{n} P(a_i) = 0 \right\}$. Déterminer $H^\perp$.
4. Calculer $d(X^n, H)$.

$\boxed{\textbf{40.2}}$ **[♦♦♢]** Notons $E = \mathcal{C}^2([-1,1],\mathbb{R})$ et $F = \{f \in E : f'' = f\}$.
Pour f et g deux fonctions de classe $\mathcal{C}^2$ sur $[-1,1]$, on pose $\langle f,g \rangle = \displaystyle\int_{-1}^{1} \left(fg + f'g'\right)$.

1. Montrer que $\langle f,g \rangle$ est un produit scalaire sur E.
2. Montrer que $(\mathrm{ch}, \mathrm{sh})$ est une base de F et vérifier qu'il s'agit d'une famille orthogonale.
3. Calculer $d(1, F)$ où 1 est la fonction constante égale à 1.

$\boxed{\textbf{40.3}}$ **[♦♦♢]** Soit le s.e.v. de $\mathbb{R}^4$ donné par

$$F = \left\{ (x,y,z,t) \in \mathbb{R}^4 : x + y - z - t = 0 \quad \text{et} \quad x + 3y + z - t = 0 \right\}.$$

On note p_F la projection orthogonale sur F.

1. Déterminer une base orthonormée de F.
2. En déduire la matrice de p_F dans la base canonique de $\mathbb{R}^4$.
3. Soit e_1 le premier vecteur dans la base canonique.
   Déterminer la distance de e_1 à F.

$\boxed{\textbf{40.4}}$ **[♦♦♢]**

1. Montrer que $(P,Q) \mapsto \langle P,Q \rangle = \sum\limits_{k=0}^{n} P^{(k)}(1)Q^{(k)}(1)$ est un produit scalaire sur $\mathbb{R}_n[X]$.
2. Calculer $d(1_{\mathbb{R}_n[X]}, F)$, la distance de $1_{\mathbb{R}_n[X]}$ à F, où $F = \{P \in \mathbb{R}_n[X], P(1) = 0\}$.

Divers.

$\boxed{\textbf{40.5}}$ **[♦♢♢]** Un drôle d'angle droit.
Montrer que $(X,Y) \mapsto X^T \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix} Y$ définit un produit scalaire sur $M_{2,1}(\mathbb{R})$.
Démontrer que les vecteurs $(1,0)$ et $(1,-3)$ sont orthogonaux pour ce produit scalaire.

$\boxed{\textbf{40.6}}$ **[♦♢♢]** Montrer que pour tout $(x_1, \dots, x_n) \in \mathbb{R}^n$, $\left(\sum\limits_{i=1}^{n} x_i \right)^2 \leq n \sum\limits_{i=1}^{n} x_i^2$.
Pour quels n-uplets a-t-on égalité ?

$\boxed{\textbf{40.7}}$ **[♦◇◇]** Soient $x_1, \ldots, x_n \in \mathbb{R}_+^*$ tels que $\sum\limits_{i=1}^{n} x_i = 1$. Montrer que $\sum\limits_{i=1}^{n} \frac{1}{x_i} \geq n^2$. Étudier le cas d'égalité.

$\boxed{\textbf{40.8}}$ **[♦◇◇]** Soit $\|\cdot\|$ la norme associée au produit scalaire canonique sur $M_n(\mathbb{R})$. Démontrer que

$$\forall (A, B) \in M_n(\mathbb{R}) \quad \|AB\| \leq \|A\| \cdot \|B\|.$$

$\boxed{\textbf{40.9}}$ **[♦♦♦]** Soit E un espace préhilbertien et n un entier supérieur à 2. On considère n vecteurs $v_1, \ldots, v_n$ tels que

$$\forall i \in [\![1, n]\!] \quad \|v_i\| = 1 \qquad \text{et} \qquad \exists k > 1 : \ \forall i \neq j \ \langle v_i, v_j \rangle \leq -\frac{1}{k}.$$

Démontrer que $k + 1 \geq n$.

$\boxed{\textbf{40.10}}$ **[♦♦◇]** Montrer que deux vecteurs x et y sont orthogonaux si et seulement si

$$\forall \lambda \in \mathbb{R}, \quad \|x + \lambda y\| \geq \|x\|.$$

$\boxed{\textbf{40.11}}$ **[♦◇◇]** Soient F et G deux sous-espaces vectoriels d'un espace préhilbertien.

1. Montrer que $(F + G)^{\perp} = F^{\perp} \cap G^{\perp}$.
2. Montrer que $F^{\perp} + G^{\perp} \subset (F \cap G)^{\perp}$.

$\boxed{\textbf{40.12}}$ **[♦◇◇]** Soit A une partie d'un espace préhilbertien. Montrer que

$$\left((A^{\perp})^{\perp}\right)^{\perp} = A^{\perp}.$$

$\boxed{\textbf{40.13}}$ **[♦♦◇]** Soit $A \in M_{n,p}(\mathbb{R})$ et f l'application linéaire canoniquement associée.

Démontrer les égalités

$$\mathrm{Ker}(A^T A) = \mathrm{Ker}(A) \qquad \text{et} \qquad (\mathrm{Im} A)^{\perp} = \mathrm{Ker}(A^T).$$

En déduire que

— si f est injective, alors $A^T A \in GL_p(\mathbb{R})$;

— si f est surjective, alors $AA^T \in GL_n(\mathbb{R})$.

$\boxed{\textbf{40.14}}$ **[♦♦♦]** Orthogonal d'un sous-espace de dimension infinie.
Soit $E = \mathcal{C}^0([0,1], \mathbb{R})$ et $F = \mathcal{C}^1([0,1], \mathbb{R})$. On munit E du produit scalaire défini par

$$\forall (f, g) \in E^2 \quad \langle f, g \rangle = \int_0^1 f(t) g(t) \mathrm{d}t.$$

Démontrer que $F^{\perp} = \{0_E\}$. A-t-on $(F^{\perp})^{\perp} = F$?

Espérance et variance

1 Espérance.

1.1 Définition et exemples.

Définition 1.

Soit (Ω, P) un espace probabilisé fini et X une variable aléatoire à valeurs dans $\mathbb{K}$ définie sur Ω. On appelle **espérance** de X et on note $E(X)$ le nombre

$$E(X) = \sum_{x \in X(\Omega)} P(X = x)x.$$

Interprétation.

On réalise un certain nombre de fois une expérience conduisant à un résultat numérique : un nombre dans l'ensemble $\{x_1, \dots, x_n\}$. Pour $i \in [\![1, n]\!]$ notons f_i la fréquence à laquelle on a obtenu x_i. La valeur moyenne obtenue lors de cette série d'expériences vaut

$$\sum_{i \in [\![1,n]\!]} f_i x_i.$$

Si X est une variable aléatoire à valeurs dans $\{x_1, \dots, x_n\}$ et qu'on note $p_i := P(X = x_i)$, l'espérance de X s'écrit

$$\sum_{i \in [\![1,n]\!]} p_i x_i.$$

Dans cette moyenne pondérée, les probabilités ont remplacé les fréquences. Or, on se souvient que le nombre $P(X = x_i)$ est interprété comme la *fréquence a priori* de l'événement $(X = x_i)$.
Ainsi, le nombre $E(X)$ peut être interprété comme la **valeur moyenne** prise par X a priori.
Si X est comme dans l'exemple un gain à un jeu, $E(X)$ représente le gain moyen a priori, ce que l'on peut *espérer* gagner en jouant au jeu. On dira aussi que c'est un indicateur de position : $E(X)$ est la position moyenne de la variable X.

Exemple 2 (Le retour du chouette jeu)**.**

On jette un dé équilibré. Si le résultat est $1, 2$ ou 3, on ne gagne rien. Si le résultat est 4 ou 5, on gagne dix euros. Si le résultat est 6, on empoche 100 euros. On note X le gain à ce jeu.
Considérons que X est une variable aléatoire sur un espace probabilisé (Ω, P). Calculer $E(X)$.

Proposition 3 (Une évidence qui mérite d'être dite)**.**

Si deux variables aléatoires ont la même loi, alors elles ont la même espérance.

Proposition 4 (Espérance des lois usuelles)**.**

Soit X, Y et Z des variables aléatoires définies sur un espace probabilisé (Ω, P), $n \in \mathbb{N}^*$, $p \in [0, 1]$.

1. Variable constante. Si X est la variable aléatoire constante égale à $a \in \mathbb{K}$, alors $\boxed{E(X) = a}$.
2. Loi de Bernoulli. Si $Y \sim \mathcal{B}(p)$, $\boxed{E(Y) = p}$. En particulier, $\forall A \in \mathcal{P}(\Omega)$ $\boxed{E(\mathbf{1}_A) = P(A)}$.
3. Loi binomiale. Si $Z \sim \mathcal{B}(n, p)$, $\boxed{E(Z) = np}$.

