Classe de Mathématiques Supérieures

Cours de Mathématiques

Table des matières

Chapitre 0

Fondements des mathématiques

Ce chapitre d'introduction a pour but de poser un socle commun de notations, d'expressions et de modes de raisonnement qui nous permettront de bien nous comprendre au cours de l'année.

Il est généralement peu populaire, parce qu'assez abstrait et manque d'exemples inspirés des mathématiques. En effet, jusqu'à ce jour, les mathématiques étaient pour nous essentiellement du calcul, et très marginalement du raisonnement. Nous avons donc à disposition très peu de raisonnements connus qui pourraient illustrer ce cours sur la manière de raisonner. Les élèves ont ainsi du mal à voir la relevance du contenu de ce cours à l'activité mathématique. Et pourtant, il est absolument fondamental.

À l'issue de ce cours, il est ainsi indispensable que vous compreniez immédiatement ce que fait le professeur lorsqu'il dit qu'il va raisonner directement, par l'absurde ou par contre-apposée ; les notations de la théorie des ensembles doivent être assimilées ; ainsi que le vocabulaire sur les applications (injection, surjection, bijection). Ces notions seront constamment utilisées dans le cours de mathématiques.

0.1 Logique

0.1.1 Assertions, théorèmes

Définition 0.1.1
Une *assertion*, ou *proposition*, est une phrase dont on peut se demander si elle est vraie ou fausse.

Exemple 0.1.2
« Il fait beau aujourd'hui » ou « J'ai oublié mon pull » sont des assertions, tandis que « Quel temps fera-t-il demain ? » n'en est pas une.

De manière inhérente à la définition d'une assertion se trouve le *principe du tiers exclus* : une assertion est vraie ou fausse, mais pas les deux à la fois. De fait, on peut associer, sans ambiguïté, à une assertion une et une seule valeur de vérité : le « vrai » ou le « faux ».

Remarquons qu'il n'est pas forcément simple d'accéder à cette valeur de vérité.

Exemple 0.1.3
« Il existe des extraterrestres » est une proposition, dont il est bien difficile à l'heure actuelle de connaître la valeur de vérité.

Définition 0.1.4
Un *théorème de logique* (ou plus simplement *théorème* ou *tautologie*) est une assertion vraie.

Dans le cours de mathématiques, vous verrez souvent apparaître des assertions que nous appellerons *lemme*, *proposition* et *corollaire*. Ces propositions sont toutes des théorèmes. On les distingue pour nuancer la notion de théorème, de manière à classifier ces derniers suivant leur importance. Sauf oubli ou manquement de la part du professeur,

- un *théorème* est une assertion vraie d'une importance fondamentale. Il ne s'agit pas forcément d'un résultat difficile ; mais c'est une pierre angulaire du cours de mathématiques.
- une *proposition* désigne la plupart des assertions vraies.
- un *lemme* est une assertion vraie. Prise en tant que telle, elle a un intérêt assez limité et sa démonstration est souvent technique et désagréable. C'est surtout un résultat intermédiaire à l'établissement d'un théorème ou d'une proposition.
- un *corollaire* est une conséquence, souvent immédiate, d'un théorème ou d'une proposition établi précédemment.

0.1.2 Connecteurs logiques

On appelle *connecteur logique* n'importe quel moyen de former une nouvelle proposition à partir d'une ou plusieurs autres, mais avec la restriction suivante : la valeur de vérité de l'assertion obtenue doit dépendre uniquement des valeurs de vérité des assertions qui sont connectées.

Autrement dit, si $\propto$ est un connecteur logique à deux assertions, on est capable de dire si la proposition $\boldsymbol{p} \propto \boldsymbol{q}$ est vraie pour peu que l'on connaisse les valeurs de vérité des propositions $\boldsymbol{p}$ et $\boldsymbol{q}$. Enfonçons le clou : pour évaluer $\boldsymbol{p} \propto \boldsymbol{q}$, ce que signifient réellement $\boldsymbol{p}$ et $\boldsymbol{q}$ n'a aucune influence sur $\boldsymbol{p} \propto \boldsymbol{q}$, seules leurs valeurs de vérité en ont.

L'intérêt de cette restriction – après tout, un connecteur logique aurait simplement pu être n'importe quel moyen de former une nouvelle proposition à partir de deux autres – est le suivant : puisqu'il nous suffit de connaître les valeurs de vérité de $\boldsymbol{p}$ et de $\boldsymbol{q}$ pour pouvoir dire si $\boldsymbol{p} \propto \boldsymbol{q}$ est vraie, ce connecteur peut simplement être décrit par la donnée des quatre valeurs $\mathbf{V} \propto \mathbf{V}$, $\mathbf{V} \propto \mathbf{F}$, $\mathbf{F} \propto \mathbf{V}$ et $\mathbf{F} \propto \mathbf{F}$. Les connecteurs logiques peuvent donc facilement être définis, par exemple à l'aide d'une *table de vérité*. Du style :

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{p} \propto \boldsymbol{q}$
V	**V**	
V	**F**	
F	**V**	
F	**F**	

Une fois la dernière colonne remplie, le connecteur $\propto$ est parfaitement défini. Notons que, du coup, il n'existe que 16 connecteurs logiques à deux assertions, puisqu'il n'y a que 16 possibilités différentes de tels tableaux.

Exemple 0.1.5
Terminons ce paragraphe en donnant un exemple de manière de relier deux propositions, mais qui ne soit pas un connecteur logique. Prenons l'adverbe **puis**, qui sert à établir un ordre chronologique entre deux évènements. Si $\boldsymbol{p}$ et $\boldsymbol{q}$ sont deux propositions, la proposition $\boldsymbol{p}$ **puis** $\boldsymbol{q}$ est vraie si $\boldsymbol{p}$ et $\boldsymbol{q}$ le sont toutes deux, et si $\boldsymbol{p}$ s'est produit avant $\boldsymbol{q}$; dans tous les autres cas, $\boldsymbol{p}$ **puis** $\boldsymbol{q}$ est fausse.

On peut d'ores et déjà deviner que « puis » n'est pas un connecteur logique, puisqu'il y a la notion de temps qui lui est inhérente. Mais pour le vérifier effectivement, il suffit d'établir que « puis » met en défaut la définition d'un connecteur logique donnée plus haut. Pour cela, prenons les propositions suivantes :

p « Aujourd'hui, j'ai pris mon petit déjeuner. »
q « Aujourd'hui, j'ai déjeuné. »

et imaginons qu'il est 23h, la journée est terminée, j'ai bien pris tous mes repas, de sorte que ***p***, ***q*** sont chacune vraie. Remarquons alors que ***p* puis *q*** est vraie. Si **puis** était un connecteur logique, ***q* puis *p*** devrait aussi être vraie, ce qui n'est pas le cas.

L'équivalence « $\Longleftrightarrow$ »

Définition 0.1.6
Deux propositions ***p*** et ***q*** sont dites équivalentes, ce qu'on note $p \Longleftrightarrow q$ si elles ont la même valeur de vérité, ce que résume la table de vérité suivante :

p	***q***	$p \Longleftrightarrow q$
V	**V**	**V**
V	**F**	**F**
F	**V**	**F**
F	**F**	**V**

On dira indifféremment que
- ***p*** et ***q*** sont équivalentes ;
- ***p*** si et seulement si ***q***.

Cette dernière terminologie est somme toute assez naturelle : à voir la table de vérité, si on sait que $p \Longleftrightarrow q$, alors ***p*** est vraie si ***q*** l'est, et seulement dans ce cas-là.

Remarquons que l'équivalence de deux propositions ne signifie pas forcément qu'elles veulent dire la même chose. Elle signifie simplement ce par quoi elle a été définie : les deux propositions ont la même valeur de vérité.

Exemple 0.1.7
« La Terre tourne autour du soleil » et « Je suis un homme » sont deux propositions équivalentes, bien qu'elles n'aient aucun rapport entre elles ; en particulier, elles ne veulent certainement pas dire la même chose.

L'intérêt de l'équivalence est le suivant : si on sait que $p \Longleftrightarrow q$ est vraie, alors on peut remplacer indifféremment ***p*** par ***q*** (et vice-versa) dans n'importe quelle assertion faisant intervenir ***p*** et des connecteurs logiques, puisque ces derniers ne dépendent que des valeurs de vérité des assertions qu'ils mettent en jeu, et pas du contenu de celles-ci.

La négation « non »

Définition 0.1.8
La négation, notée **non**, est un connecteur simple (il ne s'applique qu'à une seule proposition) défini par la table de vérité suivante :

p	non ***p***
V	**F**
F	**V**

Observons le

Théorème 0.1.9 (Double négation)
Si p *est une proposition, alors* $p \iff$ ***non*****(*****non*** p**)**.

Preuve : Il suffit d'établir la table de vérité de la proposition $p \iff$ **non(non** p**)** à l'aide des règles de manipulation de la négation et de l'équivalence, pour vérifier qu'elle est vraie :

p	non p	non(non p)	$p \iff$ non(non p)
V	F	V	V
F	V	F	V

□

Ajoutons que la négation est compatible avec l'équivalence, c'est-à-dire qu'on peut nier les deux membres d'une équivalence sans changer la vérité de celle-ci :

Théorème 0.1.10
Soient p *et* q *deux propositions. Alors*

$$(p \iff q) \iff (\textit{non } p \iff \textit{non } q)$$

Preuve : Même principe que précédemment : dressons la table de vérité de l'assertion précédente et vérifions qu'il s'agit d'un théorème.

p	q	$p \iff q$	non p	non q	non $p \iff$ non q
V	V	V	F	F	V
V	F	F	F	V	F
F	V	F	V	F	F
F	F	V	V	V	V

Les colonnes $p \iff q$ et **non** $p \iff$ **non** q sont identiques ce qui achève la démonstration. □

La disjonction « ou », la conjonction « et »

Définition 0.1.11
La *disjonction*, notée **ou**, est le connecteur double (il s'applique à deux assertions) défini par la table de vérité suivante :

p	q	p ou q
V	V	V
V	F	V
F	V	V
F	F	F

Observons que le **ou** mathématique a un sens précis, par opposition aux diverses utilisations du mot « ou » dans la langue française. En effet, suivant le contexte, il peut être interprêté différemment dans le language :

- Au restaurant, si vous prenez un menu plutôt que de commander à la carte, vous aurez le plus souvent le choix entre du fromage ou un dessert. Cela veut dire que vous pouvez prendre l'un ou l'autre de ces plats pour finir le repas, mais pas les deux. Il s'agit d'un « ou » exclusif, puisqu'il exclue le service des deux plats à la fois.

- Des amis vous proposent de jouer au football et vous leur répondez « Ok, mais s'il pleut ou s'il fait du vent, je ne jouerai pas avec vous ». Dans ce cas, vous annoncez que dès que l'un ou l'autre des évènements climatiques se produit, vous ne serez pas de la partie. Il s'agit d'un « ou » inclusif.

Le « ou » mathématique est donc inclusif.

Définition 0.1.12
La *conjonction*, notée **et**, est le connecteur double défini par la table de vérité

p	q	p et q
V	V	V
V	F	F
F	V	F
F	F	F

Établissons les relations évidentes entre le connecteurs définis jusqu'à maintenant :

Théorème 0.1.13 (Lois de De Morgan)
Soient p et q deux assertions. Alors

- ***non*(*p ou q*) $\Longleftrightarrow$ (*non p*) *et* (*non q*)**
- ***non*(*p et q*) $\Longleftrightarrow$ (*non p*) *ou* (*non q*)**

Preuve : On procède comme pour le **Théorème 1.9** :

p	q	p ou q	non(p ou q)	non p	non q	(non p) et (non q)
V	V	V	F	F	F	F
V	F	V	F	F	V	F
F	V	V	F	V	F	F
F	F	F	V	V	V	V

Les colonnes **non(*p* ou *q*)** et **(non *p*) et (non *q*)** sont identiques ce qui établit la première équivalence **non(*p* ou *q*) $\Longleftrightarrow$ (non *p*) et (non *q*)**.

De même pour la deuxième partie du théorème :

p	q	p et q	non(p et q)	non p	non q	(non p) ou (non q)
V	V	V	F	F	F	F
V	F	F	V	F	V	V
F	V	F	V	V	F	V
F	F	F	V	V	V	V

Les colonnes **non(*p* et *q*)** et **(non *p*) ou (non *q*)** sont identiques ce qui établit la première équivalence **non(*p* et *q*) $\Longleftrightarrow$ (non *p*) ou (non *q*)**. □

Exemple 0.1.14
Considérons les assertions suivantes :

p « Je pratique le tennis. »
q « Je pratique le football. »

D'après les lois de De Morgan, les assertions **(non p) et (non q)** (« Je ne pratique ni le tennis, ni le football ») et **non(p ou q)** (« Il est faux que je pratique le tennis ou le football ») sont équivalentes. Il n'y a rien de mystérieux là-dessous, c'est du bon sens.

Une conséquence, qui permet de mélanger tout ce qui a été vu jusqu'à présent :

Corollaire 0.1.15
Soient p et q deux assertions. Alors
- p ***ou*** $q \iff$ ***non***$\big($(***non*** p) ***et*** (***non*** q)$\big)$
- p ***et*** $q \iff$ ***non***$\big($(***non*** p) ***ou*** (***non*** q)$\big)$

Preuve : Partons du principe de double négation :

$$p \text{ ou } q \iff \text{non}(\text{non}(p \text{ ou } q))$$

La première loi de De Morgan nous permet de récrire le membre de droite

$$p \text{ ou } q \iff \text{non}((\text{non } p) \text{ et } (\text{non } q))$$

et le premier théorème est démontré. On procède de la même manière pour le second. □

Exemple 0.1.16
Illustrons le premier théorème, à l'aide des propositions utilisées à l'exemple précédent. Les assertions p **ou** q (« Je pratique le tennis ou le football ») et **non((non p) et (non q))** (« Il est faux que je ne pratique ni le tennis, ni le football ») sont équivalentes. À nouveau, c'est du bon sens.

L'implication $\Longrightarrow$

Définition 0.1.17
L'*implication*, notée $\Longrightarrow$, est le connecteur double défini par la table de vérité suivante :

p	q	$p \Longrightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

On dira indifféremment que
- p implique q ;
- p est une condition suffisante à q ;
- pour que q, il suffit que p ;
- q est une condition nécessaire de p ;
- si p, alors q.

Remarquons que la véracité d'une implication ne signifie en aucun cas qu'il y a un rapport entre les deux assertions. L'intuition suivant laquelle il devrait y avoir un rapport provient du choix du mot « implication » et du sens qu'il possède en Français ; mais, comme nous l'avons vu avec le connecteur « ou », le sens mathématique et le sens français d'un mot peuvent différer.

Néanmoins, la terminologie n'a pas été choisie au hasard et l'implication $p \Longrightarrow q$, si vraie, signifie bien que si p est vraie, alors q l'est aussi. Cela se voit sur la table de vérité et c'est cette constatation qui résume l'utilité principale de ce connecteur logique.

Rentrons dans les détails. Imaginons qu'on ait deux assertions p et q. Pour des raisons pratiques, il est facile de voir que p est vraie ; en revanche, la véracité de q n'est pas si évidente. Si, par un procédé quelconque, on a réussi à prouver que $p \Longrightarrow q$ est vraie, alors c'est que q l'est aussi. C'est ce qu'on appelle le raisonnement par *syllogisme*.

Exemple 0.1.18
Considérons les assertions suivantes :

p « Il pleut. »
q « Il y a des nuages. »

L'étude météorologique montre que l'implication $p \Longrightarrow q$ est vraie : la pluie est le produit de nuages de vapeur d'eau qui condensent dans l'atmosphère.

Imaginons maintenant que je sois enfermé dans une cave par mes parents abusifs. Je ne peux pas voir le ciel donc je ne sais pas s'il est nuageux. En revanche, j'entends la pluie tomber. J'en déduis qu'il y a des nuages.

0.1.3 Quelques tautologies

Voici quelques tautologies (voir la **Définition 1.4**) que vous aurez à démontrer en exercice. Le principe est exactement le même que pour les **Théorèmes 1.9, 1.13** et **1.15**. Certaines d'entre elles sont suffisamment importantes pour avoir un nom.

Théorème 0.1.19
Dans ce qui suit, p, q et r sont des assertions. Alors

$(p \textbf{ ou } p) \Longleftrightarrow p$	
$(p \textbf{ et } p) \Longleftrightarrow p$	
$p \textbf{ ou } (\textbf{non } p)$	*principe du tiers exclus*
$((p \textbf{ ou } q) \textbf{ ou } r) \Longleftrightarrow (p \textbf{ ou } (q \textbf{ ou } r))$	*associativité du* **ou**
$((p \textbf{ et } q) \textbf{ et } r) \Longleftrightarrow (p \textbf{ et } (q \textbf{ et } r))$	*associativité du* **et**
$\textbf{non}\big(p \textbf{ et } (\textbf{non } p)\big)$	
$p \textbf{ et } (q \textbf{ ou } r) \Longleftrightarrow \big((p \textbf{ et } q) \textbf{ ou } (p \textbf{ et } r)\big)$	*distributivité de* **et** *sur* **ou**
$p \textbf{ ou } (q \textbf{ et } r) \Longleftrightarrow \big((p \textbf{ ou } q) \textbf{ et } (p \textbf{ ou } r)\big)$	*distributivité de* **ou** *sur* **et**
$(\textbf{non}(\textbf{non } p)) \Longleftrightarrow p$	*loi de la double négation*
$p \Longrightarrow p$	
$(p \textbf{ et } (p \Longrightarrow q)) \Longrightarrow q$	*syllogisme*
$(p \Longrightarrow q) \Longleftrightarrow ((\textbf{non } p) \textbf{ ou } q)$	
$(p \Longrightarrow q) \Longleftrightarrow ((\textbf{non } q) \Longrightarrow (\textbf{non } p))$	*principe de contre-apposition*
$(\textbf{non } (p \Longrightarrow q)) \Longleftrightarrow (p \textbf{ et } (\textbf{non } q))$	
$((p \Longrightarrow q) \textbf{ et } (q \Longrightarrow r)) \Longrightarrow (p \Longrightarrow r)$	*transitivité de l'implication*
$((\textbf{non } p) \Longrightarrow (q \textbf{ et } (\textbf{non } q))) \Longleftrightarrow p$	*raisonnement par l'absurde*
$((p \Longrightarrow q) \textbf{ et } (q \Longrightarrow p)) \Longleftrightarrow (p \Longleftrightarrow q)$	*équivalence et double implication*

0.1.4 Modes de raisonnement en mathématiques

Syllogisme

Le raisonnement par syllogisme (on parle aussi de raisonnement direct) a déjà été expliqué dans le paragraphe consacré à l'implication.

Si on veut montrer qu'une assertion $\boldsymbol{q}$ est vraie, on essaie d'en trouver une $\boldsymbol{p}$ qui soit vraie et telle que $\boldsymbol{p} \Longrightarrow \boldsymbol{q}$.

Contre-apposée

Le raisonnement par contre-apposée repose sur la tautologie

$$(\boldsymbol{p} \Longrightarrow \boldsymbol{q}) \Longleftrightarrow ((\textbf{non } \boldsymbol{q}) \Longrightarrow (\textbf{non } \boldsymbol{p}))$$

Celle-ci nous dit que montrer $\boldsymbol{p} \Longrightarrow \boldsymbol{q}$ ou montrer que $(\textbf{non } \boldsymbol{q}) \Longrightarrow (\textbf{non } \boldsymbol{p})$, c'est la même chose. Il se trouve que, parfois, c'est plus simple de procéder ainsi.

Exemple 0.1.20
Étant donné un triangle ABC, considérons les assertions suivantes :

$\boldsymbol{p}$ « ABC est rectangle en A. »
$\boldsymbol{q}$ « $BC^2 = AB^2 + AC^2$ »

Le théorème de Pythagore nous dit que $\boldsymbol{p} \Longrightarrow \boldsymbol{q}$ est vraie. Et $(\textbf{non } \boldsymbol{q}) \Longrightarrow (\textbf{non } \boldsymbol{p})$ est sa contre-apposée ; elle se lit : « Si $BC^2 \neq AB^2 + AC^2$, alors le triangle ABC n'est pas rectangle en A. » Cette assertion est vraie, en vertu du principe de contre-apposition, puisque le théorème de Pythagore est vrai.

Toujours est-il que, si AB = 3, AC = 4 et BC = 6, on sait que ABC n'est pas rectangle en A. Et pour démontrer cela, on a utilisé le fait que $6^2 \neq 3^2 + 4^2$ et la contre-apposée du théorème de Pythagore.

Par l'absurde

Le raisonnement par l'absurde repose sur la tautologie

$$((\textbf{non } \boldsymbol{p}) \Longrightarrow (\boldsymbol{q} \textbf{ et } (\textbf{non } \boldsymbol{q}))) \Longleftrightarrow \boldsymbol{p}$$

Une petite explication s'impose. On veut montrer $\boldsymbol{p}$. Cela revient au même que trouver une assertion $\boldsymbol{q}$, telle que $\boldsymbol{q}$ et $\textbf{non } \boldsymbol{q}$ soient conséquence de $\textbf{non } \boldsymbol{p}$.

Disons-le autrement : on essaie de montrer que $\textbf{non } \boldsymbol{p}$ implique à la fois $\boldsymbol{q}$ et son contraire $\textbf{non } \boldsymbol{q}$. On est ainsi arrivé à une absurdité, d'où le nom de ce raisonnement.

Toute la difficulté consiste à trouver cette assertion $\boldsymbol{q}$.

Voici un exemple :

Exemple 0.1.21
On vous a déjà dit que -1 n'a pas de racine carrée dans $\mathbb{R}$. Montrons-le en définissant :

$$\boldsymbol{p} : \text{« } \sqrt{-1} \text{ n'est pas un nombre réel. »}$$

Pour démontrer cela par l'absurde, on part de

$$\textbf{non } \boldsymbol{p} : \text{« } \sqrt{-1} \text{ est réel. »}$$

et on voit ce qu'on peut en déduire. On sait déjà que $(\sqrt{-1})^2 = i^2 = -1$.

Mais aussi, à l'aide des règles de manipulation des racines carrées :

$$(\sqrt{-1})^2 = \sqrt{-1} \times \sqrt{-1} = \sqrt{(-1)\times(-1)} = \sqrt{1} = 1$$

On voit donc qu'en posant

$$\boldsymbol{q} : \text{« } (\sqrt{-1})^2 = -1 \text{ »}$$

on a à la fois $\boldsymbol{q}$ et **non** $\boldsymbol{q}$. Donc $\boldsymbol{p}$ est vraie.

0.2 Ensembles, prédicats et quantificateurs

0.2.1 Généralités sur les ensembles

Définition 0.2.1

- On appelle *ensemble* toute collection d'objets.
- Si E est un ensemble et *a est un objet appartenant à* E, on notera $a \in \mathrm{E}$.
- Si E et F sont des ensembles, on dit que E *est inclus dans* F, ce qu'on note $\mathrm{E} \subset \mathrm{F}$, si et seulement si tout élément de E est élément de F.
- Il existe un ensemble, appelé *ensemble vide* et noté $\emptyset$, qui est inclus dans tout ensemble.
- Si E est un ensemble, il existe un ensemble, appelé *ensemble des parties de* E et noté $\mathscr{P}(\mathrm{E})$, dont les éléments sont tous les ensembles inclus dans E.

On peut décrire un ensemble *en extension*, c'est-à-dire en donnant la liste extensive des éléments qui le composent. Par exemple, $\mathrm{E} = \{1,2,3\}$ ou bien $\mathrm{F} = \{a,b,c,d\}$. Mais comme on peut le constater, cette approche est limitée puisqu'elle ne permet de décrire que les ensembles finis. Et encore, il faut qu'ils ne soient pas trop gros, sinon on passe la journée à les décrire. La notion de prédicat, développée dans le prochain paragraphe, sera le moyen de pallier à ce problème. En attendant, voici quelques exemples.

Exemple 0.2.2

1. On note $\mathbb{N}$ l'ensemble de tous les nombres entiers positifs.
2. On note $\mathbb{Z}$ l'ensemble de tous les nombres entiers relatifs (c'est-à-dire sans considération de signe).
3. On note $\mathbb{Q}$ l'ensemble de tous les nombres rationnels, c'est-à-dire des nombres qui peuvent s'écrire comme rapport de deux nombres entiers relatifs.
4. On note $\mathbb{R}$ l'ensemble des nombres réels.
5. On a $1 \in \mathbb{N} \qquad -17 \in \mathbb{Z} \qquad \dfrac{2692}{3356} \in \mathbb{Q} \qquad \pi \in \mathbb{R}$

   et $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$
6. Si E est un ensemble, $\emptyset$ appartient à $\mathscr{P}(\mathrm{E})$; en outre, pour tout ensemble F, on a
   $$\mathrm{F} \subset \mathrm{E} \Longleftrightarrow \mathrm{F} \in \mathscr{P}(\mathrm{E})$$
7. Si $\mathrm{E} = \{1,2,3\}$, l'ensemble $\mathscr{P}(\mathrm{E})$ est
   $$\mathscr{P}(\mathrm{E}) = \big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\big\}$$

Bien évidemment, deux ensembles sont égaux si, et seulement si, ils sont les mêmes. C'est-à-dire qu'ils ont les mêmes éléments. Donc $\mathrm{E} = \mathrm{F}$ revient à dire que $\mathrm{E} \subset \mathrm{F}$ et $\mathrm{F} \subset \mathrm{E}$. Ainsi, pour démontrer l'égalité de deux ensembles, il suffit de procéder par double inclusion : montrer d'une part que tout élément de E est élement de F ; puis que tout élément de F est élément de E.

Exemple 0.2.3
On note E l'ensemble des couples (x, y) tels que

$$\begin{cases} x+y = 1 \\ x-y = -1 \end{cases}$$

et F l'ensemble contenant uniquement le couple $(0,1)$. Montrons que E = F. Comme expliqué au-dessus, on procède par double inclusion.

Commençons par montrer que $E \subset F$. Soit $(x, y) \in E$. On sait alors que

$$x+y=1 \qquad \text{et} \qquad x-y=-1$$

En ajoutant membre-à-membre ces deux relations, on obtient $2x = 0$ donc $x = 0$. Il s'ensuit que $y = 1$. Donc $(x, y) = (0,1) \in F$. Ce qui montre $E \subset F$.

Réciproquement, montrons que $F \subset E$. Prenons un élément dans F ; ce dernier n'en contient qu'un seul, qui est $(0,1)$. On observe que

$$0+1=1 \qquad \text{et} \qquad 0-1=-1$$

donc $(0,1)$ se trouve bien dans E. D'où $F \subset E$.

0.2.2 Prédicats et quantificateurs

Prédicats

Définition 0.2.4
Soit E un ensemble. Un *prédicat sur* E est une propriété portant sur un ou plusieurs objets de E, de sorte que, une fois ces derniers précisés, le résultat soit une assertion.

La définition peut paraître assez obscure ; illustrons-la immédiatement à l'aide d'exemples.

Exemple 0.2.5

1. La propriété $\boldsymbol{p}(x)$: « $x^2 > 3$ » n'a aucun sens en tant que telle puisqu'on ne sait pas qui est x. En revanche, si on remplace x par 2, on obtient $\boldsymbol{p}(2)$: « $4 > 3$ », qui est une assertion vraie.
   Si on remplace x par -1, on obtient l'assertion $\boldsymbol{p}(-1)$: « $1 > 3$ », qui est fausse.
   En fait, si on remplace x par n'importe quel nombre réel, on obtient bien une assertion : on dit que $\boldsymbol{p}(x)$ est un prédicat sur $\mathbb{R}$.
   Si on remplace x par $1+\mathrm{i}$, on obtient $\boldsymbol{p}(1+\mathrm{i})$: « $2\mathrm{i} > 3$ », qui n'a aucun sens car le symbole « $>$ » n'a pas été defini sur les nombres complexes.
2. « x est pair » n'est pas une assertion car on ne sait pas qui est x. C'est un prédicat sur $\mathbb{N}$: il dépend d'une variable x et lorsqu'on remplace x par entier, on obtient une assertion.
3. $\boldsymbol{p}(x, y)$: « $x^2 + y = 0$ » est un prédicat à deux variables sur $\mathbb{R}$ ou sur $\mathbb{C}$ (ou même sur d'autres ensembles). Si on remplace x par 3, on obtient le prédicat à une variable $\boldsymbol{p}(3, y)$: « $9 + y = 0$ ».

Quantificateurs

Si $\boldsymbol{p}(x)$ est un prédicat sur un ensemble E, on peut l'évaluer en n'importe quel x de E pour obtenir une assertion. Mais on peut aussi en définir deux autres qui sont :

- « Pour tout x dans E, $\boldsymbol{p}(x)$ » et qui s'écrit mathématiquement

  $$\forall x \in \mathrm{E} \qquad \boldsymbol{p}(x)$$

  C'est une assertion qui est vraie si tous les éléments x de E rendent $\boldsymbol{p}(x)$ vraie. Le symbole $\forall$ est appelé *quantificateur universel*.

- « Il existe x dans E, tel que $\boldsymbol{p}(x)$ » et qui s'écrit mathématiquement

$$\exists x \in \mathrm{E} \qquad \boldsymbol{p}(x)$$

Cette assertion est vraie pour peu qu'on puisse trouver un $x \in \mathrm{E}$ tel que $\boldsymbol{p}(x)$ soit vraie. Le symbole $\exists$ est appelé *quantificateur existentiel*.

Exemple 0.2.6

1. Considérons le prédicat sur $\mathbb{R}$:

$$\boldsymbol{p}(x) : \text{« } x^2 > 3 \text{ »}$$

L'assertion $\forall x \in \mathbb{R} \qquad \boldsymbol{p}(x)$

qui se récrit $\forall x \in \mathbb{R} \qquad x^2 > 3$

est clairement fausse, puisque $\boldsymbol{p}(0)$ n'est pas vraie ($0 \leqslant 3$). En revanche,

$$\exists x \in \mathbb{R} \qquad x^2 > 3$$

est vraie puisque $2^2 > 3$, par exemple.

2. L'assertion $\exists x \in \mathbb{R} \qquad x^2 = -1$

est fausse, puisqu'on a démontré que -1 n'a pas de racine carrée dans $\mathbb{R}$. Cependant,

$$\exists x \in \mathbb{C} \qquad x^2 = -1$$

est vraie puisque $\mathrm{i}^2 = -1$.

3. À partir du prédicat à deux variables réelles « $x^2 + y = 0$ », on peut former quatre nouveaux prédicats à une seule variable :

$$\boldsymbol{p}(y) : \text{« } \exists x \in \mathbb{R} \qquad x^2 + y = 0 \text{ »}$$

$$\boldsymbol{q}(y) : \text{« } \forall x \in \mathbb{R} \qquad x^2 + y = 0 \text{ »}$$

$$\boldsymbol{r}(x) : \text{« } \exists y \in \mathbb{R} \qquad x^2 + y = 0 \text{ »}$$

et $\boldsymbol{s}(x) : \text{« } \forall y \in \mathbb{R} \qquad x^2 + y = 0 \text{ »}$

Observons rapidement que $\boldsymbol{p}(y)$ est vraie pour tout $y < 0$; $\boldsymbol{q}(y)$ n'est vraie pour aucun $y \in \mathbb{R}$; $\boldsymbol{r}(x)$ est vraie pour tout x réel et $\boldsymbol{s}(x)$ n'est jamais vraie.

À chacun de ces prédicats on peut affecter un quantificateur existentiel ou universel, pour former de nouvelles assertions. Par exemple,

$$\forall y < 0 \quad \exists x \in \mathbb{R} \qquad x^2 + y = 0$$

ou $\forall x \in \mathbb{R} \quad \exists y \in \mathbb{R} \qquad x^2 + y = 0$

Il y en a évidemment de nombreux autres.

Faisons à ce stade une remarque importante : si $\boldsymbol{p}(x)$ est un prédicat sur un ensemble E, les assertions

$$\forall x \in \mathrm{E} \qquad \boldsymbol{p}(x) \qquad \text{et} \qquad \exists x \in \mathrm{E} \qquad \boldsymbol{p}(x)$$

ne dépendent plus d'aucune variable. En fait, on pourrait même remplacer x par n'importe quel autre symbole, pour peu qu'on fasse cette opération partout où x apparaît. Ainsi, les assertions précédentes sont équivalentes respectivement à

$$\forall \square \in \mathrm{E} \qquad \boldsymbol{p}(\square) \qquad \text{et} \qquad \exists \diamond \in \mathrm{E} \qquad \boldsymbol{p}(\diamond)$$

On dit que la variable x (ou $\square$, ou $\diamond$) est *muette*.

Ordre des quantificateurs

L'ordre des quantificateurs est important et ne peut pas, en général, être changé. Pour prendre un exemple concret, on note $\mathscr{C}$ l'ensemble de toutes les cerises et $\mathscr{N}$ l'ensemble de tous les noyaux de cerises. On peut alors considérer le prédicat, à deux variables C (une cerise) et n (un noyau) : « $n \in \mathrm{C}$ » et former les assertions :

$$\forall \mathrm{C} \in \mathscr{C} \quad \exists n \in \mathscr{N} \qquad n \in \mathrm{C}$$

et

$$\exists n \in \mathscr{N} \quad \forall \mathrm{C} \in \mathscr{C} \qquad n \in \mathrm{C}$$

La première dit que pour toute cerise, il y a un noyau se trouvant dedans. La seconde dit qu'il existe un noyau se trouvant dans toutes les cerises. Elles sont respectivement vraie et fausse ; et pour passer de l'une à l'autre, on a simplement échangé l'ordre des quantificateurs.

Il est toutefois des situations dans lesquelles on peut intervertir sans problème l'ordre des quantificateurs : lorsqu'on a deux $\forall$ à la suite ou bien deux $\exists$ à la suite. Ainsi, si $\boldsymbol{p}(x, y)$ est un prédicat à deux variables dans des ensembles E et F, considérons l'assertion :

$$\forall x \in \mathrm{E} \quad \forall y \in \mathrm{F} \qquad \boldsymbol{p}(x, y)$$

Elle se lit : « Pour tout x dans E et pour tout y dans F, $\boldsymbol{p}(x, y)$. » Bien évidemment, c'est la même chose que : « Pour tout y dans F et pour tout x dans E, $\boldsymbol{p}(x, y)$. » De la même manière,

$$(\exists x \in \mathrm{E} \quad \exists y \in \mathrm{F} \qquad \boldsymbol{p}(x, y)) \iff (\exists y \in \mathrm{F} \quad \exists x \in \mathrm{E} \qquad \boldsymbol{p}(x, y))$$

Quantificateurs et négation

Il est important d'être capable de nier les assertions

$$\forall x \in \mathrm{E} \qquad \boldsymbol{p}(x) \qquad \text{et} \qquad \exists x \in \mathrm{E} \qquad \boldsymbol{p}(x)$$

pour le cas où l'on souhaite raisonner par l'absurde ou par contre-apposée. À nouveau, c'est une question de bon sens.

Considérons l'assertion « $\forall x \in \mathrm{E} \qquad \boldsymbol{p}(x)$ », qui se lit « $\boldsymbol{p}(x)$ est vraie pour tout x de E. » Sa négation est évidemment « Il existe un x de E pour lequel $\boldsymbol{p}(x)$ n'est pas vraie. » C'est-à-dire

$$\boxed{\textbf{non}(\forall x \in \mathrm{E} \qquad \boldsymbol{p}(x)) \iff (\exists x \in \mathrm{E} \qquad \textbf{non } \boldsymbol{p}(x))}$$

De la même manière, l'assertion « $\exists x \in \mathrm{E} \qquad \boldsymbol{p}(x)$ », qui se lit « Il existe x dans E tel que $\boldsymbol{p}(x)$ est vraie » a pour négation « $\boldsymbol{p}(x)$ n'est vraie pour aucun x de E », ou encore « Pour tout x de E, $\boldsymbol{p}(x)$ est fausse. » Donc

$$\boxed{\textbf{non}(\exists x \in \mathrm{E} \qquad \boldsymbol{p}(x)) \iff (\forall x \in \mathrm{E} \qquad \textbf{non } \boldsymbol{p}(x))}$$

Maintenant, comment faire pour nier un enchaînement de plusieurs quantificateurs ? C'est très simple, il suffit de procéder par étapes. Prenons un exemple : on a deux ensembles E et F et un prédicat $\boldsymbol{p}(x,y)$ sur E et F. On souhaite nier l'assertion

$$\forall x \in \mathrm{E} \quad \exists y \in \mathrm{F} \qquad \boldsymbol{p}(x,y)$$

Il suffit de remarquer que « $\exists y \in \mathrm{F} \qquad \boldsymbol{p}(x,y)$ » est un prédicat sur E, qu'on note $\boldsymbol{q}(x)$. On a

$$(\forall x \in \mathrm{E} \quad \exists y \in \mathrm{F} \qquad \boldsymbol{p}(x,y)) \iff (\forall x \in \mathrm{E} \qquad \boldsymbol{q}(x))$$

Et on sait nier une assertion ne présentant qu'un seul quantificateur :

$$\begin{aligned} \textbf{non}(\forall x \in \mathrm{E} \quad \exists y \in \mathrm{F} \qquad \boldsymbol{p}(x,y)) &\iff \textbf{non}(\forall x \in \mathrm{E} \qquad \boldsymbol{q}(x)) \\ &\iff (\exists x \in \mathrm{E} \qquad \textbf{non}\ \boldsymbol{q}(x)) \\ &\iff (\exists x \in \mathrm{E} \quad \forall y \in \mathrm{F} \qquad \textbf{non}\ \boldsymbol{p}(x,y)) \end{aligned}$$

Exemple 0.2.7
Reprenons notre exemple avec les cerises et les noyaux et considérons l'assertion « Dans toute cerise, il y a un noyau ». Celle-ci se formalise :

$$\forall \mathrm{C} \in \mathscr{C} \quad \exists n \in \mathscr{N} \qquad n \in \mathrm{C}$$

En Français, elle se nie de la manière suivante : « Il y a une cerise ne contenant pas de noyau » ; et en maths :

$$\exists \mathrm{C} \in \mathscr{C} \quad \forall n \in \mathscr{N} \qquad n \notin \mathrm{C}$$

0.2.3 Sous-ensembles définis par un prédicat

Nous avons vu pour l'instant, comme seule manière de décrire mathématiquement un ensemble, l'énumération des objets qui le constituent. C'est ce qu'on a appelé « décrire l'ensemble *en extension* ». C'est un procédé assez limité, puisqu'il ne permet que de décrire des ensembles finis, et ces derniers ne doivent pas être trop gros, car on ne peut lister raisonnablement 21345 objets. Cela prendrait trop de temps.

À l'aide de la notion de prédicat, on peut maintenant décrire les ensembles *en compréhension*. Cela signifie qu'on regroupe ensemble tous les objets qui transforment un prédicat en une assertion vraie.

Plus précisément, soit E un ensemble et $\boldsymbol{p}(x)$ un prédicat sur E. On peut alors considérer l'ensemble F des éléments x de E tels que $\boldsymbol{p}(x)$ soit une assertion vraie. On note alors

$$\mathrm{F} = \{x \in \mathrm{E} \mid \boldsymbol{p}(x)\}$$

Ce sous-ensemble F de E est caractérisé par l'équivalence

$$\forall x \in \mathrm{E} \qquad (x \in \mathrm{F} \iff \boldsymbol{p}(x))$$

Exemple 0.2.8
Posons

$$\mathrm{E} = \left\{(x,y) \in \mathbb{R}^2 \mid \begin{cases} x+y = 1 \\ x-y = -1 \end{cases}\right\}$$

C'est-à-dire que E est l'ensemble des solutions du système linéaire de deux équations à deux inconnues écrit plus haut. C'est une notation claire, compacte, puisqu'elle évite d'avoir à écrire « Soit E le sous-ensemble de $\mathbb{R}^2$ constitué des solutions de l'équation ... » ; et on n'a pas à énumérer ses éléments.

On vient de voir que tout prédicat sur E permet de définir une partie de E. Réciproquement, si F $\subset$ E, F est le sous-ensemble associé au prédicat « $x \in$ F ». Il y a donc une correspondance parfaite entre prédicats sur E et sous-ensembles de E.

Théorème 0.2.9
Soit E *un ensemble. Soient* A *et* B *deux sous-ensembles de* E *définis par des prédicats* $\boldsymbol{p}(x)$ *et* $\boldsymbol{q}(x)$. *On a*

$$(\mathrm{A} \subset \mathrm{B}) \Longleftrightarrow (\forall x \in \mathrm{E} \qquad \boldsymbol{p}(x) \Longrightarrow \boldsymbol{q}(x))$$

Preuve : On a une équivalence à démontrer. D'après le fait qu'une equivalence n'est autre que deux implications simultanément satisfaites, on démontre chacune de ces implications. Rappelons que

$$\mathrm{A} = \{x \in \mathrm{E} \mid \boldsymbol{p}(x)\} \qquad \text{et} \qquad \mathrm{B} = \{x \in \mathrm{E} \mid \boldsymbol{q}(x)\}$$

Supposons que A $\subset$ B. Soit x dans E. Si $\boldsymbol{p}(x)$ est fausse, alors $\boldsymbol{p}(x) \Longrightarrow \boldsymbol{q}(x)$ est vraie, indépendamment de ce que vaut $\boldsymbol{q}(x)$. Si $\boldsymbol{p}(x)$ est vraie, c'est que $x \in$ A. Or, A $\subset$ B donc $x \in$ B également. Ce qui signifie que $\boldsymbol{q}(x)$ est vraie. Donc $\boldsymbol{p}(x) \Longrightarrow \boldsymbol{q}(x)$. Ce qui montre la première implication

$$(\mathrm{A} \subset \mathrm{B}) \Longrightarrow (\forall x \in \mathrm{E} \qquad \boldsymbol{p}(x) \Longrightarrow \boldsymbol{q}(x))$$

Réciproquement, supposons que

$$\forall x \in \mathrm{E} \qquad \boldsymbol{p}(x) \Longrightarrow \boldsymbol{q}(x)$$

Soit $x \in$ A, ce qui signifie que $\boldsymbol{p}(x)$ est vraie. Comme on sait que $\boldsymbol{p}(x) \Longrightarrow \boldsymbol{q}(x)$ est également vraie, c'est nécessairement que $\boldsymbol{q}(x)$ l'est aussi. Donc $x \in$ B, ce qui montre que tout élément de A est élément de B. On a montré la deuxième implication

$$(\forall x \in \mathrm{E} \qquad \boldsymbol{p}(x) \Longrightarrow \boldsymbol{q}(x)) \Longrightarrow (\mathrm{A} \subset \mathrm{B})$$ □

Corollaire 0.2.10
Soient A *et* B *deux sous-ensembles de* E, *définis par des prédicats* $\boldsymbol{p}(x)$ *et* $\boldsymbol{q}(x)$. *Alors*

$$(\mathrm{A} = \mathrm{B}) \Longleftrightarrow (\forall x \in \mathrm{E} \qquad \boldsymbol{p}(x) \Longleftrightarrow \boldsymbol{q}(x))$$

0.2.4 Opérations sur les parties d'un ensemble

Dans cette section, E est un ensemble donné.

Définition 0.2.11
Soient A et B deux sous-ensembles de E.

- *La réunion de* A *et* B, notée A $\cup$ B est l'ensemble

$$\mathrm{A} \cup \mathrm{B} = \{x \in \mathrm{E} \mid (x \in \mathrm{A}) \textbf{ ou } (x \in \mathrm{B})\}$$

- *L'intersection de* A *et* B, notée A $\cap$ B, est l'ensemble

$$\mathrm{A} \cap \mathrm{B} = \{x \in \mathrm{E} \mid (x \in \mathrm{A}) \textbf{ et } (x \in \mathrm{B})\}$$

- *Le différence* A *moins* B, notée A $\setminus$ B, est l'ensemble

$$\mathrm{A} \setminus \mathrm{B} = \{x \in \mathrm{E} \mid (x \in \mathrm{A}) \textbf{ et } (x \notin \mathrm{B})\} = \{x \in \mathrm{E} \mid (x \in \mathrm{A}) \textbf{ et}(\textbf{non } (x \in \mathrm{B}))\}$$

Si A contient B, on pourra noter $\overline{B}$ ou B^c pour l'ensemble $A \setminus B$. Cette notation a l'avantage d'être plus courte à écrire ; mais elle occulte l'ensemble A environnant. En général, celui-ci est clair d'après le contexte.

Mais, si $B \subset A$ et $B \subset A'$, la notation B^c n'est pas forcément très claire. Suivant les besoins imposés par le contexte, on préférera préciser l'ensemble par rapport auquel on complémente.

Voici toute une liste d'identités mélangeant ces notions ; elles ne seront pas démontrées car cela prendrait trop de temps. Certaines seront traitées en exercices.

Proposition 0.2.12
Soient A, B *et* C *des sous-ensembles de* E. *On a*

- $\emptyset^c = E \qquad E^c = \emptyset \qquad (A^c)^c = A$
- $A \cup \emptyset = \emptyset \cup A = A$ — $\emptyset$ *est neutre pour* $\cup$
  $A \cup A = A$
  $A \cup E = E \cup A = E$ — E *est absorbant pour* $\cup$
  $A \cup B = B \cup A$ — $\cup$ *est commutative*
  $A \cup B = B \iff A \subset B$
  $(A \cup B) \cup C = A \cup (B \cup C)$ — $\cup$ *est associative*
- $A \cap \emptyset = \emptyset \cap A = \emptyset$ — $\emptyset$ *est absorbant pour* $\cap$
  $A \cap A = A$
  $A \cap E = E \cup A = A$ — E *est neutre pour* $\cap$
  $A \cap B = B \cap A$ — $\cap$ *est commutative*
  $A \cap B = B \iff B \subset A$
  $(A \cap B) \cap C = A \cap (B \cap C)$ — $\cap$ *est associative*
- $(A \cap B)^c = A^c \cup B^c$
  $(A \cup B)^c = A^c \cap B^c$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ — *distributivité de* $\cap$ *sur* $\cup$
  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ — *distributivité de* $\cup$ *sur* $\cap$
  $A \cup (A \cap B) = A \cap (A \cup B) = A$
- $A \setminus \emptyset = A$
  $A \setminus A = \emptyset$
  $A \setminus B = \emptyset \iff A \subset B$
  $A \setminus B = A \setminus (A \cap B)$

0.3 Applications

Cette dernière étape a pour but de définir proprement les notions de fonction et d'application, et tout ce qui gravite autour : ensembles de départ, d'arrivée, de définition, la composition, l'injectivité, la surjectivité et la bijectivité.

À l'heure actuelle, on n'a qu'une vague idée de ce qu'est une fonction. D'abord, on n'a vu que des fonctions sur $\mathbb{R}$, à valeurs dans $\mathbb{R}$; on peut faire plus général que cela. Ensuite, la notion en elle-même, si on y réfléchit, semble se mordre la queue. En effet, si on veut exprimer le fait que f est

une fonction, on peut penser à la formulation suivante : f est une manière d'associer de manière unique à chaque x un $f(x)$. Donc la définition de f semble faire référence à f ; pour définir f, on a besoin de f. Ne parlons même pas de l'ambiguïté du mot « associer ». N'est-il pas un peu vague ?

Pour faire les choses proprement, on commence par définir une nouvelle opération entr'ensembles.

0.3.1 Le produit cartésien

Tout au long de ce paragraphe, E et F sont deux ensembles donnés.

Définition 0.3.1 (Produit cartésien)
Soient $x \in \mathrm{E}$ et $y \in \mathrm{F}$. On appelle *couple formé par x et y, »* noté (x, y), l'ensemble $\{\{x\}, \{x, y\}\}$.

Dit simplement, un couple, c'est deux éléments ordonnés. La proposition suivante énonce cette propriété fondamentale des couples :

Proposition 0.3.2 (Propriété fondamentale du produit cartésien)
Soient $x, x' \in \mathrm{E}$ et $y, y' \in \mathrm{F}$. Les couples (x, y) et (x', y') sont égaux si, et seulement si, $x = x'$ et $y = y'$.

Preuve : Je ne suis pas sûr que cela aide mais la voici. Déjà, si $x = x'$ et $y = y'$, il est évident que $(x, y) = (x', y')$.

Réciproquement, supposons les couples égaux. Cela signifie que

$$\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\} \qquad (\star)$$

On suppose également que $x \neq x'$.

> Autant le préciser maintenant : nous allons raisonner par l'absurde. C'est-à-dire qu'on montre que l'hypothèse $x \neq x'$ débouche sur une contradication ; de sorte qu'il ne peut être vrai que $x \neq x'$; ou encore, qu'il est vrai que $x = x'$.

L'élément $\{x\}$ de l'ensemble de gauche est donc égal à $\{x'\}$ ou à $\{x', y'\}$. Or, $x \neq x'$, donc $\{x\} \neq \{x'\}$ et par suite, $\{x\} = \{x', y'\}$. Il vient alors que $x' = x$, ce qui fournit la contradiction recherchée.

Ainsi, on sait maintenant que $x = x'$. Par conséquent,

$$\{\{x\}, \{x, y\}\} = \{\{x\}, \{x, y'\}\}$$

Supposons que $y \neq y'$. Alors $\{x, y\} \neq \{x, y'\}$ et il s'ensuit que $\{x, y\} = \{x\}$ et $\{x, y'\} = \{x\}$. D'où l'on déduit que $\{x, y\} = \{x, y'\}$: contradiction. Finalement, $y = y'$. □

Définition 0.3.3
On appelle *produit cartésien de* E *et* F l'ensemble $\mathrm{E} \times \mathrm{F}$ de tous les couples formés d'un élément de E et d'un élément de F :

$$\mathrm{E} \times \mathrm{F} = \{(x, y) \mid x \in \mathrm{E} \quad y \in \mathrm{F}\}$$

Le produit cartésien $\mathrm{E} \times \mathrm{E}$ sera aussi noté E^2.

Proposition 0.3.4
Soient E, F, G *et* H *quatre ensembles. On a*

1. $E \times F = \emptyset \iff (E = \emptyset \quad ou \quad F = \emptyset)$
2. $E \times F = F \times E \iff (E = F \quad ou \quad E = \emptyset \quad ou \quad F = \emptyset)$
3. $(E \times F) \cup (E \times G) = E \times (F \cup G)$
4. $(E \times F) \cup (G \times F) = (E \cup G) \times F$
5. $(E \times F) \cap (G \times H) = (E \cap G) \times (F \cap H)$

Preuve : C'est un bon exercice. □

Exemple 0.3.5
Des exemples de produits cartésiens ont été amplement dessinés au tableau et je ne perdrai pas de temps à les reproduire ici. Mais voici un contre-exemple à la relation

$$(E \times F) \cup (G \times H) = (E \cup G) \times (F \cup H)$$

dont on pourrait rêver qu'elle soit vraie. Il suffit de prendre

$$E = F = \{0\} \qquad G = H = \{1\}$$

Alors $$(E \times F) \cup (G \times H) = \{(0,0);(1,1)\}$$

tandis que $$(E \cup G) \times (F \cup H) = \{0,1\} \times \{0,1\} = \{(0,0);(0,1);(1,0);(1,1)\}$$

0.3.2 Fonctions et applications

Définition 0.3.6 (Relation)
On appelle *relation* tout triplet $\mathscr{R} = (E, F, \Gamma)$, où E et F sont deux ensembles et Γ est une partie de $E \times F$.

L'ensemble E est alors appelé *ensemble de départ* ; F est l'*ensemble d'arrivée* ; et Γ est appelé *graphe* de la relation $\mathscr{R}$.

Pour tout $(x, y) \in E \times F$, on notera $x \mathscr{R} y$ ou $x \Gamma y$ si, et seulement si, (x, y) se trouve en fait dans Γ.

Exemple 0.3.7
La définition d'un graphe est très peu restrictive : tout sous-ensemble de $E \times F$ est un graphe. Autrement dit, tout ensemble formé de couples d'un élément de E et d'un élément de F est un graphe.

Du coup, il n'est pas difficile d'en exhiber des exemples :

$$f_1 = \{(x, y) \in \mathbb{R}^2 \mid -1 \leqslant x \leqslant 3 \quad 0 \leqslant y \leqslant 2\}$$

ou $$f_2 = \{(t, t^2) \mid t \in \mathbb{R}\}$$

ou $$f_3 = \{(t^2, t) \mid t \in \mathbb{R}\}$$

ou encore $$f_4 = \{(t^2, t) \mid t > 0\}$$

sont des graphes de $\mathbb{R}$ dans $\mathbb{R}$.

On peut alors écrire que $1 \, f_2 \, 1$; ou bien $4 \, f_3 \, 2$. En revanche, il est faux que $3 \, f_4 \, -1$.

Définition 0.3.8 (Fonction)
Soit f une relation de E dans F. On dit que f *est une fonction de* E *dans* F si et seulement si

$$\forall x \in \mathrm{E} \quad \forall y, y' \in \mathrm{F} \qquad \left.\begin{array}{c}(x,y) \in f \\ (x,y') \in f\end{array}\right\} \Longrightarrow y = y'$$

On notera alors $f : \mathrm{E} \longrightarrow \mathrm{F}$ pour dire que f est une fonction de E dans F.

En Français : un graphe est une fonction si deux points du graphe ayant la même première coordonnée ont obligatoirement la même deuxième coordonnée également. Autrement dit, pour chaque $x \in \mathrm{E}$ qui est la première coordonnée d'un point du graphe, il existe un seul y, tel que (x, y) soit dans le graphe. C'est ce qu'on vérifie ici, après une définition :

Définition 0.3.9 (Domaine de définition)
Soit $f : \mathrm{E} \longrightarrow \mathrm{F}$. On appelle *domaine de définition de f* l'ensemble

$$\mathscr{D}_f = \{x \in \mathrm{E} \mid \exists y \in \mathrm{F} \quad (x,y) \in f\}$$

Proposition 0.3.10
Soit $f : \mathrm{E} \longrightarrow \mathrm{F}$. Pour tout x dans $\mathscr{D}_f$, il existe un et un seul $y \in \mathrm{F}$ tel que $(x,y) \in f$. On notera alors $y = f(x)$.

Preuve : Si x est dans le domaine de définition de f, on sait qu'il existe $y \in \mathrm{F}$ tel que $(x,y) \in f$.

Maintenant, soit $y' \in \mathrm{F}$ tel que $(x,y') \in f$ également. D'après la définition d'une fonction, le fait que (x,y) et (x,y') soient dans f implique que $y = y'$.

Il existe donc bien un unique $y \in \mathrm{F}$ tel que $(x,y) \in f$. □

> Ainsi, la notion de fonction, telle qu'elle a été proprement définie dans le cours, capture bien l'idée intuitive que l'on en a : c'est une manière d'associer à certains $x \in \mathrm{E}$ (ceux qui sont dans le domaine de définition) un et un seul $y \in \mathrm{F}$.

Définition 0.3.11 (Image, antécédent)
Soient $f : \mathrm{E} \longrightarrow \mathrm{F}$, $x \in \mathscr{D}_f$ et $y \in \mathrm{F}$. Si $y = f(x)$, on dit que *y est l'image de x par f* tandis que x est appelé *un antécédent de y par f*.

Proposition 0.3.12 (Composition)
Soient $f : \mathrm{E} \longrightarrow \mathrm{F}$ et $g : \mathrm{F} \longrightarrow \mathrm{G}$. Le graphe

$$g \circ f = \{(x,z) \in \mathrm{E} \times \mathrm{G} \mid \exists y \in \mathrm{F} \quad (x,y) \in f \text{ et } (y,z) \in g\}$$

est celui d'une fonction, appelée composée de f par g. Son domaine de définition est

$$\mathscr{D}_{g\circ f} = \{x \in \mathrm{E} \mid x \in \mathscr{D}_f \text{ et } f(x) \in \mathscr{D}_g\}$$

Enfin, $$\forall x \in \mathscr{D}_{g\circ f} \qquad (g \circ f)(x) = g(f(x))$$

Preuve : Encore un exercice amusant pour manipuler toutes nos définitions.

Vérifions tout d'abord que $g \circ f$ est bien une fonction. Pour cela, il nous faut $x \in \mathrm{E}$ et $z, z' \in \mathrm{G}$ tels que (x,z) et (x,z') sont dans $g \circ f$. On souhaite montrer que $z = z'$.

Le fait que $(x,z) \in g \circ f$ signifie qu'il existe $y \in \mathrm{F}$ tel que $(x,y) \in f$ et $(y,z) \in g$. De la même manière, il existe $y' \in \mathrm{F}$ tel que $(x,y') \in f$ et $(y',z') \in g$.

Or, f est une fonction ; puisque (x,y) et (x,y') sont dans f, on a $y = y'$ (en fait, $y = y' = f(x)$). Du coup, (y,z) et (y,z') sont dans g, qui est le graphe d'une fonction donc $z = z'$ (et en fait, $z = z' = g(y)$). On a gagné, $g \circ f$ est bien une fonction.

Calculons son domaine de définition. Par définition, il s'agit de

$$\mathscr{D}_{g\circ f} = \{x \in \mathrm{E} \mid \exists z \in \mathrm{G} \quad (x,z) \in g \circ f\}$$

Montrons qu'il est égal à l'ensemble

$$\mathrm{A} = \{x \in \mathrm{E} \mid x \in \mathscr{D}_f \quad \text{et} \quad f(x) \in \mathscr{D}_g\}$$

On procède comme souvent par double inclusion. Soit $x \in \mathscr{D}_{g\circ f}$. Il existe $z = g \circ f(x) \in \mathrm{G}$ tel que $(x,z) \in g \circ f$. Ce qui signifie qu'il existe $y \in \mathrm{F}$ tel que $(x,y) \in f$ et $(y,z) \in \mathrm{G}$. Il vient immédiatement que

$$x \in \mathscr{D}_f \qquad y = f(x) \in \mathscr{D}_g \qquad \text{et} \qquad z = g(y) = g(f(x))$$

Ce qui montre en même temps que $x \in \mathrm{A}$, et que $g \circ f(x) = g(f(x))$.

Réciproquement, supposons que $x \in \mathrm{A}$. Par définition, $x \in \mathscr{D}_f$ et $f(x) \in \mathscr{D}_g$. Ce qui signifie (voir la définition des notations $f(x)$ et $g(f(x))$), que

$$(x, f(x)) \in f \qquad \text{et} \qquad (f(x), g(f(x))) \in g$$

Donc $$(x, g(f(x))) \in g \circ f$$

et $$x \in \mathscr{D}_{g\circ f}$$ □

Proposition 0.3.13 (Associativité de la composition)
Soient $f : \mathrm{E} \longrightarrow \mathrm{F}$, $g : \mathrm{F} \longrightarrow \mathrm{G}$ *et* $h : \mathrm{G} \longrightarrow \mathrm{H}$ *trois fonctions. Alors*

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

Preuve : On montre évidemment l'égalité des graphes

$$h \circ (g \circ f) = \{(x,t) \in \mathrm{E} \times \mathrm{H} \mid \exists z \in \mathrm{G} \quad (x,z) \in g \circ f \text{ et } (z,t) \in h\}$$

et $$(h \circ g) \circ f = \{(x,t) \in \mathrm{E} \times \mathrm{H} \mid \exists y \in \mathrm{F} \quad (x,y) \in f \text{ et } (y,t) \in h \circ g\}$$

C'est un peu fastidieux, mais allons-y. Soit $(x,t) \in \mathrm{E} \times \mathrm{H}$. On a

$$\begin{aligned}
(x,t) \in h \circ (g \circ f) &\iff \left(\exists z \in \mathrm{G} \quad \begin{cases} (x,z) \in g \circ f \\ (z,t) \in h \end{cases} \right) && \text{(définition de } h \circ (g \circ f)) \\
&\iff \left(\exists z \in \mathrm{G} \quad \exists y \in \mathrm{F} \quad \begin{cases} (x,y) \in f \\ (y,z) \in g \\ (z,t) \in h \end{cases} \right) && \text{(définition de } g \circ f) \\
&\iff \left(\exists y \in \mathrm{F} \quad \begin{cases} (x,y) \in f \\ (y,t) \in h \circ g \end{cases} \right) && \text{(définition de } h \circ g) \\
(x,t) \in h \circ (g \circ f) &\iff (x,t) \in (h \circ g) \circ f && \text{(définition de } (h \circ g) \circ f)
\end{aligned}$$ □

Proposition 0.3.14 (Égalité de deux fonctions)
Soient f *et* g *deux fonctions de* E *dans* F. *Elles sont égales si, et seulement si, elles ont le même domaine de définition et*

$$\forall x \in \mathscr{D}_f = \mathscr{D}_g \qquad f(x) = g(x)$$

Preuve : Si f et g sont égales, elles ont évidemment même domaine de définition et prennent les mêmes valeurs dessus.

Réciproquement, supposons que $\mathscr{D}_f = \mathscr{D}_g$ et

$$\forall x \in \mathscr{D}_f = \mathscr{D}_g \qquad f(x) = g(x)$$

On a alors
$$\begin{aligned} \forall (x,y) \in \mathrm{E}\times\mathrm{F} \qquad (x,y) \in f &\iff (x \in \mathscr{D}_f \quad \text{et} \quad y = f(x)) \\ &\iff (x \in \mathscr{D}_g \quad \text{et} \quad y = g(x)) \\ (x,y) \in f &\iff (x,y) \in g \end{aligned}$$

Définition 0.3.15 (Application)
Soit $f : \mathrm{E} \longrightarrow \mathrm{F}$ une fonction. On dit que c'est *une application de* E *dans* F si, et seulement si, elle est définie sur E tout entier (ou encore $\mathscr{D}_f = \mathrm{E}$).

Exemple 0.3.16
Si on reprend l'**exemple 3.7**, on voit que

- f_1 n'est pas une fonction (et donc pas une application) ;
- f_2 est une fonction et une application de $\mathbb{R}$ dans $\mathbb{R}$;
- f_3 n'est pas une fonction puisque $(1,-1)$ et $(1,1)$ sont dans son graphe (même abscisse, différentes ordonnées) ;
- f_4 est une fonction de $\mathbb{R}$ dans lui-même, définie sur $\mathbb{R}_+^\star$. Ce n'est donc pas une application de $\mathbb{R}$ dans lui-même. En revanche, c'est une application de $\mathbb{R}_+^\star$ dans $\mathbb{R}$.

Les propositions précédentes sont également valables pour les applications, qui ne sont que des cas particuliers de fonctions. Notons que la composée $g \circ f$ de deux applications $f : \mathrm{E} \longrightarrow \mathrm{G}$ et $g : \mathrm{G} \longrightarrow \mathrm{H}$ est une application puisque son domaine de définition est (d'après la **proposition 3.12**) :

$$\mathscr{D}_{g\circ f} = \{x \in \mathrm{E} \mid x \in \mathrm{E} \text{ et } f(x) \in \mathrm{F}\} = \mathrm{E}$$

Définition 0.3.17 (Identité)
Soit E un ensemble. On appelle *identité de* E l'application $\mathrm{id}_\mathrm{E} : \mathrm{E} \longrightarrow \mathrm{E}$ définie par

$$\forall x \in \mathrm{E} \qquad \mathrm{id}_\mathrm{E}(x) = x$$

Proposition 0.3.18
L'identité est neutre pour la composition. Plus précisément, si F *est un ensemble et si* $f : \mathrm{E} \longrightarrow \mathrm{F}$ *et* $g : \mathrm{F} \longrightarrow \mathrm{E}$ *sont deux fonctions, on a*

$$f \circ id_\mathrm{E} = f \qquad et \qquad id_\mathrm{E} \circ g = g$$

Preuve : On utilise la **proposition 3.14** qui caractérise l'égalité entre deux fonctions, et la **proposition 3.10** qui permet de calculer le domaine de définition d'une composée :

$$\mathscr{D}_{f\circ\mathrm{id}_\mathrm{E}} = \{x \in \mathrm{E} \mid x \in \mathscr{D}_{\mathrm{id}_\mathrm{E}} \quad \text{et} \quad \mathrm{id}_\mathrm{E}(x) \in \mathscr{D}_f\} = \{x \in \mathrm{E} \mid x \in \mathrm{E} \text{ et } x \in \mathscr{D}_f\} = \mathscr{D}_f$$

et
$$\forall x \in \mathscr{D}_f \qquad f \circ \mathrm{id}_\mathrm{E}(x) = f(\mathrm{id}_\mathrm{E}(x)) = f(x)$$

f et $f \circ \mathrm{id}_\mathrm{E}$ ont le même domaine de définition et coïncident dessus ; elles sont égales.

Même chose pour $\mathrm{id}_\mathrm{E} \circ g$ et g. □

0.3.3 Injectivité, surjectivité, bijectivité

L'injectivité, la surjectivité et la bijectivité sont des propriétés relatives aux fonctions, qu'on introduit pour répondre à des questions qu'on peut se poser naturellement.

Ainsi, si $f : \mathrm{E} \longrightarrow \mathrm{F}$ et $y \in \mathrm{F}$, existe-t-il au moins un x que f envoie sur y ? Ce qui revient à dire, l'equation $f(x) = y$ d'inconnue x a-t-elle des solutions ? Et si elle a des solutions, en a-t-elle une seule ? plusieurs ?

Si on est en mesure de savoir, par un certain procédé, que l'équation $f(x) = y$ admet des solutions, cela permet de travailler avec, sans avoir à connaître celles-ci. L'idée étant que, savoir que quelque chose existe est plus utile que de ne rien savoir.

Définition 0.3.19 (Injectivité, surjectivité, bijectivité)
Soit $f : \mathrm{E} \longrightarrow \mathrm{F}$ une application. On dit qu'elle est

- *injective* si et seulement si
$$\forall x, x' \in \mathrm{E} \qquad (f(x) = f(y) \Longrightarrow x = y)$$
On dit aussi que f réalise une injection de E dans F.
- *surjective* si et seulement si
$$\forall y \in \mathrm{F} \quad \exists x \in \mathrm{E} \qquad f(x) = y$$
On dit aussi que f réalise une surjection de E sur F.
- *bijective* si et seulement si
$$\forall y \in \mathrm{F} \quad \exists ! x \in \mathrm{E} \qquad f(x) = y$$
On dit aussi que f réalise une bijection de E sur F.

Ces notions peuvent être reformulées avec le vocabulaire des fonctions qui a été défini dans les paragraphes précédents :

- f est injective si et seulement si deux éléments distincts de E ont des images distinctes. Ou encore, tout élément de F a au plus un antécédent par f.
- f est surjective si et seulement si tout élément de F est atteint par f. Ou encore, tout élément de f admet au moins un antécédent par f.
- f est bijective si et seulement si tout élément de F admet un et un seul antécédent par f

Cette reformulation montre immédiatement que

Proposition 0.3.20
Soit $f : \mathrm{E} \longrightarrow \mathrm{F}$ une application. Elle est bijective si, et seulement si, elle est à la fois injective et surjective.

Ces notions peuvent aussi être utilisées pour mesurer la taille relative de certains ensembles. Le problème ne se pose pas vraiment pour les ensembles finis : il est clair qu'un ensemble à 4 élément est plus gros qu'un ensemble à 3 éléments.

Mais que faire lorsqu'on souhaite comparer deux infinis ? Par exemple, $\mathbb{R}$ est-il plus gros que $\mathbb{N}$? $\mathbb{Q}$?

Prenons deux ensembles E et F et supposons qu'on a une injection f de E dans F. Cela signifie que des éléments distincts de E vont sur des éléments distincts de F à travers f. Donc il y a au moins suffisamment de place dans F pour caser les images d'éléments de E. Ainsi, s'il existe une injection de E dans F, c'est que F est au moins aussi gros que E.

Maintenant, supposons qu'il y a une surjection f de E sur F. Cela signifie que tout élément de F peut être associé, par f, à au moins un élément de E. Donc il y a suffisamment d'éléments dans E pour faire chacune de ces associations. Autrement dit, E est au moins aussi gros que F.

Enfin, s'il existe une bijection de E sur F, les deux propriétés précédentes sont combinées (une bijection est à la fois une injection et une surjection). Donc E et F sont de même taille.

0.3.4 Relations d'équivalence

Définition 0.3.21
Soit $\mathscr{R} = (\mathrm{E}, \mathrm{F}, \Gamma)$ une relation. On dira qu'il s'agit d'une *relation d'équivalence* si, et seulement si, les trois conditions suivantes sont satisfaites :

- $\mathscr{R}$ est *réflexive*, ce qui signifie que $\mathrm{E} = \mathrm{F}$ et
$$\forall x \in \mathrm{E} \qquad x \mathscr{R} x$$
- $\mathscr{R}$ est *symétrique* :
$$\forall x, y \in \mathrm{E} \qquad x \mathscr{R} y \implies y \mathscr{R} x$$
- $\mathscr{R}$ est *transitive* :
$$\forall x, y, z \in \mathrm{E} \qquad \left.\begin{array}{l} x \mathscr{R} y \\ y \mathscr{R} z \end{array}\right\} \implies x \mathscr{R} z$$

Dans ce cas, si $x \in \mathrm{E}$, on appelle *classe d'équivalence* de x l'ensemble
$$\mathrm{cl}(x) = \{y \in \mathrm{E} \mid x \mathscr{R} y\}$$

L'ensemble des classes d'équivalence pour $\mathscr{R}$ est noté $\mathrm{E}/\mathscr{R}$ et on l'appelle *quotient de* E *par la relation d'équivalence* $\mathscr{R}$.

La notion de relation d'équivalence interviendra de nombreuses fois dans le cours de mathématiques et y jouera un rôle fondamental. L'année prochaine encore plus que cette année. Contentons-nous pour l'instant d'en donner des exemples :

Exemple 0.3.22
Soit E un ensemble non vide. On considère la relation d'égalité sur E, en posant :
$$\forall x, y \in \mathrm{E} \qquad x \mathscr{R} y \iff x = y$$
Vérifions qu'il s'agit d'une relation d'équivalence.

- **Réflexivité** : Soit $x \in \mathrm{E}$. Alors $x = x$, ce qui établit bien que $x \mathscr{R} x$.
- **Symétrie** : Soient x et y dans E. On suppose que $x \mathscr{R} y$; par définition, cela signifie que $x = y$. Donc x et y sont le même élément et, bien évidemment, on a $y = x$ ou encore $y \mathscr{R} x$.
- **Transitivité** : Soient x, y et z dans E, tels que $x \mathscr{R} y$ et $y \mathscr{R} z$. Ceci signifie que $x = y$ et $y = z$: x, y et z sont le même élément de E. Du coup, $x \mathscr{R} z$.

L'égalité est donc une relation d'équivalence.

Exemple 0.3.23
On sait, depuis qu'on est tout petit, que tout élément de $[0\,;1[$ admet un unique développement décimal $x = 0.a_1 a_2 a_3 \ldots$ (il faudrait que je sois un peu plus précis, mais cela rendrait la discussion plus technique que le nécessite la situation).

Étant donnés x et y dans $[0\,;1]$, on notera $x \simeq y$ si, et seulement si, les deux premiers chiffres de leur écriture décimale sont égaux. Par exemple,

$$0.456 \simeq 0.45 \qquad \frac{\sqrt{2}}{2} \simeq 0.70 \qquad 0.999 \simeq 0.99$$

Il est facile de vérifier que $\simeq$ est une relation d'équivalence. Remarquons que, par définition, elle met en relation deux nombres de $[0\,;1[$, pour peu qu'ils aient les deux mêmes premiers chiffres après la virgule.

Imaginons une calculatrice de mauvaise qualité qui ne sait faire des calculs qu'avec une précision de deux chiffres après la virgule ; pour elle, $\simeq$ n'est autre que l'égalité. Mais pour une autre calculatrice un peu moins pourrie qui sait calculer avec une précision de 3 décimales, ces deux relations $=$ et $\simeq$ sont bien distinctes.

Faisons aussi une observation importante : en quelque sorte, $\simeq$ sert à regrouper entre eux les nombres qui sont indistinguables par notre calculatrice à deux décimales. Elle fournit alors un découpage naturel de $[0\,;1[$:

$$[0\,;1[= [0\,;0.01[\cup [0.01\,;0.02[\cup \cdots \cup [0.99\,;1[$$

Ces intervalles sont disjoints deux-à-deux et les éléments qu'ils contiennent sont caractérisés exactement par le fait qu'ils ont les deux mêmes premières décimales.

Ce découpage mis en évidence dans l'exemple n'est pas un hasard. Il est un cas particulier de ce qu'on appelle une partition d'un ensemble.

Définition 0.3.24
Soit E un ensemble. Soit $\mathscr{A}$ une collection de sous-ensembles de E. On dit que $\mathscr{A}$ est une partition de E si, et seulement si,

- Les éléments de $\mathscr{A}$ sont non vides :
$$\forall A \in \mathscr{A} \qquad A \neq \emptyset$$
- Les éléments de $\mathscr{A}$ sont deux-à-deux disjoints :
$$\forall A, B \in \mathscr{A} \qquad (A \neq A' \implies A \cap A' = \emptyset)$$
- Ils permettent de recomposer E :
$$E = \bigcup_{A \in \mathscr{A}} A$$

Montrons alors le point important de cette section : partitions et relations d'équivalence sont essentiellement le même phénomène, vu sous des angles différents.

Proposition 0.3.25
Soit E *un ensemble.*

1. *Soit* $\mathscr{R}$ *une relation d'équivalence sur* E. *Les classes d'équivalence forment une partition de* E.
2. *Soit* $\mathscr{A}$ *une partition de* E. *Il existe une (et une seule) relation d'équivalence sur* E

Preuve : On commence par se donner une relation d'équivalence $\mathscr{R}$ sur E. On doit montrer que l'union des classes d'équivalence est E, et que deux classes distinctes sont disjointes.

Si $x \in E$, la réflexivité de $\mathscr{R}$ nous dit que $x \mathscr{R} x$; autrement dit, $x \in \mathrm{cl}(x)$. Donc

$$E = \bigcup_{A \in E/\mathscr{R}} A$$

Ensuite, on se donne deux classes d'équivalence A et B. Par définition, il existe x et y dans E tels que $A = \mathrm{cl}(x)$ et $B = \mathrm{cl}(y)$. Supposons que $A \cap B \neq \emptyset$ et montrons que $A = B$. Il existe $z \in A \cap B$. Cela signifie, par définition d'une classe d'équivalence, que

$$x\mathscr{R}z \qquad \text{et} \qquad y\mathscr{R}z$$

Par suite, $\forall u \in \mathrm{E} \quad u \in \mathrm{A} \Longrightarrow x\mathscr{R}u$

$\Longrightarrow u\mathscr{R}x$ ($\mathscr{R}$ est symétrique)

$\Longrightarrow u\mathscr{R}z$ ($\mathscr{R}$ est transitive)

$\Longrightarrow z\mathscr{R}u$ ($\mathscr{R}$ est symétrique)

$\Longrightarrow y\mathscr{R}u$ ($\mathscr{R}$ est transitive)

$u \in \mathrm{A} \Longrightarrow u \in \mathrm{B}$

Ce qui montre que $\mathrm{A} \subset \mathrm{B}$. De la même manière, on montrerait que $\mathrm{B} \subset \mathrm{A}$. On a donc établi

$$\forall \mathrm{A}, \mathrm{B} \in \mathrm{E}/\mathscr{R} \qquad \mathrm{A} \cap \mathrm{B} \neq \emptyset \implies \mathrm{A} = \mathrm{B}$$

Par contre-apposée, $\forall \mathrm{A}, \mathrm{B} \in \mathrm{E}/\mathscr{R} \qquad (\mathrm{A} \neq \mathrm{B} \implies \mathrm{A} \cap \mathrm{B} = \emptyset)$

La première partie de la preuve est complète : $\mathrm{E}/\mathscr{R}$ partitionne bien E.

Réciproquement, on suppose qu'on a une partition $\mathscr{A}$ de E. On doit construire une relation d'équivalence dont les classes d'équivalences sont exactement les éléments de $\mathscr{A}$.

Si $x \in \mathrm{E}$, il existe $\mathrm{A} \in \mathscr{A}$ tel que $x \in \mathrm{A}$ puisque $\mathrm{E} = \bigcup_{\mathrm{B} \in \mathscr{A}} \mathrm{B}$. En outre, ce A est unique : en effet, si $\mathrm{B} \in \mathscr{A}$ est tel que $\mathrm{B} \neq \mathrm{A}$, alors A et B sont disjoints (définition d'une partition) et $\mathrm{A} \cap \mathrm{B} = \emptyset$ d'où $x \notin \mathrm{B}$.

Autrement dit, pour tout $x \in \mathrm{E}$, il existe un unique élément de $\mathscr{A}$, qu'on note finalement $\mathrm{A}(x)$, tel que $x \in \mathrm{A}(x)$. On définit alors une relation $\mathscr{R}$ de la manière suivante :

$$\forall x, y \in \mathrm{E} \qquad x\mathscr{R}y \implies y \in \mathrm{A}(x)$$

Montrons que $\mathscr{R}$ est une relation d'équivalence. D'abord, puisque $x \in \mathrm{A}(x)$ pour tout $x \in \mathrm{E}$, il est clair que $x\mathscr{R}x$: ceci établit la réflexivité de $\mathscr{R}$.

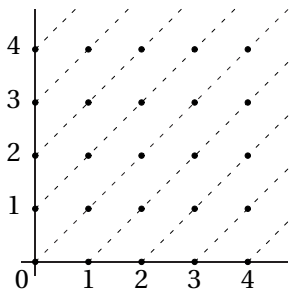
Ensuite, donnons-nous x et y dans E, tels que $x\mathscr{R}y$. Par définition, $y \in \mathrm{A}(x)$; du coup, puisque $y \in \mathrm{A}(y)$, les ensembles $\mathrm{A}(x)$ et $\mathrm{A}(y)$ ne sont pas disjoints ; par définition d'une partition, ils sont égaux. Par suite, $x \in \mathrm{A}(y)$ donc $y\mathscr{R}x$: $\mathscr{R}$ est symétrique.

Enfin, soient x, y et z dans E tels que $x\mathscr{R}y$ et $y\mathscr{R}z$. On vient de voir qu'alors, $\mathrm{A}(x) = \mathrm{A}(y)$ et $\mathrm{A}(y) = \mathrm{A}(z)$. Du coup, $z \in \mathrm{A}(x)$ et $x\mathscr{R}z$: $\mathscr{R}$ est transitive.

On a établi que $\mathscr{R}$ est une relation d'équivalence. Par définition, ses classes d'équivalence sont précisément les éléments de $\mathscr{A}$. □

Exemple 0.3.26

On peut partitionner l'ensemble $\mathbb{N}^2$ en une réunion disjointe de « lignes » obliques de coefficient directeur 1 comme représenté sur le dessin qui suit.



Compte-tenu du théorème précédent, cette partition correspond à une relation d'équivalence, notée $\mathscr{R}$ pour être original : si $n = (n_1, n_2)$ et $m = (m_1, m_2)$ sont deux couples d'entiers, ils seront équivalents si, et seulement si, ils se trouvent sur la même ligne pointillée sur le dessin. Ce qui revient à dire que la pente entre ces deux points vaut 1. Autrement dit,

$$n \mathscr{R} m \iff m_2 - n_2 = m_1 - n_1$$

Cette relation d'équivalence sera mise à profit pour construire la notion de nombre négatif et l'ensemble $\mathbb{Z}$. D'ailleurs, en supposant que les nombres négatifs n'existent pas, la bonne définition pour $\mathscr{R}$ est en fait la suivante :

$$n \mathscr{R} m \iff m_2 + n_1 = n_2 + m_1$$

Exemple 0.3.27
Nous manipulons des relations d'équivalence depuis notre plus tendre enfance. Plus précisément, depuis que nous avons appris à travailler avec des fractions dans l'ensemble $\mathbb{Q}$.

En effet, une fraction $\frac{m}{n}$ est en fait la donnée du numérateur $m \in \mathbb{Z}$ et du dénominateur $n \in \mathbb{Z}^\star$; autrement dit, du couple $(m, n) \in \mathbb{Z} \times \mathbb{Z}^\star$. Mais cette identification est trop simpliste : en effet, on dispose de la règle permettant de simplifier une fraction lorsque m et n ont un facteur commun. C'est celle-ci qui permet de dire que les fractions $\frac{m}{n}$ et $\frac{2m}{2n}$, par exemple, sont identiques.

Une manière rigoureuse de construire $\mathbb{Q}$ consiste donc à prendre l'ensemble $\mathbb{Z} \times \mathbb{Z}^\star$ et à le quotienter par la relation d'équivalence

$$(m, n) \mathscr{R} (m', n') \iff mn' - m'n = 0$$

qui n'est autre que « la règle des produits en croix. » Alors la fraction $\frac{m}{n}$ est simplement la classe d'équivalence du couple (m, n). Il y a cependant besoin de quelques rudiments d'arithmétique, qui seront présentés dans un chapitre ultérieur, pour pouvoir l'expliquer.

Chapitre 1

Ensembles Finis et Dénombrements

L'objectif de ce chapitre est d'étudier plus en profondeur les propriétés de $\mathbb{N}$, l'ensemble des entiers naturels. En particulier, on démontre le théorème de récurrence, qui est un outil fondamental pour étudier des propriétés mettant en jeu les nombres entiers.

Puis on étudie en particulier les ensembles finis et les méthodes élementaires pour compter leurs éléments. On introduira les nombres $\binom{n}{p}$, constituant le triangle de Pascal.

1.1 Théorème de Récurrence

1.1.1 L'ensemble $\mathbb{N}$ des entiers naturels

On rappelle que l'ensemble $\mathbb{N}$ des *entiers naturels* est l'ensemble des nombres entiers positifs : $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Définition 1.1.1
Soit A une partie non vide de $\mathbb{N}$. On dira que A *est majorée* si et seulement si il existe $\mathrm{N} \in \mathbb{N}$, tel que

$$\forall n \in \mathrm{A} \qquad n \leqslant \mathrm{N}$$

Un tel entier N sera appelé *majorant de* A. Si N appartient à A, on dira que N est *un plus grand élément de* A.