Exemple 5 (Le pari de Pascal)**.**

Dans son texte célèbre dit du "pari", (*Pensées, fragment 397*) Pascal met en scène un dialogue avec un athée, qu'il veut convaincre de croire en Dieu. Celui qui croit *gage* son énergie, son temps, parfois sa vie entière, et au-dessus de lui *se joue un jeu [...] où il arrivera croix ou pile*, c'est-à-dire qu'à la fin, *Dieu est, ou il n'est pas.* S'il est, celui qui a cru sortira gagnant mais... il sera perdant si Dieu n'existe pas ! Et c'est bien ce qui inquiète l'interlocuteur fictif de Pascal, qui a peur de *gager trop*, de ne pas récupérer sa mise... Savoir si l'on gagnera ou pas à ce jeu revient à savoir si Dieu existe ou pas, et Pascal nous dit que *la raison n'y peut rien déterminer* : pour celui qui croit, il y a *pareil hasard de gain et de perte.*

L'argument de Pascal en faveur de la croyance est le suivant : si on gagne, on gagne l'infini, si on perd, on perd peut-être beaucoup mais on perd une quantité finie (finitude de l'homme...) En moyenne, on gagne l'infini : son raisonnement est un calcul d'espérance ! N'oublions pas que Pascal était mathématicien en plus d'être philosophe, et qu'il s'intéressait notamment au hasard.
Posons le calcul de Pascal, en notant X ce que gagne le croyant. Le gain X vaut $+\infty$ si Dieu existe, la perte est finie s'il n'existe pas : disons qu'alors $X = -a$, où a est une quantité finie. Voici ce que le croyant gagne en moyenne :

$$E(X) = \frac{1}{2}(+\infty) + \frac{1}{2}(-a) = +\infty.$$

Notez que le choix de $(\frac{1}{2}, \frac{1}{2})$ comme distribution de probabilités n'a aucune importance, tant que l'on évite une probabilité nulle. Dans *Ma nuit chez Maud*, d'Éric Rohmer, Antoine Vitez (Vidal dans le film) en choisit une autre lorsqu'il fait le pari que l'Histoire a un sens. Jean-Louis Trintignant (Jean-Louis dans le film) lui parle alors d'espérance mathématique. L'extrait est disponible sur Youtube, mais on n'hésitera pas à regarder tout le film !

1.2 Propriétés de l'espérance.

Dans tout ce paragraphe, (Ω, P) sera un espace probabilisé fini.

Lemme 6.

Soit X une variable aléatoire définie sur (Ω, P) et à valeurs dans $\mathbb{K}$. Alors,

$$E(X) = \sum_{\omega \in \Omega} P(\{\omega\}) X(\omega).$$

Les deux propositions suivantes montrent qu'espérance et intégrale partagent de nombreuses propriétés.

Proposition 7 (Espérance et inégalités)**.**

Soient X et Y deux variables aléatoires à valeurs *réelles* sur (Ω, P). Alors,

1. Si $\forall \omega \in \Omega \; X(\omega) \geq 0$, alors $E(X) \geq 0$ (positivité).
2. Si $\forall \omega \in \Omega \; X(\omega) \geq 0$ et $E(X) = 0$, alors $P(X = 0) = 1$ (cas d'égalité).
3. Si $\forall \omega \in \Omega \; X(\omega) \leq Y(\omega)$, alors $E(X) \leq E(Y)$ (croissance).
4. $|E(X)| \leq E(|X|)$ (inégalité triangulaire)
5. $|E(XY)| \leq \sqrt{E(X^2)}\sqrt{E(Y^2)}$.

Remarque. On remarque qu'une variable aléatoire positive, d'espérance nulle n'est pas forcément nulle... mais qu'elle l'est avec probabilité 1 ! On dit qu'elle est *presque sûrement* nulle.

Proposition 8 (L'espérance est linéaire)**.**

Soient X et Y deux variables aléatoires sur (Ω, P) et à valeurs dans $\mathbb{K}$. Alors,

$$\forall \lambda, \mu \in \mathbb{K} \quad E(\lambda X + \mu Y) = \lambda E(X) + \mu E(Y).$$

Notamment, $\forall \lambda, \mu \in \mathbb{K} \;\; E(\lambda X + \mu) = \lambda E(X) + \mu$.

Dans le cas de n variables aléatoires $X_1, \ldots, X_n$ et n scalaires $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$,

$$E\left(\sum_{i=1}^{n} \lambda_i X_i\right) = \sum_{i=1}^{n} \lambda_i E(X_i).$$

Exemple 9.

Redémontrer en utilisant la linéarité de l'espérance que si $Z \sim \mathcal{B}(n, p)$, alors $E(Z) = np$.

Proposition-Définition 10.

Soit X une variable aléatoire définie sur (Ω, P) et à valeurs dans $\mathbb{K}$. La variable

$$X - E(X)$$

est d'espérance nulle. On dit que c'est une variable aléatoire **centrée**.

Le résultat ci-dessous est simple et important : il s'agit de calculer l'espérance de l'image $f(X)$ d'une variable aléatoire X en utilisant la loi de X plutôt que celle de $f(X)$.

Théorème 11 (Formule du transfert)**.**

Soit une v.a. $X : \Omega \to E$ où E est un ensemble sur lequel est défini une application $f : E \to \mathbb{K}$. Alors,

$$E\left(f(X)\right) = \sum_{x \in X(\Omega)} P(X = x) f(x).$$

Exemple 12.

Calcul de $E\left(X^2\right)$ où X suit la loi binomiale $\mathcal{B}(n, p)$.

1.3 Espérance d'un produit et indépendance.

Théorème 13.

Soient X et Y deux variables aléatoires définies sur un même espace probabilisé fini (Ω, P), et à valeurs dans $\mathbb{K}$. Si X et Y sont <u>indépendantes</u>, alors

$$E(XY) = E(X)E(Y).$$

Plus généralement, si $(X_i)_{i \in [\![1,n]\!]}$ est une famille de variables aléatoires <u>indépendantes</u>,

$$E\left(\prod_{i=1}^{n} X_i\right) = \prod_{i=1}^{n} E(X_i).$$

Exemple 14.

Soient $X_1, \ldots, X_n$ des variables aléatoires sur (Ω, P), i.i.d. de loi de Rademacher, donnée par

$$\forall k \in [\![1, n]\!] \quad X_k(\Omega) = \{-1, 1\} \quad \text{et} \quad P(X_k = 1) = P(X_k = -1) = \frac{1}{2}.$$

Notons $S_n = \sum_{k=1}^{n} X_k$. Pour $t \in \mathbb{R}$, démontrer que $E\left(\cos(tS_n)\right) = \cos^n(t)$.

2 Variance.

2.1 Définition et exemples.

Définition 15.

Soit (Ω, P) un espace probabilisé fini et X une variable aléatoire *réelle* sur Ω.
On appelle **variance** de X et on note $V(X)$ le réel

$$V(X) = E\left[(X - E(X))^2\right].$$

On appelle **écart type**, parfois noté $\sigma(X)$ le réel $\sqrt{V(X)}$.

Interprétation.

L'expression de $V(X)$ donne **l'écart quadratique moyen** de la variable X, par rapport à sa moyenne.

Plus la variance est grande, plus les valeurs prises par X sont « loin » (en moyenne) de $E(X)$.

La variance et l'écart-type sont des indicateurs de *dispersion*. Il aurait pu sembler plus naturel de considérer la quantité $E\left(|X - E(X)|\right)$, mais on verra que le *carré* qui se trouve dans la définition est bien mieux adapté à la linéarité de l'espérance (voir plus loin le travail sur les sommes de v.a.).

Proposition 16 (La variance est quadratique)**.**

Soit X une variable aléatoire réelle sur un espace probabilisé fini. On a, pour tous $a, b \in \mathbb{R}$,

$$V(aX + b) = a^2 V(X).$$

Proposition-Définition 17.

Soit X une variable aléatoire réelle sur un espace probabilisé fini telle que $\sigma(X) > 0$.
La variable aléatoire $\frac{1}{\sigma(X)}X$ est de variance 1 : elle est dite **réduite**.

La variable aléatoire $\dfrac{X - E(X)}{\sigma(X)}$ est centrée réduite.

Proposition 18 (Lien avec le moment d'ordre 2)**.**

Soit X une variable aléatoire réelle sur un espace probabilisé fini. On a

$$V(X) = E(X^2) - E(X)^2.$$

Le nombre $E(X^2)$ est appelé **moment** d'ordre 2 de la variable X.

Proposition 19 (Une évidence qui mérite d'être dite).

Si deux variables aléatoires ont la même loi, alors elles ont la même variance.

Proposition 20 (Variance des lois usuelles).

Soit X, Y et Z des variables aléatoires définies sur un espace probabilisé (Ω, P), $n \in \mathbb{N}^*$, $p \in [0, 1]$.

1. Variable constante. Si X est la variable aléatoire constante égale à $a \in \mathbb{K}$, alors $\boxed{V(X) = 0}$.
2. Loi de Bernoulli. Si $Y \sim \mathcal{B}(p)$, $\boxed{V(Y) = p(1-p)}$.
3. Loi binomiale. Si $Z \sim \mathcal{B}(n, p)$, $\boxed{V(Z) = np(1-p)}$.

Remarque. Que dire d'une réciproque pour le premier point ? Si la variance de X est nulle, alors $(X - E(X))$ est nulle... presque sûrement ! (voir proposition 7). On a donc $P(X = E(X)) = 1$.

2.2 Variance d'une somme, et covariance.

Ci-dessous, les variables aléatoires considérées sont réelles, et définies sur un espace probabilisé fini (Ω, P).

Pour comprendre d'où vient la définition suivante, calculons d'abord $V(X+Y)$, pour X et Y deux variables aléatoires définie sur un même espace probabilisé.

Définition 21.

On appelle **covariance** de deux variables aléatoires X et Y, et on note $\operatorname{cov}(X, Y)$ le nombre

$$\operatorname{cov}(X, Y) = E\left[(X - E(X))(Y - E(Y))\right].$$

Lorsque ce nombre est nul, on dit qu'elles sont **décorrélées**.

Interprétation (Interpréter le signe d'une covariance).

Lorsque X et Y ont une covariance positive, alors le produit $(X - E(X))(Y - E(Y))$ est positif... en moyenne ! Cela signifie que lorsque X est supérieure à sa moyenne, Y a tendance à l'être aussi.

Lorsque X et Y ont une covariance négative, alors le produit $(X - E(X))(Y - E(Y))$ est négatif... en moyenne ! Cela signifie que lorsque X est supérieure à sa moyenne, Y a tendance à être inférieure à la sienne, et réciproquement.

Proposition 22.