Proposition 1.1.2
Soit A *une partie non vide de* $\mathbb{N}$. *Si* A *admet un plus grand élément, celui-ci est unique.*

Preuve : On suppose que A admet des plus grands éléments N et P. Par définition, N et P sont dans A et

$$\forall n \in \mathrm{A} \qquad n \leqslant \mathrm{N} \qquad \text{et} \qquad n \leqslant \mathrm{P}$$

En particulier, puisque $\mathrm{N} \in \mathrm{A}$, on a $\mathrm{N} \leqslant \mathrm{P}$. De même, $\mathrm{P} \leqslant \mathrm{N}$. Par conséquent, $\mathrm{N} = \mathrm{P}$. □

Définition 1.1.3
Soit A une partie non vide de $\mathbb{N}$. Un entier N est appelé *plus petit élément de* A si

$$\mathrm{N} \in \mathrm{A} \qquad \text{et} \qquad \forall n \in \mathrm{A} \qquad \mathrm{N} \leqslant n$$

Proposition 1.1.4
Soit A *une partie non vide de* $\mathbb{N}$. *Si* A *admet un plus petit élément, celui-ci est unique.*

Preuve : Similaire à celle de la **proposition 1.2**. □

L'ensemble $\mathbb{N}$ possède les propriétés fondamentales suivantes :

Théorème 1.1.5
1. *Toute partie non vide de* $\mathbb{N}$ *admet un (unique) plus petit élément.*
2. *Toute partie non vide majorée de* $\mathbb{N}$ *admet un (unique) plus grand élément.*

Preuve : Le premier point est admis car sa démonstration requiert le détail de la construction de $\mathbb{N}$. Il est suffisamment intuitif pour que l'on puisse l'admettre sans problème.

Démontrons maintenant le second point. Soit A une partie non vide de $\mathbb{N}$, majorée. A admet donc des majorants et l'ensemble M des majorants de A n'est pas vide. D'après le premier point, M admet un plus petit élément que l'on note N. Nous allons établir que N est le plus grand élément de A.

D'abord, puisque N appartient à M, N est un majorant de A :

$$\forall n \in \mathrm{A} \qquad n \leqslant \mathrm{N}$$

Supposons que N n'appartient pas à A. Alors il est distinct de n'importe quel élément de A donc

$$\forall n \in \mathrm{A} \qquad n < \mathrm{N}$$

Auquel cas, $$\forall n \in \mathrm{A} \qquad n \leqslant \mathrm{N}-1$$

ce qui signifie que N – 1 est un majorant de A. Autrement dit, N – 1 appartient à M. Mais N est le plus petit élément de M. On a donc une contradiction. Par suite, N appartient à A : c'est le plus grand élément de A. □

Définition 1.1.6
Soient n et m deux entiers, avec $n \leqslant m$. L'ensemble de tous les entiers compris entre n et m est noté $[\![n ; m]\!]$. L'ensemble de tous les entiers supérieurs à n est noté $[\![n ; +\infty [\![$.

1.1.2 Raisonnements par recurrence

Le raisonnement pas récurrence est l'outil mathématique, rigoureux, pour démontrer des choses de proche-en-proche.

Théorème 1.1.7
Soit $\mathscr{P}$ *une propriété définie sur* $\mathbb{N}$. *On suppose que* $\mathscr{P}(0)$ *est vraie et que*

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

Alors $\mathscr{P}(n)$ *est vraie pour tout entier* n.

Preuve : On note A l'ensemble de tous les entiers qui vérifient la propriété $\mathscr{P}$. Supposons qu'il existe des entiers ne vérifiant pas A, c'est-à-dire que A n'est pas égal à $\mathbb{N}$ tout entier. Alors l'ensemble $\mathrm{B} = \mathbb{N} \setminus \mathrm{A}$ n'est pas vide. D'après le **théorème 1.5**, B admet un plus petit élément N.

Comme $\mathscr{P}(0)$ est vraie, 0 appartient à A et n'appartient donc pas à B. Par suite, N ne peut être nul et est donc strictement positif. Donc $N-1$ est un entier naturel, strictement plus petit que N. Dans la mesure où N est le plus petit élément de B, $N-1$ ne peut pas se trouver dans B. Il est donc dans A ; par suite, $\mathscr{P}(N-1)$ est vraie. Il s'ensuit que $\mathscr{P}(N-1+1) = \mathscr{P}(N)$ est vraie donc N appartient à A. Cela contredit le fait que N appartient à B. Donc $A = \mathbb{N}$. □

Parfois, on ne peut espérer montrer une propriété qu'à partir d'un certain rang. Il y a un théorème pour cela :

Corollaire 1.1.8
Soient n_0 un entier et $\mathscr{P}$ une propriété définie sur $[\![n_0\,;+\infty[\![$. On suppose que $\mathscr{P}(n_0)$ est vraie et que

$$\forall n \geqslant n_0 \qquad \mathscr{P}(n) \implies \mathscr{P}(n+1)$$

Alors $\mathscr{P}(n)$ est vraie pour tout entier $n \geqslant n_0$.

Preuve : On pose $\forall n \in \mathbb{N} \qquad \mathscr{Q}(n) = \mathscr{P}(n_0+n)$

Alors $\mathscr{Q}(0) = \mathscr{P}(n_0)$ est vraie.

Ensuite, soit n un entier tel que $\mathscr{Q}(n) = \mathscr{P}(n_0+n)$ soit vraie. L'entier n_0+n est supérieur à n_0, donc $\mathscr{P}(n_0+n+1) = \mathscr{Q}(n+1)$ est vraie. D'après le théorème de récurrence, $\mathscr{Q}(n)$ est vraie pour tout entier n. □

Pour d'autres propriétés, il n'est pas suffisant d'avoir $\mathscr{P}(n)$ pour avoir $\mathscr{P}(n+1)$. On a un théorème adapté à ces cas-là :

Corollaire 1.1.9
Soient n_0 un entier et $\mathscr{P}$ une propriété définie sur $[\![n_0\,;+\infty[\![$. On suppose que $\mathscr{P}(n_0)$ et $\mathscr{P}(n_0+1)$ sont vraies, et que

$$\forall n \geqslant n_0 \qquad \big(\mathscr{P}(n) \text{ et } \mathscr{P}(n+1)\big) \implies \mathscr{P}(n+2)$$

Alors $\mathscr{P}$ est vraie pour tout entier $n \geqslant n_0$.

Preuve : On pose $\forall n \geqslant n_0 \qquad \mathscr{Q}(n) = \big(\mathscr{P}(n) \text{ et } \mathscr{P}(n+1)\big)$

Par hypothèse, $\mathscr{Q}(n_0)$ est vraie.

Ensuite, soit n est un entier supérieur à n_0 tel que $\mathscr{Q}(n)$ soit vraie. Par définition de $\mathscr{Q}$, cela signifie que $\mathscr{P}(n)$ et $\mathscr{P}(n+1)$ sont vraies. D'après l'hypothèse sur $\mathscr{P}$, cela implique que $\mathscr{P}(n+2)$ est également vraie. On constate que $\mathscr{P}(n+1)$ et $\mathscr{P}(n+2)$ sont vraies, autrement dit $\mathscr{Q}(n+1)$ est vraie. Donc $\mathscr{Q}$ est héréditaire.

D'après le **corollaire 1.8**, $\mathscr{Q}(n)$ est vraie pour tout $n \geqslant n_0$. En particulier, $\mathscr{P}(n)$ est vraie. □

Corollaire 1.1.10
Soient n_0 un entier et $\mathscr{P}$ une propriété définie sur $[\![n_0\,;+\infty[\![$. On suppose que $\mathscr{P}(n_0)$ est vraie et que

$$\forall n \geqslant n_0 \qquad \big(\forall k \in [\![\, n_0\,;n\,]\!] \qquad \mathscr{P}(k)\big) \implies \mathscr{P}(n+1)$$

Alors $\mathscr{P}(n)$ est vraie pour tout entier $n \geqslant n_0$.

Preuve : On pose $\forall n \geqslant n_0 \qquad \mathscr{Q}(n) = \big(\mathscr{P}(n_0) \text{ et } \mathscr{P}(n_0+1) \text{ et } \cdots \text{ et } \mathscr{P}(n)\big)$

Les hypothèses du théorème nous disent précisément que $\mathscr{Q}(n_0)$ est vraie et que

$$\forall n \geqslant n_0 \qquad \mathscr{Q}(n) \implies \mathscr{Q}(n+1)$$

D'après le **corollaire 1.8**, $\mathscr{Q}(n)$ est vraie pour tout entier $n \geqslant n_0$. En particulier, $\mathscr{P}(n)$ est vraie pour tout entier $n \geqslant n_0$. □

1.1.3 Suites Définies par Récurrence

Définition 1.1.11

Soit E un ensemble. On appelle *suite à valeurs dans* E toute fonction de $\mathbb{N}$ dans E. Leur ensemble est donc $\mathrm{E}^{\mathbb{N}}$.

Si u est une suite à valeurs dans E, on notera u_n, plutôt que $u(n)$ sa valeur en un entier n. Si A est l'ensemble de définition de u, on notera indifféremment u ou $(u_n)_{n\in\mathrm{A}}$.

Une suite peut être définie explicitement en chaque entier n par une relation entre u_n et n. Par exemple,

$$\forall n \geqslant 1 \qquad u_n = \frac{1}{n^2}$$

Mais le principe de récurrence nous dit aussi que, si f est une application de E dans lui-même, une relation *de récurrence* telle que

$$\begin{cases} u_0 = a \\ \forall n \in \mathbb{N} \qquad u_{n+1} = f(u_n) \end{cases}$$

suffit à définir une suite, de manière unique.

Plus généralement, une suite peut aussi être définie par

– Une application $f : \mathbb{N} \times \mathrm{E} \longrightarrow \mathrm{E}$, un premier terme u_0 et une relation de récurrence

$$\forall n \in \mathbb{N} \qquad u_{n+1} = f(n, u_n)$$

– Une application $f : \mathbb{N} \times \mathrm{E} \times \mathrm{E} \longrightarrow \mathrm{E}$, deux premiers termes u_0 et u_1, et une relation de récurrence

$$\forall n \in \mathbb{N} \qquad u_{n+2} = f(n, u_n, u_{n+1})$$

– Des relations de récurrence plus compliquées sur lesquelles nous n'élaborerons pas.

Deux exemples simples de suites definies par récurrence sont les suites arithmétiques et les suites géométriques.

Définition 1.1.12 (Suite arithmétique)

Soient a et r deux nombres complexes. On appelle *suite arithmétique de premier terme a et de raison r* la suite définie par récurrence

$$u_0 = a \qquad \text{et} \qquad \forall n \in \mathbb{N} \qquad u_{n+1} = u_n + r$$

Définition 1.1.13 (Suite géométrique)

Soient a et q deux nombres complexes. On appelle *suite géométrique de premier terme a et de raison q* la suite définie par récurrence

$$u_0 = a \qquad \text{et} \qquad \forall n \in \mathbb{N} \qquad u_{n+1} = q u_n$$

Proposition 1.1.14
Soit u la suite arithmétique de premier terme a et de raison r. On a

$$\forall n \in \mathbb{N} \qquad u_n = a + nr$$

Preuve : La démonstration se fait par récurrence. On pose

$$\forall n \in \mathbb{N} \qquad \mathscr{P}(n) = \text{« } u_n = a + nr \text{ »}$$

- $\mathscr{P}$**(0) est vraie :** En effet, $u_0 = a = a + 0 \times r$.
- $\mathscr{P}(\boldsymbol{n}) \Longrightarrow \mathscr{P}(\boldsymbol{n+1})$: Soit n un entier tel que $\mathscr{P}(n)$ soit vraie, c'est-à-dire qu'on sait que $u_n = a + nr$. Alors, d'après la définition de u_{n+1} par récurrence,

  $$u_{n+1} = u_n + r = a + nr + r = a + (n+1)r$$

  et on constate que $\mathscr{P}(n+1)$ est effectivement vraie.
- **Conclusion :** $\mathscr{P}(n)$ est vraie pour tout entier n, d'après le théorème de récurrence :

  $$\forall n \in \mathbb{N} \qquad u_n = a + nr$$ □

Proposition 1.1.15
Soit u la suite géométrique de premier terme a et de raison q. On a

$$\forall n \in \mathbb{N} \qquad u_n = aq^n$$

Preuve : La démonstration se fait par récurrence. On pose

$$\forall n \in \mathbb{N} \qquad \mathscr{P}(n) = \text{« } u_n = aq^n \text{ »}$$

- $\mathscr{P}$**(0) est vraie :** En effet, $u_0 = a = a \times q^0$.
- $\mathscr{P}(\boldsymbol{n}) \Longrightarrow \mathscr{P}(\boldsymbol{n+1})$: Soit n un entier tel que $\mathscr{P}(n)$ soit vraie, c'est-à-dire qu'on sait que $u_n = aq^n$. Alors, d'après la définition de u_{n+1} par récurrence,

  $$u_{n+1} = qu_n = q \times aq^n = aq^{n+1}$$

  et on constate que $\mathscr{P}(n+1)$ est effectivement vraie.
- **Conclusion :** $\mathscr{P}(n)$ est vraie pour tout entier n, d'après le théorème de récurrence :

  $$\forall n \in \mathbb{N} \qquad u_n = aq^n$$ □

1.1.4 Notations Σ et Π

On définit et étudie les propriétés élementaires des notations $\sum$ et $\prod$.

Définition 1.1.16
Soit u une suite à valeurs complexes. Soit n_0 un entier. On pose

$$\sum_{i=n_0}^{n_0} u_i = u_{n_0} \qquad \text{et} \qquad \forall n \geqslant n_0 \qquad \sum_{i=n_0}^{n+1} u_i = u_{n+1} + \sum_{i=n_0}^{n} u_i$$

et

$$\prod_{i=n_0}^{n_0} u_i = u_{n_0} \qquad \text{et} \qquad \forall n \geqslant n_0 \qquad \prod_{i=n_0}^{n+1} u_i = u_n \times \prod_{i=n_0}^{n} u_i$$

Proposition 1.1.17
Soit u une suite à valeurs complexes. Soient $n < m < p$ trois entiers. On a

$$\sum_{i=n}^{m} u_i + \sum_{i=m+1}^{p} u_i = \sum_{i=n}^{p} u_i$$

et

$$\prod_{i=n}^{m} u_i \times \prod_{i=m+1}^{p} u_i = \prod_{i=n}^{p} u_i$$

Preuve : On fixe deux entiers $n < m$ et on pose

$$\forall p \geqslant m+1 \qquad \mathscr{P}(p) : \text{« } \sum_{i=n}^{m} u_i + \sum_{i=m+1}^{p} u_i = \sum_{i=n}^{p} u_i \text{ »}$$

- $\mathscr{P}(\boldsymbol{m+1})$ **est vraie :** En effet, d'après la **définition 1.16**,

$$\sum_{i=n}^{m} u_i + \sum_{i=m+1}^{m+1} u_i = \sum_{i=n}^{m} u_i + u_{m+1} = \sum_{i=n}^{m+1} u_i$$

- $\mathscr{P}(\boldsymbol{p}) \Longrightarrow \mathscr{P}(\boldsymbol{p+1})$: Soit $p \geqslant m+1$ un entier tel que $\mathscr{P}(p)$ soit vraie, c'est-à-dire qu'on sait

$$\sum_{i=n}^{m} u_i + \sum_{i=m+1}^{p} u_i = \sum_{i=n}^{p} u_i$$

Alors $$\sum_{i=n}^{m} u_i + \sum_{i=m+1}^{p+1} u_i = \sum_{i=n}^{m} u_i + \sum_{i=m+1}^{p} u_i + u_{p+1} = \sum_{i=n}^{p} u_i + u_{p+1} = \sum_{i=n}^{p+1} u_i$$

Ici, on a utilisé successivement la **définition 1.16**[1], puis l'hypothèse de récurrence, et enfin la **définition 1.16** à nouveau.[2] On constate que $\mathscr{P}(p+1)$ est effectivement vraie.

- **Conclusion :** $\mathscr{P}(p)$ est vraie pour tout entier $p \geqslant m+1$, d'après le théorème de récurrence :

$$\forall p \geqslant m+1 \qquad \sum_{i=n}^{m} u_i + \sum_{i=m+1}^{p} u_i = \sum_{i=n}^{p} u_i$$

Puisque $n < m$ étaient des entiers arbitraires, on a gagné. La preuve pour les produits est exactement la même. □

Proposition 1.1.18
Soient u et v deux suites à valeurs complexes. Pour tous entiers n et m, avec $n \leqslant m$, on a

$$\sum_{i=n}^{m} u_i + \sum_{i=n}^{m} v_i = \sum_{i=n}^{m} (u_i + v_i)$$

et

$$\prod_{i=n}^{m} u_i \times \prod_{i=n}^{m} v_i = \prod_{i=n}^{m} (u_i v_i)$$

Preuve : Soit n un entier fixé. On définit une nouvelle suite w de la manière suivante :

$$\forall m \geqslant n \qquad w_m = \sum_{i=n}^{m} u_i + \sum_{i=n}^{m} v_i$$

On a $$w_n = \sum_{i=n}^{n} u_i + \sum_{i=n}^{n} v_i = u_n + v_n = \sum_{i=n}^{n} (u_i + v_i)$$

[1] Avec $n_0 = m+1$ et $n = p$.
[2] Avec $n_0 = n$ et $n = p$.

et $\forall m \geqslant n \qquad w_{m+1} = \sum_{i=n}^{m+1} u_i + \sum_{i=n}^{m+1} v_i$

$$= \Big(\sum_{i=n}^{m} u_i + u_{m+1}\Big) + \Big(\sum_{i=n}^{m} v_i + v_{m+1}\Big)$$

$$w_{m+1} = w_m + (u_{m+1} + v_{m+1})$$

On voit que la suite $(w_m)_{m\geqslant n}$ satisfait la même relation de récurrence que $\big(\sum_{i=n}^{m}(u_i+v_i)\big)_{m\geqslant n}$. Ces deux suites sont donc égales, puisqu'une suite définie par récurrence est uniquement déterminée.

La preuve pour les produits est une copie conforme de ce qui précède, à ceci près qu'on remplace les Σ par des Π. □

1.2 Ensembles finis

1.2.1 Définitions

Lorsqu'on a défini les notions d'injection, surjection et bijection, on a expliqué qu'elles pouvaient servir à comparer la taille de deux ensembles A et B.

- S'il existe une injection de A dans B, cela signifie qu'on peut envoyer tous les éléments de A sur des éléments de B deux à deux distincts. Intuitivement, B doit donc avoir plus d'éléments que A.
- S'il existe une surjection de A sur B, tout élément de B provient d'au moins un élément de A. Intuitivement, A a au moins autant d'éléments de B.
- S'il existe une bijection de A sur B, ces deux ensembles doivent avoir gross-modo le même nombre d'éléments.

Dans ce paragraphe, nous obtenons ces résultats intuitifs dans le cas d'ensembles finis.

Lemme 1.2.1
Soient n et m deux entiers non nuls. Ils sont égaux si, et seulement si, il existe une bijection de $[\![1\,;n]\!]$ *sur* $[\![1\,;p]\!]$.

Preuve : On démontre ceci par récurrence. Pour tout entier n, on note $\mathscr{P}(n)$ la proposition : « Si p est un entier tel qu'il existe une bijection de $[\![1\,;n]\!]$ sur $[\![1\,;p]\!]$ alors $n=p$. »

- **$\mathscr{P}(1)$ est vraie :** Supposons qu'il existe une bijection de $[\![1\,;1]\!]$ sur $[\![1\,;p]\!]$. Notons-la b. Puisque b est surjective, 1 et p sont atteints : il existe n_1 et n_2 dans $[\![1\,;1]\!]$, tels que

  $$b(n_1) = 1 \qquad \text{et} \qquad b(n_2) = p$$

  Or, $[\![1\,;1]\!] = \{1\}$ donc $n_1 = n_2 = 1$. On en déduit que

  $$p = b(n_2) = b(n_1) = 1$$

  ce qui établit $\mathscr{P}(1)$.
- **$\mathscr{P}(n) \Longrightarrow \mathscr{P}(n+1)$** : Soit n un entier positif, tel que $\mathscr{P}(n)$ soit satisfaite. Soit p un entier tel qu'il existe une bijection, notée b, de $[\![1\,;n+1]\!]$ sur $[\![1\,;p]\!]$. On considère deux cas :
  – Si $b(n+1) = p$, on pose

  $$\forall k \in [\![1\,;n]\!] \qquad f(k) = b(k)$$

En d'autres termes, f est la restriction de b à $[\![1\,;n]\!]$. Montrons que f est une bijection de $[\![1\,;n]\!]$ sur $[\![1\,;p-1]\!]$.
On commence par établir que f est à valeurs dans $[\![1\,;p-1]\!]$. En effet, comme b est injective et $b(n+1)=p$, les valeurs prises par b dans $[\![1\,;n]\!]$ sont différentes de p. Donc sont comprises entre 1 et $p-1$.
Puis on montre que f est injective. Supposons que m_1 et m_2 sont dans $[\![1\,;n]\!]$, tels que $f(m_1)=f(m_2)$. D'après la définition de f, il vient $b(m_1)=b(m_2)$. Or, b est injective donc $m_1=m_2$: f est aussi injective.
Enfin, on montre que f est surjective sur $[\![1\,;p-1]\!]$. Soit k un élément de cet ensemble. *A fortiori*, k appartient à $[\![1\,;p]\!]$ et comme b est surjective, il existe $m\in[\![1\,;n+1]\!]$ tel que $b(m)=k$. Or, $b(m)=k\neq p$, b est injective et $b(n+1)=p$ donc m est différent de $n+1$. C'est-à-dire que $m\leqslant n$. D'où $k=b(m)=f(m)$; tout élément de $[\![1\,;p-1]\!]$ est atteint par f donc f est surjective.
On voit donc que f est une bijection de $[\![1\,;n]\!]$ sur $[\![1\,;p-1]\!]$. D'après $\mathscr{P}(n)$, $n=p-1$. Ou encore, $n+1=p$. Ce qui établit $\mathscr{P}(n+1)$.

– Si $b(n+1)\neq p$, on note $a=b(n+1)$. On définit alors

$$\forall k\in[\![1\,;p]\!]\qquad \sigma(k)=\begin{cases} p \text{ si } k=a\\ a \text{ si } k=p\\ k \text{ sinon}\end{cases}$$

En d'autres termes, σ est l'application de $[\![1\,;p]\!]$ dans lui-même qui échange a et p, mais laisse tous les autres éléments inertes. Il est clair que σ est une bijection de $[\![1\,;p]\!]$ sur lui-même, puisque $\sigma\circ\sigma=\mathrm{id}$. La composée de deux bijections est une bijection donc $\sigma\circ b$ est une bijection de $[\![1\,;n]\!]$ sur $[\![1\,;p]\!]$. En oute,

$$\sigma\circ b(n+1)=\sigma(b(n+1))=\sigma(a)=p$$

D'après l'étude du premier cas, $n+1=p$. Ce qui établit $\mathscr{P}(n+1)$.

- **Conclusion :** D'après le théorème de récurrence, $\mathscr{P}(n)$ est vraie pour tout entier n. Ce qui achève la démonstration. □

Ce lemme permet de poser la définition suivante :

Définition 1.2.2
Un ensemble non vide E est dit *fini* si, et seulement si, il existe un (unique) entier positif p tel que E soit en bijection avec $[\![1\,;p]\!]$. Cet entier est appelé *cardinal* de E, noté $\mathrm{Card}\,\mathrm{E}$ ou $|\mathrm{E}|$. Par convention, l'ensemble vide est fini et son cardinal vaut 0.

Notons qu'à partir du moment où on a un ensemble fini E, dont on note p le cardinal, on peut énumérer ses éléments. En effet, il existe une bijection σ de $[\![1\,;p]\!]$ sur E. Les objets $\sigma(1)$, $\sigma(2)$, …, $\sigma(p)$ sont donc deux-à-deux distincts (injectivité) et constituent tous les éléments de E. Donc

$$\mathrm{E}=\{\sigma(1),\ldots,\sigma(p)\}$$

et cette écriture décrit E en extension.

1.2.2 Parties d'un ensemble fini

Lemme 1.2.3
Soit E *un ensemble fini, non vide, de cardinal* p. *Soit* $a\in\mathrm{E}$. *L'ensemble* $\mathrm{E}\setminus\{a\}$ *est fini, de cardinal* $p-1$.

Preuve : Supposons d'abord que $p = 1$. Il existe une bijection de $[\![1\,;1]\!]$ sur E, donc E est un singleton. Donc $E \setminus \{a\} = \emptyset$ et a pour cardinal 0, qui vaut bien $p-1$.

Maintenant, supposons $p > 1$, de sorte que $p-1 > 0$. On sait qu'il existe une bijection b de E sur $[\![1\,;p]\!]$, d'après la **définition 2.2**.

Si $b(a) = p$, alors sa restriction à $E \setminus \{a\}$ est une bijection sur $[\![1\,;p-1]\!]$ (voir la preuve du **lemme 2.1**). Donc $E \setminus \{a\}$ est de cardinal $p-1$.

Si $b(a)$ est différent de p (disons $b(a) = n$), on note σ la bijection de $[\![1\,;n]\!]$ sur lui-même qui échange n et p. Alors $b \circ \sigma$ est une bijection de E sur $[\![1\,;n]\!]$ telle que $b \circ \sigma(a) = n$. On est ramené au cas précédent et on en déduit que $|E \setminus \{a\}| = p-1$. □

Théorème 1.2.4
Soit E *un ensemble fini, soit* $F \subset E$. *Alors* $|F| \leqslant |E|$, *avec égalité si et seulement si* $F = E$.

Preuve : On démontre le résultat par récurrence en notant, pour tout entier p, $\mathscr{P}(p)$ la proposition : « Soit E un ensemble de cardinal p. Pour tout $F \subset E$, on a $|F| \leqslant |E|$, avec égalité si et seulement si $F = E$. »

- $\mathscr{P}$**(0) est vraie :** En effet, il n'y a qu'un seul ensemble de cardinal nul, c'est l'ensemble vide. Et il n'a qu'un seul sous-ensemble, qui est aussi l'ensemble vide, de même cardinal.
- $\mathscr{P}(p) \Longrightarrow \mathscr{P}(p+1)$: Soit p un entier tel que $\mathscr{P}(p)$ soit satisfaite. On se donne E un ensemble de cardinal $p+1$ et F un sous-ensemble de E. Si $F = E$, alors $|E| = |F|$. Si F est strictement inclus dans E, $E \setminus F$ n'est pas vide et on prend a dedans. De sorte que

  $$F \subset E \setminus \{a\} \qquad \text{avec} \qquad |E \setminus \{a\}| = p+1-1 = p$$

  F est un sous-ensemble d'un ensemble de cardinal p, donc l'hypothèse de récurrence nous assure que $|F| \leqslant p$. En particulier, $|F| < p+1 = |E|$. Et $\mathscr{P}(p+1)$ est démontrée.
- **Conclusion :** Par récurrence, $\mathscr{P}(p)$ est vraie pour tout entier p. □

Théorème 1.2.5
Un sous-ensemble de $\mathbb{N}$ *est fini si, et seulement si, il est majoré.*

Preuve : Soit $A \subset \mathbb{N}$ un ensemble majoré. D'après la **définition 1.1**, il existe n_0 tel que

$$\forall n \in A \qquad n \leqslant n_0$$

Autrement dit,

$$A \subset [\![0\,;n_0]\!]$$

D'après le **théorème 2.4**, A est fini car $[\![0\,;n_0]\!]$ l'est.

La réciproque se démontre par récurrence. Si p est un entier positif, on note $\mathscr{P}(p)$ la proposition : « Tout ensemble fini inclus dans $\mathbb{N}$, de cardinal p, est majoré. »

- $\mathscr{P}$**(1) est vraie :** On a déjà vu qu'un ensemble à un élément est un singleton, qui est clairement majoré.
- $\mathscr{P}(p) \Longrightarrow \mathscr{P}(p+1)$: Soit p strictement positif, tel que $\mathscr{P}(p)$ vraie. Soit E un ensemble fini de cardinal $p+1$. Alors E n'est pas vide et il admet un plus petit élément. L'ensemble $E \setminus \{a\}$ est de cardinal p, d'après le **lemme 2.3**. Par hypothèse de récurrence, $E \setminus \{a\}$ est majoré : il existe n_0 tel que

  $$\forall n \in E \setminus \{a\} \qquad n \leqslant n_0$$

  Or, a est le plus petit élément de E. Donc si $b \in E \setminus \{a\}$, on a

$$a \leqslant b \leqslant n_0$$

Au final, E est majoré par n_0. Donc $\mathscr{P}(p+1)$ est vraie.

- **Conclusion :** Par récurrence, $\mathscr{P}(p)$ est vraie pour tout entier $p \neq 0$.

Ce qui, bien sûr, achève la démonstration. □

Théorème 1.2.6
Soit E *une partie finie de* $\mathbb{N}$*, de cardinal* $p > 0$*. Il existe une unique bijection strictement croissante de* $[\![1\,;p]\!]$ *sur* E.

Preuve : Récurrence, encore... Pour tout entier $p > 0$, on note $\mathscr{P}(p)$ la proposition : « Si E est une partie de $\mathbb{N}$, de cardinal p, il existe une unique bijection strictement croissante de $[\![1\,;p]\!]$ sur E. »

- **$\mathscr{P}(1)$ est vraie :** Soit E un ensemble de cardinal 1. C'est un singleton : il existe un entier a tel que $E = \{a\}$. L'unique bijection de $[\![1\,;1]\!]$ sur E est l'application $1 \longmapsto a$. Elle est évidemment strictement croissante.
- **$\mathscr{P}(p) \Longrightarrow \mathscr{P}(p+1)$** : Soit p strictement positif, tel que $\mathscr{P}(p)$ soit vraie. Soit E une partie de $\mathbb{N}$ de cardinal $p+1$. Puisque E est fini, donc majoré, il admet un plus grand élément a d'après le **théorème 1.5**. L'ensemble $E \setminus \{a\}$ a pour cardinal p donc d'après $\mathscr{P}(p)$, il exist une unique bijection strictement croissante de $[\![1\,;p]\!]$ sur E, que l'on note b. On prolonge b à $[\![1\,;p+1]\!]$ en posant $b(p+1) = a$, ce qui fournit une bijection strictement croissante de $[\![1\,;p+1]\!]$ sur E. Reste à montrer l'unicité. Si f est une bijection strictement croissante de $[\![1\,;p+1]\!]$ sur E, $f(p+1)$ doit être supérieur à tout élément de E. Donc $f(p+1) = a = b(p+1)$. Par suite, la restriction de f à $[\![1\,;p]\!]$ est une bijection strictement croissante de $[\![1\,;p]\!]$ sur $E \setminus \{a\}$. Cette restriction doit donc être égale à b, d'après la définition même de b. Donc f coincide avec b à la fois sur $[\![1\,;p]\!]$ et en $p+1$. Ces deux applications sont égales.
- **Conclusion :** $\mathscr{P}(p)$ est vraie pour tout entier $p > 0$. □

Si E est un ensemble de cardinal $p > 0$, la donnée de cette bijection strictement croissante b de $[\![1\,;p]\!]$ sur E nous donne une *énumération* des éléments de E : c'est-à-dire qu'il y a un seul élément de E qu'on peut appeler le premier, un seul qu'on peut appeler le deuxième, etc. On dira que $b(1) < b(2) < \cdots < b(p)$ est une énumération des éléments de E.

1.3 Dénombrements

1.3.1 Unions et intersections d'ensembles finis

Proposition 1.3.1
Soient E *et* F *deux ensembles finis disjoints. Alors* $E \cup F$ *est fini et* $|E \cup F| = |E| + |F|$.

Preuve : Soient E et F deux ensembles finis, de cardinaux respectifs p et q. Il existe deux bijections $f : E \longrightarrow [\![1\,;p]\!]$ et $g_1 : F \longrightarrow [\![1\,;q]\!]$. Alors $g = p + g_1$ est une bijection de F sur $[\![p+1\,;p+q]\!]$. On pose

$$\forall n \in E \cup F \qquad h(n) = \begin{cases} f(n) \text{ si } n \in E \\ g(n) \text{ si } n \in F \end{cases}$$

Comme E et F sont disjoints, cette définition est bien posée. Et h est clairement une bijection de $E \cup F$ sur $[\![1\,;p+q]\!]$. Si on souhaite s'en convaincre, il suffit de composer h avec l'application

$$\begin{aligned}[[1\,;p+q]] &\longrightarrow \mathrm{E}\cup\mathrm{F}\\ n &\longmapsto \begin{cases} f^{-1}(n) \text{ si } 1\leqslant n\leqslant p\\ g^{-1}(n) \text{ si } p+1\leqslant n\leqslant p+q\end{cases}\end{aligned}$$

Donc $$|\mathrm{E}\cup\mathrm{F}| = |\mathrm{E}| + |\mathrm{F}|$$ □

Corollaire 1.3.2
Soient E *un ensemble fini et* $\mathrm{F}\subset\mathrm{E}$. *Alors* $|\mathrm{E}\setminus\mathrm{F}| = |\mathrm{E}| - |\mathrm{F}|$.

Preuve : L'ensemble $\mathrm{E}\setminus\mathrm{F}$ est inclus dans E fini, donc est lui-même fini d'après le **théorème 2.4**. De plus, F et $\mathrm{E}\setminus\mathrm{F}$ sont disjoints donc d'après la **proposition 3.1**,

$$|\mathrm{F}| + |\mathrm{E}\setminus\mathrm{F}| = |\mathrm{F}\cup(\mathrm{E}\setminus\mathrm{F})| = |\mathrm{E}|$$

Par suite, $$|\mathrm{E}\setminus\mathrm{F}| = |\mathrm{E}| - |\mathrm{F}|$$ □

Corollaire 1.3.3
Soient A *et* B *deux ensembles finis, inclus dans un même ensemble* E. *Alors* $\mathrm{A}\cup\mathrm{B}$ *est fini et*

$$|\mathrm{A}\cup\mathrm{B}| = |\mathrm{A}| + |\mathrm{B}| - |\mathrm{A}\cap\mathrm{B}|$$

Preuve : Les ensembles $\mathrm{A}\setminus(\mathrm{A}\cap\mathrm{B})$ et B sont disjoints deux-à-deux. En effet, si x appartient à la fois à $\mathrm{A}\setminus(\mathrm{A}\cap\mathrm{B})$ et B, il est alors à la fois dans A et B, donc dans $\mathrm{A}\cap\mathrm{B}$. Ce qui est contradictoire. Donc $(\mathrm{A}\setminus(\mathrm{A}\cap\mathrm{B}))\cap\mathrm{B} = \emptyset$, comme annoncé.

Ces trois ensembles sont également finis, dans la mesure où ils sont tous inclus dans des ensembles finis d'après le **théorème 2.4**. D'après le **corollaire 3.2**,

$$|\mathrm{A}\setminus(\mathrm{A}\cap\mathrm{B})| = |\mathrm{A}| - |\mathrm{A}\cap\mathrm{B}|$$

On a aussi
$$\begin{aligned}\mathrm{B}\cup\big(\mathrm{A}\setminus(\mathrm{A}\cap\mathrm{B})\big) &= \mathrm{B}\cup\big(\mathrm{A}\cap(\mathrm{A}\cap\mathrm{B})^c\big) = \mathrm{B}\cup\big(\mathrm{A}\cap(\mathrm{A}^c\cup\mathrm{B}^c)\big)\\ &= \mathrm{B}\cup\big(\underbrace{(\mathrm{A}\cap\mathrm{A}^c)}_{=\emptyset}\cup(\mathrm{A}\cap\mathrm{B}^c)\big) = \mathrm{B}\cup(\mathrm{A}\cap\mathrm{B}^c)\\ &= (\mathrm{B}\cup\mathrm{A})\cap\underbrace{(\mathrm{B}\cup\mathrm{B}^c)}_{=\mathrm{E}}\\ \mathrm{B}\cup\big(\mathrm{A}\setminus(\mathrm{A}\cap\mathrm{B})\big) &= \mathrm{A}\cup\mathrm{B}\end{aligned}$$

D'après le **corollaire 3.2**,

$$|\mathrm{A}\cup\mathrm{B}| = |\mathrm{B}| + |\mathrm{A}\setminus(\mathrm{A}\cap\mathrm{B})| = |\mathrm{B}| + |\mathrm{A}| - |\mathrm{A}\cap\mathrm{B}|$$ □

1.3.2 Produits cartésiens d'ensembles finis

Proposition 1.3.4
Soient A *et* B *deux ensembles finis. Leur produit cartésien* $\mathrm{A}\times\mathrm{B}$ *est fini, de cardinal* $|\mathrm{A}|\times|\mathrm{B}|$.

Preuve : Notons p et q les cardinaux respectifs de A et B. On sait qu'il existe une bijection f de $[[1\,;p]]$ sur A et on a donc

$$\mathrm{A} = \{f(1),\dots,f(p)\}$$

et on pose $$\forall i\in[[1\,;p]] \qquad \mathrm{A}_i = \big\{f(i)\big\}\times\mathrm{B} = \big\{(f(i),b)\mid b\in\mathrm{B}\big\}$$

Pour chaque i compris entre 1 et p, l'ensemble A_i est en bijection avec B. En effet, on peut poser

$$\forall b \in B \qquad \sigma_i(b) = \big(f(i), b\big) \in A_i$$

et σ_i est clairement bijective. Comme B est lui-même en bijection avec $[\![1\,;q]\!]$, on en déduit que A_i est fini, de cardinal q.

Montrons maintenant que les ensembles $(A_i)_{1\leqslant i\leqslant p}$ sont disjoints deux-à-deux. Soient i et j, compris entre 1 et p, tels que $A_i \cap A_j$ ne soit pas vide. Il existe donc un élément dans cet intersection ; il s'écrit sous la forme $(f(i), b_i)$ et $(f(j), b_j)$ avec b_i et b_j dans B. Comme deux couples sont égaux si et seulement si leurs coordonnées sont égales, on en déduit que $f(i) = f(j)$. Or, f est injective donc $i = j$. Par contre-apposée, si $i \neq j$, l'intersection $A_i \cap A_j$ est vide.

Enfin, montrons que la réunion des $(A_i)_{1\leqslant i\leqslant p}$ est égale à $A \times B$. Soit (a,b) dans cet ensemble. Comme f est surjective, il existe $i \in [\![1\,;p]\!]$, tel que $a = f(i)$. Donc

$$(a,b) = \big(f(i), b\big) \in A_i$$

L'ensemble $A \times B$ est donc la réunion disjointe des ensembles $(A_i)_{1\leqslant i\leqslant p}$. Par suite,

$$|A \times B| = \sum_{i=1}^{p} |A_i| = \sum_{i=1}^{p} q = pq = |A| \times |B| \qquad \square$$

Corollaire 1.3.5
Soit A *un ensemble fini, soit p un entier non nul. L'ensemble* A^p *est fini, de cardinal* $|A|^p$.

Preuve : Récurrence immédiate. $\square$

1.3.3 Applications entre ensembles finis

Théorème 1.3.6
Soient E *et* F *deux ensembles finis. Soit* f *une application de* E *dans* F. *On a* $|f(E)| \leqslant |E|$.

Preuve : L'ensembles $f(E)$ est fini d'après le **théorème 2.4**, puisqu'inclus dans F. Chaque y de $f(E)$ admet des antécédents. On en choisit un, qu'on note $\sigma(y)$. Montrons que σ est une bijection de $f(E)$ sur $\sigma(f(E))$.

La surjectivité est claire, puisque $\sigma(f(E))$ est l'ensemble des éléments de E atteints par σ : ils sont bien tous atteints.

Pour l'injectivité, supposons que y_1 et y_2 sont dans $f(E)$, tels que $\sigma(y_1) = \sigma(y_2)$. Par définition de σ, on a alors

$$y_1 = f(\sigma(y_1)) = f(\sigma(y_2)) = y_2$$

donc σ est injective.

Deux ensembles en bijection ont même cardinal. Il ne reste plus qu'à appliquer le **théorème 2.4** pour avoir

$$|f(E)| = \big|\sigma(f(E))\big| \leqslant |E| \qquad \square$$

Théorème 1.3.7
Soient E *et* F *deux ensembles finis et* f *une application de* E *dans* F. *Elle est injective si et seulement si* $|f(E)| = |E|$.

Preuve : f est surjective sur $f(\mathrm{E})$, puisque les éléments de cet ensemble sont précisément ceux atteints par f. Si on suppose de plus que f est injective, elle réalise une bijection de E sur $f(\mathrm{E})$. Ces deux ensembles ont donc même cardinal.

Réciproquement, si f n'est pas injective, il existe a et a' dans E, distincts, tels que $f(a) = f(a')$. La restriction de f à $\mathrm{E} \setminus \{a'\}$ atteint tous les éléments de $f(\mathrm{E})$ donc son image est $f(\mathrm{E})$. D'après le **théorème 3.6** et le **lemme 2.3**,

$$|f(\mathrm{E})| \leqslant |\mathrm{E} \setminus \{a'\}| = |\mathrm{E}| - 1 < \mathrm{E}$$

A fortiori, $|f(\mathrm{E})| \neq |\mathrm{E}|$. □

Corollaire 1.3.8
Soient E *et* F *deux ensembles finis de même cardinal. Soit* f *une application de* E *dans* F. *Les assertions suivantes sont équivalentes :*

1. f *est injective.*
2. f *est surjective.*
3. f *est bijective.*

Preuve : Supposons la première proposition vraie : f est injective. D'après le **théorème 3.7**, $|f(\mathrm{E})| = |\mathrm{E}|$. Mais comme E et F ont même cardinal, $|\mathrm{E}| = |\mathrm{F}|$. Il s'ensuit que $|f(\mathrm{E})| = |\mathrm{F}|$. Le **théorème 2.4** nous assure alors que $f(\mathrm{E}) = \mathrm{F}$: f est surjective et on a montré

$$1 \implies 2$$

Supposons maintenant f surjective, ce qui est équivalent à dire que $\mathrm{F} = f(\mathrm{E})$. Puisque F et E ont même cardinal, on a $|f(\mathrm{E})| = |\mathrm{E}|$. D'après le **théorème 3.7**, f est injective. Elle est donc aussi bijective. On a ainsi montré

$$2 \implies 3$$

Bien entendu, la troisième proposition implique la première, par définition de la bijectivité. Ce qui achève la démonstration. □

Théorème 1.3.9
Soient E *et* F *deux ensembles finis. L'ensemble des applications de* E *dans* F *est fini, de cardinal* $|\mathrm{F}|^{|\mathrm{E}|}$.

Preuve : On note p le cardinal de E et q le cardinal de F. On sait qu'on peut énumérer les éléments de E :

$$\mathrm{E} = \{x_1, \ldots, x_p\}$$

Posons
$$\begin{aligned} b : \ \mathrm{F}^{\mathrm{E}} &\longrightarrow \mathrm{F}^p \\ f &\longmapsto \big(f(x_1), \ldots, f(x_p)\big) \end{aligned}$$

et montrons que b est une bijection.

On commence par l'injectivité. Soient f et g deux applications de E dans F, telles que $b(f)$ et $b(g)$ sont égaux. Par définition de b,

$$\big(f(x_1), \ldots, f(x_p)\big) = \big(g(x_1), \ldots, g(x_p)\big)$$

Deux q-uplets sont égaux s'ils ont les mêmes coordonnées donc

$$\forall i \in [\![1 ; p]\!] \qquad f(x_i) = g(x_i)$$

Autrement dit, f et g coincident sur E et sont donc égales.

Montrons maintenant que b est surjective. Soit $(y_1,\dots,y_p)$ un élément quelconque de F^p. On définit l'application suivante :

$$\forall i \in [\![1\,;p]\!] \qquad f(x_i) = y_i$$

Il est clair que $b(f) = (y_1,\dots,y_p)$ donc b est surjective.

Les ensembles F^{E} et F^p sont donc en bijection ; d'une part F^{E} est donc fini, et d'autre part, $|\mathrm{F}^{\mathrm{E}}| = |\mathrm{F}^p|$. Ne reste plus qu'à appliquer le **corollaire 3.5**. □

Corollaire 1.3.10
Soit E *un ensemble fini.* $\mathscr{P}(\mathrm{E})$ *est fini, de cardinal* $2^{|\mathrm{E}|}$.

Preuve : L'ensemble $\{0,1\}^{\mathrm{E}}$ des applications de E dans $\{0,1\}$ a pour cardinal $2^{|\mathrm{E}|}$ d'après le **théorème 3.9**. Il suffit donc de montrer qu'il est en bijection avec $\mathscr{P}(\mathrm{E})$.

Si f est une application de E dans $\{0,1\}$, on pose

$$\mathrm{A}(f) = f^{-1}(1) = \{x \in \mathrm{E} \mid f(x) = 1\} \subset \mathrm{E}$$

Cette relation définit une application $\mathrm{A} : \{0,1\}^{\mathrm{E}} \longrightarrow \mathscr{P}(\mathrm{E})$. Montrons qu'elle est bijective.

Commençons par l'injectivité. Soient f et g deux applications de E dans $\{0,1\}$ distinctes. Ceci signifie qu'elles ne prennent pas la même valeur en au moins un point : il existe $x_0 \in \mathrm{E}$ tel que que $f(x_0) \neq g(x_0)$. L'un de ces deux nombres vaut 1, l'autre 0 ; disons par exemple que

$$f(x_0) = 1 \qquad \text{et} \qquad g(x_0) = 0$$

Ceci signifie que $x_0 \in \mathrm{A}(f)$ mais $x_0 \notin \mathrm{A}(g)$

Donc $\mathrm{A}(f)$ et $\mathrm{A}(g)$ sont distincts. L'application A est bien injective.

Pour la surjectivité, donnons-nous $\mathrm{F} \subset \mathrm{E}$. On pose

$$\forall x \in \mathrm{E} \qquad f(x) = \begin{cases} 1 \text{ si } x \in \mathrm{F} \\ 0 \text{ sinon} \end{cases}$$

Alors, par définition, $\mathrm{A}(f) = \mathrm{F}$ et on a fini. □

Théorème 1.3.11
Soient E *et* F *deux ensembles finis, de cardinaux respectifs p et n. L'ensemble* $\mathscr{I}(\mathrm{E},\mathrm{F})$ *des injections de* E *dans* F *est fini, de cardinal* $\prod_{k=0}^{p-1}(n-k)$. *Ce nombre est noté* A_n^p, *et est appelé nombre d'arrangements de p objets parmi n.*

Preuve : Pour tous ensembles finis E et F, l'ensemble $\mathscr{I}(\mathrm{E},\mathrm{F})$ est inclus dans l'ensemble fini F^{E} (**théorème 3.9**) donc il est lui-même fini.

On définit, pour tout entier p non nul, la propriété $\mathscr{P}(p)$: « Pour tout entier n non nul, si E est un ensemble de cardinal p et F est un ensemble de cardinal n, l'ensemble $\mathscr{I}(\mathrm{E},\mathrm{F})$ a pour cardinal $\prod_{i=0}^{p-1}(n-i)$. »

- **$\mathscr{P}(1)$ est vraie** : En effet, dans le cas où E n'a qu'un seul élément, toute application de E dans F est injective donc $\mathscr{I}(\mathrm{E},\mathrm{F}) = \mathrm{F}^{\mathrm{E}}$. D'après le **théorème 3.9**, cet ensemble est de cardinal $n^1 = \prod_{i=0}^{0}(n-i)$.

- $\mathscr{P}(p) \Longrightarrow \mathscr{P}(p+1)$: Soit p un entier strictement positif. On suppose que l'ensemble des injections d'un ensemble (quelconque) à p éléments dans un ensemble (quelconque) à n éléments est de cardinal $\prod_{i=0}^{p-1}(n-i)$.
  Soient E un ensemble fini de cardinal $p+1$ et F un ensemble fini de cardinal n. On énumère les éléments de F :

  $$\mathrm{F} = \{x_1, \ldots, x_n\}$$

  et on se donne un élément a E. Comme $p+1 \geqslant 2$, l'ensemble $\mathrm{E} \setminus \{a\}$ n'est pas vide, et est fini de cardinal p. On définit

  $$\forall k \in [\![1\,;n]\!] \qquad \mathscr{I}(k) = \{f \in \mathscr{I}(\mathrm{E},\mathrm{F}) \mid f(a) = x_k\}$$

  Les ensembles $\big(\mathscr{I}(k)\big)_{1\leqslant k\leqslant n}$ sont clairement disjoints car une application ne peut prendre qu'une seule valeur en a. Et leur réunion est $\mathscr{I}(\mathrm{E},\mathrm{F})$ tout entier car toute injection de E dans F doit prendre une valeur en a.
  On calcule maintenant le cardinal de $\mathscr{I}(k)$, pour k fixé entre 1 et n. C'est simple : les restrictions à $\mathrm{E} \setminus \{a\}$ de fonctions dans $\mathscr{I}(k)$ sont précisément les injections de $\mathrm{E} \setminus \{a\}$ dans $\mathrm{F} \setminus \{x_k\}$. D'après $\mathscr{P}(p)$,

  $$\big|\mathscr{I}(k)\big| = \prod_{i=0}^{p-1}(n-1-i) = \prod_{i=0}^{p-1}\big(n-(i+1)\big) = \prod_{i=1}^{p}(n-i)$$

  Enfin, on a dit que $\mathscr{I}(\mathrm{E},\mathrm{F})$ est la réunion disjointe de tous les $\mathscr{I}(k)$ donc

  $$\big|\mathscr{I}(\mathrm{E},\mathrm{F})\big| = \sum_{k=1}^{n}\big|\mathscr{I}(k)\big| = n \times \prod_{i=1}^{p}(n-i) = \prod_{i=0}^{p}(n-i)$$

  ce qui achève de démontrer $\mathscr{P}(p+1)$.
- **Conclusion :** La propriété $\mathscr{P}(p)$ est vraie pour tout entier p non nul. □

Définition 1.3.12
Soit E un ensemble non vide. Une bijection de E est appelée *permutation de* E. L'ensemble des permutations de E est noté $\mathfrak{S}_\mathrm{E}$ ou $\mathfrak{S}(\mathrm{E})$.

Corollaire 1.3.13
Soit E *un ensemble fini, de cardinal* $n > 0$. *L'ensemble* $\mathfrak{S}(\mathrm{E})$ *est fini, de cardinal* $\prod_{i=1}^{n} i$. *Ce nombre est appelé factorielle de* n, *et on le note* $n!$. *Par convention, on pose* $0! = 1$.

Preuve : L'ensemble $\mathfrak{S}(\mathrm{E})$ est égal à $\mathscr{I}(\mathrm{E},\mathrm{E})$, d'après le **corollaire 3.8**. Et le **théorème 3.11** nous donne le cardinal de cet ensemble, qui est précisément $n!$. □

Théorème 1.3.14
Soit E *un ensemble fini, de cardinal* $n > 0$. *Soit* $p \in [\![0\,;n]\!]$. *L'ensemble des parties de* E *à* p *éléments est fini, de cardinal* $\mathrm{A}_n^p / p!$. *Ce nombre est appelé nombre de combinaisons de* p *objets parmi* p *et on le note* C_n^p *ou* $\binom{n}{p}$. *Ce dernier symbole se lit « p parmi n ».*

Par convention, si $p > n$, *on pose* $\binom{n}{p} = 0$.

Preuve : On se donne un ensemble fini E de cardinal $n > 0$, et $p \in [\![1\,;n]\!]$. On note $\mathscr{P}_p(\mathrm{E})$ l'ensemble des parties de E de cardinal p. Bien entendu, $\mathscr{P}_p(\mathrm{E})$ est fini, puisqu'inclus dans $\mathscr{P}(\mathrm{E})$ qui est lui-même fini.

Chaque A dans $\mathscr{P}_p(\mathrm{E})$ a pour cardinal p ; il existe donc une bijection x_A de $[\![1\,;p]\!]$ sur A. Si σ est une permutation de $[\![1\,;p]\!]$, $x_\mathrm{A}\circ\sigma$ est une bijection de $[\![1\,;p]\!]$ dans A, donc en particulier une injection de $[\![1\,;p]\!]$ dans E. On définit alors

$$\begin{aligned}\mathrm{F}:\ \mathfrak{S}_p\times\mathscr{P}_p(\mathrm{E}) &\longrightarrow \mathscr{I}([\![1\,;p]\!],\mathrm{E})\\ (\sigma,\mathrm{A}) &\longmapsto x_\mathrm{A}\circ\sigma\end{aligned}$$

On montre que F est bijective, de sorte que les ensembles $\mathfrak{S}_p\times\mathscr{P}_p(\mathrm{E})$ et $\mathscr{I}([\![1\,;p]\!],\mathrm{E})$ ont même cardinal. Il suffit d'appliquer les résultats précédents pour obtenir

$$p!\,|\mathscr{P}_p(\mathrm{E})| = |\mathfrak{S}_p\times\mathscr{P}_p(\mathrm{E})| = |\mathscr{I}([\![1\,;p]\!],\mathrm{E})| = \mathrm{A}_n^p$$

et
$$|\mathscr{P}_p(\mathrm{E})| = \mathrm{A}_n^p/p!$$

Voilà pour le plan de bataille. Commençons par établir l'injectivité de F. Soient σ, σ' deux permutations de $[\![1\,;p]\!]$ et A, A′ deux sous-ensembles de E de cardinal p, tels que $\mathrm{F}(\sigma,\mathrm{A}) = \mathrm{F}(\sigma,\mathrm{A}')$. Cela signifie que

$$x_\mathrm{A}\circ\sigma = x_{\mathrm{A}'}\circ\sigma'$$

En particulier, ces deux applications ont la même image. Mais

$$x_\mathrm{A}\circ\sigma([\![1\,;p]\!]) = x_\mathrm{A}\big(\sigma([\![1\,;p]\!])\big) = x_\mathrm{A}([\![1\,;p]\!]) = \mathrm{A}$$

De même
$$x_{\mathrm{A}'}\circ\sigma'([\![1\,;p]\!]) = \mathrm{A}'$$

Il s'ensuit que
$$\mathrm{A} = \mathrm{A}' \qquad \text{d'où} \qquad x_\mathrm{A} = x_{\mathrm{A}'}$$

Puis
$$x_\mathrm{A}\circ\sigma = x_\mathrm{A}\circ\sigma'$$

Mais x_A est une bijection, donc on peut composer à gauche par x_A^{-1} et il vient $\sigma = \sigma'$. L'injectivité est établie.

Montrons maintenant que F est surjective. Soit f une injection de $[\![1\,;p]\!]$ dans E. D'après le **théorème 3.7**, l'ensemble $\mathrm{A} = f([\![1\,;p]\!])$ est de cardinal p, donc appartient à $\mathscr{P}_p(\mathrm{E})$. On pose

$$\sigma = x_\mathrm{A}^{-1}\circ f$$

σ est la composée de deux injections, donc est injective. Mais son ensemble de départ et d'arrivée sont tous deux $[\![1\,;p]\!]$; le **théorème 3.8** garantit alors la bijectivité de σ. Donc σ appartient à $\mathfrak{S}_p$. Par construction,

$$\mathrm{F}(\sigma,\mathrm{A}) = x_\mathrm{A}\circ\sigma = x_\mathrm{A}\circ x_\mathrm{A}^{-1}\circ f = f$$

et F est surjective. □

Proposition 1.3.15
Soient n et p deux entiers. On a

$$\binom{n}{p} = \binom{n}{n-p}$$

Preuve : D'après le **théorème 3.14**, on a

$$\binom{n}{p} = \frac{A_n^p}{p!} = \frac{n!}{(n-p)!\,p!} = \frac{A_n^{n-p}}{(n-p)!} = \binom{n}{n-p}$$ □

Proposition 1.3.16
Soient n et p deux entiers. On a

$$\binom{n}{p} + \binom{n}{p+1} = \binom{n+1}{p+1}$$

Preuve : On a

$$\begin{aligned}\binom{n}{p} + \binom{n}{p+1} &= \frac{n!}{p!\,(n-p)!} + \frac{n!}{(p+1)!\,(n-p-1)!} \\ &= \frac{n!}{p!\,(n-p-1)!}\left(\frac{1}{n-p} + \frac{1}{p+1}\right) \\ &= \frac{n!}{p!\,(n-p-1)!} \times \frac{n+1}{(p+1)(n-p)} \\ &= \frac{(n+1)!}{(p+1)!\,(n-p)!}\end{aligned}$$

$$\binom{n}{p} + \binom{n}{p+1} = \binom{n+1}{p+1}$$

Ce qui achève la démonstration. □

Chapitre 2

Structures Algébriques Construction de $\mathbb{Z}$ et $\mathbb{Q}$

De nombreux ensembles rencontrés en mathématiques ont des propriétés élémentaires communes : par exemple, dans les ensembles de nombres, on peut additionner et multiplier ; certaines fonctions peuvent être ajoutées, multipliées, composées ; etc. On souhaite donc, dans ce chapitre, présenter du vocabulaire permettant de décrire les propriétés élémentaires d'ensembles, lorsque ceux-ci sont munis d'opérations.

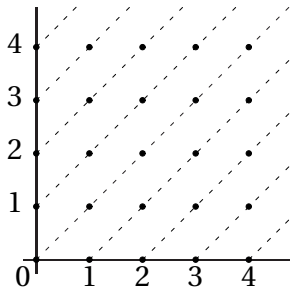
On en profite également pour illustrer l'utilité des relations d'équivalences pour créer de nouveaux ensembles. En l'occurence, $\mathbb{Z}$ et $\mathbb{Q}$; on expliquera alors quelles structures algébriques ces ensembles possèdent.

2.1 Les entiers relatifs

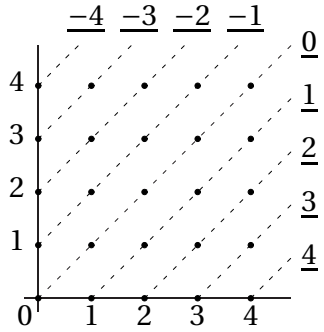
L'ensemble $\mathbb{N}$ étudié dans le chapitre précédent possède un inconvénient : on peut ajouter deux de ses éléments, mais on ne peut pas tous les soustraire les uns aux autres. Par exemple, $4-3$ est une opération qu'on peut effectuer dans $\mathbb{N}$ alors que $3-5$ ne veut rien dire.

En général, si m et n sont deux entiers, l'opération $m-n$ n'a de sens dans $\mathbb{N}$ que si $m \geqslant n$. On souhaite donc créer un ensemble $\mathbb{Z}$, contenant $\mathbb{N}$, dans lequel on peut toujours effectuer l'opération $m-n$ entre deux entiers m et n, même si $m \leqslant n$.

L'ensemble $\mathbb{N}^2$ peut être partitionné en la réunion disjointe des « droites » de pente 1 :



Notre idée, pour « créer » les nombres négatifs est la suivante. L'ensemble de toutes ces droites est appelé $\mathbb{Z}$. La diagonale sera appelée $\underline{0}$; celle immédiatement à droite, partant de $(1,0)$ sera appelée $\underline{1}$; la suivante $\underline{2}$; etc. Celle qui part de $(0,1)$ est appelée $\underline{-1}$; celle immédiatement à gauche, $\underline{-2}$; et ainsi de suite.



Jusqu'à présent, pas de difficulté : il s'agit simplement de donner un nom à des objets. Ce qu'il nous faut vérifier, c'est qu'on peut aussi créer des opérations, notées $\oplus$ et $\otimes$ sur $\mathbb{Z}$, possédant les propriétés usuelles, et telles que la structure additive et multiplicative de $\mathbb{N}$ soit conservée. C'est-à-dire que l'on souhaite que

$$\underline{n} \oplus \underline{m} = \underline{n+m} \qquad \text{et} \qquad \underline{m} \otimes \underline{n} = \underline{n \times m}$$

2.1.1 Construction de $\mathbb{Z}$

On définit $\forall (m,n),(m',n') \in \mathbb{N}^2 \qquad (m,n) \sim (m',n') \iff m'+n = m+n'$

Proposition 2.1.1
$\sim$ est une relation d'équivalence sur $\mathbb{N}^2$.

Preuve : Il s'agit de vérifier que $\sim$ satisfait aux trois propriétés caractérisant une relation d'équivalence.

D'abord, si $(m,n) \in \mathbb{N}^2$, on a $m+n = m+n$ ce qui établit que $(m,n) \sim (m,n)$: $\sim$ est réflexive.

Ensuite, si $(m,n) \sim (m',n')$, on sait que $m'+n = m+n'$. Dans la mesure où l'égalité est une relation symétrique, on a $m+n' = m'+n$. Ceci équivaut à dire que $(m',n') \sim (m,n)$: $\sim$ est symétrique.

Enfin, supposons que $(m,n) \sim (m',n')$ et que $(m',n') \sim (m'',n'')$. Par définition,

$$m'+n = m+n' \qquad \text{et} \qquad m''+n' = m'+n''$$

En ajoutant ces deux égalités membre-à-membre, il vient

$$m'+n+m''+n' = m+n'+m'+n''$$

ou encore $$(m'+n')+(m''+n) = (m'+n')+(m+n'')$$

Les deux membres sont supérieurs à $m'+n'$, donc on a le droit de leur soustraire $m'+n'$, pour obtenir

$$m''+n = m+n''$$

Autrement dit, $(m,n) \sim (m'',n'')$: $\sim$ est transitive. □

Définition 2.1.2
L'ensemble quotient $\mathbb{N}^2/\sim$ est appelé *ensemble des entiers relatifs* et noté $\mathbb{Z}$. Si $(m,n) \in \mathbb{N}^2$, sa classe d'équivalence sera notée $\overline{(m,n)}$. Enfin, pour tout entier n, on notera

$$\underline{n} = \overline{(n,0)}$$

Proposition 2.1.3
L'application $\iota : \begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & \underline{n} \end{array}$ *est injective.*

Preuve : Soient m et n deux entiers tels que $\underline{n} = \underline{m}$. Par définition,

$$\overline{(n,0)} = \overline{(m,0)}$$

ce qui équivaut à dire que

$$m+0 = n+0$$

Donc $m = n$ et ι est bien injective. □

On a $\iota(\mathbb{N}) \subset \mathbb{Z}$ et l'injectivité de ι assure que les $(\iota(n))_{n\in\mathbb{N}}$ sont bien distincts deux-à-deux dans $\mathbb{Z}$. Donc on peut considérer (et c'est un abus de notation) que $\mathbb{N} \subset \mathbb{Z}$, puisque les images des éléments de $\mathbb{N}$ par ι sont « bien séparés » dans $\mathbb{Z}$. De fait, par la suite, on considérera que n et $\underline{n}$ sont le même objet si $n \in \mathbb{N}$.

On souhaite maintenant définir une addition $\oplus$ et une multiplication $\otimes$ dans notre nouvel ensemble $\mathbb{Z}$. Et ces opérations doivent prolonger les opérations dans $\mathbb{N}$: il faut que

$$\forall m,n \in \mathbb{N} \qquad \underline{n} \oplus \underline{m} = \underline{m+n} \qquad \text{et} \qquad \underline{n} \oplus \underline{m} = \underline{m \times n}$$

On va définir $\oplus$ et $\otimes$ pour qu'elles fassent juste cela. Donnons-nous deux entiers naturels m et n, ainsi que des couples (a,b) et (c,d) dans $\mathbb{N}^2$, tels que

$$\underline{m} \sim (a,b) \qquad \text{et} \qquad \underline{n} \sim (c,d)$$

c'est-à-dire que $\qquad m+b = a \qquad \text{et} \qquad n+d = c$

Comme m et n sont entiers, on sait que $a \geqslant b$ et $c \geqslant d$ donc on a le droit de calculer $a-b$ et $c-d$ dans $\mathbb{N}$. Par suite,

$$m = a-b \qquad \text{et} \qquad n = c-d$$

de sorte que $\qquad m+n = a+c-(b+d) \qquad \text{et} \qquad mn = ac+bd-ad-bc$

puis $\qquad (m+n)+(b+d) = a+c \qquad \text{et} \qquad mn+(ad+bc) = ac+bd$

c'est-à-dire $\qquad (m+n,0) \sim (a+c,b+d) \qquad \text{et} \qquad (mn,0) \sim (ac+bd,ad+bc)$

De manière équivalente, $\qquad \underline{m+n} = \overline{(a+c,b+d)} \qquad \text{et} \qquad \underline{m \times n} = \overline{(ac+bd,ad+bc)}$

Il apparaît donc que la seule manière naturelle de définir la somme et le produit de $\overline{(a,b)}$ par $\overline{(b,c)}$ est la suivante :

$$\overline{(a,b)} \oplus \overline{(b,c)} = \overline{(a+c,b+d)}$$

et $\qquad \overline{(a,b)} \otimes \overline{(b,c)} = \overline{(ac+bd,ad+bc)}$

Mais il faut vérifier que la définition est bien posée : est-il bien certain que, si $\overline{(a,b)} = \overline{(a',b')}$ et $\overline{(c,d)} = \overline{(c',d')}$, alors

$$\overline{(a+c,b+d)} \stackrel{?}{=} \overline{(a'+c',b'+d')}$$

et
$$\overline{(ac+bd,ad+bc)} \stackrel{?}{=} \overline{(a'c'+b'd',a'd'+b'c')}$$

Le lemme suivant répond à cette question :

Lemme 2.1.4
Soient (a,b), (c,d), (a',b') et (c',d') dans $\mathbb{N}^2$, tels que

$$(a,b) \sim (a',b') \qquad et \qquad (c,d) \sim (c',d')$$

Alors $\quad (a+c,b+d) \sim (a'+b',c'+d') \quad$ *et* $\quad (ac+bd,ad+bc) \sim (a'c'+b'd',a'd'+b'c')$

Preuve : On sait que $\quad a'+b = a+b' \quad$ et $\quad c'+d = c+d'$

En ajoutant membre-à-membre ces deux relations, il vient

$$(a'+c')+(b+d) = (a+c)+(b'+d')$$

d'où
$$(a+c,b+d) \sim (a'+c',b'+d')$$

Cette partie était facile. Pour le produit, cela se corse si l'on s'y prend mal. Commençons par partir de $a'+b = a+b'$, qu'on multiplie par c pour obtenir

$$bc+a'c = ac+b'c \tag{1}$$

Puis on multiplie $a+b' = a'+b$ par d :

$$ad+b'd = bd+a'd \tag{2}$$

Ensuite, on multiplie $c'+d = c+d'$ par a' :

$$a'c'+a'd = a'd'+ca' \tag{3}$$

Enfin, on multiplie $c+d' = c'+d$ par b' :

$$b'd'+b'c = b'c'+b'd \tag{4}$$

Et on ajoute membre-à-membre les relations (**1**),..., (**4**) :

$$(ad+bc+a'c'+b'd')+(a'c+b'd+a'd+b'c) = (a'd'+b'c'+ac+bd)+(a'c+b'd+a'd+b'c)$$

On constate que le même terme $a'c+b'd+a'd+b'c$ est présent dans les deux membres de cette égalité, ce qui permet de le simplifier d'où

$$(a'c'+b'd')+(ad+bc) = (ac+bd)+(a'd'+b'c')$$

ce qui signifie exactement que

$$(ac+bd,ad+bc) \sim (a'c'+b'd',a'd'+b'c') \qquad \square$$

Corollaire 2.1.5
Il existe deux applications $\oplus$ et $\otimes$, de $\mathbb{Z}^2$ dans $\mathbb{Z}$, vérifiant

$$\forall (a,b),(c,d) \in \mathbb{N}^2 \qquad \overline{(a,b)} \oplus \overline{(c,d)} = \overline{(a+c,b+d)}$$

et $\qquad \forall (a,b),(c,d) \in \mathbb{N}^2 \qquad \overline{(a,b)} \otimes \overline{(c,d)} = \overline{(ac+bd,ad+bc)}$

2.1.2 Structure de groupe additif de $\mathbb{Z}$

Nous allons étudier les propriétés des deux opérations $\oplus$ et $\otimes$ définies sur $\mathbb{Z}$ au paragraphe précédent. Mais avant cela, on présente du vocabulaire général sur les opérations dans un ensembles.

Définition 2.1.6 (Loi de composition interne)
Soit E un ensemble. On appelle *loi de composition interne sur* E toute application $\star : \mathrm{E} \times \mathrm{E} \longrightarrow \mathrm{E}$. En général, au lieu de noter $\star(x, y)$, on écrira $x \star y$.

Le paragraphe précédent montre que $\oplus$ et $\otimes$ sont des lois de composition internes sur $\mathbb{Z}$.

Définition 2.1.7 (Associativité, commutativité, élément neutre)
Soit $(\mathrm{E}, \star)$ un ensemble muni d'un loi de composition interne. On dira que :

- $\star$ est *associative* si, et seulement si,
$$\forall x, y, z \in \mathrm{E} \qquad (x \star y) \star z = x \star (y \star z)$$
- $\star$ est *commutative* si, et seulement si,
$$\forall x, y \in \mathrm{E} \qquad x \star y = y \star x$$
- $\star$ *admet un élément neutre* si, et seulement si, il existe $e \in \mathrm{E}$ tel que
$$\forall x \in \mathrm{E} \qquad x \star e = e \star x = x$$

Proposition 2.1.8
Soit $(\mathrm{E}, \star)$ *un ensemble muni d'une loi de composition interne. S'il y a un élément neutre, celui-ci est unique.*

Preuve : En effet, soient e et e' deux éléments neutres dans E. Puisque e est neutre, on sait que $e \star e' = e'$; et comme e' est neutre, on a $e \star e' = e$. Par suite, $e = e'$. □

Puisque cet élément neutre, quand il existe, est unique, on lui donne un nom particulier. Généralement, 1_{E} ou tout simplement 1 ; quand en plus la loi $\star$ est commutative, il est de coutume de le noter plutôt 0_{E} ou 0.

Définition 2.1.9 (Inverses)
Soit $(\mathrm{E}, \star)$ un ensemble muni d'une loi de composition interne et admettant un élément neutre noté 1. Soit $x \in \mathrm{E}$. On dira que x *est inversible* si, et seulement si, il existe $y \in \mathrm{E}$ tel que $x \star y = y \star x = 1$. Un tel y est appelé *un inverse de* x.

Définition 2.1.10 (Groupes)
Soit $(\mathrm{E}, \star)$ un ensemble muni d'une loi de composition interne. On dira que E est un *groupe* si, et seulement si,

- $\star$ est associative ;
- E admet un élément neutre ;
- tout élément de E est inversible.

Proposition 2.1.11
Soit $(\mathrm{G}, \star)$ *un groupe. Si* $x \in \mathrm{G}$*, il admet un inverse et celui-ci est unique. On le note* x^{-1} *en général, mais si* G *est commutatif, on le note plutôt* $-x$.

Preuve : Soient y et y' deux inverses de x. Par définition,

$$x \star y = y \star x = 1 \qquad \text{et} \qquad x \star y' = y' \star x = 1$$

Puisque 1 est neutre, on a

$$y' = y' \star 1$$

Or,

$$1 = x \star y$$

donc

$$y' = y' \star 1 = y' \star (x \star y)$$

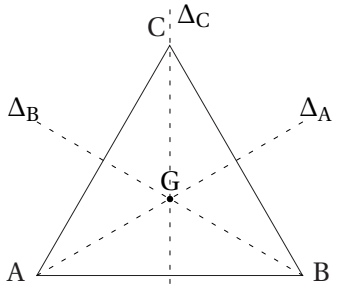
Comme $\star$ est associative,

$$y' = \underbrace{(y' \star x)}_{=1} \star y = 1 \star y = y$$

ce qui prouve que $y' = y$: x admet bien ununique inverse. □

Exemple 2.1.12
Un des exemples fondamentaux de groupes est $\mathbb{Z}$. Démontrer ce fait est l'objectif de ce chapitre et nous le laissons pour plus tard.

En attendant, considérons un autre ensemble qui apparaît en géométrie. Soit ABC un triangle équilatéral. On considère l'ensemble E des applications du plan dans lui-même, laissant ABC invariant. Ce dernier est représenté ci-dessous, ainsi que ses médianes et son centre de gravité G, qui seront utiles pour déterminer les éléments de E.



La loi de composition utilisée sera évidemment la composition des applications. Celle-ci est évidemment interne, puisque si f et g sont dans E, on a

$$f(\text{ABC}) = \text{ABC} \qquad \text{et} \qquad g(\text{ABC}) = \text{ABC}$$

donc

$$f \circ g(\text{ABC}) = f(g(\text{ABC})) = f(\text{ABC}) = \text{ABC}$$

de sorte que

$$\forall f, g \in \text{E} \qquad f \circ g \in \text{E}$$

En outre, on sait déjà que la composition est associative. On peut aussi énumérer les éléments de E. Il y a :

- L'identité, notée Id, qui est d'ailleurs neutre pour E.
- Les rotations r_+ et r_-, de centre G et d'angles respectivement $\frac{2\pi}{3}$ et $-\frac{2\pi}{3}$. Observons d'ailleurs que $r_+ \circ r_- = r_- \circ r_+ = \text{Id}$ donc ces deux éléments de E sont inversibles.
- Les symétries orthogonales s_A, s_B, s_C d'axes respectifs Δ_A, Δ_B, Δ_C. On remarque d'ailleurs que

  $$s_A \circ s_A = s_B \circ s_B = s_C \circ s_C = \text{Id}$$

  ce qui établit qu'elles sont toutes inversibles.

On peut enfin, pour connaître entièrement la structure de groupe de E, en dresser sa table de Pythagore. Il s'agit d'un tableau donnant tous les résultats de compositions entre éléments de E :

$\circ$	Id	r_+	r_-	s_A	s_B	s_C
Id	Id	r_+	r_-	s_A	s_B	s_C
r_+	r_+	r_-	Id	s_C	s_A	s_B
r_-	r_-	Id	r_+	s_B	s_C	s_A
s_A	s_A	s_B	s_C	Id	r_+	r_-
s_B	s_B	s_C	s_A	r_-	Id	r_+
s_C	s_C	s_A	s_B	r_+	r_-	Id

Cette table est construite de la manière suivante : à la ligne f et colonne g, on place le résultat de la composition $f \circ g$. E est un groupe à 6 éléments.

Théorème 2.1.13 (Calculs d'inverses dans un groupe)
Soit $(G, \star)$ *un groupe. Soient* x *et* y *deux éléments de* G. *Alors*

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

En particulier, si G *est commutatif,*

$$-(x+y) = -x - y = -y - x$$

Preuve : C'est une simple vérification, en utilisant l'associativité de $\star$:

$$(x \star y) \star (y^{-1} \star x^{-1}) = ((x \star y) \star y^{-1}) \star x^{-1} = (x \star (\underbrace{y \star y^{-1}}_{=1})) \star x^{-1} = x \star x^{-1} = 1$$

donc $x \star y$ admet bien $y^{-1} \star x^{-1}$ comme inverse. □

Théorème 2.1.14 (Structure de groupe de $\mathbb{Z}$)
$(\mathbb{Z}, \oplus)$ *est un groupe commutatif.*

Preuve : Par construction, la loi $\oplus$ est interne à $\mathbb{Z}$. Vérifions les autres propriétés caractérisant un groupe commutatif.

- **Commutativité** : Soient x et y dans $\mathbb{Z}$. Par définition de $\mathbb{Z} = \mathbb{N}^2/\sim$, il existe des entiers naturels a, b, c et d tels que

  $$x = \overline{(a,b)} \qquad \text{et} \qquad y = \overline{(c,d)}$$

  D'après le **Corollaire 1.5**,

  $$x \oplus y = \overline{(a,b)} \oplus \overline{(c,d)} = \overline{(a+c, b+d)}$$

  tandis que $$y \oplus x = \overline{(c,d)} \oplus \overline{(a,b)} = \overline{(c+a, d+b)}$$

  Mais l'addition « + » est l'addition dans $\mathbb{N}$; on sait qu'elle est commutative. Donc $x \oplus y = y \oplus x$.
- **Associativité** : Soient x, y et z trois éléments de $\mathbb{Z}$. Puisque $\mathbb{Z} = \mathbb{N}^2/\sim$, il existe des entiers naturels a, b, c, d, e et f tels que

  $$x = \overline{(a,b)} \qquad y = \overline{(c,d)} \qquad \text{et} \qquad z = \overline{(e,f)}$$

  D'après le **Corollaire 1.5**, on a

  $$y \oplus z = \overline{(c,d)} \oplus \overline{(e,f)} = \overline{(c+e, d+f)}$$

puis $$x \oplus (y \oplus z) = \overline{(a,b)} \oplus \overline{(c+e, d+f)} = \overline{(a+(c+e), b+(d+f))}$$

Rappelons que l'addition « + » est l'opération usuelle dans $\mathbb{N}$, dont on sait déjà qu'elle est associative. Donc

$$x \oplus (y \oplus z) = \overline{((a+c)+e, (b+d)+f)}$$

On utilise encore deux fois de suite le **Corollaire 1.5** :

$$x \oplus (y \oplus z) = \overline{(a+c, b+d)} \oplus \overline{(e,f)} = \left(\overline{(a,b)} \oplus \overline{(c,d)}\right) \oplus \overline{(e,f)} = (x \oplus y) \oplus z$$

- **Élément neutre** : Remarquons que $\underline{0}$ est neutre pour $\oplus$. En effet, soit $z \in \mathbb{Z}$; il existe des entiers naturels a et b tels que $z = \overline{(a,b)}$ et d'après le **corollaire 1.15**,

$$\underline{0} \oplus z = \overline{(0,0)} \oplus \overline{(a,b)} = \overline{(a+0, b+0)} = \overline{(a,b)} = z$$

De même, $$z \oplus \underline{0} = z$$

On peut aussi utiliser la commutativité de $\oplus$, déjà démontrée.

- **Existence d'inverses** : Soit $x = \overline{(a,b)} \in \mathbb{Z}$ et posons $x' = \overline{(b,a)}$. On a alors

$$x \oplus x' = \overline{(a,b)} \oplus \overline{(b,a)} = \overline{(b+a, a+b)} = \overline{(0,0)} = \underline{0}$$

puisque $$0 + (b+a) = (a+b) + 0$$

Donc x est inversible, d'inverse x'.

Ceci achève la démonstration. □

> Évidemment, une question naturelle est : « Comment a-t-on deviné quel est l'inverse de x ? » La réponse est simple : on l'a cherché d'abord au brouillon. Il s'agissait de trouver des entiers naturels c et d tels que
>
> $$\overline{(a,b)} \oplus \overline{(c,d)} = \underline{0}$$
>
> c'est-à-dire $$\overline{(a+c, b+d)} = \overline{(0,0)}$$
>
> ou encore $$a + c = b + d$$
>
> C'est là qu'on voit que $c = b$ et $d = a$ font l'affaire.

2.1.3 Relation d'ordre sur $\mathbb{Z}$

Comme expliqué à la **proposition 1.11**, l'inverse d'un élément x d'un groupe commutatif est noté $-x$ et on l'appelle *opposé de x* plutôt qu'*inverse de x*. On a déjà noté

$$\mathbb{N} = \{\underline{n} \mid n \in \mathbb{N}\} \subset \mathbb{Z}$$

Posons aussi $\mathbb{N}^\star = \mathbb{N} \setminus \{\underline{0}\}$ $-\mathbb{N} = \{-\underline{n} \mid n \in \mathbb{N}\}$ $-\mathbb{N}^\star = -\mathbb{N} \setminus \{\underline{0}\}$

Proposition 2.1.15
Soit $(a,b) \in \mathbb{N}^2$. *On a*

$$\overline{(a,b)} = \underline{0} \iff a = b$$

$$\overline{(a,b)} \in \mathbb{N}^\star \iff a > b$$

et
$$\overline{(a,b)} \in (-\mathbb{N}^\star) \iff a < b$$

Preuve : On a successivement

$$\begin{aligned}\overline{(a,b)} = \underline{0} &\iff (a,b) \sim (0,0) \iff 0+b = a+0\\ &\iff a = b\end{aligned}$$

De même
$$\begin{aligned}\overline{(a,b)} \in \mathbb{N}^\star &\iff \exists n \in \mathbb{N} \qquad (a,b) \sim (n,0)\\ &\iff \exists n \in \mathbb{N}^\star \qquad n+b = a\\ &\iff a > b\end{aligned}$$

La dernière proposition se démontre encore de la même manière. Ou bien, on peut utiliser le fait que $-\overline{(a,b)} = \overline{(b,a)}$ et donc

$$\overline{(a,b)} \in (-\mathbb{N}^\star) \iff \underbrace{-\overline{(a,b)}}_{=\overline{(b,a)}} \in \mathbb{N}^\star \iff b > a \qquad \square$$

Mais, étant donnés deux entiers naturels a et b, on sait qu'on peut toujours les comparer et qu'on est nécessairement dans l'un des trois cas ci-dessus. Ceux-ci sont mutuellement exclusifs. Par suite,

Corollaire 2.1.16
Les ensembles $\{\underline{0}\}$, $\mathbb{N}^\star$ *et* $-\mathbb{N}^\star$ *forment une partition de* $\mathbb{Z}$.

En d'autres termes, un entier relatif est soit nul, soit dans $\mathbb{N}^\star$, soit dans $-\mathbb{N}^\star$.

Si l'on regarde le dessin se trouvant au début du chapitre, il est presque naturel de vouloir séparer les « droites » de $\mathbb{N}^2$ en trois catégories : la diagonale $\{\underline{0}\}$, les droites en-dessous de la diagonale (celles-ci forment l'ensemble $\mathbb{N}^\star$) et les droites au-dessus de la diagonale (et qui forment $-\mathbb{N}^\star$). Le théorème précédent met en valeur ce découpage, et toute notre construction donne rend logique les notations $\underline{n}$ et $-\underline{n}$ pour $n \in \mathbb{N}$.