Si X et Y sont deux variables aléatoires réelles, leur covariance s'exprime comme

$$\operatorname{cov}(X, Y) = E(XY) - E(X)E(Y).$$

Proposition 23.

Si X et Y sont indépendantes, alors elles sont décorrélées.

Exemple 24 (Deux variables décorrélées mais pas indépendantes)**.**

Soient X et Y deux v.a. définies sur un espace probabilisé, indépendantes et de même loi de Bernoulli de paramètre $p \in]0,1[$. On note $U = X + Y$ et $V = X - Y$.
Vérifier que U et V sont décorrélées puis justifier qu'elles ne sont pas indépendantes.

Proposition 25 (La covariance est presque un produit scalaire)**.**

Soient $X, \widetilde{X}, Y$ trois variables aléatoires sur (Ω, P).

1. $\mathrm{cov}(X,Y) = \mathrm{cov}(Y,X)$.
2. Pour $(\lambda,\mu) \in \mathbb{R}^2$, $\mathrm{cov}(\lambda X + \mu \widetilde{X}, Y) = \lambda \mathrm{cov}(X,Y) + \mu \mathrm{cov}(\widetilde{X},Y)$.
3. $\mathrm{cov}(X,X) = V(X) \geq 0$.
4. $|\mathrm{cov}(X,Y)| \leq \sqrt{V(X)}\sqrt{V(Y)}$.

Remarque. La covariance est donc un produit scalaire imparfait pour lequel la variance serait le carré de la norme... Que manque-t-il à cov pour être un produit scalaire ? La propriété de définition : si $\mathrm{cov}(X,X) = 0$, alors X n'est pas forcément nulle : elle est constante et égale à son espérance... *presque sûrement.*

Proposition 26 (Variance d'une somme de deux variables aléatoires)**.**

Soient X et Y deux variables aléatoires réelles sur (Ω, P). Alors,

$$V(X+Y) = V(X) + V(Y) + 2\,\mathrm{cov}(X,Y).$$

Dans le cas où X et Y sont décorrélées (et en particulier si elles sont indépendantes) on a

$$V(X+Y) = V(X) + V(Y).$$

Proposition 27 (cas de n variables)**.**

Soit $(X_i)_{i \in [\![1,n]\!]}$ une famille de n variables aléatoires réelles sur (Ω, P). On a

$$V\left(\sum_{i=1}^n X_i\right) = \sum_{i=1}^n V(X_i) + 2 \sum_{1 \leq i < j \leq n} \mathrm{cov}(X_i, X_j).$$

Si les variables ci-dessus sont deux à deux décorrélées, alors

$$V\left(\sum_{i=1}^n X_i\right) = \sum_{i=1}^n V(X_i).$$

Cette égalité est notamment vraie lorsque $X_1, \dots, X_n$ sont deux à deux indépendantes.

2.3 Inégalités probabilistes.

Les variables aléatoires considérées dans ce qui suit sont supposées définies sur un espace probabilisé (Ω, P).

Proposition 28 (Inégalité de Markov)**.**

Soit une variable aléatoire *réelle positive* $X : \Omega \to \mathbb{R}_+$, et $a \in \mathbb{R}_+^*$. Alors,

$$P(X \geq a) \leq \frac{E(X)}{a}.$$

L'inégalité suivante permet de majorer la probabilité qu'une variable aléatoire soit « loin » de sa moyenne.

Proposition 29 (Inégalité de Bienaymé-Tchebychev)**.**

Soit X une variable aléatoire réelle sur Ω et $a \in \mathbb{R}_+^*$. Alors,

$$P\left(|X - E(X)| \geq a\right) \leq \frac{V(X)}{a^2}.$$

Exemple 30 (Des inégalités pas si bonnes dans la pratique)**.**

Soit X une v.a. sur (Ω, P) de loi binomiale $\mathcal{B}(10^3, \frac{1}{2})$. Majorer la probabilité de l'événement $(X \geq 600)$ d'abord avec l'inégalité de Markov, ensuite avec l'inégalité de Bienaymé-Tchebychev. L'utilisation d'une machine nous donne que cette probabilité est de l'ordre de 10^{-10}. Commenter.

Exemple 31 (Inégalité de concentration : distance entre moyennes empiriques et théoriques)**.**

Soit $n \in \mathbb{N}^*$. On considère n variables aléatoires $X_1, \ldots, X_n$ sur (Ω, P).
On les suppose « i.i.d. »(*indépendantes et identiquement distribuées*, c'est-à-dire indépendantes et de même loi). Notons $m = E(X_1)$ et $\sigma^2 = V(X_1)$. On a

$$\forall \varepsilon > 0 \qquad P\left(\left|\frac{1}{n}\sum_{i=1}^{n} X_i - m\right| \geq \varepsilon\right) \leq \frac{\sigma^2}{n\varepsilon^2}.$$

La majoration par un $O\left(\frac{1}{n}\right)$ montre que la probabilité que la moyenne empirique $\frac{1}{n}\sum_{i=1}^{n} X_i$ des n variables aléatoires soit éloignée de sa moyenne théorique m est petite lorsque n est grand.

On observe donc un phénomène de **concentration** : plus n devient grand, plus la variable aléatoire $\frac{1}{n}\sum_{i=1}^{n} X_i$ prend des valeurs concentrées autour de m. Cette convergence est une loi de la nature observée dans le monde physique. L'observer mathématiquement nous conduit à penser que le modèle probabiliste qui a été développé jusqu'ici n'est pas trop mauvais...

On retrouvera cette description de la concentration en spé avec la *Loi faible des grands nombres.*

Exercices

$\boxed{41.1}$ **[♦♦♢]**
Soit X une variable aléatoire sur un espace probabilisé (Ω, P) et à valeurs dans $[\![1, n]\!]$ ($n \in \mathbb{N}^*$). Montrer que

$$E(X) = \sum_{k=1}^{n} P(X \geq k).$$

Défi : écrire une preuve utilisant la linéarité de l'espérance.

$\boxed{41.2}$ **[♦♦♢]**
Soit X une variable aléatoire sur un espace probabilisé $(\Omega, \mathcal{F}, P)$ et telle que

$$E(X) = a \quad \text{et} \quad E(X^2) = E(X^4) = 1.$$

1. Démontrer que nécessairement, a est compris entre -1 et 1.
2. Donner la loi de X.

$\boxed{41.3}$ **[♦♦♢]** Soient X et Y deux variables aléatoires indépendantes, de même loi, et strictement positives. Démontrer que $E\left(X/Y\right) \geq 1$.

$\boxed{41.4}$ **[♦♦♦]** Soit n un entier naturel non nul.
Sur un espace probabilisé (Ω, P), on considère n variables aléatoires $X_1, \ldots, X_n$ indépendantes, toutes de loi uniforme sur $\{1, \ldots, n\}$. Calculer

$$E\left[\text{Card}\{X_1, \ldots, X_n\}\right].$$

En donner un équivalent lorsque n tend vers $+\infty$.
Écrire le cardinal comme une somme.

$\boxed{41.5}$ **[♦♦♢]** Mélange de sérums.
Soit une certaine maladie M. On considère une population dans laquelle la probabilité qu'une personne prise au hasard soit malade de M vaut 0.1. On dispose d'un test (infaillible) pour dépister M. On choisit 100 personnes au hasard, que l'on répartit, toujours au hasard en 10 groupes de 10 personnes. Au lieu de tester les sérums des 100 personnes, on mélange les sérums par groupe et on teste chaque mélange. Si le test d'un mélange est négatif, alors aucune des 10 personnes du groupe n'est malade. Si le test est positif, c'est qu'il y a au moins un malade dans le groupe et on dépiste alors chaque membre du groupe individuellement.

1. Soit Y le nombre de personnes malades dans un groupe donné. Quelle est la loi de Y ? Calculer les probabilités que
   (a) personne ne soit malade dans le groupe.
   (b) il y ait exactement une personne malade dans le groupe
   (c) au moins une personne soit malade dans le groupe
2. Soit N le nombre total de test que l'on doit effectuer selon cette méthode. Soit X le nombre de groupe dont le mélange est testé positivement.
   (a) Exprimer N en fonction de X.
   (b) Quelle est la loi de X ?
   (c) Calculer $P(N = 110)$ et $P(N = 100)$.
   (d) Calculer $E(N)$, $V(N)$ et σ_N. Interpréter.
3. Au lieu de faire des groupes de 10 personnes, on fait des groupes de n personnes.
   Quelle est la valeur de n qui minimise en moyenne le nombre de tests effectué ?

$\boxed{41.6}$ **[♦♦♢]** ♡♡♡
Soit $n \in \mathbb{N}^*$. Sur un espace probabilisé (Ω, P), on considère une famille $(X_i)_{1\leq i\leq n+1}$ de variables aléatoires indépendantes suivant une loi de Bernoulli de paramètre $p \in]0,1[$.

1. On pose $Y_k = X_k + X_{k+1}$.
   (a) Déterminer la loi de Y_k.
   (b) Calculer l'espérance et la variance de Y_k.
   (c) Calculer la covariance de Y_i et Y_j pour $i \neq j$.
2. On pose $S_n = \sum\limits_{k=1}^{n} Y_k$. Calculer l'espérance et la variance de S_n.
3. Soit $\varepsilon > 0$. Majorer $P\left(|\frac{1}{n}S_n - 2p| \geq \varepsilon\right)$ par une expression tendant vers 0 lorsque n tend vers $+\infty$.

$\boxed{41.7}$ **[♦♦♦]** Sommation d'un nombre aléatoire de variables aléatoires.
Soient $(X_1, \dots, X_n, N)$ une famille de variables aléatoires réelles sur un espace probabilisé fini (Ω, P).
On suppose que ces variables sont indépendantes, que $X_1, \dots, X_n$ ont même loi, et que N prend des valeurs entières entre 1 et n. Soit $S_N = X_1 + \dots X_N$ la variable aléatoire définie par

$$S_N : \begin{cases} \Omega & \to & \mathbb{R} \\ \omega & \mapsto & \sum\limits_{k=1}^{N(\omega)} X_k(\omega) \end{cases}.$$

Calculer l'espérance de S_N en fonction de celles de X_1 et de N.

$\boxed{41.8}$ **[♦♦♦]** Massacre !
On considère n couples mariés, donc $2n$ personnes, qui assistent à un banquet. Un fou furieux débarque et abat m personnes au hasard. En moyenne, combien de couples survivent (à deux) à l'hécatombe ?

$\boxed{41.9}$ **[♦♦♦]** On se donne $n \geq 2$ variables aléatoires indépendantes $X_1, \dots, X_n$ de loi $\mathcal{B}(p)$ avec $p \in]0,1[$.
On pose $U = \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$ et $M = UU^T$.

1. Donner la loi de $\mathrm{rg}(M)$ et de $\mathrm{tr}(M)$.
2. Avec quelle probabilité la matrice M est-elle une matrice de projection ?
3. On suppose $n = 2$. Soit $V = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ et $S = V^T M V$. Déterminer $E(S)$ et $V(S)$.

$\boxed{41.10}$ **[♦♦♦]** Soit $(X_k)_{k\in\mathbb{N}^*}$ une suite de variables aléatoires i.i.d. à valeurs dans $\mathbb{Z}$, et définies sur un espace probabilisé dont la probabilité est noté P.
C'est une petite entorse au programme de sup, cette suite (infinie) de variables aléatoires, mais bon...
On note $S_0 = 0$, et pour tout $n \in \mathbb{N}^*$, on note $S_n = X_1 + \dots + X_n$ et

$$N_n = \mathrm{Card}\left\{S_k, k \in [\![0, n]\!]\right\}.$$

1. Soit $n \in \mathbb{N}$. Montrer que

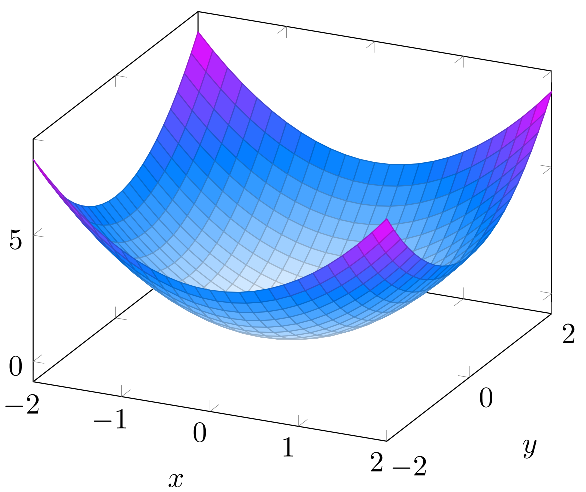
$$P\left(S_{n+1} \notin \{S_0, \dots, S_n\}\right) = P\left(S_0 \neq 0, \dots, S_n \neq 0\right).$$

2. Démontrer la convergence de la suite $\left(\frac{1}{n}E(N_n)\right)_{n\in\mathbb{N}^*}$.

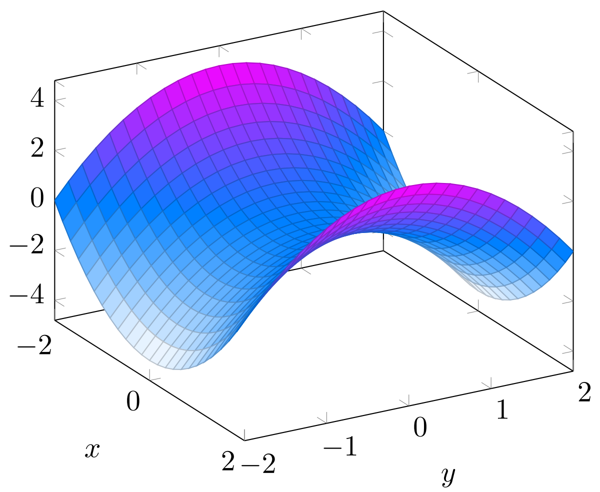
---

42 Fonctions de deux variables

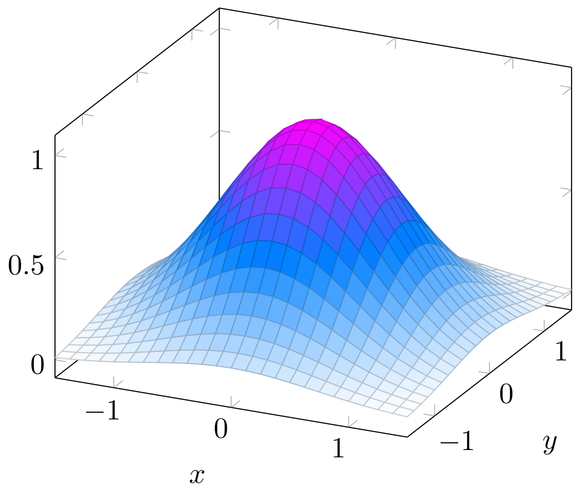
$z = x^2 + y^2$



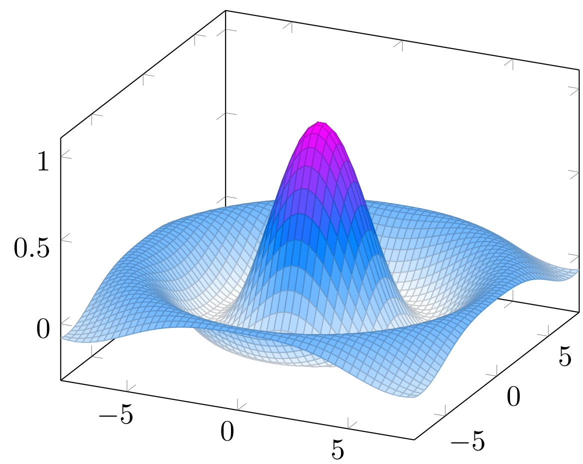
$z = x^2 - y^2$



$z = e^{-(x^2+y^2)}$



$z = \frac{\sin(\sqrt{x^2+y^2})}{\sqrt{x^2+y^2}}$



Dans ce cours, on s'intéresse aux fonctions du type

$$f : \left\{ \begin{array}{ccc} D & \to & \mathbb{R} \\ (x,y) & \mapsto & f(x,y) \end{array} \right. , \quad \text{où } D \subset \mathbb{R}^2$$

L'ensemble des points (x, y, z) de $\mathbb{R}^3$ tels que $(x, y) \in D$ et $z = f(x, y)$ est une **nappe** ou **surface**, appelée représentation graphique de f.

L'espace vectoriel $\mathbb{R}^2$ est muni de son produit scalaire usuel, et $\|\cdot\|$ désignera la norme euclidienne sur $\mathbb{R}^2$:

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

1 Fonctions définies sur un ouvert de $\mathbb{R}^2$ et à valeurs réelles.

1.1 Ouverts de $\mathbb{R}^2$

Définition 1.

Soit $a \in \mathbb{R}^2$ et $r > 0$.

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

$$\mathcal{B}(a,r) = \left\{ x \in \mathbb{R}^2 \quad \|x-a\| < r \right\}.$$

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

$$\overline{\mathcal{B}}(a,r) = \left\{ x \in \mathbb{R}^2 \quad \|x-a\| \leq r \right\}.$$

On pourrait bien entendu utiliser le mot *disque* ici, mais la notion de boule a vocation à être généralisée à $\mathbb{R}^n$ et même à des espaces vectoriels normés quelconques.

Exemple 2.

Représenter $\overline{\mathcal{B}}\left(0_{\mathbb{R}^2}, \frac{1}{2}\right)$. Représenter la boule ouverte de centre $(2, 1)$ et de rayon 1.

Définition 3.

On dit qu'une partie X de $\mathbb{R}^2$ est un **ouvert** si

$$\forall x \in X \quad \exists r > 0 \quad \mathcal{B}(x,r) \subset X.$$

Exemple 4.

Dessiner un ouvert de $\mathbb{R}^2$.
Montrer qu'une boule ouverte de $\mathbb{R}^2$ est un ouvert de $\mathbb{R}^2$.
Montrer qu'une intersection finie d'ouverts de $\mathbb{R}^2$ est un ouvert de $\mathbb{R}^2$.

1.2 Limite et continuité d'une fonction définie sur un ouvert de $\mathbb{R}^2$.

Définition 5.

Soit U un ouvert de $\mathbb{R}^2$, $f : U \to \mathbb{R}$, $a \in U$ et $\ell \in \mathbb{R}$.

On dit que f **tend vers** ℓ en a, noté $f(x) \xrightarrow[x\to a]{} \ell$ si

$$\forall \varepsilon > 0 \qquad \exists \eta > 0 \qquad \forall x \in U \qquad \|x - a\| \leq \eta \implies |f(x) - \ell| \leq \varepsilon$$

Il y a unicité de la limite, de sorte qu'on peut en parler, et noter ce nombre (éventuellement infini) $\lim\limits_{x\to a} f(x)$. Toute fonction ayant une limite finie en a est bornée au voisinage de a.

Définition 6.

Soit U un ouvert de $\mathbb{R}^2$, $f : U \to \mathbb{R}$, et $a \in U$ ainsi que $\ell \in \mathbb{R}$.

- On dit que f est **continue en** a si $f(x) \xrightarrow[x\to a]{} f(a)$.
- On dit que f est **continue sur** U si f est continue en tout $a \in U$.

On pourrait donner une caractérisation séquentielle, puis prouver que l'ensemble des fonctions continues en a est stable par somme, produit... Il faudrait aussi s'occuper de composition. Cela attendra la spé !

2 Dérivées partielles.

2.1 Dérivées partielles, gradient.

Définition 7.