Cela nous donne alors envie de définir les notions d'entiers relatifs positifs et négatifs et de définir un ordre sur $\mathbb{Z}$:

Définition 2.1.17 (Ordre sur $\mathbb{Z}$)
- Si x et y sont deux entiers, on dira que x *est inférieur à* y, ce qu'on notera $x \leqslant y$, si et seulement si $y - x \in \mathbb{N}$.
- Si $0 \leqslant x$, on dira que x *est positif*. Si de plus $x \neq 0$, on dira que x *est strictement positif*, ce qu'on notera $0 < x$.
- Si $x \leqslant 0$, on dira que x *est négatif*. Si de plus $x \neq 0$, on dira que x *est strictement négatif*, ce qu'on notera $x < 0$.

Proposition 2.1.18
La relation $\leqslant$ *définit un ordre total sur* $\mathbb{Z}$. *De plus, celui-ci est compatible avec l'addition :*

$$\forall x,y,z,t \in \mathbb{Z} \qquad \left.\begin{array}{l} x \leqslant y \\ z \leqslant t \end{array}\right\} \iff x+z \leqslant y+t$$

Enfin,
$$\forall x,y \in \mathbb{Z} \qquad (x \leqslant y \iff (-y) \leqslant (-x))$$

Preuve : Commençons par montrer que $\leqslant$ est un ordre total.

- **Réflexivité** : Soit $x \in \mathbb{Z}$. On a $x - x = 0$, puisque $-x$ est l'opposé de x. Donc $x - x \in \mathbb{N}$, ce qui veut dire que $x \leqslant x$.
- **Antisymétrie** : Soient x et y dans $\mathbb{Z}$, tels que $x \leqslant y$ et $y \leqslant x$. Cela signifie donc que

  $$y - x \in \mathbb{N} \qquad \text{et} \qquad x - y \in \mathbb{N}$$

  On déduit de la première relation d'appartenance que $x - y \in (-\mathbb{N})$. Supposons que $x \neq y$, de sorte qu'en fait

  $$x - y \in (-\mathbb{N}^\star) \qquad \text{et} \qquad x - y \in \mathbb{N}^\star$$

  On obtient $$x - y \in \mathbb{N}^\star \cap (-\mathbb{N}^\star)$$

  mais cet ensemble est vide d'après le **corollaire 1.16**. D'où une absurdité et par suite $x = y$.
- **Transitivité** : Soient x, y et z dans $\mathbb{Z}$, tels que $x \leqslant y$ et $y \leqslant z$. Par définition,

  $$y - x \in \mathbb{N} \qquad \text{et} \qquad z - y \in \mathbb{N}$$

  Du coup, $$z - x = (z - y) + (y - x) \in \mathbb{N}$$

  puisque la somme de deux entiers naturels est un entier naturel.
- **Totalité** : Soient x et y dans $\mathbb{Z}$. Alors $y - x$ est soit dans $\mathbb{N}$, soit dans $-\mathbb{N}^\star$ d'apres le **corollaire 1.16**. Dans le premier cas, on a $x \leqslant y$. Dans le second cas, c'est que $x - y \in \mathbb{N}^\star$ donc $y \leqslant x$. x et y sont donc toujours comparables.

Montrons la compatibilité avec l'addition. Soient x, y, z et t quatre entiers relatifs, tels que

$$x \leqslant y \qquad \text{et} \qquad z \leqslant t$$

Par définition, $$y - x \in \mathbb{N} \qquad \text{et} \qquad t - z \in \mathbb{N}$$

Alors, la somme de deux entiers naturels étant un entier naturel,

$$y + t - (x + z) = y + t - x - z = (y - x) + (t - z) \in \mathbb{N}$$

de sorte que $$x + z \leqslant y + t$$

Enfin, montrons que le passage à l'opposé change l'ordre dans $\mathbb{Z}$. Soient x et y dans $\mathbb{Z}$, tels que $x \leqslant y$. Par définition, $y - x \in \mathbb{N}$. Or,

$$y - x = -(-y) + (-x) = (-x) - (-y) \in \mathbb{N}$$

donc $$(-y) \leqslant (-x)$$ □

À ce stade, et compte-tenu du **Corollaire 1.16**, les entiers relatifs sont partagés en trois catégories mutuellement disjointes : $\underline{0}$, les entiers naturels non nuls (qui sont les entiers relatifs strictement positifs) et les opposés des entiers naturels non nuls (qui sont les entiers strictement négatifs). Autrement dit, on retrouve bien ce qu'on avait admis sur l'ensemble $\mathbb{Z}$:

$$\mathbb{Z} = \{\underline{0}, \pm\underline{1}, \pm\underline{2}, \ldots\}$$

De fait, on peut maintenant laisser tomber les soulignés, qui n'étaient là que pour éviter la confusion le $\mathbb{Z}$ qu'on est en train de construire, et le $\mathbb{Z}$ dont l'existence avait été admise dans les classes précédentes.

2.1.4 Structure d'anneau sur $\mathbb{Z}$

Une autre structure algébrique intervenant souvent en mathématiques est celle d'anneau, que nous allons immédiatement définir :

Définition 2.1.19 (Anneau)
Soit E un ensemble, muni de deux lois de composition internes + et $\star$. On dira que E *est un anneau* si, et seulement si, (E, +) est un groupe commutatif d'élément neutre 0 et

- $\star$ est associative ;
- $\star$ admet un élément neutre, noté 1 ;
- $\star$ est distributive sur + :

$$\forall x, y, z \in \mathrm{E} \qquad x \star (y + z) = (x \star y) + (y \star z)$$

et

$$\forall x, y, z \in \mathrm{E} \qquad (x + y) \star z = (x \star z) + (y \star z)$$

Si, de plus, $\star$ est commutative, on dira que E *est un anneau commutatif*.

Exemple 2.1.20
Outre $\mathbb{Z}$, dont on va montrer qu'il s'agit d'un anneau, on en a déjà rencontré plusieurs au cours de notre scolarité. Soit A un ensemble ; on note $\mathrm{E} = \mathscr{P}(\mathrm{A})$ l'ensemble de ses parties. On a déjà vu au tout début de l'année que $\cap$ et $\cup$ sont des lois de composition internes sur E.

De plus, $(\mathrm{E}, \cup)$ est un groupe commutatif : on sait que $\cup$ est associative, commutative, admet $\emptyset$ pour élément neutre et que tout sous-ensemble B de A admet un opposé pour $\cup$, qui est B^c.

On sait aussi que $\cap$ est associative, commutative, distributive sur $\cup$ (lois de De Morgan), admet A pour élément neutre. $(\mathrm{E}, \cup, \cap)$ est un anneau commutatif.

Théorème 2.1.21 (Structure d'anneau de $\mathbb{Z}$)
$(\mathbb{Z}, \oplus, \otimes)$ *est un anneau commutatif.*

Preuve : On sait déjà que $(\mathbb{Z}, \oplus)$ est un groupe commutatif : il s'agit du **Théorème 1.14**. Restent à établir :

- **Commutativité de** $\otimes$: Soient x et y dans $\mathbb{Z}$. Soient a, b, c et d dans $\mathbb{N}$ tels que

  $$x = \overline{(a, b)} \qquad \text{et} \qquad y = \overline{(c, d)}$$

  D'après le **Corollaire 1.5**,

  $$x \otimes y = \overline{(ac + bd, ad + bc)} \qquad \text{et} \qquad y \otimes x = \overline{(ca + db, da + cb)}$$

  Or, l'addition et la multiplication dans $\mathbb{N}$ sont commutatives, donc

  $$ac + bd = ca + db \qquad \text{et} \qquad ad + bc = da + cb$$

  et par suite,

  $$x \otimes y = y \otimes x$$

- **Associativité de** $\otimes$: Soient x, y et z dans $\mathbb{Z}$. Soient a, b, c, d, e et f dans $\mathbb{N}$ tels que

  $$x = \overline{(a, b)} \qquad y = \overline{(c, d)} \qquad \text{et} \qquad z = \overline{(e, f)}$$

  D'après le **Corollaire 1.5**, on sait que

  $$x \otimes y = \overline{(ac + bd, ad + bc)}$$

  et

  $$(x \otimes y) \otimes z = \overline{\big((ac + bd)e + (ad + bc)f, (ac + bd)f + (ad + bc)e\big)}$$

De même, $x \otimes (y \otimes z) = \overline{\big(a(ce+df)+b(cf+de), a(cf+de)+b(ce+df)\big)}$

En utilisant les propriétés usuelles de l'addition et de la multiplication dans $\mathbb{N}$, il vient

$$(x \otimes y) \otimes z = \overline{(ace+bde+adf+bcf, acf+bdf+ade+bce)}$$

tandis que $x \otimes (y \otimes z) = \overline{(ace+adf+bcf+bde, acf+ade+bce+bdf)}$

La commutativité de l'addition dans $\mathbb{N}$ assure alors qu'on a bien

$$(x \otimes y) \otimes z = x \otimes (y \otimes z)$$

- **Élément neutre pour** $\otimes$: On devine bien que cet élément neutre pour la multiplication sera $1 = \overline{(1,0)}$. On vérifie en effet que si $x = \overline{(a,b)} \in \mathbb{Z}$, alors

$$x \otimes 1 = \overline{(a \times 1 + b \times 0, a \times 0 + b \times 1)} = \overline{(a,b)} = x$$

- **Distributivité de** $\otimes$ **sur** $\oplus$: Soient des entiers relatifs

$$x = \overline{(a,b)} \qquad y = \overline{(c,d)} \qquad \text{et} \qquad z = \overline{(e,f)}$$

On a
$$\begin{aligned} x \otimes (y \oplus z) &= \overline{(a,b)} \otimes \overline{(c+e, d+f)} \\ &= \overline{\big(a(c+e)+b(d+f), a(d+f)+b(c+e)\big)} \\ &= \overline{\big((ac+bd)+(ae+bf), (ad+bc)+(af+be)\big)} \\ &= \overline{(ac+bd, ad+bc)} \oplus \overline{(ae+bf, af+be)} \\ x \otimes (y \oplus z) &= (x \otimes y) \oplus (x \otimes z) \end{aligned}$$

□

Proposition 2.1.22 (Relation entre somme et produit)
Soient x et y deux entiers relatifs.

- *Si* $x > 0$, $$x \otimes y = \underbrace{y \oplus y \oplus \cdots \oplus y}_{x \text{ fois}}$$
- *Si* $x < 0$, $$xy = -(\underbrace{y \oplus y \oplus \cdots \oplus y}_{-x \text{ fois}})$$

Preuve : Fixons $y \in \mathbb{Z}$. On pose

$$\forall n \in \mathbb{N}^\star \qquad u_n = n \otimes y$$

Alors
$$u_1 = 1 \otimes y = y$$

et
$$\forall n \in \mathbb{N}^\star \qquad u_{n+1} = (n+1) \otimes y = n \otimes y + y = u_n + y$$

Mais on a vu dans le cours sur les nombres entiers qu'il y a une seule suite définie par récurrence de cette maniere : c'est celle de terme général $\sum_{k=1}^{n} y$. Par suite,

$$\forall n \in \mathbb{N}^\star \qquad u_n = \sum_{k=1}^{n} y = y \oplus \cdots \oplus y$$

Ceci démontre la première assertion. La seconde en est une conséquence : soit $x \in (-\mathbb{N}^\star)$ et notons $n = -x \in \mathbb{N}^\star$. Alors

$$x \otimes y = -(-x \otimes y) = -n \otimes y = -(\underbrace{y \oplus \cdots \oplus y}_{n \text{ fois}}) \qquad \square$$

On a établi les propriétés bien connues de $\mathbb{Z}$, ce qui justifie le retour aux notations habituelles $+$ et $\times$ pour l'addition et la multiplication.

2.2 Construction de $\mathbb{Q}$

Cependant, $\mathbb{Z}$ présente un inconvénient : les seuls entiers relatifs inversibles sont 1 et -1. En effet, soit $x \in \mathbb{Z}$, inversible pour la multiplication. Il existe $y \in \mathbb{Z}$, tel que $xy = 1$. On remarque que x et y sont de même signe pour que leur produit soit positif.

Supposons qu'ils sont tous deux positifs ; aucun d'eux ne peut être nul, puisque leur produit serait nul. Et si $x > 1$, alors $x \geqslant 2$ et $xy \geqslant 2y \geqslant 2$ ce qui contredit le fait que $xy = 1$. Par suite, $x = 1$.

De même, si x et y sont négatifs, alors $-x$ et $-y$ sont positifs et vérifient $(-x)(-y) = 1$. D'après ce qui précède, $-x = 1$ et $x = -1$.

Ainsi, dans $\mathbb{Z}$, on ne peut diviser que par 1 et -1. Et pourtant, il est tout-a-fait imaginable de diviser un entier par un autre : une pomme peut être coupée en deux moitiés égales, un gateau peut être coupé en parts égales, etc.

On cherche donc à construire un ensemble, contenant $\mathbb{Z}$, dans lequel il soit en outre possible de diviser. Commençons par une définition :

Définition 2.2.1 (Anneaux intègre)
Soit A un anneau. On dit qu'un élément $x \in A$ est *un diviseur de 0* si, et seulement si,

$$\exists y \in A \setminus \{0\} \qquad xy = 0$$

Un anneau qui n'a pas de diviseur de 0 autre que 0 est dit *intègre*.

Exemple 2.2.2
Prenons l'ensemble A de fonctions de $\mathbb{R}$ dans $\mathbb{R}$. C'est un anneau pour les opérations d'addition et de multiplication des fonctions. Celui-ci contient des diviseurs de 0.

Par exemple, on considère les fonctions f et g définies par

$$\forall x \in \mathbb{R} \qquad f(x) = \begin{cases} 1 & \text{si } x \geqslant 0 \\ 0 & \text{si } x < 0 \end{cases} \qquad \text{et} \qquad g(x) = \begin{cases} 0 & \text{si } x \geqslant 0 \\ 1 & \text{si } x < 0 \end{cases}$$

f et g sont toutes deux dans $A \setminus \{0\}$, puisqu'elles ne sont pas identiquement nulles. Et pourtant $fg = 0$.

La procédure permettant de construire $\mathbb{Q}$ à partir de $\mathbb{Z}$ est très générale et peut être en fait appliquée à tout anneau commutatif intègre. Commençons par établir que

Proposition 2.2.3 (Intégrité de $\mathbb{Z}$)
$\mathbb{Z}$ est un anneau intègre, ce qui signifie que

$$\forall x, y \in \mathbb{Z} \qquad xy = 0 \implies (x = 0 \quad ou \quad y = 0)$$

Preuve : Soient x et y deux entiers relatifs tels que $xy = 0$. S'ils sont tous deux positifs, c'est qu'ils sont en fait dans $\mathbb{N}$ et on sait alors que $x = 0$ ou $y = 0$. Si l'un d'eux est négatif, par exemple x, on a aussi $0 = -xy = (-x)y$ et on est ramené au cas précédent. $\square$

Dans ce qui suit, A est un anneau commutatif intègre. On notera $A^\star = A \setminus \{0\}$ et on définit sur $A \times A^\star$ la relation suivante :

$$\forall (a,b),(c,d) \in \mathbb{A} \times A^\star \qquad (a,b) \sim (c,d) \iff ad - bc = 0$$

Proposition 2.2.4
$\sim$ est une relation d'équivalence sur $A \times A^\star$.

Preuve : Comme d'habitude, on vérifie la réflexivité, la symétrie et la transitivité de $\sim$.

- **Réflexivité** : Soient a et b dans A, avec $b \neq 0$. Alors
$$ab - ba = ab - ab = 0 \qquad \text{d'où} \qquad (a,b) \sim (a,b)$$
- **Symétrie** : Soient (a,b) et (c,d) dans $A \times A^\star$ tels que $(a,b) \sim (c,d)$. Par définition, $ad - bc = 0$; mais l'addition et la multiplication sont commutatives dans A donc $cb - da = 0$ ce qui prouve que $(c,d) \sim (a,d)$.
- **Transitivité** : Soient (a,b), (c,d) et (e,f) dans $A \times A^\star$. On suppose que
$$(a,b) \sim (c,d) \qquad \text{et} \qquad (c,d) \sim (e,f)$$
Alors
$$ad - bc = 0 \qquad \text{et} \qquad cf - de = 0$$
On multiplie la première relation par f et l'on utilise la deuxième pour trouver :
$$adf = bcf = bde$$
donc
$$d(af - be) = 0$$
Mais $d \neq 0$ et A est intègre donc $af - be = 0$. Ce qui assure que $(a,b) \sim (e,f)$. □

Définition 2.2.5
L'ensemble quotient $(A \times A^\star)/\sim$ est noté $\mathbb{K}$. On l'appelle *corps des fractions sur* A.
Si $(a,b) \in A \times A^\star$, sa classe d'équivalence est notée $\frac{a}{b}$. Auquel cas,

- a est appelé *numérateur* de la fraction $\frac{a}{b}$;
- b est appelé *dénominateur* de la fraction $\frac{a}{b}$.

Le passage au quotient par la relation d'équivalence $\sim$ est exactement ce qu'il fallait pour retrouver les règles de simplification de fractions dont on a l'habitude. Par exemple, $\frac{2}{3} = \frac{10}{15}$ puisque $2 \times 15 - 3 \times 10 = 0$. On constate bien en effet que 5 est multiple commun du numérateur et du dénominateur de $\frac{10}{15}$, et tout se passe comme si on l'avait simplifié.

Plus généralement, si $\frac{a}{b} \in \mathbb{K}$, alors

$$\forall c \in A^\star \qquad \frac{a}{b} = \frac{ac}{bc} \qquad \text{puisque} \qquad abc - bac = 0$$

Proposition 2.2.6 (Injection de A dans $\mathbb{K}$)
L'application ι définie par

$$\forall m \in A \qquad \iota(m) = \frac{m}{1}$$

est injective.

Preuve : Soient m et n dans A tels que $\iota(m) = \iota(n)$, c'est-à-dire que $\frac{m}{1} = \frac{n}{1}$. Par définition,

$$m \times 1 - 1 \times n = 0$$

donc $m = n$: ι est injective. □

On voit donc que les éléments $\left(\frac{m}{1}\right)_{m\in A}$ sont deux-à-deux distincts dans $\mathbb{K}$, ce qui permet de considérer que A se trouve dans $\mathbb{K}$. De fait, on identifiera A et ι(A), c'est-à-dire que toute fraction $\frac{m}{1}$ avec $m \in A$ sera simplement notée m, comme s'il s'agissait d'un élément de A.

On souhaite maintenant définir des opérations sur $\mathbb{K}$, puisque, rappelons-le, notre objectif est d'avoir un ensemble contenant A, dans lequel on a en plus le droit de diviser par tout élément non nul.

L'addition et la multiplication dans $\mathbb{K}$ doivent répondre évidemment au cahier des charges suivant : sur A, elles doivent coïncider avec l'addition et la multiplication usuelles. Soient $\frac{a}{b}$ et $\frac{c}{d}$ deux fractions. Supposons temporairement que ce sont aussi des éléments de A, notés m et n, de sorte que

$$\frac{a}{b} = m \qquad \text{et} \qquad \frac{c}{d} = n$$

ce qui veut dire que $a = bm$ et $c = dn$

Par suite, $ad = mbd$ et $bc = nbd$

d'où $ad + bc = (m+n)bd$

et $$\frac{ad+bc}{bd} = m + n$$

On a donc envie de poser $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$.

Pour définir le produit, c'est plus simple, puisqu'on a simplement

$$ac = bdmn \qquad \text{ce qui veut dire que} \qquad \frac{ac}{bd} = mn$$

Il est donc naturel de définir $\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$. Il faut, avant cela, vérifier la compatibilité de ces opérations avec la relation $\sim$.

Lemme 2.2.7
Soient a, b, c, d, a', b', c' et d' dans A, *avec b, b', d, d' non nuls, tels que*

$$\frac{a}{b} = \frac{a'}{b'} \qquad et \qquad \frac{c}{d} = \frac{c'}{d'}$$

Alors $$\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'} \qquad et \qquad \frac{ac}{bd} = \frac{a'c'}{b'd'}$$

Preuve : Commençons par montrer que $\frac{ac}{bd} = \frac{a'c'}{b'd'}$ car c'est assez simple. On sait que

$$ab' = ba' \qquad \text{et} \qquad cd' = dc'$$

donc $acb'd' = bda'c'$ ou encore $(ac)(b'd') - (bd)(a'c') = 0$

Autrement dit, $$\frac{ac}{bd} = \frac{a'c'}{b'd'}$$

On repart de $ab' = ba'$ et $cd' = dc'$. En multipliant la première relation par dd' et la deuxième par bb', il vient

$$adb'd' = bda'd' \qquad \text{et} \qquad bcb'd' = bdb'c'$$

On ajoute alors ces deux expressions :

$$(ad+bc)b'd' = bd(a'd'+b'c')$$

d'où
$$\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$$ □

Corollaire 2.2.8
Il existe deux lois de composition internes sur $\mathbb{K}$*, notées* $+$ *et* $\times$*, telles que*

$$\forall (a,b),(c,d) \in \mathrm{A}\times\mathrm{A}^\star \qquad \frac{a}{b}+\frac{c}{d} = \frac{ad+bc}{bd} \qquad \textit{et} \qquad \frac{a}{b}\times\frac{c}{d} = \frac{ac}{bd}$$

Définition 2.2.9 (Corps)
Soit E un ensemble muni de deux lois de composition internes $+$ et $\star$. On dit que E *est un corps* si, et seulement si,

- $(\mathrm{E},+,\star)$ est un anneau, d'éléments neutre 0 ;
- Tout élément de E, autre que 0, est inversible pour la loi $\star$.

Théorème 2.2.10
Le corps des fractions d'un anneau commutatif est un corps commutatif.

Preuve : Il s'agit de montrer que $\mathbb{K}$ est un corps. Rappelons les étapes : $(\mathbb{K},+)$ doit être un groupe commutatif, $(\mathbb{K},\times)$ doit être un anneau commutatif et tout élément de $\mathbb{K}$ autre que le neutre pour $+$ doit être inversible pour $\times$.

- $+$ **et** $\times$ **sont commutatives** : On a, d'après la commutativité de l'anneau A,

$$\forall \frac{a}{b},\frac{c}{d} \in \mathbb{K} \qquad \frac{a}{b}\times\frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d}\times\frac{a}{b}$$

et
$$\forall \frac{a}{b},\frac{c}{d} \in \mathbb{K} \qquad \frac{a}{b}+\frac{c}{d} = \frac{ad+bc}{bd} = \frac{bc+ad}{db} = \frac{c}{d}+\frac{a}{b}$$

- $+$ **et** $\times$ **sont associatives** : Soit $\frac{a}{b}$, $\frac{c}{d}$ et $\frac{e}{f}$ trois éléments de $\mathbb{K}$. On commence par le cas de $\times$, un peu moins calculatoire. D'après le **Corollaire 2.5**,

$$\frac{a}{b}\times\frac{c}{d} = \frac{ac}{bd} \qquad \text{et} \qquad \frac{c}{d}\times\frac{e}{f} = \frac{ce}{df}$$

puis
$$\left(\frac{a}{b}\times\frac{c}{d}\right)\times\frac{e}{f} = \frac{(ac)e}{(bd)f} \qquad \text{et} \qquad \frac{a}{b}\times\left(\frac{c}{d}\times\frac{e}{f}\right) = \frac{a(ce)}{b(df)}$$

Or, A est un anneau donc la multiplication dans A est associative d'où

$$(ac)e = a(ce) \qquad \text{et} \qquad (bd)f = b(df)$$

Par suite,
$$\left(\frac{a}{b}\times\frac{c}{d}\right)\times\frac{e}{f} = \frac{a}{b}\times\left(\frac{c}{d}\times\frac{e}{f}\right)$$

On passe maintenant à l'addition. Toujours d'après le **Corollaire 2.5**,

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$$

et
$$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{(ad+bc)f+(bd)e}{(bd)f}$$

De même,
$$\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a(df)+b(cf+de)}{b(df)}$$

Mais comme A est un anneau, l'addition et la multiplication y sont associatives, et la multiplication se distribue sur l'addition. Donc

$$(ad+bc)f+(bd)e=adf+bcf+bde=a(df)+b(cf+de)$$

et
$$(bd)f=b(df)$$

Finalement,
$$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)$$

L'addition dans $\mathbb{K}$ est associative.

- **Éléments neutre pour** $+$ **et** $\times$: Il suffit de remarquer que

$$\forall\frac{a}{b}\in\mathbb{K}\qquad\frac{a}{b}+\frac{0}{1}=\frac{a\times1+0\times b}{b\times1}=\frac{a}{b}$$

et
$$\forall\frac{a}{b}\in\mathbb{K}\qquad\frac{a}{b}\times\frac{1}{1}=\frac{a\times1}{b\times1}=\frac{a}{b}$$

Donc les fractions $0=\frac{0}{1}$ et $1=\frac{1}{1}$ sont neutre dans $\mathbb{K}$, respectivement pour l'addition et la multiplication.

- **Inverses** : Remarquons que

$$\forall\frac{a}{b}\in\mathbb{K}\qquad\frac{a}{b}+\frac{-a}{b}=\frac{ab+(-ab)}{b^2}=\frac{ab-ab}{b^2}=\frac{0}{1}=0$$

donc tout élément $\frac{a}{b}$ de $\mathbb{K}$ est inversible, d'inverse $\frac{-a}{b}$.
Ensuite, si $\frac{a}{b}$ est une fraction dans $\mathbb{K}$, non nulle, on sait que

$$\frac{a}{b}\neq\frac{0}{1}\qquad\text{ou encore}\qquad a\times1\neq0\times b$$

c'est-à-dire que
$$a\neq0$$

De fait, on peut former la fraction $\frac{b}{a}$. Du coup,

$$\frac{a}{b}\times\frac{b}{a}=\frac{ab}{ba}=\frac{ab}{ab}=\frac{1}{1}$$

et $\frac{a}{b}$ est inversible pour $\times$, d'inverse $\frac{b}{a}$. □

Puisque $\mathbb{Z}$ est un anneau intègre, le paragraphe précédent montre que l'on peut former son corps des fractions.

Définition 2.2.11
Le corps des fractions de $\mathbb{Z}$ est noté $\mathbb{Q}$. On l'appelle **ensemble des rationnels**. C'est un corps commutatif, contenant $\mathbb{Z}$.

2.3 Compléments de vocabulaire sur les structures

2.3.1 Sous-groupes et morphismes de groupes

Définition 2.3.1 (Sous-groupes)
Soit $(G,\star)$ un groupe. Soit H une partie de G. On dira que H est un sous-groupe de G si, et seulement si, $(H,\star)$ est un groupe.

Commençons par lever deux ambiguïtés. On suppose qu'on a un groupe G et un sous-groupe H. Alors G a un élément neutre qu'on appelle 1_G et H a un élément neutre qu'on appelle 1_H. On sait

$$\forall x \in G \qquad x \star 1_G = 1_G \star x = x$$

En particulier, $$1_H \star 1_G = 1_H$$

Mais aussi $$1_H \star 1_H = 1_H$$

donc $$1_H \star 1_H = 1_H \star 1_G$$

Ne reste qu'à multiplier cette égalité par 1_H^{-1} à gauche pour trouver $1_H = 1_G$: le neutre pour la structure de groupe de G est aussi le neutre pour la structure de groupe de H.

Faisons de même pour les inverses. Si $x \in H$, il admet un inverse dans H puisque H est un groupe : il existe $x_H^{-1} \in H$ tel que

$$x \star x_H^{-1} = x_H^{-1} \star x = 1_H$$

Mais il admet aussi un inverse x_G^{-1} pour la structure de groupe de G :

$$x \star x_G^{-1} = x_G^{-1} \star x = 1_G$$

Or, on vient de voir que $1_G = 1_H$. Donc x_G^{-1} est aussi inverse de x dans H. L'inverse dans un groupe étant unique (**Proposition 1.11**), il vient $x_G^{-1} = x_H^{-1}$.

Tout ceci se résume en :

Lemme 2.3.2
Soient G *un groupe et* H *un sous-groupe. Alors* $1_G = 1_H$ *; de plus, pour tout* $x \in H$*, son inverse pour la structure de groupe de* H *est son inverse pour la structure de groupe de* G.

Du coup, il n'y a pas d'ambiguïté possible lorsqu'on parle de 1 ou de x^{-1} lorsque $x \in H$.

Donnons maintenant une caractérisation des sous-groupes, qui permettra d'établir facilement qu'un objet est un groupe.

Proposition 2.3.3
Soit $(G,\star)$ *un groupe. Soit* H *une partie non vide de* G*. Alors* H *est un sous-groupe de* G *si, et seulement si,*

$$\forall x, y \in H \qquad x \star y^{-1} \in H$$

Preuve : Supposons que H est un sous-groupe de G. Étant donnés x et y dans H, y^{-1} se trouve aussi dans H ; et la loi $\star$ étant interne à H, on a $x \star y^{-1} \in H$.

Réciproquement, supposons que

$$\forall x, y \in H \qquad x \star y^{-1} \in H$$

Commençons par montrer que $\star$ est une loi de composition interne à H. Soit $x \in \mathrm{H}$; un tel x existe puisque H n'est pas vide. On sait alors que $x \star x^{-1} \in \mathrm{H}$ donc $1 \in \mathrm{H}$. Du coup, $1 \star x^{-1} \in \mathrm{H}$ et on a montré que

$$\forall x \in \mathrm{H} \qquad x^{-1} \in \mathrm{H}$$

Donnons-nous deux éléments x et y dans H. On sait maintenant que $y^{-1} \in \mathrm{H}$; on sait également que $(y^{-1})^{-1} = y$ donc

$$x \star y = x \star (y^{-1})^{-1} \in \mathrm{H}$$

Ceci établit bien que $\star$ est une loi de composition interne à H.

Elle est associative, puisque $\mathrm{H} \subset \mathrm{G}$ et qu'elle est associative sur G. On a vu que $1 \in \mathrm{H}$, qui est alors neutre pour H vu qu'il l'est pour G. Enfin, si $x \in \mathrm{H}$, on a vu que $x^{-1} \in \mathrm{H}$ également : tout élément de H admet un inverse. □

Ce théorème est utile pour montrer qu'un objet H est un groupe sans avoir à vérifier tous les axiomes d'un groupe : en effet, si l'on sait que H est un sous-ensemble d'un groupe G, alors il suffit de vérifier que H n'est pas vide et que

$$\forall x, y \in \mathrm{H} \qquad x \star y^{-1} \in \mathrm{H}$$

pour avoir que H est un groupe.

On a déjà montré que $\mathbb{Z}$ et $\mathbb{Q}$ sont des groupes additifs. D'autres exemples de groupes sont $\mathbb{R}$ et $\mathbb{C}$; ou encore $\mathbb{G}^A$, l'ensemble des fonctions d'un ensemble A dans un groupe G ; ou enfin, l'ensemble des bijections d'un ensemble A, qui est un groupe pour la composition des applications. Tous ces exemples, vus en cours, peuvent être utilisés comme étant des groupes bien connus. Et lorsqu'on doit montrer qu'un ensemble H est un groupe, on pourra simplement montrer que c'est un sous-groupe d'un de ces groupes connus.

Exemple 2.3.4
Soit n un entier naturel. On considère l'ensemble

$$\{nx \mid x \in \mathbb{Z}\} = \{0, \pm n, \pm 2n, \ldots\}$$

Celui-ci est communément noté $n\mathbb{Z}$. Il n'est bien sûr pas vide, puisqu'il contient 0 ; et l'on a $n\mathbb{Z} \subset \mathbb{Z}$.

Soient m et p deux éléments de $n\mathbb{Z}$. Par définition, il existe des entiers relatifs x et y tels que

$$m = nx \qquad \text{et} \qquad p = ny$$

Alors
$$m - p = nx - ny = n(x - y)$$

Or, $x - y \in \mathbb{Z}$ donc $m - p$ est bien dans $n\mathbb{Z}$. De ce fait, $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Exemple 2.3.5
Dans le cours sur les nombres complexes, on a été amené à considérer l'ensemble $\mathbb{U}$ des nombres complexes de module 1 :

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

C'est un sous-ensemble de $\mathbb{C}^\star$, qui est un groupe pour la multiplication. Montrons que c'en est un sous-groupe. On sait, d'après les propriétés du module, que

$$\forall z, w \in \mathbb{U} \qquad |zw^{-1}| = \frac{|z|}{|w|} = \frac{1}{1} = 1$$

donc
$$\forall z, w \in \mathbb{U} \qquad zw^{-1} \in \mathbb{U}$$

ce qui montre que $\mathbb{U}$ est un groupe.

Exemple 2.3.6
Si n est un entier naturel non nul, on considère maintenant l'ensemble $\mathbb{U}_n$ des racines n-ème de l'unité :

$$\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$$

On sait déjà que $\mathbb{U}_n \subset \mathbb{U}$ (voir cours sur les nombres complexes). Montrons qu'il s'agit d'un sous-groupe de $\mathbb{U}$. Si z et w sont dans $\mathbb{U}_n$, on a

$$(zw^{-1})^n = \frac{z^n}{w^n} = \frac{1}{1} = 1$$

donc
$$zw^{-1} \in \mathbb{U}_n$$

$\mathbb{U}_n$ est un sous-groupe de $\mathbb{U}$.

Définition 2.3.7 (Morphismes de groupes)
Soient $(G, \star)$ et $(G', \bullet)$ deux groupes. On dira qu'une application $f : G \longrightarrow G'$ est un *morphisme de groupes* si, et seulement si,

$$\forall x, y \in G \qquad f(x \star y) = f(x) \bullet f(y)$$

Définition 2.3.8 (Isomorphisme de groupes)
On appelle *isomorphisme de groupes* tout morphisme de groupes bijectif.

Définition 2.3.9 (Endomorphisme, automorphisme)
Un *endomorphisme* de groupe est un morphisme d'un groupe dans lui-même. Un *automorphisme* de groupe est un endomorphisme bijectif.

Les morphismes de groupes sont tout simplement les applications qui sont compatibles avec la structure de groupe.

Exemple 2.3.10
Considérons les groupes $G = 2\mathbb{Z}$ et $H = 6\mathbb{Z}$. L'application

$$\begin{aligned} f : \ 6\mathbb{Z} &\longrightarrow 2\mathbb{Z} \\ x &\longmapsto x \end{aligned}$$

est un morphisme de groupes. Elle est clairement injective ; en revanche, elle n'est pas surjective car 4 n'a pas d'antécédent par f.

On peut aussi considérer

$$\begin{aligned} g : \ 2\mathbb{Z} &\longrightarrow 6\mathbb{Z} \\ x &\longmapsto 3x \end{aligned}$$

C'est aussi un morphisme de groupes. L'injectivité est claire. Enfin, si $y \in 6\mathbb{Z}$, c'est un multiple de 6, donc en particulier $\frac{y}{3}$ est un entier pair et se trouve dans $2\mathbb{Z}$. Et on a $f(\frac{y}{3}) = y$ donc f est un isomorphisme de groupes.

On voit donc que $2\mathbb{Z}$ et $6\mathbb{Z}$ sont isomorphes, c'est-à-dire qu'ils ont à peu près la même structure. Ce qui n'est pas étonnant, puisque tous deux « ressemblent » à $\mathbb{Z}$. Dans un cas, on n'a gardé que les entiers relatifs pairs, dans l'autre les multiples de 6.

Exemple 2.3.11
Les ensembles $(\mathbb{R}_+^\star, \times)$ et $(\mathbb{R}, +)$ sont des groupes, d'éléments neutres respectivement 1 et 0. On sait que

$$\forall x > 0 \qquad \ln(xy) = \ln x + \ln y$$

et que le logarithme réalise une bijection de $\mathbb{R}_+^\star$ sur $\mathbb{R}$. En d'autres termes, ln est un isomorphisme de $(\mathbb{R}^\star, \cdot)$ sur $(\mathbb{R}, +)$.

Exemple 2.3.12
On considère les groupes $(\mathbb{R}, +)$ et $\mathbb{U}$. On définit

$$\forall x \in \mathbb{R} \qquad f(x) = \mathrm{e}^{\mathrm{i}x}$$

Le cours sur les nombres complexes nous dit que f est un morphisme surjectif de $(\mathbb{R}, +)$ sur $\mathbb{U}$.

En revanche, f n'est pas injectif puisque $f(2\pi) = f(0) = 1$.

Définition 2.3.13 (Noyau, Image)
Soient G et G′ deux groupes, soit f un morphisme de G dans G′. On appelle *noyau* de f l'ensemble

$$\mathrm{Ker}\, f = \{g \in \mathrm{G} \mid f(g) = 1_{\mathrm{G}'}\}$$

On appelle *image* de f l'ensemble

$$\mathrm{Im}\, f = \{f(g) \mid g \in \mathrm{G}\} = f(\mathrm{G})$$

Exemple 2.3.14
Reprenons le dernier exemple :

$$\forall x \in \mathbb{R} \qquad f(x) = \mathrm{e}^{\mathrm{i}x}$$

On a $$\mathrm{Ker}\, f = \{x \in \mathbb{R} \mid f(x) = 1\} = \{x \in \mathbb{R} \mid \mathrm{e}^{\mathrm{i}x} = 1\}$$

Le cours sur les nombres complexes assure que $\mathrm{Ker}\, f = 2\pi\mathbb{Z}$. Tandis que $\mathrm{Im}\, f = \mathbb{U}$, d'après l'existence de la forme trigonométrique.

Proposition 2.3.15
Soient G *et* G′ *deux groupes, soit* f *un morphisme de* G *dans* G′. *On a*

$$f(1_G) = 1_{G'} \qquad \textit{et} \qquad \forall x \in G \qquad f(x^{-1}) = f(x^{-1})$$

De plus,

- f *est injective si, et seulement si,* $\mathrm{Ker}\, f = \{1_G\}$;
- f *est surjective si, et seulement si,* $\mathrm{Im}\, f = G'$.

Preuve : Notons $y = f(1_G)$. On a alors, puisque f est un morphisme de groupes,

$$y \bullet y = f(1_G) \bullet f(1_G) = f(1_G \star 1_G) = f(1_G) = y$$

Comme G′ est un groupe, il contient y^{-1} qu'on multiplie à gauche membre-à-membre pour obtenir $y = 1_{G'}$.

Ensuite, soit $x \in G$. On a

$$f(x) \bullet f(x^{-1}) = f(x \star x^{-1}) = f(1_G) = 1_{G'}$$

donc $f(x^{-1})$ est l'inverse de $f(x)$.

La proposition sur la surjectivité de f est une trivialité, dans la mesure où $\mathrm{Im}\, f = f(G)$; f est surjective si et seulement si elle atteint tout élément de G′, c'est-à-dire si $f(G) = G'$.

Montrons enfin que f est injective si, et seulement si, $\mathrm{Ker}\, f = \{1_G\}$. On suppose d'abord que f est injective ; alors $1_{G'}$ a un seul antécédent. Mais on sait déjà que $f(1_G) = 1_{G'}$; donc $\mathrm{Ker}\, f = \{1_G\}$. Réciproquement, supposons que $\mathrm{Ker}\, f = \{1_G\}$. Soient x et y dans G tels que $f(x) = f(y)$. Alors

$$f(x \star y^{-1}) = f(x) \bullet f(y^{-1}) = f(x) \bullet f(y)^{-1} = f(x) \bullet f(x)^{-1} = 1_{G'}$$

donc $$x \star y^{-1} \in \mathrm{Ker}\, f \qquad \text{et} \qquad x \star y^{-1} = 1_G$$

Il s'ensuit que $x = y$ et f est injective. □

2.3.2 Sous-anneaux et morphismes d'anneaux

Définition 2.3.16 (Sous-anneaux)
Soit $(A, +, \star)$ un anneau, soit $B \subset A$. On dit que B *est un sous-anneau de* A si, et seulement si, $1_A \in B$ et $(B, +, \star)$ est un anneau.

Si B est un sous-anneau de A, on sait en particulier que $(B, +)$ est un sous-groupe de $(A, +)$. Le **lemme 3.2** peut être appliqué pour en déduire que $0_B = 0_A$ et que l'opposé d'un $x \in B$ est le même pour les deux structures d'anneaux de A et B.

Montrons aussi que $1_B = 1_A$. Comme 1_A est neutre pour A, on a en particulier

$$\forall x \in B \qquad 1_A \star x = x \star 1_A = x$$

Ce qui veut dire que 1_A est neutre pour $(B, \star)$ et appartient à B. La **Proposition 1.8** montre alors que $1_A = 1_B$.

Également, montrons que les notions d'inverse dans B et A coïncident. Soit $x \in B$, inversible, dont on note y l'inverse dans B. Alors

$$x \star y = y \star x = 1_B = 1_A$$

Donc x est aussi inversible dans A et y est son inverse pour la structure d'anneau de A.