Soient U ouvert de $\mathbb{R}^2$, $f : U \to \mathbb{R}$ et $a = (x_0, y_0) \in U$.

- On dit que f admet une **première dérivée partielle** en a si $x \mapsto f(x, y_0)$ est dérivable en x_0. Dans ce cas, on note $\frac{\partial f}{\partial x}(x_0, y_0)$ sa limite :

$$\frac{\partial f}{\partial x}(x_0, y_0) = \lim_{h\to 0} \frac{f(x_0 + h, y_0) - f(x_0, y_0)}{h}.$$

- On dit que f admet une **deuxième dérivée partielle** en a si $y \mapsto f(x_0, y)$ est dérivable en y_0. Dans ce cas, on note $\frac{\partial f}{\partial y}(x_0, y_0)$ sa limite :

$$\frac{\partial f}{\partial y}(x_0, y_0) = \lim_{h\to 0} \frac{f(x_0, y_0 + h) - f(x_0, y_0)}{h}.$$

Regarder $x \mapsto f(x, y_0)$ pour y_0 fixé, ou $y \mapsto f(x_0, y)$ pour x_0 fixé, c'est privilégier deux directions dans l'approche de (x_0, y_0) celles des deux vecteurs de la base canonique : on verra en spé la notion de dérivée selon un vecteur quelconque.

Ces dérivées définissent des fonctions définies sur U :

$$\frac{\partial f}{\partial x} : (x, y) \mapsto \frac{\partial f}{\partial x}(x, y) \qquad \text{et} \qquad \frac{\partial f}{\partial y} : (x, y) \mapsto \frac{\partial f}{\partial x}(x, y).$$

On pourra aussi noter $\partial_1 f$ la première dérivée partielle de f et $\partial_2 f$ sa seconde dérivée partielle.

Les règles de calcul des dérivées pour les fonctions d'une variable s'étendent, notamment la linéarité :

$$\partial_i (\lambda f + \mu g) = \lambda \partial_i f + \mu \partial_i g.$$

Définition 8.

Si $f : U \to \mathbb{R}$ admet des dérivées partielles en $a \in U$, on définit son **gradient** en a noté $\nabla f(a)$ ou parfois $\overrightarrow{\mathrm{grad}} f(a)$ par

$$\nabla f(a) = \begin{pmatrix} \dfrac{\partial f}{\partial x}(a) \\ \dfrac{\partial f}{\partial y}(a) \end{pmatrix}$$

Méthode.

Calculer la première dérivée partielle, c'est par définition dériver $x \mapsto f(x, y)$ pour y *fixé* : on dérive en traitant y comme une constante.
Pour le calcul de la seconde dérivée partielle, c'est x qui est traité comme une constante.

Exemples 9.

1. $f : (x, y) \mapsto x^2 + x^2 y - 2y^2$. Calculer $\dfrac{\partial f}{\partial x}(x, y)$ et $\dfrac{\partial f}{\partial y}(x, y)$ puis $\nabla f(1, 2)$.
2. Si g est dérivable sur $\mathbb{R}$, on pose $F(x, y) = g\left(\dfrac{y}{x}\right)$ définie sur $\mathbb{R}^* \times \mathbb{R}$.
   Calculer $\dfrac{\partial F}{\partial x}(x, y)$ et $\dfrac{\partial F}{\partial y}(x, y)$ et $\nabla F(x, y)$.

Exemple 10 (⚠).

Contrairement au cas d'une fonction d'une variable réelle, l'existence des dérivées partielles en a n'implique pas la continuité en a. On le constatera sur l'exemple ci-dessous :

f définie sur $\mathbb{R}^2$ par $\begin{cases} f(x, y) = \dfrac{xy}{x^2 + y^2} & \text{si } (x, y) \neq (0, 0) \\ f(0, 0) = 0 & \text{sinon} \end{cases}$ admet des dérivées partielles en $(0, 0)$ mais n'est pas continue en $(0, 0)$.

2.2 Fonctions de classe $\mathcal{C}^1$.

Définition 11.

Soit U ouvert de $\mathbb{R}^2$ et $f : U \to \mathbb{R}$.
On dit que f est **de classe** $\mathcal{C}^1$ sur U si f possède deux dérivées partielles en tout point de U **et** que ces dérivées partielles sont continues sur U.
On note $\mathcal{C}^1(U, \mathbb{R})$ l'ensemble des fonctions de classe $\mathcal{C}^1$ sur U.

Exemples 12.

1. Si I, J sont deux intervalles ouverts de $\mathbb{R}$ et $\varphi \in \mathcal{C}^1(I, \mathbb{R})$, $\psi \in \mathcal{C}^1(J, \mathbb{R})$ alors la fonction $(x, y) \mapsto \varphi(x)\psi(y)$ est de classe $\mathcal{C}^1$ sur $I \times J$ (qui est un ouvert de $\mathbb{R}^2$: exercice).
2. $(x, y) \mapsto \arctan\left(\frac{y}{x}\right)$ est de classe $\mathcal{C}^1$ sur $\mathbb{R}_+^* \times \mathbb{R}$.
3. $(x, y) \mapsto \|(x, y)\|$ est de classe $\mathcal{C}^1$ sur $\mathbb{R}^2 \setminus \{(0, 0)\}$.

Proposition 13 (DL à l'ordre 1)**.**

Toute fonction $f \in \mathcal{C}^1(U, \mathbb{R})$ admet le DL à l'ordre 1 suivant en tout point $a = (x_0, y_0) \in U$

$$f(x_0 + h, y_0 + k) \underset{(h,k)\to(0,0)}{=} f(x_0, y_0) + h\frac{\partial f}{\partial x}(x_0, y_0) + k\frac{\partial f}{\partial y}(x_0, y_0) + o\left(\|(h, k)\|\right).$$

Ou encore

$$f(a + H) \underset{H\to(0,0)}{=} f(a) + \langle \nabla f(a), H\rangle + o\left(\|H\|\right).$$

Le gradient de f en a définit la direction dans laquelle f croît le plus vite au voisinage de a.

Corollaire 14 (non non, cela n'est pas si évident)**.**

Soit U un ouvert de $\mathbb{R}^2$. Toute fonction de classe $\mathcal{C}^1$ sur U y est continue.

Définition 15 (Plan tangent à la surface en un point)**.**

Soit f une fonction de $\mathcal{C}^1$ sur un ouvert U de $\mathbb{R}^2$. On considère un point $(x_0, y_0, z_0) \in \mathbb{R}^3$ appartenant à la surface d'équation $z = f(x, y)$, c'est-à-dire tel que $(x_0, y_0) \in U$ et $z_0 = f(x_0, y_0)$.
Le plan d'équation

$$z - z_0 = (x - x_0)\frac{\partial f}{\partial x}(x_0, y_0) + (y - y_0)\frac{\partial f}{\partial y}(x_0, y_0)$$

est appelé **plan tangent** en (x_0, y_0) à la surface $z = f(x, y)$.

Revenons à une courbe d'équation $y = f(x)$. En un point (x_0, y_0) de la courbe, la tangente offre la meilleure approximation par une droite affine, d'équation $y - y_0 = f'(x_0)(x - x_0)$. Ce que l'on donne ici, c'est la meilleure approximation de la surface par un plan affine.

3 Deux questions naturelles.

3.1 Comment dériver une composée ?

Théorème 16 (Règle de la chaîne (1)).

Soient U un ouvert de $\mathbb{R}^2$ I un intervalle de $\mathbb{R}$.
Soient $f \in \mathcal{C}^1(U, \mathbb{R})$ et $\gamma : t \mapsto (x(t), y(t)) \in \mathcal{C}^1(I, U)$.
Alors $F : t \mapsto f(x(t), y(t))$ est de classe $\mathcal{C}^1$ sur I avec

$$\forall t \in I \qquad F'(t) = \frac{\mathrm{d}}{\mathrm{d}t} f(x(t), y(t)) = x'(t)\,\frac{\partial f}{\partial x}(x(t), y(t)) + y'(t)\,\frac{\partial f}{\partial y}(x(t), y(t))\,.$$

$$\text{soit} \qquad \forall t \in I \quad (f \circ \gamma)'(t) = \langle \gamma'(t), \nabla f(\gamma(t)) \rangle.$$

On dit qu'on a calculé la dérivée de f suivant l'arc paramétré γ.

Exemple 17.

Soit $f \in \mathcal{C}^1(\mathbb{R}^2, \mathbb{R})$. Calculer la dérivée de $\varphi : t \mapsto f\left(t^3, \cos t\right)$.

Théorème 18 (Règle de la chaîne (2)).

Soient U et V deux ouverts de $\mathbb{R}^2$, φ_1 et φ_2 dans $\mathcal{C}^1(U, \mathbb{R})$ et $\varphi : \left\{ \begin{array}{ccc} U & \to & \mathbb{R}^2 \\ (u, v) & \mapsto & (\varphi_1(u, v), \varphi_2(u, v)) \end{array} \right.$.
Si $f \in \mathcal{C}^1(V, \mathbb{R})$ et $\varphi(U) \subset V$, alors $f \circ \varphi$ est de classe $\mathcal{C}^1$ sur U et

$$\forall (u, v) \in U \qquad \begin{aligned} \frac{\partial (f \circ \varphi)}{\partial u}(u, v) &= \frac{\partial \varphi_1}{\partial u}(u, v) \times \frac{\partial f}{\partial x}(\varphi(u, v)) + \frac{\partial \varphi_2}{\partial u}(u, v) \times \frac{\partial f}{\partial y}(\varphi(u, v))\,. \\ \frac{\partial (f \circ \varphi)}{\partial v}(u, v) &= \frac{\partial \varphi_1}{\partial v}(u, v) \times \frac{\partial f}{\partial x}(\varphi(u, v)) + \frac{\partial \varphi_2}{\partial v}(u, v) \times \frac{\partial f}{\partial y}(\varphi(u, v))\,. \end{aligned}$$

Méthode (À la physicienne).