Lemme 2.3.17
Soient A *un anneau et* B *un sous-anneau. Alors*

- $0_B = 0_A$ *et* $1_B = 1_A$ *;*
- *L'opposé d'un* $x \in B$ *est le même pour les structures d'anneau de* A *et* B*. On a le même résultat pour les inverses, si* x *est inversible dans* B*.*

Proposition 2.3.18
Soient A *un anneau et* B *un sous-ensemble de* A*. Alors* B *est un sous-anneau de* A *si, et seulement si,* B *contient* 1_A *et*

$$\forall x, y, z \in B \qquad xy + z \in B$$

Preuve : La preuve n'est pas plus compliquée que celle de la **Proposition 3.3**. □

Définition 2.3.19 (Morphismes d'anneaux)
Soient $(A, +, \times)$ et $(A', \oplus, \otimes)$ deux anneaux. Soit $f : A \longrightarrow A'$; on dira que f *est un morphisme d'anneaux* si, et seulement si, $f(1_A) = 1_{A'}$ et

$$\forall x, y, z \in A \qquad f(x \times y + z) = f(x) \otimes f(y) \oplus f(z)$$

On observe qu'un morphisme f entre les anneaux A et A′ est en particulier un morphisme entre les groupes commutatifs $(A, +)$ et $(A', \oplus)$, de sorte que ce qui a été vu dans le paragraphe précédent s'applique :

$$f(0_A) = 0_{A'} \qquad \text{et} \qquad \forall x \in A \qquad f(-x) = -f(x)$$

Définition 2.3.20 (Noyau, Image)
Soit f un morphisme entre les anneaux A et A′. On appelle *noyau* de f l'ensemble

$$\mathrm{Ker}\, f = \{x \in A \mid f(x) = 0_{A'}\}$$

et *image* de f l'ensemb ;e

$$\mathrm{Im}\, f = \{f(x) \mid x \in A\} = f(A)$$

Puisqu'un morphisme d'anneaux est aussi un morphisme de groupes, on utilise la **Proposition 3.15** pour en déduire

Proposition 2.3.21
Soit f *un morphisme entre les anneaux* A *et* A′*. Alors*

- f *est injective si, et seulement si,* $\mathrm{Ker}\, f = \{0_A\}$ *;*
- f *est surjective si, et seulement si,* $\mathrm{Im}\, f = A'$*.*

2.3.3 Règles de calcul dans un anneau

Proposition 2.3.22
Soit $(A,+,\star)$ *un anneau. Alors*

$$\forall x \in A \qquad x \star 0_A = 0_A \star x = 0_A$$

et

$$\forall x \in A \qquad (-1_A) \star x = x \star (-1_A) = -x$$

Preuve : Soit $x \in A$ et notons $y = x \star 0_A$. On a alors, par distributivité de $\star$ sur $+$,

$$y + y = x \star 0_A + x \star 0_A = x \star (0_A + 0_A) = x \star 0_A = y$$

On ajoute alors $-y$ aux deux membres pour trouver $y = 0_A$. On procède de la même manière pour $0_A \star x$.

Ensuite, notons $z = (-1_A) \star x$. Alors, toujours à l'aide de la distributivité de $\star$ sur $+$:

$$z + x = (-1_A) \star x + 1_A \star x = (-1_A + 1_A) \star x = 0_A \star x = 0_A$$

Donc z est un opposé de x ; mais dans un groupe, tout élément a un unique opposé donc $z = -x$.
On montrerait de la même manière que $x \star (-1_A) = -x$. □

Chapitre 3

Arithmétique des Entiers Relatifs

L'ensemble $\mathbb{Z}$ a été construit en détail dans le chapitre précédent, mais seules ses propriétés élémentaires ont été étudiées. Dans ce chapitre, on explore plus en détail sa structure de groupe et ses sous-groupes, ce qui va aboutir naturellement aux notions arithmétiques élémentaires : PGCD, PPCM, théorème de Bezout, théorèmes de Gauss, décomposition d'un entier en produit de facteurs premiers.

3.1 Étude des sous-groupes de $\mathbb{Z}$

3.1.1 PGCD et PPCM

Définition 3.1.1 (Divisibilité)
Soient p et q deux entiers relatifs. On dira que p *divise* q, ou que p *est un diviseur de* q, ou encore que q *est un multiple de* p, ce qu'on notera $p|q$, si, et seulement si,

$$\exists n \in \mathbb{Z} \qquad q = np$$

Une remarque immédiate : 0 ne divise personne dans $\mathbb{Z}$, mis-à part lui-même. Voici les propriétés élémentaires de cette relation :

Proposition 3.1.2
La relation | est réflexive et transitive. De plus,

$$\forall p, q \in \mathbb{Z} \qquad (p|q \quad et \quad q|p) \implies p = \pm q$$

et

$$\forall p, q \in \mathbb{N} \qquad p|q \implies p \leqslant q$$

On observe donc que la divisibilité n'est pas antisymétrique sur $\mathbb{Z}$; en revanche, elle l'est sur $\mathbb{N}$ et constitue donc une relation d'ordre sur cet ensemble.
Preuve : Il est clair que tout entier relatif se divise lui-même, puisque

$$\forall x \in \mathbb{Z} \qquad x = 1 \times x$$

Ceci fournit la réflexivité.

Soient m, n et p sont trois entiers relatifs tels que $m|n$ et $n|p$. Il existe des entiers relatifs m' et n' tels que

$$n = mm' \qquad \text{et} \qquad p = nn'$$

Par suite, $$p = nn' = mm'n'$$

Donc $m|p$ et la transitivité est établie.

Ensuite, soient p et q dans $\mathbb{Z}$ tels que $p|q$ et $q|p$. Si l'un d'eux est nul, l'autre aussi, auquel cas on a bien $p = \pm q$. On les suppose donc tous deux non nuls. Il existe alors deux entiers relatifs p' et q', non nuls, tels que

$$q = pp' \qquad \text{et} \qquad p = qq'$$

Alors $$q = pp' = qq'p' \qquad \text{et} \qquad q(1 - q'p') = 0$$

Comme $\mathbb{Z}$ est intègre et que $q \neq 0$, c'est que $p'q' = 1$. Ce qui n'est possible que si $p' = 1$ et $q' = 1$, ou bien $p' = -1$ et $q' = -1$. Respectivement, on a $p = q$ ou $p = -q$.

Finalement, soient p et q deux entiers naturels tels que $p|q$. Si p est nul, il est clair que $p \leqslant q$; supposons donc que $p > 0$. Il existe un entier naturel non nul p' tel que $q = pp'$. Donc

$$q = \underbrace{p + \cdots + p}_{p' \text{ fois}} \geqslant p$$ □

Une fois deux entiers choisis, on peut s'intéresser en particulier à l'ensemble de leurs diviseurs et de leurs multiples communs.

Proposition 3.1.3 (PGCD et PPCM)
Soient x et y deux entiers relatifs. L'ensemble $\{n \in \mathbb{N} \mid n|x \text{ et } n|y\}$ admet un plus grand élément, appelé plus grand diviseur commun à x et y. On le note $pgcd(x, y)$ ou $x \wedge y$.

L'ensemble $\{n \in \mathbb{N}^\star \mid x|n \text{ et } y|n\}$ admet un plus petit élément, appelé plus petit multiple commun à x et y. On le note $ppcm(x, y)$ ou $x \vee y$.

Preuve : Soit n un diviseur commun à x et y. D'après la **proposition 1.2**, on a $n \leqslant x$ et $n \leqslant y$. L'ensemble $\{n \in \mathbb{N} \mid n|x \text{ et } n|y\}$ est une partie de $\mathbb{N}$, non vide (1 s'y trouve), majoré par le plus grand des deux entiers x et y. Il admet donc un plus grand élément, qui est le PGCD de x et y.

On sait que toute partie de $\mathbb{N}$ admet un plus petit élément, donc le PPCM existe. □

Définition 3.1.4
On dira que *deux entiers x et y sont premiers entre eux* si, et seulement si, leur PGCD vaut 1.

A priori, pour calculer un PGCD de deux entiers a et b, il faut donc s'y prendre de manière assez brutale : on recherche tous les diviseurs de a, tous les diviseurs de b ; on garde ceux qui sont communs et on cherche le plus grand d'entre eux. Trivial à expliquer, mais désagréable à mettre en œuvre, puisque la recherche des diviseurs d'un nombre entier est fastidieuse.

Exemple 3.1.5
Cherchons le PGCD de 13616 et 828. On commence par chercher les diviseurs de chacun de ces deux nombres (cela prend bien 10 minutes pour le premier). Les diviseurs positifs de 13616 sont :

1 2 4 8 16 23 37 46 69 74 92 148 184 296 368 592 851 1702 3404 6808 13616

Les diviseurs de 828 sont

1 2 3 4 6 9 12 18 23 36 46 69 92 138 207 276 414 828

Leurs diviseurs communs sont

$$1 \quad 2 \quad 4 \quad 23 \quad 46 \quad 69 \quad 92$$

d'où $$\text{pgcd}\,(13616, 828) = 92$$

Il existe, bien sûr, des méthodes plus efficaces pour calculer un PGCD. L'une d'elle, l'algorithme d'Euclide, est simple et rapide. Elle repose sur le théorème de division euclidienne.

3.1.2 La division euclidienne

Dans le chapitre précédent, on a montré en exemple que pour tout entier relatif p, l'ensemble $p\mathbb{Z} = \{pn \mid n \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$. Il s'agit de l'ensemble des multiples de p, ou encore des nombres qui sont divisibles par p. Autrement dit,

$$\forall p, q \in \mathbb{Z} \qquad p|q \iff q \in p\mathbb{Z}$$

On va montrer que tout sous-groupe de $\mathbb{Z}$ est de cette forme.

Mais, avant de faire cela, il est nécessaire d'établir le résultat à la base de la structure additive de $\mathbb{Z}$: le théorème de division euclidienne. C'est celui-ci qu'on utilise depuis l'école primaire pour poser des divisions entre nombres entiers. Celui-ci sert, en outre, à décrire l'algorithme d'Euclide pour le calcul des PGCDs.

Théorème 3.1.6 (Division euclidienne)
Soit m et n deux entiers naturels, avec n non nul. Il existe un unique couple d'entiers naturels (q, r) tel que

$$m = nq + r \qquad et \qquad 0 \leqslant r < n$$

Preuve : On considère l'ensemble

$$\mathrm{A} = \{pn \mid p \in \mathbb{N}\} \cap [\![\, 0\,;\, m \,]\!]$$

A n'est pas vide, puisqu'il contient 0. Et il est majoré par m, puisqu'inclus dans $[\![\, 0\,;\, m \,]\!]$. On sait alors qu'il admet un plus grand élément ; il existe donc $q \in \mathbb{N}$ tel que

$$qn \leqslant m \qquad \text{et} \qquad \forall p > q \quad pn > m$$

Posons alors $$r = m - qn$$

r est un entier naturel, puisque $qn \leqslant m$. Par définition de q, on sait que

$$m < (q+1)n = qn + n = m - r + n$$

d'où l'on déduit que $$r < n$$

L'existence du couple (q, r) est bien assurée.

Montrons maintenant son unicité. Soient q' et r' des entiers naturels tels que

$$m = nq' + r' \qquad \text{et} \qquad 0 \leqslant r' < n$$

L'un des deux nombres r ou r' est plus grand que l'autre ; supposons par exemple que $r \geqslant r'$. Alors

$$-n < -r \leqslant 0 \qquad \text{et} \qquad 0 \leqslant r' < n$$

et $$-n < r' - r < n$$

Mais comme $r' - r \geqslant 0$, on a en fait

$$0 \leqslant r' - r < n$$

Du fait que $$m = nq + r = nq' + r'$$

on tire $$r' - r = n(q - q')$$

donc $$0 \leqslant n(q - q') < n$$

et enfin $$0 \leqslant q - q' < 1 \qquad (\text{car } n > 0)$$

Le seul entier naturel strictement inférieur à 1 est 0. Donc $q = q'$ et $r = r'$. □

Outre son intérêt en général, la division euclidienne fournit une méthode permettant de calculer explicitement le PGCD de deux entiers. Cet algorithme repose sur l'observation suivante :

Lemme 3.1.7
Soient a et b deux entiers naturels non nuls, avec $a < b$. On note r le reste de la division euclidienne de b par a. Alors

$$pgcd(a,b) = pgcd(r,a)$$

Preuve : En notant q le quotient de la division euclidienne de b par a, on a

$$b = aq + r \qquad \text{avec} \qquad r < a$$

Du coup, tout diviseur commun à a et r est un diviseur commun à a et b.

Mais on a aussi $r = b - aq$: tout diviseur commun à a et b est un diviseur commun à a et r.

Finalement, les diviseurs communs à a et r sont les diviseurs communs à a et b. En particulier, $a \wedge b = a \wedge r$. □

On peut déduire de ce lemme l'algorithme suivant de calcul du PGCD de deux nombres entiers naturels a et b avec $a < b$:

```
Calculer le reste r de la division de b par a.
Si r=0, alors pgcd(a,b)=a.
Si r<>0, recommencer avec a=r et b=a.
```

En effet, posons $a_0 = a$, $b_0 = b$ et r_0 le reste de la division euclidienne de b par a. Si $r_0 = 0$, c'est que a divise b et le PGCD de a et b est a. Si $r_0 \neq 0$, on pose $a_1 = r_0$ et $b_1 = a$. Le **lemme 1.7** assure que $\text{pgcd}(a_0, b_0) = \text{pgcd}(a_1, b_1)$.

On note r_1 le reste de la division de b_1 par a_1. Si $r_1 = 0$, c'est que a_1 divise b_1 et il vient que $\text{pgcd}(a_1, b_1) = a_1$. Si $r_1 \neq 0$, on pose $a_2 = r_1$ et $b_2 = a_1$. On utilise le **lemme 1.7** pour dire que $\text{pgcd}(a_1, b_1) = \text{pgcd}(a_2, b_2)$. Et on recommence.

Plus précisément, voici comment on définit ces suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$. Cela se fait évidemment par récurrence. On initialise ces suites avec

$$a_0 = a \qquad \text{et} \qquad b_0 = b$$

Et, supposant calculés $a_0, \ldots, a_n$ et $b_0, \ldots, b_n$, on note q_n et r_n le quotient et le reste de la division euclidienne de b_n par a_n :

$$b_n = a_n q_n + r_n \qquad \text{avec} \qquad 0 \leqslant r_n < a_n$$

et on pose $$b_{n+1} = a_n \qquad \text{et} \qquad a_{n+1} = r_n = b_n - a_n q_n$$

Exemple 3.1.8
Reprenons l'exemple précédent avec $a_0 = 828$ et $b_0 = 13616$. On a

$$13616 = 16 * 828 + 368$$

On pose $a_1 = 368$ et $b_1 = 828$ et on effectue la division euclidienne de b_1 par a_1 :

$$828 = 2 * 368 + 92$$

On pose $a_2 = 92$ et $b_2 = 368$. Il vient :

$$368 = 4 * 92$$

Le reste est nul. C'est que $a_2 = 92$ est le PGCD de 828 et 13616.

3.1.3 Sous-groupes de $\mathbb{Z}$

Théorème 3.1.9
Soit G *un sous-groupe de* $\mathbb{Z}$. *Il existe un unique entier naturel* p *tel que* $G = p\mathbb{Z}$. *Ce nombre est appelé générateur principal de* G.

Preuve : On suppose que $G \neq \{0\}$, puisque dans ce cas le théorème est trivial. Et on considère l'ensemble

$$G_+ = G \cap \mathbb{N}^\star = \{x \in G \mid x > 0\}$$

G_+ n'est pas vide : en effet, si x est un élément non nul de G, il est soit strictement positif, soit strictement négatif. Si $x > 0$, il est dans G_+ ; si $x < 0$, c'est $-x$ qui se trouve dans G_+.

G_+, comme toute partie de $\mathbb{N}$, admet un plus petit élément, qu'on note p. Cet entier se trouve dans G_+ et vérifie :

$$p > 0 \qquad \text{et} \qquad \forall x \in G_+ \quad p \leqslant x$$

L'ensemble $p\mathbb{Z}$ est évidemment inclus dans G, puisque G est un groupe et contient p. Montrons l'inclusion réciproque. Soit $x \in G_+$; puisque x et p sont des entiers naturels avec $p > 0$, le théorème de division euclidienne peut être utilisé. Il existe des entiers naturels q et r tels que

$$x = pq + r \qquad \text{et} \qquad 0 \leqslant r < p$$

Or, x et pq sont dans G. Donc $r = x - pq$ également. Comme $r < p$, il ne peut se trouver dans G_+ ; c'est donc en particulier que $r \leqslant 0$. Par suite, $r = 0$ et $x = pq$. Tout élément de G_+ est un multiple de p.

Maintenant, soit $x \in G$. Si $x = 0$, il est bien dans $p\mathbb{Z}$; si $x > 0$, il est dans G_+ et on vient de voir que c'est un multiple de p ; si $x < 0$, alors $-x$ est un multiple de p et x aussi. Finalement, $G \subset p\mathbb{Z}$, ce qui démontre que $G = p\mathbb{Z}$.

On établit maintenant l'unicité d'un tel p. Soit p' un entier naturel non nul tel que

$$G = p\mathbb{Z} = p'\mathbb{Z}$$

Donc $$p|p' \qquad \text{et} \qquad p'|p$$

La **Proposition 1.2** permet de conclure que $p' = \pm p$. Comme p et p' sont des entiers naturels, on a $p = p'$. □

3.2 Le théorème de Bezout et ses conséquences

3.2.1 Théorème de Bezout

Le théorème de Bezout sert à caractériser des entiers qui sont premiers entre eux. Afin de le démontrer, nous aurons besoin du lemme suivant caractérsant le PGCD de deux entiers :

Lemme 3.2.1
Soient a et b deux nombres entiers. L'ensemble

$$a\mathbb{Z} + b\mathbb{Z} = \{am + bn \mid (m,n) \in \mathbb{N}^2\}$$

est un sous-groupe de $\mathbb{Z}$. Son générateur principal est le PGCD de a et b.

Preuve : L'ensemble $a\mathbb{Z} + b\mathbb{Z}$ est un sous-ensemble de $\mathbb{Z}$, non vide : il contient $0 = 0 \times a + 0 \times b$. Soient x et x' dans cet ensemble. Par définition, il existe des entiers relatifs m, n, m', n' tels que

$$x = am + bn \qquad \text{et} \qquad x' = am' + bn'$$

Par suite,

$$x - y = a(m - m') + b(n - n')$$

qui est bien dans $a\mathbb{Z} + b\mathbb{Z}$. Il s'agit bien d'un sous-groupe de $\mathbb{Z}$.

D'après le **théorème 1.9**, il existe un entier naturel d tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Puisqu'on peut écrire

$$a = a \times 1 + b + \times 0 \qquad \text{et} \qquad b = a \times 0 + b \times 1$$

il vient que

$$a \in d\mathbb{Z} \qquad \text{et} \qquad b \in d\mathbb{Z}$$

Donc d est un diviseur commun à a et b. Il reste à montrer que c'est le plus grand.

Pour cela, remarquons qu'il existe deux entiers relatifs m et n tels que $d = am + bn$. Si d' est un autre diviseur commun à a et b, cette expression montre qu'il divise d. En particulier, $d' \leqslant d$. Donc d est bien le plus grand de tous les diviseurs communs à a et b. □

Corollaire 3.2.2
Soient a et b deux entiers relatifs. Il existe des entiers relatifs u et v tels que $au + bv = pgcd(a,b)$. En particulier,

$$\forall d \in \mathbb{Z} \qquad (d|a \quad et \quad d|b) \implies d|pgcd(a,b)$$

Corollaire 3.2.3 (Théorème de Bezout)
Soient a et b deux entiers relatifs. Ils sont premiers entre eux si, et seulement si, il existe des entiers relatifs u et v tels que $au + bv = 1$

Étant donnés deux entiers naturels a et b avec $a < b$, il peut être intéressant de savoir calculer ces nombres u et v tels que $au + bv = \text{pgcd}(a,b)$. C'est à nouveau l'algorithme d'Euclide qu'il faut utiliser. Considérons les suites qu'il fournit, définies par

$$\begin{cases} a_0 = a \\ b_0 = b \\ q_n = \text{quotient de la division euclidienne de } b_n \text{ par } a_n \\ b_{n+1} = a_n \\ a_{n+1} = b_n - a_n q_n \end{cases}$$

C'est la suite $(a_n)_{n\in\mathbb{N}}$ qui fournit le PGCD de a et b en premier : si N est le premier rang tel que $a_N = 0$, c'est que le pgcd de a et b vaut a_{N-1}. Le tout est donc de trouver comment exprimer cette suite en fonction de a et b.

Lemme 3.2.4
Soient $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ et $(q_n)_{n\in\mathbb{N}}$ les suites définies ci-dessus. On pose :

$$\begin{cases}\alpha_{-1}=0\\ \beta_{-1}=1\end{cases}\qquad\begin{cases}\alpha_0=1\\ \beta_0=0\end{cases}$$

et
$$\forall n\in\mathbb{N}\qquad\begin{cases}\alpha_{n+1}=-\alpha_n q_n+\alpha_{n-1}\\ \beta_{n+1}=-\beta_n q_n+\beta_{n-1}\end{cases}$$

Alors
$$\forall n\in\mathbb{N}\qquad a_n=\alpha_n a+\beta_n b$$

Preuve : Le lemme se démontre par récurrence. Il est vrai pour $n=0$ puisque

$$a_0=a=1\times a+0\times b=\alpha_0 a+\beta_0 b$$

De plus,
$$\alpha_1=-\alpha_0 q_0+\alpha_{-1}=-q_0\qquad\text{et}\qquad\beta_1=-\beta_0 q_0+\beta_{-1}=1$$

On en déduit que le lemme est également vrai pour $n=1$:

$$a_1=b_0-a_0q_0=1\times b+(-q_0)\times a=\alpha_1 a+\beta_1 b$$

Supposons maintenant le résultat vrai jusqu'à un rang $N\geqslant 1$, c'est-à-dire que

$$\forall n\leqslant N\qquad a_n=\alpha_n a+\beta_n b$$

On a
$$a_{N+1}=b_N-a_N q_N$$

Mais on sait que
$$b_N=a_{N-1}=\alpha_{N-1}a+\beta_{N-1}b\qquad\text{et}\qquad a_N=\alpha_N a+\beta_N b$$

Par suite,
$$\begin{aligned}a_{N+1}&=\underbrace{\alpha_{N-1}a+\beta_{N-1}b}_{=b_N}-q_N(\underbrace{\alpha_N a+\beta_N b}_{=a_N})\\&=(\alpha_{N-1}-\alpha_N q_N)a+(\beta_{N-1}-\beta_N q_N)b\\a_{N+1}&=\alpha_{N+1}a+\beta_{N+1}b\end{aligned}$$

ce qui établit le lemme au rang $N+1$. Par récurrence, on a montré que

$$\forall n\in\mathbb{N}\qquad a_n=\alpha_n a+\beta_n b$$ □

Ainsi, on a simplement besoin de calculer ces suites $(\alpha_n)_{n\in\mathbb{N}}$ et $(\beta_n)_{n\in\mathbb{N}}$ jusqu'au rang N pour lequel $a_N=0$; on aura alors

$$\alpha_{N-1}a+\beta_{N-1}b=\text{pgcd}(a,b)$$

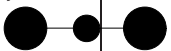
Voici une manière de faire ces calculs efficacement. On met en œuvre l'algorithme d'Euclide. Celui-ci fournit la suite $(q_n)_{n\in\mathbb{N}}$. On dresse alors un tableau à trois colonnes ; pour tout entier n, la n-ème ligne de ce tableau contient le quotient q_n de la division euclidienne de b_n par a_n, l'entier α_n et l'entier β_n.

Ligne	Quotient	α	β
-1		0	1
0	q_0	1	0
1	q_1	α_1	β_1
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$n-1$	q_{n-1}	α_{n-1}	β_{n-1}
n	q_n	α_n	β_n
$n+1$	q_{n+1}	α_{n+1}	β_{n+1}

Au début, seules les lignes -1 et 0 sont remplies. Supposons les lignes -1 à n remplies. Pour remplir la ligne $n+1$, il suffit d'appliquer les formules

$$\alpha_{n+1} = \alpha_{n-1} - \alpha_n q_n \qquad \text{et} \qquad \beta_{n+1} = \beta_{n-1} - \beta_n q_n$$

C'est-à-dire, pour le calcul de α_{n+1} par exemple :

Ligne	Quotient	α	β
-1		0	1
0	q_0	1	0
1	q_1	α_1	β_1
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$n-1$	q_{n-1}	α_{n-1}	β_{n-1}
n			β_n
$n+1$	q_{n+1}	α_{n+1}	β_{n+1}

α_{n+1} est simplement obtenu en soustrayant à α_{n-1} le résultat de la multiplication entourée. De même pour le calcul de β_{n+1}.

Exemple 3.2.5
Voici à quoi ressemble ce tableau dans le cas de l'exemple $a = 828$ et $b = 13616$. On avait calculé

$$q_0 = 16 \qquad q_1 = 2 \qquad q_2 = 4$$

et pour $n = 3$, l'algorithme s'arrête car $a_3 = 0$. On aura donc $\alpha_2 \times 828 + \beta_2 \times 13616 = 92$.

Notre tableau se construit de proche-en-proche :

Étape $n = 1$

Quotient	α	β
	0	1
16	1	0
2	-16	1

$\alpha_1 = 0 - 1 \times 16 \qquad \beta_1 = 1 - 0 \times 16$

Étape $n = 2$

Quotient	α	β
	0	1
16	1	0
2	-16	1
4	33	-2

$\alpha_2 = 1 + 16 \times 2 \qquad \beta_2 = 0 - 2 \times 1$

On peut vérifier que $33 \times 828 - 2 \times 13616 = 92$

3.2.2 Les théorèmes de Gauss

Théorème 3.2.6 (Théorème de Gauss 1)
Soient a et b deux entiers relatifs premiers entre eux. Soit $c \in \mathbb{Z}$. Si $a|bc$, alors $a|c$.

Preuve : On peut supposer que a, b et c sont des entiers naturels, simplement en changeant leur signe ; ceci ne change rien aux hypothèses.

Comme a et b sont premiers entre eux, le **théorème de Bezout** assure l'existence d'entiers relatifs u et v tels que $au + bv = 1$. De sorte que

$$auc + vbc = c$$

Mais $a|auc$ et $a|vbc$ puisque $a|bc$. Donc $a|c$. □

L'hypothèse a et b premiers entre eux est indispensable pour rendre vraie la conclusion du théorème. En effet, si a et b ne sont pas premiers entre eux, il existe des entiers c tels que $a|bc$, sans que $a|c$. Par exemple, on prend

$$a = 2 \qquad b = 4 \qquad \text{et} \qquad c = 3$$

Théorème 3.2.7 (Théorème de Gauss 2)
Soient a et b deux entiers relatifs, premiers entre eux. Soit $c \in \mathbb{Z}$. Si $a|c$ et $b|c$, alors $ab|c$.

Preuve : On peut à nouveau supposer que a, b et c sont des entiers positifs. Comme a et b sont premiers entre eux, il existe des entiers relatifs u et v tels que $au + bv = 1$. Par suite,

$$auc + bvc = c$$

Mais $ab|auc$ puisque $b|c$, et $ab|bvc$ puisque $a|c$. Donc $ab|c$. □

À nouveau, l'hypothèse « a et b premiers entre eux » est indispensable. En effet, si ce n'est pas le cas, on peut mettre en défaut la conclusion du **théorème de Gauss 2** : par exemple, prendre $a = 4$, $b = 6$ et $c = 12$. Il est bien vrai que a et b divisent c, mais $ab = 24$ ne divise pas c.

Exemple 3.2.8
Si un nombre entier est divisible par 2 et 3, il est aussi divisible par 6.

3.2.3 Relation entre PGCD et PPCM

Étant donnés deux entiers relatifs a et b, on a vu (**lemme 2.1**) que le PGCD de a et b est le générateur principal du sous-groupe $a\mathbb{Z} + b\mathbb{Z}$. On commence par montrer que le PPCM de a et b réalise aussi une condition similaire :

Lemme 3.2.9
Soient a et b deux entiers relatifs. L'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. Son générateur principal est le PPCM de a et b. De plus, tout multiple commun à a et b est divisible par $ppcm(a, b)$.

Preuve : Il est clair que $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$: cet ensemble n'est pas vide (contient 0) ; et si deux entiers relatifs sont divisibles à la fois par a et b, leur différence l'est aussi.

D'après le **théorème 1.9**, il existe un entier naturel p tel que $a\mathbb{Z} \cap b\mathbb{Z} = p\mathbb{Z}$. Montrons qu'il s'agit du PPCM de a et b. Puisque p est dans $a\mathbb{Z} \cap b\mathbb{Z}$, il est divisible à la fois par a et b : c'est un multiple commun à ces deux nombres.

En outre, si p' est un autre multiple commun à a et b, c'est qu'il est dans $a\mathbb{Z} \cap b\mathbb{Z} = p\mathbb{Z}$. Donc $p|p'$ et en particulier, $p \leqslant p'$.

p est bien plus petit que tous les autres multiples communs à a et b. □

Théorème 3.2.10
Soient a et b deux entiers relatifs. On note $d = pgcd(a,b)$ et $p = ppcm(a,b)$. Alors $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux et $p = \frac{|ab|}{d}$.

Preuve : D'après le **corollaire 2.2**, il existe des entiers relatifs u et v tels que $au + bv = d$. Comme $d|a$ et $d|b$, les nombres $\frac{a}{d}$ et $\frac{b}{d}$ sont entiers. On a alors

$$\frac{a}{d}u + \frac{b}{d}v = 1$$

D'après le **théorème de Bezout**, $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux.

Posons $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$, de sorte que $a = da'$ et $b = db'$. Alors

$$\frac{ab}{d} = \frac{d^2a'b'}{d} = da'b' = ab' = a'b$$

On voit que $\frac{|ab|}{d}$ est un multiple commun à a et b. Montrons que c'est le plus petit.

Soit m un multiple commun à a et b. Il existe des entiers u et v tels que $m = au = bv$. En remplaçant a par da' et b par db', on trouve que $a'u = b'v$. Or, a' et b' sont premiers entre eux ; d'après le **théorème de Gauss 1**, $a'|v$. Il existe un entier relatif c tel que $v = ca'$.
On a alors :

$$m = bv = bca' = \frac{ab}{d}c$$

et

$$\frac{|ab|}{d}\Big|m$$

$\frac{|ab|}{d}$ est bien le PPCM de a et b. □

Corollaire 3.2.11
Si a et b sont deux entiers premiers entre eux, alors $ppcm(a,b) = |ab|$.

3.3 Nombres premiers

Définition 3.3.1 (Nombres premiers)
Soit p un entier naturel. On dira que p *est premier* si, et seulement si, p admet exactement deux diviseurs dans $\mathbb{N}$: 1 et p. On note $\mathscr{P}$ l'ensemble des nombres premiers.

Observons que 1 ne peut être premier d'après cette définition : il n'a qu'un seul diviseur positif, qui est 1. Également, il est immédiat que deux nombres premiers distincts p et q sont premiers entre eux : les diviseurs de p sont 1 et p ; ceux de q sont 1 et q. Comme $p \neq q$, c'est que leur PGCD est 1.

Théorème 3.3.2 (Existence de la décomposition en produit de nombres premiers)
Soit $n \geqslant 2$ un entier naturel. Il existe existe $k \in \mathbb{N}^\star$ et des nombres premiers $p_1, \ldots, p_k$ tels que $n = \prod_{k=1}^{n} p_i$.

Preuve : On démontre ceci par récurrence. Le résultat est vrai pour $n = 2$ puisque 2 est premier.

Soit $n \geqslant 2$; on suppose le théorème démontré pour $2, \dots, n$. Si $n+1$ est premier, il suffit de prendre $p_1 = n+1$. S'il n'est pas premier, c'est qu'il admet soit un seul diviseur, soit au moins trois.

Mais comme $n+1 \neq 1$, il ne peut avoir un seul diviseur. Il en a donc au moins trois. Et parmi eux, il y en a un qui est différent de 1 et de $n+1$; on en choisit un, qu'on note m. On a donc

$$m|(n+1) \qquad m \neq 1 \qquad \text{et} \qquad m \neq n+1$$

En posant $r = \frac{n+1}{m}$, on a en particulier $r \neq 1$ et $r < n+1$. D'après l'hypothèse de récurrence, m et r peuvent s'écrire comme produits de nombres premiers. Par suite, il en est de même pour $n+1 = mr$. □

Le lemme suivant sera utile pour établir l'unicité de cette décomposition :

Lemme 3.3.3
Soient $k \in \mathbb{N}^\star$, $p_1, \dots, p_k$ des nombres premiers distincts deux-à-deux et $\alpha_1, \dots, \alpha_k$ des entiers naturels non nuls. Si p est un nombre premier qui divise $\prod_{j=1}^{k} p_j^{\alpha_j}$, alors il existe un unique $i \in [\![1\,;k]\!]$ tel que $p = p_i$.

Preuve : Supposons l'existence fausse, c'est-à-dire que l'ensemble $\mathscr{A}$ des entiers n tels que

- il existe des entiers naturels non nuls $\alpha_1, \dots, \alpha_k$ tels que $n = \prod_{j=1}^{k} p_j^{\alpha_j}$;
- il existe p premier divisant n, mais $p \notin \{p_1, \dots, p_k\}$.

n'est pas vide. Il s'agit d'une partie de $\mathbb{N}$ qui admet donc un plus petit élément. Il existe donc des entiers naturels non nuls $v_1, \dots, v_k$ tels que

$$n = \prod_{j=1}^{k} p_j^{v_j} = \operatorname{Min} \mathscr{A}$$

Puisque $v_1 > 0$, on a

$$n = p_1 \times p_1^{v_1 - 1} \times \prod_{j=2}^{k} p_j^{v_j}$$

Soit p un diviseur premier de n, distinct de $p_1, \dots, p_k$. Puisque p et p_1 sont premiers entre eux, le **théorème de Gauss 1** assure que

$$p | p_1^{v_1 - 1} \prod_{j=2}^{k} p_j^{v_j} \qquad \text{et du coup} \qquad p_1^{v_1 - 1} \prod_{j=2}^{k} p_j^{v_j} \in \mathscr{A}$$

Mais cet entier est inférieur à n, puisqu'il vaut $\frac{n}{p_1}$. Ceci contredit le fait que $n = \operatorname{Min} \mathscr{A}$. Donc $\mathscr{A}$ est vide : pour tout diviseur premier p d'un entier de la forme $\prod_{j=1}^{k} p_j^{\alpha_j}$ avec $\alpha_1, \dots, \alpha_k$ entiers naturels non nul, il existe $i \in [\![1\,;k]\!]$ tel que $p = p_i$.

Comme $p_1, \dots, p_k$ sont distincts, cet i est en fait unique. □

Théorème 3.3.4 (Unicité de la décomposition en produit de nombres premiers)
Soit $n \geqslant 2$ un entier. Il existe un unique entier naturel k non nul, une unique famille $p_1 < \cdots < p_k$ de nombres premiers et une unique famille $(\alpha_1, \dots, \alpha_k)$ d'entiers naturels non nuls, tels que

$$n = \prod_{j=1}^{k} p_j^{\alpha_j}$$

Preuve : L'existence d'une telle famille est assurée par le théorème précédent. Reste à montrer l'unicité.

Soient des entiers k, ℓ non nuls, des nombres premiers $p_1 < \cdots < p_k$ et $q_1 < \cdots < q_\ell$, et des familles $(\alpha_1, \ldots, \alpha_k)$ et $(\beta_1, \ldots, \beta_\ell)$ d'entiers naturels non nuls, tels que

$$n = \prod_{j=1}^{k} p_j^{\alpha_j} = \prod_{j=1}^{\ell} q_j^{\beta_j}$$

Notons $\mathrm{P} = \{p_1, \ldots, p_k\}$ et $\mathrm{Q} = \{q_1, \ldots, q_\ell\}$. D'après le **lemme 3.3**, $\mathrm{Q} \subset \mathrm{P}$ et $\mathrm{P} \subset \mathrm{Q}$. Donc $\mathrm{P} = \mathrm{Q}$ et en particulier $k = \ell$. Comme il y a un unique manière d'ordonner une famille d'entiers naturels distincts (voir cours sur les ensembles finis), on en déduit que

$$p_1 = q_1 \qquad p_2 = q_2 \qquad \cdots \qquad p_k = q_k$$

Il ne reste qu'à montrer que les exposants coïncident. Pour cela, on considère l'ensemble

$$\mathrm{A} = \{i \in [\![1 ; k]\!] \mid \alpha_i \neq \beta_i\}$$

Supposons A non vide. Il admet alors un plus petit élément noté j. Rappelons que

$$\prod_{i=1}^{k} p_i^{\alpha_i} = \prod_{i=1}^{k} p_i^{\beta_i}$$

Par définition de j, on peut simplifier les termes communs aux deux membres pour obtenir :

$$\prod_{i=j}^{k} p_i^{\alpha_i} = \prod_{i=j}^{k} p_i^{\beta_i}$$

Comme $\alpha_j \neq \beta_j$, on peut suppose, par exemple, que c'est α_j qui est strictement inférieur à β_j. Alors, en simplifiant par $p_j^{\alpha_j}$, on voit que

$$p_j \mid \prod_{i=j+1}^{k} p_i^{\alpha_i}$$

D'après le **lemme 3.3**, p_j appartient à $\{p_{j+1}, \ldots, p_k\}$. C'est impossible, puisque $p_j < p_{j+1}$.

Donc A est vide et

$$\forall i \in [\![1 ; k]\!] \qquad \alpha_i = \beta_i$$

Ce qui achève la démonstration. □

Ce théorème peut être reformulé de manière plus agréable une fois introduite la notion de

Définition 3.3.5 (Support d'un entier)
Soit $n \geqslant 2$ un entier naturel. On appelle *support de n* l'ensemble des nombres premiers qui divisent n :

$$\mathrm{Supp}\,(n) = \{p \in \mathscr{P} \mid p | n\}$$

Théorème 3.3.6 (Existence et unicité de la décomposition en produit de nombres premiers)
Soit $n \geqslant 2$ un entier naturel. Il existe une unique famille $(v_p(n))_{p \in \mathscr{P}}$ d'entiers naturels telle que

$$n = \prod_{p \in \mathscr{P}} p^{v_p(n)}$$

Évidemment, ce produit est fini puisque si $p \notin \mathrm{Supp}\,(n)$, le nombre v_p est nul donc $p^{v_p} = 1$. Le nombre $v_p(n)$ est appelé *valuation p-adique de n*.

Chapitre 4

Introduction à l'algèbre linéaire

Dans tous les chapitres du cours d'algèbre, la lettre $\mathbb{K}$ désigne un corps commutatif.

4.1 Espaces Vectoriels

4.1.1 Définition et exemples

Définition 4.1.1
Soit $(E,+)$ un groupe commutatif d'élément neutre 0. On dit que E est muni d'une structure de $\mathbb{K}$-*espace vectoriel* si, et seulement si, il existe une application

$$\begin{aligned} \mathbb{K}\times E &\longrightarrow E \\ (\lambda, x) &\longmapsto \lambda\cdot x \end{aligned}$$

satisfaisant les propriétés suivantes :

1. $\forall (x,y)\in E^2 \quad \forall \lambda\in\mathbb{K} \qquad \lambda\cdot(x+y)=\lambda\cdot x+\lambda\cdot y$
2. $\forall (\lambda,\mu)\in\mathbb{K}^2 \quad \forall x\in E \qquad (\lambda+\mu)\cdot x=\lambda\cdot x+\mu\cdot y$
3. $\forall (\lambda,\mu)\in\mathbb{K}^2 \quad \forall x\in E \qquad \lambda\cdot(\mu\cdot x)=(\lambda\mu)\cdot x$
4. $\forall x\in E \qquad 1\cdot x=x$

Les éléments de E sont alors appelés *vecteurs* et ceux de $\mathbb{K}$ sont appelés *scalaires*. L'opération + est appelée *addition* et l'opération $\cdot$ est appelée *multiplication externe*.

Beaucoup d'objets étudiés jusqu'à présent sont des espaces vectoriels. Voici des exemples :

Exemple 4.1.2

1. $\mathbb{R}$ est un $\mathbb{R}$-espace vectoriel.
2. $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel et un $\mathbb{C}$-espace vectoriel.
3. Le plan vectoriel $\overrightarrow{\mathscr{P}}$ est un espace vectoriel sur $\mathbb{R}$.
4. L'espace vectoriel de dimension 3 $\overrightarrow{\mathscr{E}}$ est un $\mathbb{R}$-espace vectoriel.
5. Plus généralement, si $n\geqslant 1$, l'ensemble $\mathbb{K}^n$ est un $\mathbb{K}$-espace vectoriel lorsqu'on a défini les opérations suivantes :

$$\forall (x_1,\dots,x_n)\in\mathbb{K}^n \quad \forall (y_1,\dots,y_n)\in\mathbb{K}^n \qquad (x_1,\dots,x_n)+(y_1,\dots,y_n)=(x_1+y_1,\dots,x_n+y_n)$$

et

$$\forall (x_1,\dots,x_n)\in\mathbb{K}^n \quad \forall \lambda\in\mathbb{R} \qquad \lambda\cdot(x_1,\dots,x_n)=(\lambda x_1,\dots,\lambda x_n)$$

6. Si A est un ensemble non vide et E est un $\mathbb{K}$-espace vectoriel, l'ensemble $\mathscr{F}(A,E)$ est un $\mathbb{K}$-espace vectoriel lorsqu'on le munit des opérations

$$\forall (f,g) \in \mathscr{F}(A,E)^2 \quad \forall a \in A \qquad (f+g)(a) = f(a) + g(a)$$

et $$\forall f \in \mathscr{F}(A,E) \quad \forall \lambda \in \mathbb{K} \quad \forall a \in A \qquad (\lambda \cdot f)(a) = \lambda \cdot (f(a))$$

En particulier, l'ensemble des fonctions de A dans $\mathbb{K}$ est un espace vectoriel sur $\mathbb{K}$.