En notant $x(u, v) = \varphi_1(u, v)$ et $y(u, v) = \varphi_2(u, v)$,

$$\frac{\partial (f \circ \varphi)}{\partial u} = \frac{\partial f}{\partial x}\frac{\partial x}{\partial u} + \frac{\partial f}{\partial y}\frac{\partial y}{\partial u} \qquad \text{et} \qquad \frac{\partial (f \circ \varphi)}{\partial v} = \frac{\partial f}{\partial x}\frac{\partial x}{\partial v} + \frac{\partial f}{\partial y}\frac{\partial y}{\partial v}.$$

Exemple 19 (Changement de variable affine).

Soient a, b, c, d, e, f six réels et $g \in \mathcal{C}^1(\mathbb{R}^2, \mathbb{R})$. Calculer les dérivées partielles de

$$h : (x, y) \mapsto g(ax + by + c, dx + ey + f).$$

3.2 Que peut-on dire au sujet des extrema ?

Définition 20.

Soit $A \subset \mathbb{R}^2$, $f : A \to \mathbb{R}$ et $a \in A$. On dit que

- f admet un **maximum local** en a si $f(a)$ majore $f(A)$ au voisinage de a, soit
$$\exists r > 0 \qquad \forall x \in A \qquad \|x - a\| \leq r \Longrightarrow f(x) \leq f(a).$$
- f admet un **minimum local** en a si $f(a)$ minore $f(A)$ au voisinage de a, soit
$$\exists r > 0 \qquad \forall x \in A \qquad \|x - a\| \leq r \Longrightarrow f(x) \geq f(a).$$
- f présente un **extremum local** en a si elle y admet un maximum ou un minimum local.
- **Extremum global** : un maximum (resp. minimum) global est une valeur de f qui majore f (resp. minore f) sur toute la partie A.

Exemple 21.

$f : (x, y) \mapsto x^2 + y^2$ présente un minimum global en $(0, 0)$.

Proposition 22.

Soit f de classe $\mathcal{C}^1$ sur U ouvert de $\mathbb{R}^2$ et $a \in U$.

Si f admet un extremum local en a, alors
$$\frac{\partial f}{\partial x}(a) = \frac{\partial f}{\partial y}(a) = 0 \qquad \text{autrement dit} \qquad \nabla f(a) = (0, 0).$$
On dit alors que a est un **point critique**.

Exemple 23 (La réciproque est fausse !)**.**

Comme d'ailleurs pour les fonctions d'une seule variable, la réciproque est fausse.

Vérifier ainsi que $(0, 0)$ est un point critique de $f : (x, y) \mapsto x^2 - y^2$ mais n'est pas un extremum. Observer ce point sur la première page de ce poly.

Exemples 24.

1. $f : (x, y) \mapsto x^2 + y^2 - 2x - 4y$ admet un minimum global en un point de $\mathbb{R}^2$ à préciser.
2. La fonction $f : (x, y) \mapsto x^3 + y^3 - 6(x^2 - y^2)$ présente un minimum local en $(4, 0)$, un maximum local en $(0, -4)$. Les autres points critiques ne sont pas des extrema.

Exercices

$\boxed{42.1}$ **[♦◇◇]** Étudier l'existence des dérivées partielles pour les fonctions suivantes :

1. $(x,y) \mapsto \max(|x|,|y|)$
2. $(x,y) \mapsto |x|+|y|$
3. $(x,y) \mapsto \begin{cases} \frac{\sin(x^2)+\sin(y^2)}{\sqrt{x^2+y^2}} & \text{si } (x,y) \neq (0,0) \\ 0 & \text{sinon} \end{cases}$

$\boxed{42.2}$ **[♦◇◇]** Soit $f \in \mathcal{C}^1(\mathbb{R}^2,\mathbb{R})$. Calculer les dérivées (partielles éventuellement) des fonctions définies par

$g(x,y) = f(y,x)$ $\qquad$ $h(x,y) = f(x,x)$ $\qquad$ $j(x,y) = f(y,f(x,x))$ $\qquad$ $k(x) = f(x,f(x,x))$

$\boxed{42.3}$ **[♦♦◇]** Soit h une fonction continue sur $\mathbb{R}$.
Résoudre l'équation aux dérivées partielles $\dfrac{\partial f}{\partial x}(x,y) = h(x) \quad \text{sur } \mathbb{R}^2$.

$\boxed{42.4}$ **[♦♦◇]** Résoudre l'équation aux dérivées partielles $\dfrac{\partial f}{\partial x}(x,y) - \dfrac{\partial f}{\partial y}(x,y) = 0$, en utilisant le changement de variable $u = x+y$, $v = x-y$.

$\boxed{42.5}$ **[♦♦◇]** Résoudre l'équation aux dérivées partielles

$$x\frac{\partial f}{\partial x}(x,y) + y\frac{\partial f}{\partial y}(x,y) = \sqrt{x^2+y^2} \quad \text{sur} \quad \mathbb{R}_+^* \times \mathbb{R},$$

en utilisant les coordonnées polaires.

$\boxed{42.6}$ **[♦♦◇]** Soit $f : \mathbb{R}_+^* \times \mathbb{R} \to \mathbb{R}$ une fonction de classe $\mathcal{C}^1$. On définit la fonction associée en coordonnées polaires :

$$g : (r,\theta) \mapsto f(r\cos\theta, r\sin\theta), \quad \text{définie sur } \mathbb{R}_+^* \times \left]-\tfrac{\pi}{2},\tfrac{\pi}{2}\right[.$$

Pour $\theta \in \left]-\frac{\pi}{2},\frac{\pi}{2}\right[$, on définit la **base polaire** $(\overrightarrow{u_r},\overrightarrow{u_\theta})$ par

$$\overrightarrow{u_r} = (\cos\theta,\sin\theta) \qquad \text{et} \qquad \overrightarrow{u_\theta} = (-\sin\theta,\cos\theta)$$

Démontrer que g est de classe $\mathcal{C}^1$ sur $\mathbb{R}_+^* \times \left]-\frac{\pi}{2},\frac{\pi}{2}\right[$ puis que

$$\nabla f = \frac{\partial g}{\partial r}\overrightarrow{u_r} + \frac{1}{r}\frac{\partial g}{\partial \theta}\overrightarrow{u_\theta}.$$

$\boxed{42.7}$ **[♦♦◇]** Étudier les extrema locaux des fonctions suivantes :

1. $f : (x,y) \mapsto x^3+y^3$ sur $\mathbb{R}^2$
2. $f : (x,y) \mapsto x^2+y^2+\sin(x^2+y^2)$ sur $[-1,1]^2$
3. $f : (x,y) \mapsto x^2+3y^2+2xy-2x-10y+6$ sur $\mathbb{R}^2$
4. $f : (x,y) \mapsto e^{x\cos y}$ sur $\mathbb{R}^2$.
5. $f : (x,y) \mapsto x^3+5y^3+3x^2y+3xy^2-3y^2$ sur $T = \left\{(x,y) \in \mathbb{R}^2 \mid -1 \leq x \leq y \leq 1\right\}$.

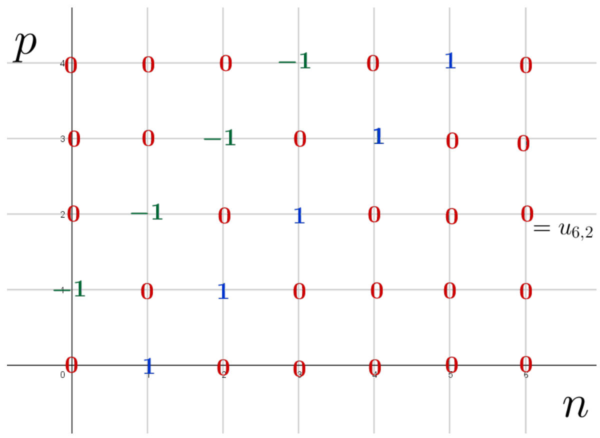
---

43 Familles sommables

Introduction.

Exemple 1 (Pour poser le problème).

Soit la famille $(u_{n,p})_{(n,p)\in\mathbb{N}^2}$ définie pour tout $(n,p) \in \mathbb{N}^2$ par $u_{n,p} = \begin{cases} 1 & \text{si } n = p+1 \\ -1 & \text{si } p = n+1 \\ 0 & \text{sinon} \end{cases}$.



Calculer : $\displaystyle\sum_{n=0}^{+\infty}\sum_{p=0}^{+\infty} u_{n,p}$, $\displaystyle\sum_{p=0}^{+\infty}\sum_{n=0}^{+\infty} u_{n,p}$, $\displaystyle\sum_{N=0}^{+\infty}\sum_{n+p=N} u_{n,p}$. Commenter.

1 Sommer des réels positifs.

1.0 Travailler dans $[0, +\infty]$.

On note $\boxed{[0, +\infty] = \mathbb{R}_+ \cup \{+\infty\}}$. On étend la relation d'ordre sur $\mathbb{R}_+$ à $[0, +\infty]$ en posant

$$\forall x \in \mathbb{R}_+ \quad x \leq +\infty, \quad \text{et on convient que} \quad +\infty \leq +\infty.$$

Ainsi, $+\infty$ est un majorant de toute partie de $[0, +\infty]$.

Pour ce qui concerne le produit et la somme, convenons que

$\forall x \in \mathbb{R}_+ \;\; x+(+\infty) = (+\infty)+x = +\infty \;\mid\; \forall y \in \mathbb{R}_+^* \;\; y\times(+\infty) = (+\infty)\times y = +\infty, \;\mid\; 0\times(+\infty) = (+\infty)\times 0 = 0.$

On étend enfin la notion de borne supérieure.

Définition 2.

On appelle **borne supérieure** d'une partie A de $[0, +\infty]$ le plus petit des majorants de A dans $[0, +\infty]$. Cet élément de $[0, +\infty]$ est noté $\sup(A)$.

Il est clair que toute partie non vide de $[0, +\infty]$ possède une borne supérieure dans $[0, +\infty]$. Par exemple

$$\sup([0, 1[) = 1, \qquad \sup(\,]0, +\infty[\,) = +\infty, \qquad \sup(\mathbb{N}) = +\infty.$$

Méthode (Passage au sup : l'argument clé du cours)**.**

Soient $M \in [0, +\infty]$ un réel et A une partie de $[0, +\infty]$. Pour démontrer l'inégalité $\sup(A) \leq M$, il suffira de montrer que M est un majorant de A. Autrement dit

$$(\forall x \in A \quad x \leq M) \quad \Longrightarrow \quad \sup(A) \leq M.$$

La caractérisation séquentielle de la borne supérieure s'étend aussi.

1.1 Somme d'une famille de réels positifs.

Définition 3.

Soit $(u_i)_{i\in I}$ une famille de réels <u>positifs</u>. On appelle **somme** de cette famille, notée $\sum_{i\in I} u_i$ le nombre

$$\sum_{i\in I} u_i = \sup\left\{\sum_{i\in F} u_i,\;\; F \subset I,\;\; F \text{ finie}\right\} \quad (\in [0, +\infty])\,.$$

Proposition 4.

Soit $(u_i)_{i\in I}$ une famille de réels positifs et $I' \subset I$. On a $\sum_{i\in I'} u_i \leq \sum_{i\in I} u_i$.

Proposition 5.

Soit $(u_i)_{i\in I}$ et $(v_i)_{i\in I}$ deux familles de réels positifs telles que $\forall i \in I\ u_i \leq v_i$. On a $\displaystyle\sum_{i\in I} u_i \leq \sum_{i\in I} v_i$.

Proposition 6 (Lien avec les sommes finies, les sommes de séries)**.**

Soit $(u_i)_{i\in I}$ une famille de réels positifs.

1. Si I est finie le nombre $\displaystyle\sum_{i\in I} u_i$ est à la fois la somme (finie) des nombres de la famille, et la somme de la famille (au sens de la définition précédente).

2. Si $I = \mathbb{N}$, alors $\displaystyle\sum_{i\in I} u_i = \sum_{k=0}^{+\infty} u_k$, le nombre à droite étant la somme de la série $\sum u_n$ (avec la convention que cette somme vaut $+\infty$ si cette série à termes positifs diverge).

Proposition 7 (Invariance de la somme par permutation, cas positif)**.**

Soit $(u_i)_{i\in I}$ une famille de nombres réels positifs et σ une bijection de I dans I. On a

$$\sum_{i\in I} u_{\sigma(i)} = \sum_{i\in I} u_i.$$

1.2 Familles sommables de réels positifs.

Définition 8.

Une famille de réels positifs $(u_i)_{i\in I}$ est dite **sommable** si sa somme est finie, ce qui se note

$$\sum_{i\in I} u_i < +\infty.$$

Proposition 9 (Opérations)**.**

Soit $(u_i)_{i\in I}$ et $(v_i)_{i\in I}$ deux familles de réels positifs (indexées par le même ensemble) et $\lambda \in \mathbb{R}_+$.

- La famille $(u_i + v_i)_{i\in I}$ est sommable si et seulement si la famille $(u_i)_{i\in I}$ et la famille $(v_i)_{i\in I}$ le sont. Dans tous les cas,

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

- Si $(u_i)_{i\in I}$ est sommable alors $(\lambda u_i)_{i\in I}$ l'est aussi. Dans tous les cas, $\displaystyle\sum_{i\in I} \lambda u_i = \lambda \sum_{i\in I} u_i$.

1.3 Sommation par paquets.

Théorème 10 (de sommation par paquets, cas positif)**.**

Soit $(u_i)_{i\in I}$ une famille de réels positifs.
On suppose que I s'écrit comme une réunion disjointe $I = \bigcup\limits_{j\in J} I_j$. Alors

$$\sum_{j\in J}\left(\sum_{i\in I_j} u_i\right) = \sum_{i\in I} u_i.$$

Corollaire 11 (si cette somme est finie, alors c'est sommable)**.**

Une famille $(u_i)_{i\in I}$ de nombres positifs est sommable si et seulement si

1. pour tout $j \in J$, $(u_i)_{i\in I_j}$ est sommable,
2. la famille $\big(\sum\limits_{i\in I_j} u_i\big)_{j\in J}$ est sommable.

Remarque. Un calcul de somme comme celle du théorème 10 est toujours justifié, par la seule positivité quitte à avoir un résultat infini. Le corollaire nous dit que faire les calculs permet de prouver la sommabilité.

Considérons en particulier le cas où les indices appartiennent à un produit cartésien, et où les « paquets » sont faits *sur les lignes ou sur les colonnes.*

Théorème 12 (de Fubini positif)**.**

Soit $(u_{i,j})_{(i,j)\in I\times J}$ une famille de réels positifs indexée par un produit cartésien $I \times J$. On a

$$\sum_{(i,j)\in I\times J} u_{i,j} = \sum_{i\in I}\sum_{j\in J} u_{i,j} = \sum_{j\in J}\sum_{i\in I} u_{i,j}.$$

Exemple 13 (Sommes triangulaires, cas positif)**.**

Soit $(u_{n,p})_{(n,p)\in\mathbb{N}^2}$ une famille de nombres réels positifs indexée par $\mathbb{N}^2$. On a

$$\sum_{(n,p)\in\mathbb{N}^2} u_{n,p} = \sum_{n=0}^{+\infty}\sum_{k=0}^{n} u_{k,n-k}.$$

Exemple 14.

Calculer la somme de la famille $\left(\dfrac{1}{p^2q^2}\right)_{(p,q)\in(\mathbb{N}^*)^2}$.

Montrer que la famille $\left(\dfrac{1}{(p+q)^2}\right)_{(p,q)\in(\mathbb{N}^*)^2}$ n'est pas sommable.

Exemple 15.

Démontrer l'identité $\sum_{p=2}^{+\infty} (\zeta(p) - 1) = 1$.

Exemple 16.

Soit $a \in [0, 1[$. En considérant la famille $(a^{pq})_{(p,q)\in(\mathbb{N}^*)^2}$, démontrer l'identité

$$\sum_{n=1}^{+\infty} \frac{a^n}{1 - a^n} = \sum_{n=1}^{+\infty} d(n)a^n,$$

où pour tout entier $n \in \mathbb{N}^*$, $d(n)$ est le nombre de diviseurs positifs de n.

2 Sommer des nombres complexes.

2.1 Familles sommables de nombres complexes : l'espace $\ell^1(I)$.

Définition 17.

Une famille $(u_i)_{i\in I}$ de $\mathbb{K}^I$ est dite **sommable** si $\sum_{i\in I} |u_i| < +\infty$.

L'ensemble des familles sommables de $\mathbb{K}^I$ est noté $\ell^1(I)$.

Proposition 18.

Si $(u_i)_{i\in I}$ est une famille sommable, alors toute sous-famille $(u_i)_{i\in I'}$ (avec $I' \subset I$) l'est aussi.

Proposition 19.

Soit $(u_i)_{i\in I} \in \mathbb{K}^I$ et $(v_i)_{i\in I}$ une famille de nombres réels positifs telles que

$$\forall i \in I \quad |u_i| \leq v_i.$$

Si la famille $(v_i)_{i\in I}$ est sommable, alors $(u_i)_{i\in I} \in \ell^1(I)$.

Proposition 20.

L'ensemble $\ell^1(I)$ des familles sommables de $\mathbb{K}^I$ est un sous-espace vectoriel de $\mathbb{K}^I$.

2.2 Somme d'une famille sommable de nombres complexes.

Définition 21 (Somme d'une famille sommable : le cas réel)**.**

Soit $(u_i)_{i\in I}$ une famille sommable de nombres réels. On pose

$$I_+ = \{i \in I \mid u_i \geq 0\} \quad \text{et} \quad I_- = \{i \in I \mid u_i < 0\}.$$

Les familles $(u_i)_{i\in I_+}$ et $(-u_i)_{i\in I_-}$ sont des familles sommables de réels positifs.

On appelle **somme** de la famille $(u_i)_{i\in I}$ et on note $\sum\limits_{i\in I} u_i$ le nombre réel défini par

$$\sum_{i\in I} u_i = \sum_{i\in I_+} u_i - \sum_{i\in I_-}(-u_i).$$

Définition 22 (Somme d'une famille sommable : le cas complexe)**.**

Soit $(u_i)_{i\in I}$ une famille sommable de nombres complexes.
Les familles $(\mathrm{Re}(u_i))_{i\in I}$ et $(\mathrm{Im}(u_i))_{i\in I}$ sont des familles réelles sommables.

On appelle **somme** de la famille $(u_i)_{i\in I}$ et on note $\sum\limits_{i\in I} u_i$ le nombre complexe défini par

$$\sum_{i\in I} u_i = \sum_{i\in I} \mathrm{Re}(u_i) + i \sum_{i\in I} \mathrm{Im}(u_i).$$

Par définition, la partie réelle de la somme c'est la somme des parties réelles, idem pour les parties imaginaires.

Proposition 23 (Lien avec les séries)**.**

Une famille $(u_n)_{n\in\mathbb{N}}$ est sommable si et seulement si la série $\sum u_n$ est absolument convergente.
Si c'est le cas,

$$\sum_{n\in\mathbb{N}} u_n = \sum_{n=0}^{+\infty} u_n,$$

le membre de gauche étant la somme de la famille, et celui de droite la somme de la série.