4.1.2 Règles de calcul

Les propriétés définissant un espace vectoriel sont le minimum vital pour pouvoir travailler avec ces objets. Comme (E, +) est un groupe commutatif, on sait déjà (voir le chapitre sur les structures) que 0_E est l'unique élement neutre pour l'addition et que tout élément de E admet un unique opposé.

Nous allons donc, dans cette partie, élaborer sur la **définition 1.1** pour obtenir les autres règles de calcul élémentaires dans un espace vectoriel.

On commence par rappeler :

Proposition 4.1.3
Soit E *un* $\mathbb{K}$*-espace vectoriel. L'ensemble*

$$\{e \in E \mid \forall x \in E \quad x + e = e + x = x\}$$

est un singleton.

Preuve : Déjà fait dans le chapitre sur les structures algébriques. □

Proposition 4.1.4
Soit E *un* $\mathbb{K}$*-espace vectoriel, soit* $x \in E$*. L'ensemble*

$$\{y \in E \mid x + y = y + x = 0_E\}$$

est un singleton. L'unique élément qu'il contient est noté $-x$*.*

Preuve : Même chose. □

Corollaire 4.1.5
Soit E *un espace vectoriel. Alors*

$$\forall x \in E \qquad 0_{\mathbb{K}} \cdot x = 0_E$$

$$\forall \lambda \in \mathbb{K} \qquad \lambda \cdot 0_E = 0_E$$

et enfin $$\forall \lambda \in \mathbb{K} \quad \forall x \in E \qquad \lambda \cdot x = 0_E \iff x = 0_E \text{ ou } \lambda = 0_{\mathbb{K}}$$

Preuve : Soit $x \in E$. D'après le point *2* de la **définition 1.1**,

$$0_{\mathbb{K}} \cdot x = (0_{\mathbb{K}} + 0_{\mathbb{K}}) \cdot x = 0_{\mathbb{K}} \cdot x + 0_{\mathbb{K}} \cdot x$$

On ajoute aux deux membres de cette égalité le vecteur $-0_{\mathbb{K}} \cdot x$ pour conclure :

$$0_E = 0_{\mathbb{K}} \cdot x$$

Pour le second point, on procède de manière similaire. Soit $\lambda \in \mathbb{K}$. D'après le point *2* de la **définition 1.1**,

$$\lambda \cdot 0_E = \lambda \cdot (0_E + 0_E) = \lambda \cdot 0_E + \lambda \cdot 0_E$$

On ajoute alors aux deux membres le vecteur $-(\lambda \cdot 0_E)$ pour obtenir

$$0_E = \lambda \cdot 0_E$$

Le dernier point est une équivalence, dont une direction vient d'être démontrée. On prouve l'autre direction. Soient $x \in E$ et $\lambda \in \mathbb{K}$ tels que $\lambda \cdot x = 0_E$. Soit λ est nul, auquel cas on a fini ; soit λ n'est pas nul, auquel cas on peut écrire, d'après les règles *3* et *4* de la **définition 1.1**,

$$x = 1 \cdot x = (\lambda^{-1}\lambda) \cdot x = \lambda^{-1} \cdot (\lambda \cdot x) = \lambda^{-1} \cdot 0_E = 0_E \qquad \square$$

Corollaire 4.1.6
Soit E *un* $\mathbb{K}$*-espace vectoriel. Alors*

$$\forall x \in E \qquad (-1) \cdot x = -x$$

Preuve : Soit x un élément quelconque de E. Pour établir que $(-1) \cdot x$ n'est autre que $-x$, il suffit de montrer, d'après la **proposition 1.4**, que $(-1) \cdot x + x = 0_E$. On utilise les règles *4* et *2* de la **définition 1.1** ainsi que le **corollaire 1.5** :

$$(-1) \cdot x + x = (-1) \cdot x + 1 \cdot x = (-1+1) \cdot x = 0_{\mathbb{K}} \cdot x = 0_E \qquad \square$$

Corollaire 4.1.7
Soit E *un espace vectoriel. On a*

$$\forall \lambda \in \mathbb{K} \quad \forall x \in E \qquad -(\lambda \cdot x) = (-\lambda) \cdot x$$

Preuve : Soient $x \in E$ et $\lambda \in \mathbb{K}$. D'après le **corollaire 1.5** et le point *3* de la **définition 1.1**,

$$-(\lambda \cdot x) = (-1) \cdot (\lambda \cdot x) = (-1 \times \lambda) \cdot x = (-\lambda) \cdot x \qquad \square$$

Corollaire 4.1.8
Soit E *un espace vectoriel. On a*

$$\forall \lambda \in \mathbb{K} \quad \forall (x, y) \in E^2 \qquad \lambda \cdot (x - y) = \lambda \cdot x - \lambda \cdot y$$

et

$$\forall (\lambda, \mu) \in \mathbb{K} \quad \forall x \in E \qquad (\lambda - \mu) \cdot x = \lambda \cdot x - \mu \cdot y$$

Preuve : C'est simple, d'après tout ce qui précède. En effet, si λ est un scalaire et x, y sont deux vecteurs,

$$\lambda \cdot (x - y) = \lambda \cdot x + \lambda \cdot (-y) = \lambda \cdot x + \lambda \cdot (-1 \cdot y) = \lambda \cdot x + (-\lambda \cdot y) = \lambda \cdot x - \lambda \cdot y$$

De même, si λ et μ sont deux scalaires et x est un vecteur,

$$(\lambda - \mu) \cdot x = \lambda \cdot x + (-\mu \cdot x) = \lambda \cdot x - \mu \cdot x \qquad \square$$

Toutes ces propriétés montrent qu'au final, la multiplication externe et l'addition se manipulent de la même manière que le produit ou l'addition usuels sur les réels, avec les mêmes règles de distributivité, de signes, le fait qu'un produit est nul si et seulement si l'un des termes est nul,

etc. Donc, comme tout marche comme d'habitude, on laisse tomber la notation $\lambda \cdot x$ et on écrira simplement λx.

De même, on abandonne les 0_E et $0_{\mathbb{K}}$ pour la notation uniforme 0, en sachant que le contexte rendra clair à chaque fois de quel 0 il s'agit.

4.1.3 Sous-espaces vectoriels

L'un des buts de l'algèbre est d'étudier des ensembles, munis d'une structure (règles de calcul), de la manière la plus générale possible. Pour certaines structures algébriques, il y a besoin de livres entiers pour faire cela. Pour d'autres, comme les espaces vectoriels, deux années de cours suffisent. Mais dans tous les cas, le plan d'étude est de décomposer notre gros ensemble en sous-ensembles ayant la même structure algébrique, puis de les décomposer eux-mêmes, et encore et encore, en espérant qu'à un moment on aura atteint un état « irréductible » de la structure étudiée, suffisamment simple pour qu'il puisse être compris entièrement. C'est la raison pour laquelle on introduit la notion de sous-espace :

Définition 4.1.9
Soit E un $\mathbb{K}$-espace vectoriel. Soit $F \subset E$. On dira que F est un $\mathbb{K}$-sous-espace vectoriel de E si et seulement si F, muni de la restriction à $F \times F$ de l'addition, et de la restriction à $\mathbb{K} \times F$ de la multiplication, est un $\mathbb{K}$-espace vectoriel.

Montrer qu'une partie F d'un espace vectoriel E est un sous-espace vectoriel requiert *a priori* la vérification des 4 propriétés de la **définition 1.1**. C'est douloureux et on donne un critère permettant de vérifier sans trop de mal si F est ou pas un sous-espace vectoriel de E.

Théorème 4.1.10
Soit E *un* $\mathbb{K}$*-espace vectoriel. Soit* F *un sous-ensemble de* E. F *est un sous-espace vectoriel de* E *si et seulement si* F *n'est pas vide et*

$$\forall (x,y) \in F^2 \quad \forall \lambda \in \mathbb{K} \qquad \lambda x - y \in F \tag{1}$$

Preuve : Il est clair que si F est un sous-espace vectoriel de E, il n'est pas vide (il contient 0) et il vérifie la propriété énoncée dans la proposition.

Réciproquement, soit F un sous-ensemble de E, non vide, tel que

$$\forall (x,y) \in F^2 \quad \forall \lambda \in \mathbb{K} \qquad \lambda x - y \in F$$

En particulier,
$$\forall x, y \in F \qquad x - y \in F$$

donc $(F,+)$ est un sous-groupe de $(E,+)$.

Puis on prend x quelconque dans F, $y = 0$ et λ quelconque dans $\mathbb{K}$ et on applique la propriété (**1**). On conclut que $\lambda x \in F$. Donc la multiplication externe, restreinte à $\mathbb{K} \times F$ prend bien ses valeurs dans F.

Ces opérations vérifient clairement les propriétés *1*, *2*, *3* et *4* d'un espace vectoriel, dans la mesure où $F \subset E$. □

Exemple 4.1.11
À l'aide du **théorème 1.10**, il est quasiment immédiat que les ensembles suivant sont des espaces vectoriels :

1. $i\mathbb{R}$ est un $\mathbb{R}$-espace vectoriel (sous-espace de $\mathbb{C}$) ;

2. l'ensemble des fonctions de $\mathbb{R}$ dans lui-même, admettant une limite nulle en $+\infty$ (sous-espace de $\mathbb{R}^{\mathbb{R}}$) ;
3. l'ensemble des fonctions continues sur $\mathbb{R}$ (sous-espace de $\mathbb{R}^{\mathbb{R}}$) ;
4. l'ensemble des fonctions polynomiales de degré inférieur ou égal à un entier n donné (sous-espace de $\mathbb{R}^{\mathbb{R}}$).
5. et plein d'autres.

En revanche, l'ensemble $\left\{x \in \mathbb{R}^n \mid \sum_{i=1}^{n} x_i = 1\right\}$ n'est pas un sous-espace vectoriel de $\mathbb{R}^n$. De même que l'ensemble des fonctions sur $\mathbb{R}$ qui tendent vers $26,92$ en $+\infty$. Pour une raison très simple : aucun d'eux ne contient 0.

On peut se demander quelles opérations laissent stables les sous-espaces vectoriels. Si l'union de deux sous-espaces vectoriels n'est pas toujours un sous-espace vectoriel, on a en revanche :

Théorème 4.1.12
Soit E *un* $\mathbb{K}$*-espace vectoriel. Soit* $\mathscr{F}$ *une famille quelconque, non vide, de sous-espaces vectoriels de* E. *L'ensemble* $\mathrm{G} = \bigcap_{\mathrm{F}\in\mathscr{F}} \mathrm{F}$ *est un sous-espaces vectoriel de* E.

Preuve : Il suffit d'appliquer le critère donné par le **théorème 1.10**. D'une part, G n'est pas vide puisqu'il contient le vecteur nul. D'autre part, donnons-nous x et y dans G et λ un scalaire. Par définition de G,

$$\forall \mathrm{F} \in \mathscr{F} \qquad x \in \mathrm{F} \qquad \text{et} \qquad y \in \mathrm{F}$$

Si F est un élément quelconque de $\mathscr{F}$, c'est un sous-espace vectoriel de E donc $\lambda x - y$ s'y trouve. Ceci étant établi pour tout $\mathrm{F} \in \mathscr{F}$, on a montré que

$$\lambda x - y \in \bigcap_{\mathrm{F}\in\mathscr{F}} \mathrm{F} = \mathrm{G}$$

C'est tout ce dont on a besoin pour conclure : G est un sous-espace de E. □

4.1.4 Sous-espace engendré par une partie de E

Théorème 4.1.13
Soit E *un* $\mathbb{K}$*-espace vectoriel. Soit* A *une partie de* E. *Il existe un unique sous-espace vectoriel de* E *contenant* A, *qui soit contenu dans tous les sous-espaces vectoriels de* E *contenant* A. *On l'appelle sous-espace de* E *engendré par* A *et on le note Vect*A, *qui se lit vectorialisé de* A.

Preuve : On note $\mathscr{F}$ l'ensemble de tous les sous-espaces vectoriels de E qui contiennent A. Évidemment, la famille $\mathscr{F}$ n'est pas vide : elle contient E, qui est bien un sous-espace vectoriel de E contenant A. D'après le **théorème 1.12**, l'ensemble

$$\mathrm{G} = \bigcap_{\mathrm{F}\in\mathscr{F}} \mathrm{F}$$

est un sous-espace vectoriel de E.

Évidemment, G contient A : tout élément de $\mathscr{F}$ contient A, donc leur intersection doit aussi contenir A.

Enfin, par définition de G, il est contenu dans n'importe quel élément de $\mathscr{F}$; c'est-à-dire que tout sous-espace contenant A contient G. C'est ce qu'on voulait. □

Bien entendu, cette présentation de VectA comme intersection d'une tonne de sous-espaces vectoriels de E n'est pas très agréable et on souhaiterait caracteriser ses éléments autrement. On introduit pour cela la notion de combinaison linéaire.

Définition 4.1.14 (Combinaison linéaire)
Soit A une partie non vide de E. On dit d'un élément x de E qu'il est une combinaison linéaire finie d'éléments de A si et seulement si

$$\exists n \in \mathbb{N}^\star \quad \exists (a_1, \dots, a_n) \in \mathrm{A}^n \quad \exists (\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n \qquad x = \sum_{k=1}^{n} \lambda_k a_k$$

Si A est vide, on décide par convention que 0 est la seule combinaison linéaire de A.

En français, une combinaison linéaire d'éléments de A, c'est une somme finie d'éléments de A, affectés de coefficients scalaires.

Théorème 4.1.15
Soit E *un* $\mathbb{K}$*-espace vectoriel. Soit* A *une partie de* E. *Le sous-espace engendré par* A *est l'ensemble de toutes les combinaisons linéaires finies d'éléments de* A.

Preuve : Notons CombA l'ensemble de toutes les combinaisons linéaires finies d'éléments de A et montrons que CombA = VectA. On pourrait procéder par double inclusion, mais on peut aussi utiliser le **théorème 1.13** qui caractérise VectA comme étant l'unique sous-espace de E contenant A, contenu dans tout sous-espace contenant A.

Autrement dit, si on montre que

1. CombA est un sous-espace vectoriel de E ;
2. CombA contient A ;
3. CombA est contenu dans tout sous-espace de E qui contient A,

alors automatiquement, CombA ne peut être que VectA.

Le deuxième point est trivial : tout élément de A est une combinaison linéaire d'éléments de A.

Le premier point est clair aussi, à la lumière du **théorème 1.10** : soient x et y des éléments de CombA, soit $\lambda \in \mathbb{K}$. Les vecteurs x et y sont des sommes finies d'éléments de A affectés de coefficients scalaires ; donc $\lambda x - y$ est aussi une somme finie d'éléments de A affectés de coefficients. C'est-à-dire que $\lambda x - y$ est une combinaison linéaire de A.

Enfin, le troisième point n'est pas plus difficile à prouver. Si F est un sous-espace vectoriel de E contenant A, il doit aussi contenir toute combinaison linéaire finie d'éléments de A. □

4.1.5 Somme de deux sous-espaces vectoriels

On a dit plus haut qu'en général, l'union de deux sous-espaces vectoriels F et G n'en est pas un. Mais on peut en créer un qui soit le plus économique possible, grâce au **théorème 1.13** : on sait que Vect (F ∪ G) sera un sous-espace vectoriel, contenant F et G, et le plus petit possible réalisant cette propriété.

Définition 4.1.16
Soit E un $\mathbb{K}$-espace vectoriel. Soient F et G deux sous-espaces vectoriels de E. Le sous-espace engendré par F ∪ G est appelé *somme de* F *et* G, et on le note F + G.

Proposition 4.1.17
Soit E *un* $\mathbb{K}$*-espace vectoriel. Soient* F *et* G *deux sous-espaces vectoriels de* E. *On a*

$$F+G=\{x+y \mid x\in F \quad y\in G\}$$

Preuve : Soit H l'ensemble $\{x+y \mid x\in F \quad y\in G\}$. On prouve le théorème de la même manière que dans la preuve du **théorème 1.15**, dans la mesure où F+G = Vect (F∪G) est le plus petit sous-espace de E contenant F et G.

Il est immédiat que H contient F et G, puisque tout élément de F ou de G est une somme d'un élément de F et d'un élément de G.

H est aussi un sous-espace vectoriel de E, en vue du **théorème 1.10**.

Et tout sous-espace de E contenant F ∪ G doit contenir au grand minimum les sommes d'éléments de F et G. Donc doit contenir H.

D'après le **théorème 1.15**, H est le sous-espace de E engendré par F ∪ G. □

4.1.6 Sous-espaces en somme directe

Définition 4.1.18
Soit E un $\mathbb{K}$-espace vectoriel. Soient F et G deux sous-espaces vectoriels de E. On dit qu'*ils sont en somme directe* si et seulement si $F\cap G=\{0\}$. On notera leur somme $F\oplus G$.

L'intérêt de la notion de somme directe est rendu évident par le théorème suivant :

Théorème 4.1.19
Soit E *un* $\mathbb{K}$*-espace vectoriel. Soient* F *et* G *deux sous-espaces vectoriels de* E. *Ils sont en somme directe si et seulement si*

$$\forall z\in F+G \quad \exists!(x,y)\in F\times G \qquad z=x+y$$

Preuve : On suppose que F et G sont en somme directe, c'est-à-dire que $F\cap G=\{0\}$. Soit $z\in F+G$; d'après la **proposition 1.17**, il existe $x\in F$ et $y\in G$, tels que $z=x+y$. Supposons qu'on ait aussi $x'\in F$ et $y'\in G$, tels que $z=x'+y'$. Alors

$$x+y=x'+y'$$

d'où

$$x-x'=y'-y$$

Or, F et G sont des sous-espaces vectoriels de E donc $x-x'\in F$ et $y-y'\in G$. Mais ces deux vecteurs sont égaux donc leur valeur commune est dans $F\cap G$. Ce dernier sous-espace est réduit à $\{0\}$. Donc

$$x-x'=0 \qquad \text{et} \qquad y-y'=0$$

ou encore

$$x'=x \qquad \text{et} \qquad y'=y$$

Réciproquement, on suppose que

$$\forall z\in F+G \qquad \exists!(x,y)\in F\times G \qquad z=x+y$$

En particulier, $0=0+0$ est la seule et unique manière de décomposer 0 comme somme d'un élément de F et d'un élément de G. Soit $z\in F\cap G$. Alors $z-z=0$ est une décomposition de 0 comme somme d'un élément de F et d'un élément de G. Donc $z=0$; par suite, $F\cap G=\{0\}$. Ces sous-espaces sont en somme directe. □

Définition 4.1.20
Soit E un $\mathbb{K}$-espace vectoriel. Soient F et G deux sous-espaces vectoriels de E. On dit qu'ils sont supplémentaires dans E si et seulement si

$$E = F \oplus G$$

Exemple 4.1.21
Considérons l'espace vectoriel $E = \mathbb{C}^{\mathbb{R}}$. On note P le sous-espace vectoriel des applications paires et I le sous-espace vectoriel des applications impaires. Ces sous-espaces sont supplémentaires dans E.

En effet, ils sont en somme directe : si f est une fonction à la fois paire et impaire,

$$\forall x \in \mathbb{R} \qquad f(x) = f(-x) = -f(x)$$

donc

$$\forall x \in \mathbb{R} \qquad f(x) = 0$$

et

$$P \cap I = \{0\}$$

Et leur somme est égale à E tout entier. En effet, si f est une fonction complexe d'une variable réelle, on peut écrire

$$\forall x \in \mathbb{R} \qquad f(x) = \frac{f(x) + f(-x)}{2} + \frac{f(x) - f(-x)}{2}$$

Les fonctions

$$g : x \longmapsto \frac{f(x) + f(-x)}{2} \qquad \text{et} \qquad h : x \longmapsto \frac{f(x) - f(-x)}{2}$$

sont respectivement paire et impaire. On les appelle naturellement partie paire et partie impaire de f.

Par exemple, ch est la partie paire de l'exponentielle, tandis que sh est sa partie impaire. Également, cos est la partie impaire de $x \longmapsto e^{ix}$ tandis que i sin est sa partie impaire.

Si E est un $\mathbb{K}$-espace vectoriel, tel que F et G sont supplémentaires dans E, on voit que tout z de E peut être décomposé de manière unique sous la forme $z = x + y$, avec $x \in F$ et $y \in G$. Le premier est appelé *projection de z sur* F *parallèlement à* G, et on le note $p_F(z)$. L'autre est appelé *projection de z sur* G *parallèlement à* F et on le note $p_G(z)$.

4.2 Applications linéaires

Les applications linéaires sont les applications entre espaces vectoriels qui sont compatibles avec la structure d'espace vectoriel. Cela sera rendu plus précis immédiatement. Puis on étudiera les propriétés immédiates de ces opérations.

4.2.1 Définitions

Définition 4.2.1
Soient E et F deux $\mathbb{K}$-espaces vectoriels. Soit f une application de E dans F. On dit que f est linéaire si et seulement si

$$\forall (x, y) \in E^2 \quad \forall \lambda \in \mathbb{K} \qquad f(\lambda x + y) = \lambda f(x) + f(y)$$

L'ensemble des applications linéaires de E dans F est noté $\mathscr{L}(E, F)$.

Théorème 4.2.2
Soient E *et* F *deux* $\mathbb{K}$*-espaces vectoriels. L'ensemble* $\mathscr{L}(E, F)$ *est un sous-espace vectoriel de* F^E.

Preuve : Bien évidemment, l'application nulle est linéaire donc $\mathscr{L}(E,F)$ n'est pas vide.

Soient f et g deux applications linéaires de E dans F, soit λ un scalaire arbitraire. On souhaite montrer que $\lambda f + g$ est linéaire. Il suffit de valider la définition :

$$\begin{aligned}\forall (x,y)\in E^2 \quad \forall \mu \in \mathbb{K} \qquad (\lambda f+g)(\mu x+y) &= (\lambda f)(\mu x+y) + g(\mu x+y)\\ &= \lambda f(\mu x+y) + \mu g(x) + g(y)\\ &= \mu\lambda f(x) + \lambda f(y) + \mu g(x) + g(y)\\ &= \mu(\lambda f(x) + g(x)) + \lambda f(y) + g(y)\\ (\lambda f+g)(\mu x+y) &= \mu(\lambda f+g)(x) + (\lambda f+g)(y)\end{aligned}$$

On voit que $\lambda f + g$ est linéaire. D'après le **théorème 1.10**, $\mathscr{L}(E,F)$ est un sous-espace vectoriel de F^E. □

Définition 4.2.3
Soit E un $\mathbb{K}$-espace vectoriel. L'ensemble $\mathscr{L}(E,E)$ est noté de manière plus abrégée $\mathscr{L}(E)$. Ses éléments sont appelés endomorphismes de E.

Proposition 4.2.4
Soient E *et* F *deux* $\mathbb{K}$*-espaces vectoriels. Soit* $f \in \mathscr{L}(E,F)$*, bijective. Alors* f^{-1} *est linéaire, c'est-à-dire que* $f^{-1} \in \mathscr{L}(F,E)$.

Preuve : Soient y_1 et y_2 dans F, soit λ un scalaire. Comme f est bijective, on a

$$y_1 = f(f^{-1}(y_1)) \qquad \text{et} \qquad y_2 = f(f^{-1}(y_2))$$

d'où
$$\lambda y_1 + y_2 = \lambda f(f^{-1}(y_1)) + f(f^{-1}(y_2))$$

Comme f est linéaire, il vient

$$\lambda y_1 + y_2 = f\big(\lambda f^{-1}(y_1) + f^{-1}(y_2)\big)$$

Il suffit d'appliquer f^{-1} :

$$f^{-1}(\lambda y_1 + y_2) = \lambda f^{-1}(y_1) + f^{-1}(y_2)$$ □

Définition 4.2.5
Une application linéaire bijective entre espaces vectoriels est appelée *isomorphisme d'espaces vectoriels*.

Si E et F sont des $\mathbb{K}$-espaces vectoriels, et s'il existe un isomorphisme de E sur F, on dit que E et F sont *isomorphes*.

Définition 4.2.6
Soit E un $\mathbb{K}$-espace vectoriel. Un isomorphisme de E dans lui-même est appelé *automorphisme de* E. Leur ensemble est noté $\mathscr{GL}(E)$, et on l'appelle *groupe linéaire de* E. Autrement dit,

$$\mathscr{GL}(E) = \{f \in \mathscr{L}(E) \mid f \text{ bijective}\}$$

Définition 4.2.7
Soit E un $\mathbb{K}$-espace vectoriel. L'ensemble $\mathscr{L}(E,\mathbb{K})$ est appelé *dual* de E. Ses éléments sont appelés des *formes linéaires*.

4.2.2 Noyau et image

Définition 4.2.8
Soient E et F deux $\mathbb{K}$-espaces vectoriels. Soit $f \in \mathscr{L}(E,F)$. On appelle *noyau de* f l'ensemble

$$\operatorname{Ker} f = f^{-1}(\{0\}) = \{x \in E \mid f(x) = 0\}$$

On appelle *image de* F l'ensemble

$$\operatorname{Im} f = f(E) = \{f(x) \mid x \in E\} = \{y \in F \mid \exists x \in E \quad f(x) = y\}$$

Théorème 4.2.9
Soient E *et* F *deux* $\mathbb{K}$*-espaces vectoriels. L'image par* f *de tout sous-espace vectoriel de* E *est un sous-espace vectoriel de* F. *L'image réciproque par* f *de tout sous-espace vectoriel de* F *est un sous-espace vectoriel de* E. *En particulier,* $\operatorname{Ker} f$ *et* $\operatorname{Im} f$ *sont des sous-espaces vectoriels, respectivement de* E *et* F.

Preuve : On se donne E′ un sous-espace de E. L'image de E′ est

$$f(E') = \{f(x) \mid x \in E'\}$$

Bien entendu, $f(E')$ n'est pas vide puisqu'il contient 0 :

$$f(0) = f(0+0) = f(0) + f(0) \qquad \text{et} \qquad f(0) = 0$$

Ensuite, soient y_1 et y_2 dans $f(E')$, et $\lambda \in \mathbb{K}$. Par définition de $f(E')$, il existe $x_1, x_2 \in E'$ tels que

$$y_1 = f(x_1) \qquad \text{et} \qquad y_2 = f(x_2)$$

Par suite, $$\lambda y_1 - y_2 = \lambda f(x_1) - f(x_2) = f(\lambda x_1 - x_2)$$

en utilisant la linéarité de f. Or, E′ est un sous-espace vectoriel de E donc $\lambda x_1 - x_2$ s'y trouve. Il s'ensuit que $\lambda y_1 - y_2$ appartient à $f(E')$. Ce qui achève de montrer que cet ensemble est un sous-espace vectoriel de F.

À présent, soit F′ un sous-espace vectoriel de F. On rappelle que

$$f^{-1}(F') = \{x \in E \mid f(x) \in F'\}$$

Bien entendu, $f^{-1}(F')$ contient 0 puisque $f(0) = 0 \in F'$. Puis on se donne x_1 et x_2 dans $f^{-1}(F')$, ainsi que λ un scalaire. On a

$$f(\lambda x_1 - x_2) = \lambda f(x_1) - f(x_2)$$

Puisque $f(x_1)$ et $f(x_2)$ appartiennent à F′ et que ce dernier est un espace vectoriel, on voit que $f(\lambda x_1 - x_2)$ appartient à F′. Autrement dit, $\lambda x_1 - x_2$ est dans $f^{-1}(F')$, qui est donc un sous-espace de E. □

Proposition 4.2.10
Soient E *et* F *deux* $\mathbb{K}$*-espaces vectoriels. Soit* $f \in \mathscr{L}(E,F)$.

1. f *est injective si et seulement si* $\operatorname{Ker} f = \{0\}$.
2. f *est surjective si et seulement si* $\operatorname{Im} f = F$.

Preuve : La deuxième proposition est une tautologie. Pour la première, supposons f injective. Comme $f(0) = 0$, 0 est l'unique antécédent de 0. C'est-à-dire que $\operatorname{Ker} f = \{0\}$.

Réciproquement, si cette proposition est satisfaite, montrons que f est injective. Soient x et y dans E, tels que $f(x) = f(y)$. Alors

$$0 = f(x) - f(y) = f(x-y)$$

donc $x-y$ appartient au noyau de f. Ce dernier est réduit à $\{0\}$ donc $x-y=0$. Ou encore $x=y$. f est injective. □

Théorème 4.2.11
Soient E *et* F *deux* $\mathbb{K}$*-espaces vectoriels. Soit* $f \in \mathscr{L}(E,F)$. *Tout supplémentaire de Ker* f *est isomorphe à Im* f.

Preuve : L'énoncé fait plus peur qu'il ne le devrait... On se donne G un supplémentaire de $\operatorname{Ker} f$, de sorte que $\operatorname{Ker} f \oplus G = E$ et on pose

$$\forall x \in G \qquad b(x) = f(x)$$

On définit ainsi une application $b : G \longrightarrow \operatorname{Im} f$, qui se comporte exactement comme f sur G. Du coup, il est clair que b est linéaire. Montrons qu'elle est bijective. D'une part

$$\operatorname{Ker} b = \{x \in G \mid b(x) = 0\} = \{x \in G \mid f(x) = 0\} = \operatorname{Ker} f \cap G = \{0\}$$

D'après la **proposition 2.10**, b est injective.

Puis on se donne $y \in \operatorname{Im} f$ et on montre qu'il est atteint par b. Par définition de $\operatorname{Im} f$, il existe $x \in E$ tel que $f(x) = y$. Puis, comme $\operatorname{Ker} f$ et G sont supplémentaires, x peut être décomposé sous la forme

$$x = x_1 + x_2 \qquad \text{avec} \qquad x_1 \in \operatorname{Ker} f \qquad \text{et} \qquad x_2 \in G$$

Donc
$$y = f(x) = \underbrace{f(x_1)}_{=0} + f(x_2) = f(x_2) = b(x_2)$$

et
$$y \in \operatorname{Im} b$$

D'après la **proposition 2.10**, b est surjective. G et $\operatorname{Im} f$ sont isomorphes. □

4.2.3 Formes linéaires

Définition 4.2.12
Soit E un $\mathbb{K}$-espace vectoriel. Un sous-espace de E est appelé *hyperplan* si, et seulement si, il est le noyau d'une forme linéaire non nulle.

Proposition 4.2.13
Soit E *un* $\mathbb{K}$*-espace vectoriel. Soit* H *un hyperplan. Il existe* $x_0 \in E$ *tel que* $H \oplus \operatorname{Vect} x_0$. *En d'autres termes, tout hyperplan admet des supplémentaires, dont au moins un est une droite.*

Preuve : Soit H un hyperplan. D'après la **définition 2.12**, il existe une forme linéaire non nulle f sur E, telle que $H = \operatorname{Ker} f$.

Comme f n'est pas nulle, il existe $x_0 \in E$, tel que $f(x_0) \neq 0$. Quitte à diviser x_0 par $f(x_0)$, on peut supposer que $f(x_0) = 1$. Montrons que

$$E = \operatorname{Ker} f \oplus \operatorname{Vect} x_0$$

D'une part, on montre que la somme est directe. Si $x \in \operatorname{Ker} f \cap \operatorname{Vect} x_0$, on a d'une part $f(x) = 0$ et d'autre part, x est proportionnel à x_0. Donc il existe $\lambda \in \mathbb{K}$, tel que $x = \lambda x_0$. Et on a

$$0 = f(x) = f(\lambda x_0) = \lambda f(x_0) = \lambda$$

d'où $$x = \lambda x_0 = 0$$

Puis on montre que la somme directe de ces deux sous-espaces est E. Il suffit d'observer

$$\forall x \in \mathrm{E} \qquad x = f(x)x_0 + \big(x - f(x)x_0\big)$$

Le vecteur $f(x)x_0$ appartient à $\mathrm{Vect}\, x_0$ tandis que $x - f(x)x_0$ est dans $\mathrm{Ker}\, f$ puisque

$$f\big(x - f(x)x_0\big) = f(x) - f(x)f(x_0) = f(x) - f(x) = 0$$

On a gagné ! □

Proposition 4.2.14
Soient f et g deux formes linéaires non nulles sur un espace vectoriel E. *Les noyaux de f et g sont égaux si et seulement si f et g sont proportionnelles.*

Preuve : Il est clair que si f et g sont proportionnelles, leurs noyaux sont les mêmes : le coefficient de proportionnalité, non nul, ne change pas le fait que $f(x)$ ou $g(x)$ est nul.

Réciproquement, supposons que $\mathrm{Ker}\, f$ et $\mathrm{Ker}\, g$ sont égaux. D'après la **proposition 2.13**, ce sous-espace admet un supplémentaire dirigé par un vecteur x_0 tel que $f(x_0) = 1$. Si $x \in \mathrm{E}$, il se décompose suivant la somme directe $\mathrm{E} = \mathrm{Ker}\, f \oplus \mathrm{Vect}\, x_0$: il existe $y \in \mathrm{Ker}\, f$ et $\lambda \in \mathbb{K}$ tels que

$$x = y + \lambda x_0$$

On a $$f(x) = f(y) + \lambda f(x_0) = \lambda$$

tandis que $$g(x) = g(x) + \lambda g(x_0) = \lambda g(x_0) = g(x_0) f(x)$$

On n'oublie pas en effet que $\mathrm{Ker}\, f = \mathrm{Ker}\, g$ donc $g(x) = 0$. Comme x était quelconque, on a montré que $g = g(x_0) f$. □

4.2.4 Endomorphismes particuliers

Définition 4.2.15
Soit E un $\mathbb{K}$-espace vectoriel. Soit α un scalaire. On appelle homothétie de rapport α l'automorphisme de E défini par

$$\forall x \in \mathrm{E} \qquad f(x) = \alpha x$$

Rien à dire sur les homothéties : ce sont les applications linéaires les plus simples possibles – mise-à-part l'application nulle.

Définition 4.2.16
Soit E un $\mathbb{K}$-espace vectoriel. Soit $p \in \mathscr{L}(\mathrm{E})$. On dit que p est un projecteur si et seulement si $p^2 = p$.

On rappelle qu'au **paragraphe 1.6**, on a défini une opération appelée projection sur un sous-espace parallèlement à un autre. Il est temps d'y revenir, de montrer qu'il s'agit d'un projecteur, et de montrer que tout projecteur est une projection.

Rappelons le contexte : on a deux sous-espaces supplémentaires F et G de E. Cela signifie que, si x est un vecteur quelconque de E, il se décompose de manière unique comme somme d'un vecteur de F et d'un de G. On note respectivement ces vecteurs $p_F x$ et $p_G x$ de sorte que

$$x = p_F(x) + p_G(x) \qquad \text{avec} \qquad p_F(x) \in F \quad \text{et} \quad p_G(x) \in G$$

C'est $p_F(x)$ qu'on appelle la projection de x sur F parallèlement à G. Vérifions d'abord que p_F est un endomorphisme de E.

Soient x et y dans E et $\lambda \in \mathbb{K}$. On a

$$x = p_F(x) + p_G(x) \qquad \text{et} \qquad y = p_F(y) + p_G(y)$$

d'où
$$\lambda x + y = \big(\lambda p_F(x) + p_F(y)\big) + \big(\lambda p_G(x) + p_G(y)\big)$$

On voit qu'on a décomposé $\lambda x + y$ comme somme d'un vecteur de F et d'un vecteur de G. Cette décomposition étant unique, et la composante suivant F étant $p_F(\lambda x + y)$, on a

$$p_F(\lambda x + y) = \lambda p_F(x) + p_F(y)$$

Autrement dit, p_F est linéaire.

Montrons qu'il s'agit d'un projecteur. C'est simple : si $x \in E$, on a $p_F(x) = p_F(x) + 0$, qui est une décomposition de $p_F(x)$ suivant F et G. Donc

$$p_F\big(p_F(x)\big) = p_F(x) \qquad \text{c'est-à-dire} \qquad p_F^2 = p_F$$

Toute projection est donc un projecteur. Il reste à montrer que ces deux notions coïncident :

Théorème 4.2.17
Soit E *un* $\mathbb{K}$*-espace vectoriel. Soit p un projecteur. C'est la projection sur $\operatorname{Im} p$ parallèlement à $\operatorname{Ker} p$. En outre, $I - p$ est la projection sur $\operatorname{Ker} p$ parallèlement à $\operatorname{Im} p$.*

Preuve : Par définition, p est un endomorphisme de E tel que $p^2 = p$. Le théorème annonce que p est la projection sur $\operatorname{Im} p$ parallèlement à $\operatorname{Ker} p$; cela sous-entend que ces deux sous-espaces sont supplémentaires. Donc commençons par le démontrer. Si $x \in E$, on a

$$x = p(x) + \big(x - p(x)\big)$$

Bien évidemment, $p(x)$ appartient à $\operatorname{Im} p$; et $x - p(x)$ appartient à $\operatorname{Ker} p$ puisque

$$p\big(x - p(x)\big) = p(x) - p(p(x)) = p(x) - p^2(x) = p(x) - p(x) = 0$$

donc
$$E = \operatorname{Ker} p + \operatorname{Im} p$$

Le fait que la somme est directe est simple : soit $x \in \operatorname{Ker} p \cap \operatorname{Im} p$. Puisqu'il est dans l'image de p, il existe $y \in E$ tel que $p(y) = x$. Et comme x est dans le noyau de p, on a

$$0 = p(x) = p^2(y) = p(y) = x$$

Identifions maintenant $I - p$. Bien évidemment, $I - p$ est un endomorphisme de E, comme somme d'endomorphismes de E. De plus,

$$(I - p)^2 = (I - p) \circ (I - p) = I - p - p + p^2 = I - p$$

puisque $p^2 = p$. Donc $I - p$ est un projecteur. D'après ce qui précède, c'est la projection sur $\operatorname{Im}(I - p)$ parallèlement à $\operatorname{Ker}(I - p)$. On voit que

$$\operatorname{Ker}(I - p) = \{x \in E \mid (I - p)(x) = 0\} = \{x \in E \mid x - p(x) = 0\} = \{x \in E \mid p(x) = x\} = \operatorname{Im} p$$

De même $$\operatorname{Ker} p = \operatorname{Ker}(\mathrm{I} - (\mathrm{I} - p)) = \operatorname{Im}(\mathrm{I} - p)$$

$\mathrm{I} - p$ est bien la projection sur $\operatorname{Ker} p$ parallèlement à $\operatorname{Im} p$. □

Définition 4.2.18
Soit E un $\mathbb{K}$-espace vectoriel. Soient F et G des sous-espaces supplémentaires. On appelle symétrie par rapport à G parallèlement à F l'application $s = \mathrm{I} - 2p_{\mathrm{F}}$.

Théorème 4.2.19
Soit E *un espace vectoriel. Soit s une symétrie. s est linéaire et* $s^2 = I$.

Réciproquement, si s est un endomorphisme de E *tel que* $s^2 = \mathrm{I}$, *s est la symétrie par rapport à* $Ker(s - \mathrm{I})$, *parallèlement à* $Ker(s + \mathrm{I})$.

Preuve : On commence par la première partie. On se donne une symétrie s ; c'est-à-dire que l'espace est décomposé comme somme directe $\mathrm{E} = \mathrm{F} \oplus \mathrm{G}$ et on a $s = \mathrm{I} - 2p_{\mathrm{F}}$. Dans la mesure où p_{F} est un endomorphisme de E, d'après ce qui a été vu sur les projecteurs, s est également un endomorphisme. En outre, $p_{\mathrm{F}}^2 = p_{\mathrm{F}}$ donc

$$s^2 = (\mathrm{I} - 2p_{\mathrm{F}})^2 = \mathrm{I} - 2p_{\mathrm{F}} - 2p_{\mathrm{F}} + 4p_{\mathrm{F}}^2 = \mathrm{I}$$

ce qui prouve la première partie du théorème.