Proposition 24 (Approcher la somme par une somme finie)**.**

Soit $(u_i)_{i\in I}$ une famille sommable. Pour tout $\varepsilon > 0$, il existe une partie F finie de I telle que

$$\left| \sum_{i\in I} u_i - \sum_{i\in F} u_i \right| \leq \varepsilon.$$

Théorème 25 (Linéarité de la somme).

$$(u_i)_{i\in I} \mapsto \sum_{i\in I} u_i \text{ est une forme linéaire sur } \ell^1(I).$$

Proposition 26 (Croissance de la somme).

Si $(u_i)_{i\in I}$ et $(v_i)_{i\in I}$ sont deux familles sommables telles que $\forall i \in I\ u_i \leq v_i$, alors

$$\sum_{i\in I} u_i \leq \sum_{i\in I} v_i.$$

Corollaire 27 (Inégalité triangulaire).

$$\forall (u_i)_{i\in I} \in \ell^1(I) \qquad \left|\sum_{i\in I} u_i\right| \leq \sum_{i\in I} |u_i|.$$

Théorème 28 (Permutation des termes de la somme d'une famille sommable).

Soit $(u_i)_{i\in I}$ une famille sommable de nombres complexes et σ une bijection de I dans I. On a

$$\sum_{i\in I} u_{\sigma(i)} = \sum_{i\in I} u_i.$$

En particulier, on peut permuter les termes de la somme d'une série absolument convergente.

2.3 Sommation par paquets.

Théorème 29 (de sommation par paquets).

Soit $(u_i)_{i\in I}$ une famille de nombres complexes
On suppose que I s'écrit comme une réunion disjointe $I = \bigcup_{j\in J} I_j$.

Si u est sommable,

$$\boxed{\sum_{j\in J}\left(\sum_{i\in I_j} u_i\right) = \sum_{i\in I} u_i.}$$

Rappel d'une condition nécessaire et suffisante pour que u soit sommable

$$u \in \ell^1(I) \quad\iff\quad \left\{ \begin{array}{c} \text{pour tout } j \in J,\ \sum_{i\in I_j} |u_i| < +\infty \\ \text{la famille } \left(\sum_{i\in I_j} |u_i|\right)_{j\in J} \text{ est sommable} \end{array} \right\}.$$

Théorème 30 (de Fubini)**.**

Soit $(u_{i,j})_{(i,j)\in I\times J}$ une famille de nombres complexes indexée par un produit cartésien $I \times J$.

Si u est <u>sommable</u>,
$$\boxed{\sum_{(i,j)\in I\times J} u_{i,j} = \sum_{i\in I}\sum_{j\in J} u_{i,j} = \sum_{j\in J}\sum_{i\in I} u_{i,j}.}$$

Rappel de deux conditions nécessaires et suffisantes pour que u soit sommable

$$u \in \ell^1(I) \iff \left\{\begin{array}{l} \text{pour tout } j \in J,\ \sum_{i\in I} |u_{i,j}| < +\infty \\ \text{et } \Big(\sum_{i\in I} |u_{i,j}|\Big)_{j\in J} \text{ est sommable} \end{array}\right\} \iff \left\{\begin{array}{l} \text{pour tout } i \in I,\ \sum_{j\in J} |u_{i,j}| < +\infty \\ \text{et } \Big(\sum_{j\in J} |u_{i,j}|\Big)_{i\in I} \text{ est sommable} \end{array}\right\}.$$

Exemple 31 (Sommes triangulaires)**.**

Soit $(u_{n,p})_{(n,p)\in\mathbb{N}^2}$ une famille sommable de nombres complexes. On a
$$\sum_{(n,p)\in\mathbb{N}^2} u_{n,p} = \sum_{n=0}^{+\infty}\sum_{k=0}^{n} u_{k,n-k}.$$

Méthode (Le calcul d'abord, la justification ensuite)**.**

En pratique, on pourra écrire une sommation par paquets ou un échange de somme "sous réserve de sommabilité", le temps de voir si on aboutit ainsi à un résultat intéressant.

Le cas échéant, il est encore temps de prouver la sommabilité en sommant les modules.
On insiste sur le fait que les calculs de somme sur les modules sont justifiés par la seule positivité !

Exemple 32 (Retour sur un exemple)**.**

Soit $z \in \mathbb{C}$ tel que $|z| < 1$. Démontrer que la famille $(z^{pq})_{(p,q)\in(\mathbb{N}^*)^2}$ est sommable.

Expliquer pourquoi on peut déduire du travail fait à l'exemple 16 que
$$\sum_{n=1}^{+\infty} \frac{z^n}{1-z^n} = \sum_{n=1}^{+\infty} d(n) z^n,$$
où pour tout entier $n \in \mathbb{N}^*$, $d(n)$ est le nombre de diviseurs positifs de n.

Exemple 33.

Soit $z \in \mathbb{C}$ tel que $|z| < 1$. Démontrer les identités
$$\sum_{n=1}^{+\infty} \frac{z^{2n-1}}{1-z^{2n-1}} = \sum_{n=1}^{+\infty} \frac{z^n}{1-z^{2n}}, \quad \text{et} \quad \sum_{n=0}^{+\infty} \frac{z^{2^n}}{1-z^{2^{n+1}}} = \frac{z}{1-z}.$$

2.4 Produits.

Proposition 34.

Si $(a_i)_{i\in I}$ et $(b_j)_{j\in J}$ sont deux familles sommables, alors la famille $(a_ib_j)_{(i,j)\in I\times J}$ est sommable et
$$\sum_{(i,j)\in I\times J} a_ib_j = \left(\sum_{i\in I} a_i\right)\left(\sum_{j\in J} b_j\right).$$
Ce résultat s'étend à un produit fini de familles sommables.

Théorème 35 (Produit de Cauchy de deux séries absolument convergentes)**.**

Soit $\sum a_n$ et $\sum b_n$ deux séries de nombres complexes toutes deux absolument convergentes.

La série de terme général
$$\sum_{p+q=n} a_pb_q,$$
est absolument convergente. On l'appelle **produit de Cauchy** de $\sum a_n$ et $\sum b_n$.

On a
$$\left(\sum_{n=0}^{+\infty} a_n\right)\left(\sum_{n=0}^{+\infty} b_n\right) = \sum_{n=0}^{+\infty}\left(\sum_{p+q=n} a_pb_q\right).$$

Exemple 36.

Démontrer que pour tout $z\in\mathbb{C}$ tel que $|z|<1$,
$$\frac{1}{(1-z)^2} = \sum_{n=0}^{+\infty}(n+1)z^n.$$

Exemple 37 (Propriété de morphisme de l'exponentielle, et retour sur le début de l'année)**.**

Pour tout $z\in\mathbb{C}$ on <u>définit</u> le nombre $\exp(z)$ par
$$\exp(z) := \sum_{n=0}^{+\infty}\frac{z^n}{n!};$$
(on avait prouvé qu'il s'agit bien d'une série absolument convergente).

Démontrer que
$$\forall (z,\widetilde{z})\in\mathbb{C}^2 \quad \exp(z+\widetilde{z}) = \exp(z)\exp(\widetilde{z}).$$
Démontrer que $\exp : x\mapsto \exp(x)$ est dérivable sur $\mathbb{R}$ et qu'elle est sa propre dérivée.

Exercices

On rappelle que, d'après le critère de convergence des séries de Riemann, la fonction $\zeta : x \mapsto \sum\limits_{n=1}^{+\infty} \frac{1}{n^x}$ est bien définie sur $]1, +\infty[$.

$\boxed{\textbf{43.1}}$ **[♦♦◇]** Calculer la somme de $\left(\dfrac{1}{(i+j^2)(i+j^2+1)}\right)_{i\geq 0, j\geq 1}$ (on suppose $\zeta(2)$ connu). En déduire

$$\sum_{n=1}^{+\infty} \frac{\lfloor\sqrt{n}\rfloor}{n(n+1)}.$$

$\boxed{\textbf{43.2}}$ **[♦♦◇]** Montrer que $\left(\dfrac{1}{(|p|+|q|)^s}\right)_{(p,q)\in\mathbb{Z}^2\setminus\{(0,0)\}}$ est une famille sommable si et seulement si $s > 2$.

Exprimer alors sa somme à l'aide de la fonction ζ.

$\boxed{\textbf{43.3}}$ **[♦♦◇]** [Mines MP 2019]

Calculer $\displaystyle\sum_{n=2}^{+\infty}(n-1)\left(2^n(\zeta(n)-1)-1\right)$.

$\boxed{\textbf{43.4}}$ **[♦♦♦]** [Produit eulérien pour la fonction ζ]

Notons $\mathcal{P}$ l'ensemble des nombres premiers. L'objectif de cet exercice est de démontrer que pour tout $x > 1$, on a

$$\boxed{\zeta(x) = \prod_{p\in\mathcal{P}}\left(1 - \frac{1}{p^{-x}}\right)},$$

en expliquant en particulier le sens du produit. Cette identité due à Euler permet d'entrevoir l'importance de la fonction ζ en arithmétique.

Pour $n \in \mathbb{N}^*$, on note p_n le n-ème nombre premier et $u_n(x) = \displaystyle\prod_{k=1}^{n} \frac{1}{1-p_k^{-x}}$.

1. Justifier pour $x > 1$ l'égalité $u_n(x) = \displaystyle\sum_{(j_1,\dots,j_n)\in\mathbb{N}^n} p_1^{-j_1 x}\cdots p_n^{-j_n x}$.
2. En déduire l'inégalité
$$|\zeta(x) - u_n(x)| \leq \sum_{m\geq p_{n+1}} \frac{1}{m^x}.$$
3. Conclure.

Remarque : la divergence en 1 de ζ témoigne de l'infinité de l'ensemble des nombres premiers : si $\mathcal{P}$ était fini, le produit le serait, et ζ aurait en 1 une limite finie.