Réciproquement, on suppose que s est un endomorphisme de E tel que $s^2 = \mathrm{I}$. Le théorème annonce qu'il s'agit de la symétrie par rapport à $\operatorname{Ker}(s - \mathrm{I})$, parallèlement à $\operatorname{Ker}(s + \mathrm{I})$. Donc une première chose à vérifier est que ces sous-espaces sont supplémentaires. On commence par remarquer que si x est un vecteur quelconque,

$$x = \frac{x + s(x)}{2} + \frac{x - s(x)}{2}$$

Or, $$\frac{x + s(x)}{2} \in \operatorname{Ker}(s - \mathrm{I})$$

puisque $$\begin{aligned}(s - \mathrm{I})(x + s(x)) &= s(x + s(x)) - (x + s(x)) \\ &= s(x) + \underbrace{s^2(x)}_{=x} - x - s(x) = 0\end{aligned}$$

De même $$\frac{x - s(x)}{2} \in \operatorname{Ker}(s + \mathrm{I})$$

donc on a déjà montré que $\mathrm{E} = \operatorname{Ker}(s - \mathrm{I}) + \operatorname{Ker}(s + \mathrm{I})$ et il reste à voir que la somme est directe. Soit $x \in \operatorname{Ker}(s - \mathrm{I}) \cap \operatorname{Ker}(s + \mathrm{I})$. On a donc

$$s(x) - x = 0 \qquad \text{et} \qquad s(x) + x = 0$$

d'où $$2x = 0 \qquad \text{et} \qquad x = 0$$

On a montré $$\mathrm{E} = \operatorname{Ker}(s - \mathrm{I}) \oplus \operatorname{Ker}(s + \mathrm{I})$$

Reste à montrer que s est bien la symétrie par rapport à $\operatorname{Ker}(s - \mathrm{I})$, parallèlement à $\operatorname{Ker}(s + \mathrm{I})$. Pour cela, on regarde la **définition 2.18** : il suffit d'établir que $s = \mathrm{I} - 2p$, où p est la projection sur $\operatorname{Ker}(s + \mathrm{I})$ parallèlement à $\operatorname{Ker}(s - \mathrm{I})$. On montre que ces deux applications coincïdent en tout point. Soit x un élément de E. Il se décompose de manière unique suivant notre somme directe : il existe $x_1 \in \operatorname{Ker}(s - \mathrm{I})$ et $x_2 \in \operatorname{Ker}(s + \mathrm{I})$, uniques, tels que $x = x_1 + x_2$.

Par définition de p, on a d'ailleurs $x_2 = p(x)$. De plus, par définition de x_1 et x_2,

$$(s-\mathrm{I})(x_1) = 0 \qquad \text{donc} \qquad s(x_1) = x_1$$

et $$(s+\mathrm{I})(x_2) = 0 \qquad \text{donc} \qquad s(x_2) = -x_2$$

Par conséquent, $$s(x) = s(x_1) + s(x_2) = x_1 - x_2 = \underbrace{x_1 + x_2}_{=x} - 2x_2 = x - 2p(x)$$

et on a $s = \mathrm{I} - 2p$, comme annoncé. □

4.2.5 Équations linéaires

Définition 4.2.20
Soient E et F deux $\mathbb{K}$-espaces vectoriels. Soient $f \in \mathscr{L}(\mathrm{E},\mathrm{F})$ et $b \in \mathrm{F}$. *Résoudre l'équation linéaire « $f(x) = b$ »*, c'est déterminer l'ensemble $\{x \in \mathrm{E} \mid f(x) = b\}$.

> Il est clair que l'équation « $f(x) = b$ » n'a des chances d'admettre des solutions que si $b \in \mathrm{Im}\, f$. D'où l'intérêt de savoir déterminer cet ensemble.

Proposition 4.2.21
Soient E *et* F *deux* $\mathbb{K}$*-espaces vectoriels. Soient* $f \in \mathscr{L}(\mathrm{E},\mathrm{F})$ *et* $b \in \mathrm{F}$. *On suppose avoir trouvé* $x_0 \in \mathrm{E}$ *tel que* $f(x_0) = b$. *L'ensemble des solutions de l'équation « $f(x) = b$ » est*

$$\{x_0 + y \mid y \in \mathit{Ker}\, f\}$$

Preuve : On note

$$\mathscr{S} = \{x \in \mathrm{E} \mid f(x) = b\} \qquad \text{et} \qquad \mathscr{S}' = \{x_0 + y \mid y \in \mathrm{Ker}\, b\}$$

et il s'agit de montrer que ces ensembles sont égaux. On prend d'abord un élément x de $\mathscr{S}'$. Il existe $y \in \mathrm{Ker}\, f$ tel que $x = x_0 + y$ et il s'ensuit que $x \in \mathscr{S}$ puisque

$$f(x) = f(x_0 + y) = \underbrace{f(x_0)}_{=b} + \underbrace{f(y)}_{=0} = b$$

Réciproquement, soit $x \in \mathscr{S}$. On a

$$f(x) = b \qquad \text{et} \qquad f(x_0) = b$$

donc $$f(x - x_0) = f(x) - f(x_0) = b - b = 0$$

et il s'ensuit que $y = x - x_0$ appartient à $\mathrm{Ker}\, f$. Et on a bien $x = x_0 + y$. □

Chapitre 5

Polynômes à une indéterminée

Comme toujours, $\mathbb{K}$ est un corps commutatif.

5.1 L'algèbre des polynômes

5.1.1 Suites à support fini

Définition 5.1.1
Soit P une suite à valeurs dans $\mathbb{K}$. On appelle *support* de P, noté $\operatorname{Supp} P$, l'ensemble

$$\operatorname{Supp} P = \{n \in \mathbb{N} \mid P_n \neq 0\}$$

Définition 5.1.2
On appelle *polynôme à coefficients dans* $\mathbb{K}$ toute suite à support fini. Leur ensemble est noté $\mathbb{K}[X]$. On parle aussi de suite dont les termes sont *presque tous nuls*.

Exemple 5.1.3
Dans la mesure où, par définition, $\emptyset$ est fini, toute suite de support vide est un polynôme. Mais en fait, il n'y a qu'une seule et unique suite de support vide puisque

$$\forall P \in \mathbb{K}[X] \qquad \operatorname{Supp} P = \emptyset \iff \forall n \in \mathbb{N} \quad P_n = 0$$

Le seul polynôme de support vide est donc celui dont tous les termes sont nuls. Naturellement, on l'appelle polynôme nul et on le note 0 dans la suite du cours.

Il y a plein d'autres exemples de polynômes. Par exemple, la suite de support $\{0,1\}$, définie par

$$P_0 = 1 \qquad P_1 = 1$$

Proposition 5.1.4
Soit P un polynôme non nul. Le support de P est non vide majoré.

Preuve : Comme expliqué dans l'exemple ci-dessus, le fait que $\operatorname{Supp} P$ soit vide équivaut à la nullité de P. Et il est majoré, comme toute partie finie de $\mathbb{N}$. □

Définition 5.1.5
Soit P un polynôme non nul. On appelle

- *degré* de P, noté $\deg P$, le plus grand élément de $\operatorname{Supp} P$;
- *valuation* de P, notée $\operatorname{val} P$, le plus petit élément de $\operatorname{Supp} P$.

Par convention, le polynôme nul est de degré $-\infty$ et de valuation $+\infty$.

> Remarquons que ces notions de degré et valuation d'un polynôme non nul existent bien, puisque son support n'est pas vide et majoré.

Définition 5.1.6
Soit P un polynôme non nul, de degré p. Les termes de la suite P sont appelés *coefficients* de P. Le coefficient P_p est appelé coefficient dominant de P. S'il est égal à 1, on dit que P est unitaire. Si P est nul ou de degré 0, on dit qu'il est constant et on note $P = P_0$.

> Naturellement, puisque les polynômes sont des fonctions définies sur $\mathbb{N}$ et que leurs coefficients sont les valeurs de ces fonctions, deux polynômes sont égaux si, et seulement si, ils ont les mêmes coefficients.

5.1.2 Structure d'espace vectoriel

Comme $\mathbb{K}[X]$ est un sous-ensemble de l'espace $\mathbb{K}^{\mathbb{N}}$ des fonctions de $\mathbb{N}$ dans $\mathbb{K}$ (qu'on a appelées « suites »), on peut raisonnablement se demander s'il s'agit d'un sous-espace vectoriel pour les opérations d'addition des suites et de multiplication par un scalaire. On définit donc

$$\forall (P,Q) \in \mathbb{K}[X]^2 \quad \forall n \in \mathbb{N} \qquad (P+Q)_n = P_n + Q_n$$

et

$$\forall \lambda \in \mathbb{K} \quad \forall P \in \mathbb{K}[X] \quad \forall n \in \mathbb{N} \qquad (\lambda P)_n = \lambda P_n$$

Théorème 5.1.7
Muni de ces opérations, $\mathbb{K}[X]$ *est un sous-espace vectoriel de* $\mathbb{K}^{\mathbb{N}}$. *De plus*

$$\forall (P,Q) \in \mathbb{K}[X]^2 \qquad \begin{cases} deg(P+Q) \leqslant Max(degP, degQ) \\ val(P+Q) \geqslant Min(valP, valQ) \end{cases}$$

et

$$\forall \lambda \in \mathbb{K} \setminus \{0\} \quad \forall P \in \mathbb{K}[X] \qquad \begin{cases} deg(\lambda P) = degP \\ val(\lambda P) = valP \end{cases}$$

Preuve : Il suffit de montrer que $\mathbb{K}[X]$ est stable par addition et par multiplication par les scalaires.

On se donne P et Q deux polynômes. Si l'un des deux est nul, il est clair que $P+Q$ est un polynôme et que les inégalités sur le degré et la valuation sont vérifiées. On suppose donc qu'aucun des deux n'est nul. Par définition du degré et de la valuation, on a

$$\forall n \geqslant \mathrm{Max}(\deg P, \deg Q) \qquad P_n = 0 \qquad \text{et} \qquad Q_n = 0$$

donc

$$\forall n \geqslant \mathrm{Max}(\deg P, \deg Q) \qquad P_n + Q_n = 0$$

En d'autres termes,

$$\mathrm{Supp}\,(P+Q) \subset [\![\, 0\,;\, \mathrm{Max}(\deg P, \deg Q)\,]\!]$$

On sait qu'un ensemble est fini si, et seulement si, il est majoré ; donc $\mathrm{Supp}\,(P+Q)$ est fini : $P+Q$ est un polynôme et on a immédiatement

$$\deg(P+Q) \leqslant \text{Max}(\deg P, \deg Q)$$

si Supp $(P+Q)$ n'est pas vide. Évidemment, cette inégalité est immédiate si Supp $(P+Q)$ est vide, puisque le polynôme nul a pour degré $-\infty$. On a, tout aussi facilement, que

$$\forall n \leqslant \text{Min}(\text{val}\, P, \text{val}\, Q) \qquad P_n + Q_n = 0$$

donc $$\text{val}\,(P+Q) \geqslant \text{Min}(\text{val}\, P, \text{val}\, Q)$$

On passe maintenant à la multiplication par les scalaires. Soient P un polynôme et λ un scalaire. Si λ est nul, alors λP est le polynôme nul ; en particulier c'est un polynôme. Donc on suppose maintenant que λ n'est pas nul. Dans la mesure où un produit est nul si et seulement si un de ses termes est nul, on a

$$\forall n \in \mathbb{N} \qquad \lambda P_n = 0 \iff P_n = 0$$

donc $$\text{Supp}\,(\lambda P) = \text{Supp}\, P$$

λP est donc un polynôme, de mêmes degré et valuation que P. □

5.1.3 Structure d'algèbre

Nous allons maintenant définir une nouvelle opération interne entre les polynômes, appelée multiplication. Elle est fondée sur le

Lemme 5.1.8
Soient P *et* Q *deux polynômes. On pose*

$$\forall n \in \mathbb{N} \qquad (PQ)_n = \sum_{k=0}^{n} P_k Q_{n-k}$$

La suite PQ *est en fait un polynôme, de degré deg*P + *deg*Q *et de valuation val*P + *val*Q. *On l'appelle produit des polynômes* P *et* Q.

Preuve : On suppose que ni P ni Q n'est nul, car dans ce cas le lemme est trivial : PQ est simplement le polynôme nul. Posons

$$p = \deg P \qquad \text{et} \qquad q = \deg Q$$

Soit $n \geqslant p+q+1$. Alors

$$\forall k \leqslant p \qquad -k \geqslant -p \qquad \text{d'où} \qquad n-k \geqslant q+1$$

Par conséquent, $$\forall k \in [\![0\,;\,p]\!] \qquad P_k \underbrace{Q_{n-k}}_{=0} = 0$$

et évidemment, $$\forall k \in [\![1+p\,;\,n]\!] \qquad \underbrace{P_k}_{=0} Q_{n-k} = 0$$

donc $$(PQ)_n = 0$$

Ceci montre que le support de la suite PQ est borné (donc fini), puisqu'inclus dans $[\![0\,;\,p+q]\!]$. Donc PQ est un polynôme, de degré inférieur à $p+q$. Reste à montrer que le terme de degré $p+q$ n'est pas nul. Il vaut, par définition,

$$(PQ)_{p+q} = \sum_{k=0}^{p+q} P_k Q_{p+q-k}$$

Mais comme $P_k = 0$ si $k > p$ et $Q_{p+q-k} = 0$ si $k < p$, on a

$$(PQ)_{p+q} = P_p Q_q$$

qui n'est pas nul, puisque ni P_p ni Q_q n'est nul. La partie sur la valuation se démontre de la même manière. □

Proposition 5.1.9
$(\mathbb{K}[X], +, \times)$ *est un anneau commutatif.*

Preuve : La plupart de ces propositions sont des trivialités, conséquences immédiates des propriétés connues sur les éléments de $\mathbb{K}$. On se donne trois polynômes P, Q et R et un scalaire $\mathbb{K}$:

$$\forall n \in \mathbb{N} \qquad (PQ)_n = \underbrace{\sum_{k=0}^{n} P_k Q_{n-k} = \sum_{k=0}^{n} P_{n-k} Q_k}_{\text{changement d'indice } k=n-k} = \sum_{k=0}^{n} Q_k P_{n-k} = (QP)_n$$

$$\begin{aligned} \forall n \in \mathbb{N} \qquad \big(P(Q+R)\big)_n &= \sum_{k=0}^{n} P_k (Q+R)_{n-k} = \sum_{k=0}^{n} P_k (Q_{n-k} + R_{n-k}) \\ &= \sum_{k=0}^{n} P_k Q_{n-k} + \sum_{k=0}^{n} P_k R_{n-k} = (PQ)_n + (PR)_n \end{aligned}$$

et $$\forall n \in \mathbb{N} \qquad \big((\lambda P)Q\big)_n = \sum_{k=0}^{n} (\lambda P)_k Q_{n-k} = \sum_{k=0}^{n} \lambda P_k Q_{n-k} = \lambda \sum_{k=0}^{n} P_k Q_{n-k} = \lambda (PQ)_n$$

Ces relations démontrent les propriétés *1, 3, 4*.

La proposition annonce un élément neutre, qui serait l'unique polynôme unitaire de degré 0. Déjà, cet « unique polynôme unitaire de degré 0 » existe-t-il ? Un polynôme de degré 0 est entièrement déterminé par son terme de degré 0, puisque tous les autres termes sont nuls. Le fait qu'il soit unitaire impose à ce coefficient de valoir 1. Donc il existe en effet un et un seul polynôme unitaire de degré 0 et il est défini par

$$\forall n \in \mathbb{N} \qquad 1_n = \begin{cases} 0 \text{ si } n \geqslant 1 \\ 1 \text{ si } n = 0 \end{cases}$$

Vérifions qu'il est neutre pour la multiplication : si P est n'importe quel polynôme, on a effectivement

$$\forall n \in \mathbb{N} \qquad (1\,P)_n = \sum_{k=0}^{n} 1_k P_{n-k} = 1_0 P_n + \sum_{k=1}^{n} \underbrace{1_k}_{=0} P_{n-k} = P_n$$

La dernière chose à vérifier est l'associativité. On se donne trois polynômes P, Q et R :

$$\begin{aligned}
\forall n \in \mathbb{N} \qquad \big(\mathrm{P}(\mathrm{QR})\big)_n &= \sum_{k=0}^{n} \mathrm{P}_k (\mathrm{QR})_{n-k} \\
&= \underbrace{\sum_{k=0}^{n} \mathrm{P}_k \sum_{j=0}^{n-k} \mathrm{Q}_j \mathrm{R}_{n-k-j} = \sum_{k=0}^{n} \mathrm{P}_k \sum_{j=k}^{n} \mathrm{Q}_{j-k} \mathrm{R}_{n-j}}_{\text{changement d'indice } j=j+k} \\
&= \sum_{k=0}^{n} \sum_{j=k}^{n} \mathrm{P}_k \mathrm{Q}_{j-k} \mathrm{R}_{n-j} = \sum_{0 \leqslant k \leqslant j \leqslant n} \mathrm{P}_k \mathrm{Q}_{j-k} \mathrm{R}_{n-j} \\
&= \sum_{j=0}^{n} \sum_{k=0}^{j} \mathrm{P}_k \mathrm{Q}_{j-k} \mathrm{R}_{n-j} = \sum_{j=0}^{n} \mathrm{R}_{n-j} \sum_{k=0}^{j} \mathrm{P}_k \mathrm{Q}_{j-k} \\
\big(\mathrm{P}(\mathrm{QR})\big)_n &= \sum_{j=0}^{n} (\mathrm{PQ})_j \mathrm{R}_{n-j} = \big((\mathrm{PQ})\mathrm{R}\big)_n
\end{aligned}$$

□

On dit que l'ensemble $\mathbb{K}[X]$ est muni d'une structure d'algèbre commutative : une algèbre commutative est un espace vectoriel qui a en plus une structure d'anneau. Les algèbres sont, comme on peut s'en douter, des structures très riches, mais leur étude n'est pas au programme.

Théorème 5.1.10
$\mathbb{K}[X]$ *est une algèbre intègre, c'est-à-dire que*

$$\forall (\mathrm{P}, \mathrm{Q}) \in \mathbb{K}[X]^2 \qquad \mathrm{PQ} = 0 \iff (\mathrm{P} = 0 \text{ } \textit{ou} \text{ } \mathrm{Q} = 0)$$

Preuve : C'est une conséquence immédiate du fait que PQ a pour degré $\deg \mathrm{P} + \deg \mathrm{Q}$. Si cette somme a pour degré $-\infty$, c'est que l'un des degrés $\deg \mathrm{P}$ ou $\deg \mathrm{Q}$ est $-\infty$. □

Définition 5.1.11
Si P est un polynôme et N est un entier, on pose

$$\mathrm{P}^{\mathrm{N}} = \begin{cases} 1 \text{ si } \mathrm{N} = 0 \\ \underbrace{\mathrm{P} \times \cdots \times \mathrm{P}}_{\mathrm{N} \text{ fois}} \text{ si } \mathrm{N} > 0 \end{cases}$$

5.1.4 Indéterminée

Définition 5.1.12
On appelle *indéterminée* le polynôme X, de degré 1, défini par

$$\forall n \in \mathbb{N} \qquad \mathrm{X}_n = \begin{cases} 0 \text{ si } n \neq 1 \\ 1 \text{ si } n = 1 \end{cases}$$

Proposition 5.1.13
Pour tout entier N*, on a*

$$\forall n \in \mathbb{N} \qquad (\mathrm{X}^{\mathrm{N}})_n = \begin{cases} 0 \textit{ si } n \neq \mathrm{N} \\ 1 \textit{ si } n = \mathrm{N} \end{cases}$$

Preuve : On procède par récurrence en définissant, pour tout entier N, la proposition

$$\mathscr{P}(\mathrm{N}) : \text{« } \forall n \in \mathbb{N} \qquad (\mathrm{X}^{\mathrm{N}})_n = \begin{cases} 0 \text{ si } n \neq \mathrm{N} \\ 1 \text{ si } n = \mathrm{N} \end{cases} \text{ »}$$

- $\mathscr{P}$**(0) est vraie** : en effet, X^0 a été défini comme égal à 1 : seul son coefficient de degré 0 n'est pas nul, et vaut 1.
- $\mathscr{P}$**(N)** $\Longrightarrow$ $\mathscr{P}$**(N + 1)** : soit N un entier, tel que $\mathscr{P}(\mathrm{N})$ soit vraie, c'est-à-dire que X^{N} est le polynôme, dont tous les coefficients sont nuls, sauf celui de degré N qui vaut 1. Autrement dit, X^{N} est de valuation N et de degré N. D'après le **lemme 1.8**,

  $$\deg \mathrm{X}^{\mathrm{N}+1} = \deg(\mathrm{X}^{\mathrm{N}} \times \mathrm{X}) = \deg \mathrm{X}^{\mathrm{N}} + \deg \mathrm{X} = \mathrm{N} + 1$$

  $$\mathrm{val}\, \mathrm{X}^{\mathrm{N}+1} = \mathrm{val}\, \mathrm{X}^{\mathrm{N}} + \mathrm{val}\, \mathrm{X} = \mathrm{N} + 1$$

  et le coefficient de degré N + 1 de $\mathrm{X}^{\mathrm{N}+1}$ est le produit des coefficients de degré N de X^{N} et de degré 1 de X : il s'agit de 1. Donc

  $$\forall n \in \mathbb{N} \qquad (\mathrm{X}^{\mathrm{N}+1})_n = \begin{cases} 0 \text{ si } n \in [\![0 ; \mathrm{N}]\!] \text{ car } \mathrm{val}\, \mathrm{X}^{\mathrm{N}+1} = \mathrm{N} + 1 \\ 1 \text{ si } n = \mathrm{N} + 1 \\ 0 \text{ si } n \geqslant \mathrm{N} + 2 \text{ car } \deg \mathrm{X}^{\mathrm{N}+1} = \mathrm{N} + 1 \end{cases}$$

  Ceci démontre $\mathscr{P}(\mathrm{N} + 1)$.
- **Conclusion :** $\mathscr{P}(\mathrm{N})$ est vraie pour tout entier N, ce qui achève la démonstration de la proposition.

Corollaire 5.1.14
Pour tous entiers n et p, on a $\mathrm{X}^{n+p} = \mathrm{X}^n \mathrm{X}^p$.

Preuve : C'est une conséquence presqu'immédiate (il faut faire une récurrence) de la **proposition 1.12**. □

Corollaire 5.1.15
Tout polynôme peut s'écrire de manière unique comme combinaison linéaire finie des polynômes $(\mathrm{X}^{\mathrm{N}})_{\mathrm{N} \in \mathbb{N}}$. *Plus précisément,*

$$\forall \mathrm{P} \in \mathbb{K}[\mathrm{X}] \qquad \mathrm{P} = \sum_{k=0}^{\infty} \mathrm{P}_k \mathrm{X}^k$$

> Bien que la somme ci-dessus semble être infinie, il n'en est rien puisque presque tous les coefficients d'un polynôme sont nuls.

Preuve : Soit P un polynôme. On définit

$$\mathrm{Q} = \sum_{k=0}^{\infty} \mathrm{P}_k \mathrm{X}^k$$

et on montre que Q et P sont égaux. Pour cela, il suffit qu'ils aient les mêmes coefficients. C'est simple : d'après la définition de la somme dans $\mathbb{K}[\mathrm{X}]$ et la **proposition 1.12**,

$$\forall n \in \mathbb{N} \qquad \mathrm{Q}_n = \sum_{k=0}^{\infty} \mathrm{P}_k (\mathrm{X}^k)_n = \mathrm{P}_n$$

Corollaire 5.1.16
Soient P *et* Q *deux polynômes. Alors*

$$PQ = \sum_{n=0}^{\infty} \Big(\sum_{k=0}^{n} P_k Q_{n-k} \Big) X^n = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} P_n Q_m X^{n+m}$$

Preuve : D'après la définition du terme général du polynôme PQ et le **corollaire 1.15**,

$$PQ = \sum_{n=0}^{\infty} \Big(\sum_{k=0}^{n} P_k Q_{n-k} \Big) X^n$$

Mais on a aussi

$$P = \sum_{n=0}^{\infty} P_n X^n \qquad \text{et} \qquad Q = \sum_{m=0}^{\infty} Q_m X^m$$

donc

$$\begin{aligned} PQ &= \Big(\sum_{n=0}^{\infty} P_n X^n \Big) Q = \sum_{n=0}^{\infty} P_n Q X^n \\ &= \sum_{n=0}^{\infty} \Big(\sum_{m=0}^{\infty} Q_m X^m \Big) P_n X^n \\ &= \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} P_n Q_m X^{n+m} \end{aligned}$$

La première égalité est simplement la récriture de P, à l'aide du **corollaire 1.15**. La deuxième égalité est dûe à la distributivité de la multiplication sur l'addition. Pour obtenir la troisième égalité, on récrit Q à l'aide du **corollaire 1.15**. Puis on utilise une dernière fois la distributivité de la multiplication sur l'addition. □

5.1.5 Composition

Définition 5.1.17
Soient P et Q deux polynômes. On définit le *polynôme composé*, noté $P \circ Q$ ou $P(Q)$, par la relation :

$$P(Q) = \sum_{k=0}^{\infty} P_k Q^k$$

Proposition 5.1.18
Voici les propriétés de la composition :

1. *Associativité :* $\forall (P,Q,R) \in \mathbb{K}[X]^3 \qquad P(Q(R)) = \big(P(Q)\big)(R)$
2. *Distributivité à droite sur l'addition :*

$$\forall (P,Q,R) \in \mathbb{K}[X]^3 \qquad (P+Q)(R) = P(R) + Q(R)$$

3. *Distributivité à droite sur la multiplication :*

$$\forall (P,Q,R) \in \mathbb{K}[X]^3 \qquad (PQ)(R) = P(R)\,Q(R)$$

Preuve : La propriété la plus difficile est la première et on la laisse pour la fin. La distributivité par rapport à l'addition est triviale : si P, Q et R sont trois polynômes,

$$(P+Q)(R) = \sum_{n=0}^{\infty} (P+Q)_n R^n = \sum_{n=0}^{\infty} (P_n + Q_n) R^n = \sum_{n=0}^{\infty} P_n R^n + \sum_{n=0}^{\infty} Q_n R^n = P(R) + Q(R)$$

Montrons ensuite la distributivité par rapport à la multiplication. C'est une conséquence du **corollaire 1.16** et de la distributivité par rapport à l'addition :

$$PQ = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} P_n Q_m X^{n+m}$$

donc
$$(PQ)(R) = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} P_n Q_m R^{n+m} = P(R)Q(R)$$

Pour démontrer l'associativité, il convient de se convaincre que

$$\forall n \in \mathbb{N} \quad \forall (Q,R) \in \mathbb{K}[X] \qquad X^n(Q(R)) = (X^n(Q))(R) \tag{1}$$

On le démontre par récurrence et voici la manière dont elle s'amorce. On a clairement

$$X^0(Q(R)) = 1(Q(R)) = 1 = (1(Q))(R)$$

$$X^1(Q(R)) = X(Q(R)) = Q(R) = (X(Q))(R)$$

Pour la suite, on a besoin de la distributivité à droite de la composition sur le produit et de l'identité précédente :

$$\begin{aligned} X^2(Q(R)) &= (X \times X)(Q(R)) = X(Q(R)) \times X(Q(R)) \\ &= (X(Q))(R) \times (X(Q))(R) = (X(Q) \times X(Q))(R) = (X^2(Q))(R) \end{aligned}$$

C'est cette manipulation qu'on implémente pour montrer l'hérédité. Si on suppose avoir démontré que $X^n(Q(R)) = (X^n(Q))(R)$, il vient

$$\begin{aligned} X^{n+1}(Q(R)) &= X(Q(R)) \times X^n(Q(R)) = (X(Q))(R) \times (X^n(Q))(R) \\ &= (X^n(Q) \times X(Q))(R) = (X^{n+1}(Q))(R) \end{aligned}$$

Remarquez comme on a utilisé la distributivité par rapport à la multiplication, puis l'hypothèse de récurrence, et la distributivité sur la multiplication de nouveau.

Bref, la relation (**1**) est démontrée par récurrence. À partir de maintenant, c'est simple : si P, Q et R sont trois polynômes,

$$\begin{aligned} P(Q(R)) &= \Big(\sum_{n=0}^{\infty} P_n X^n \Big)(Q(R)) = \sum_{n=0}^{\infty} P_n X^n(Q(R)) = \sum_{n=0}^{\infty} P_n (X^n(Q))(R) \\ &= \Big(\sum_{n=0}^{\infty} P_n X^n(Q) \Big)(R) = (P(Q))(R) \end{aligned}$$ □

5.2 Structure multiplicative de $\mathbb{K}[X]$

5.2.1 Éléments inversibles

Définition 5.2.1
Soit $P \in \mathbb{K}[X]$. On dit que P est *inversible* si, et seulement si, il existe $Q \in \mathbb{K}[X]$ tel que $PQ = 1$. L'ensemble des éléments inversibles est noté $\mathbb{K}[X]^\times$.

Théorème 5.2.2
$\mathbb{K}[X]^\times$ *est constitué des polynômes de degré 0.*

Preuve : Soit P un polynôme de degré 0. D'après le **corollaire 1.13**, $P = P_0 \times 1$, qu'on abrège en $P = P_0$. Puisque le degré de P est 0, et pas $-\infty$, on sait que P_0 n'est pas nul. Donc si on pose $Q = \dfrac{1}{P_0}$, on a

$$PQ = (P_0 X^0) \times (\frac{1}{P_0} X^0) = \frac{P_0}{P_0} X^0 \times X^0 = X^{0+0} = 1$$

donc P est inversible.

Réciproquement, si P est inversible, on sait qu'il existe $Q \in \mathbb{K}[X]$ tel que $PQ = 1$: c'est la **définition 2.1**. D'après le **lemme 1.8**,

$$0 = \deg 1 = \deg P + \deg Q$$

Comme $\deg P$ et $\deg Q$ sont des entiers positifs (il est clair que le polynôme nul ne peut être inversible), on a $\deg P = \deg Q = 0$. □

5.2.2 Divisibilité dans $\mathbb{K}[X]$

Définition 5.2.3
Soient P et Q deux polynômes. On dit que P *divise* Q ou encore que Q *est un multiple de* P si, et seulement si, il existe un polynôme R tel que $Q = PR$. On notera alors $P|Q$.

> On voit qu'un polynôme inversible divise n'importe quel polynôme. En effet, si P est inversible, il existe $P^{-1} \in \mathbb{K}[X]^\times$ tel que $PP^{-1} = 1$. Si Q est n'importe quel autre polynôme,
>
> $$Q = 1 \times Q = P \times (P^{-1}Q)$$
>
> et P divise bien Q.
>
> Un autre cas trivial de divisibilité est celui des polynômes de valuation non nulle. Par exemple, si $\mathrm{val}\, P = 2$, cela signifie que les coefficients de degré 0 et 1 de P sont nuls. D'après le **corollaire 1.14**, on peut écrire alors :
>
> $$P = \sum_{k=0}^{\infty} P_k X^k = \sum_{k=2}^{\infty} P_k X^k = X^2 \sum_{k=2}^{\infty} P_k X^{k-2} = X^2 \sum_{k=0}^{\infty} P_{k+2} X^k$$
>
> et on voit que $X^2|P$. On souhaiterait maintenant un algorithme pour étudier les cas moins clairs de divisibilité. C'est l'algorithme de division euclidienne, qu'on étudie dans le paragraphe suivant.
>
> On peut aussi remarquer que n'importe quel polynôme divise le polynôme nul, puisque $0 = P \times 0$ quel que soit le polynôme P. Mais que le polynôme nul ne divise personne, sauf lui-même.

Proposition 5.2.4
Voici les propriétés élémentaires de la relation de divisibilité :

1. *Réflexivité :* $\forall P \in \mathbb{K}[X] \qquad P|P$;
2. *Transitivité :* $\forall (P,Q,R) \in \mathbb{K}[X]^3 \qquad (P|Q \text{ et } Q|R) \implies P|R$;
3. *Si* P *et* Q *sont des polynômes tels que* $P|Q$, *alors* $P^n|Q^n$ *pour tout entier* n ;
4. *Si* P, Q, R, S *sont des polynômes tels que* $P|Q$ *et* $R|S$, *alors* $PR|QS$;
5. *Si* P, Q *et* R *sont trois polynômes tels que* $P|Q$ *et* $P|R$, *alors* $P|(Q+R)$;
6. *Si* P *et* Q *sont des polynômes tels que* $P|Q$ *et* $Q|P$, *alors il existe* $\lambda \in \mathbb{K}[X]^\times$, *tel que* $P = \lambda Q$.

Preuve : Démontrons ces propriétés une par une.

1. Si $P \in \mathbb{K}[X]$, on peut écrire $P = P \times 1$ donc $P|P$.

2. Soient P, Q et R trois polynômes tels que P|Q et Q|R. Par définition, il existe des polynômes Q_1 et R_1 tels que

$$PQ_1 = Q \qquad \text{et} \qquad QR_1 = R$$

D'où $$R = QR_1 = PQ_1R_1 \qquad \text{et} \qquad P|R$$

3. Si P|Q, il existe par définition un polynôme R tel que P = QR. Donc pour tout entier n, $P^n = Q^nR^n$ et il s'ensuit que $P^n|Q^n$.
4. On suppose que P|Q et R|S. Par définition, il existe Q_1 et S_1 tels que

$$PQ_1 = Q \qquad \text{et} \qquad RS_1 = S$$

Donc $$PRQ_1S_1 = QS \qquad \text{et} \qquad PR|QS$$

5. Si P|Q et P|R, il existe des polynômes Q_1 et R_1 tels que

$$PQ_1 = Q \qquad \text{et} \qquad PR_1 = R$$

Donc $$Q + R = PQ_1 + PR_1 = P(Q_1 + R_1) \qquad \text{et} \qquad P|(Q + R)$$

6. Enfin, si P|Q et Q|P, il existe deux polynômes Q_1 et P_1 tels que

$$PQ_1 = Q \qquad \text{et} \qquad QP_1 = P$$

d'où $$P = QP_1 = PQ_1P_1$$

et $$P(1 - Q_1P_1) = 0$$

Comme on a vu que $\mathbb{K}[X]$ est intègre (**théorème 1.10**), il s'ensuit que P = 0 ou $1 - Q_1P_1 = 0$.
Si P = 0, alors $Q = Q_1P = 0$ et on a $Q = P = 1 \times P$, avec 1 qui est inversible.
Si c'est $1 - Q_1P_1$ qui est nul, on voit que $Q_1P_1 = 1$. Donc P_1 est inversible et on a bien $P = P_1Q$ avec $P_1 \in \mathbb{K}[X]^\star$.

Définition 5.2.5
Soit $P \in \mathbb{K}[X]$. On dit que P *est irréductible* si et seulement si

$$\forall (Q,R) \in \mathbb{K}[X]^2 \qquad P = QR \implies (P \in \mathbb{K}[X]^\star \qquad \text{ou} \qquad Q \in \mathbb{K}[X]^\star)$$

> Autrement dit, un polynôme est irréductible si, et seulement si, il est divisible uniquement par les inversibles, et ses multiples par des inversibles. Des exemples simples d'irréductibles sont les polynômes constants non nuls, ou les polynômes de degré 1.
>
> Cette notion est à rapprocher de celle des nombres premiers, qui sont uniquement divisibles par 1 et par eux-mêmes. Nous allons d'ailleurs voir que, comme les nombres premiers, les irréductibles de $\mathbb{K}[X]$ sont les briques élémentaires de la structure multiplicative de $\mathbb{K}[X]$.

Théorème 5.2.6
Tout polynôme s'écrit de manière unique comme produit d'irréductibles unitaires et d'un scalaire.

Preuve : L'unicité sera prouvée plus tard, à la fin du chapitre. Mais l'existence de la décomposition en produit d'irréductibles est faisable maintenant. Donc prouvons-la, par récurrence. Si n est un entier, on définit la proposition $\mathscr{P}(n)$: « Tout polynôme de degré inférieur à n peut s'écrire comme produit d'irréductibles unitaires et d'un inversible. »

- $\mathscr{P}$**(0) est vraie :** Un polynôme de degré 0 est inversible d'après le **théorème 2.2**, donc s'écrit bien comme le produit d'un scalaire par le polynôme irréductible 1.
- $\mathscr{P}(n) \Longrightarrow \mathscr{P}(n+1)$: soit n un entier tel que $\mathscr{P}(n)$ soit vraie. On se donne un polynôme P, de degré inférieur à $n+1$.
  Si $\deg P < n+1$, alors il suffit d'appliquer $\mathscr{P}(n)$ pour avoir l'existence de la décomposition de P en produit d'irréductibles unitaires.
  Si $\deg P = n+1$, alors il y a deux possibilités. Soit P est lui-même irréductible, auquel cas on peut écrire
  $$P = P_{n+1} \times \frac{P}{P_{n+1}}$$
  qui est bien le produit d'un scalaire par un irréductible unitaire. Soit P n'est pas irréductible, auquel cas il existe des polynômes non inversibles Q et R tels que $P = QR$. On a vu au **théorème 2.2** que $\mathbb{K}[X]^\times$ est l'ensemble des polynômes constants non nuls. Donc Q et R ne sont pas constants et ne peuvent être nuls, puisque P ne l'est pas. Ils sont donc de degré supérieur à 1. Donc
  $$n+1 = \deg P = \deg Q + \deg R$$
  et
  $$\deg Q \leqslant n \qquad \deg R \leqslant n$$
  D'après $\mathscr{P}(n)$, Q et R peuvent être décomposés en produits d'irréductibles unitaires par un scalaire. Quand on fait leur produit, on obtient une décomposition pour P. Ce qui achève de prouver $\mathscr{P}(n+1)$.
- **Conclusion :** $\mathscr{P}(n)$ est vraie pour tout entier n, ce qui achève la démonstration. □

5.2.3 Division euclidienne dans $\mathbb{K}[X]$

Théorème 5.2.7
Soient P *et* S *deux polynômes, avec* S *non nul. Il existe un unique couple* $(Q,R) \in \mathbb{K}[X]^2$*, tel que*
$$P = QS + R \qquad \textit{et} \qquad \deg R < \deg S$$
Q *et* R *sont respectivement appelés quotient et reste de la division euclidienne de* P *par* S.

Preuve : Faisons cela par récurrence sur le degré de P. La preuve est importante, car elle nous fournira au passage l'algorithme permettant de trouver le quotient et le reste d'une division euvlidienne. On fixe un polynôme S, quelconque, pourvu qu'il ne soit pas nul. On note $s = \deg S$. Enfin, on définit, pour tout entier p, la propriété $\mathscr{P}(n)$: « Si P est un polynôme de degré inférieur à n, il existe un couple $(Q,R) \in \mathbb{K}[X]^2$, tel que $P = QS + R$ et $\deg R < \deg S$. »

- $\mathscr{P}(s-1)$ **est vraie :** en effet, si $\deg P < s = \deg Q$, il suffit de prendre $Q = 0$ et $R = P$.
- $\mathscr{P}(n) \Longrightarrow \mathscr{P}(n+1)$ **:** soit n un entier supérieur à $s-1$. On suppose que $\mathscr{P}(n)$ est vraie. Et on se donne un polynôme P de degré inférieur à $n+1$.
  Si $\deg P \leqslant n$, alors l'existence d'un quotient et d'un reste sont garantis par $\mathscr{P}(n)$. On suppose donc $\deg P = n+1$, de sorte que

$$P = \sum_{k=0}^{n+1} P_k X^k = P_{n+1} X^{n+1} + \sum_{k=0}^{n} P_k X^k$$

En outre, $$S = \sum_{k=0}^{s} S_k X^k$$

donc $$\frac{P_{n+1}}{S_s} X^{n+1-s} S = \sum_{k=0}^{s} \frac{S_k P_{n+1}}{S_s} X^{n+1+k-s}$$

Ce polynôme est de degré $n+1$ et son terme dominant est $P_{n+1}X^{n+1}$. Donc le polynôme $P - \frac{P_{n+1}}{S_s} X^{n+1-s} S$ est de degré inférieur à n. D'après $\mathscr{P}(n)$, il existe deux polynômes Q et R, tels que

$$P - \frac{P_{n+1}}{S_s} X^{n+1-s} S = QS + R \qquad \text{avec} \qquad \deg R < s$$

d'où $$P = \left(Q + \frac{P_{n+1}}{S_s} X^{n+1-s}\right) S + R \qquad \text{avec} \qquad \deg R < s$$

Ceci démontre $\mathscr{P}(n+1)$.

- **Conclusion :** $\mathscr{P}(n)$ est vraie pour tout entier n supérieur à $s-1$.

Ceci achève la preuve de l'existence d'une division euclidienne. Assurons-nous de l'unicité. Soit P un polynôme ; on suppose avoir déterminé (Q_1, R_1) et (Q_2, R_2) dans $\mathbb{K}[X]^2$, tels que

$$P = Q_1 S + R_1 = Q_2 S + R_2 \qquad \text{avec} \qquad \deg R_1, \deg R_2 < s$$

Alors $$(Q_1 - Q_2) S = R_2 - R_1$$

Or, $$\deg (Q_1 - Q_2) S = \deg S + \deg (Q_1 - Q_2) = \deg (R_2 - R_1) < s$$

Cette relation est impossible à moins que $\deg (Q_1 - Q_2)$ soit négatif ; la seule possibilité est donc $\deg (Q_1 - Q_2) = -\infty$, c'est-à-dire $Q_1 = Q_2$.

Une fois ceci acquis, on a

$$P = Q_1 S + R_1 = Q_1 S + R_2$$

donc $$R_1 = R_2$$

Le quotient et le reste d'une division euclidienne sont uniques. □

On peut maintenant caractériser la divisibilité à l'aide de la division euclidienne :

Proposition 5.2.8
Soient P *et* S *deux polynômes, avec* S *non nul. Alors* S|P *si et seulement si le reste de la division euclidienne de* P *par* S *est nul.*

Preuve : C'est trivial. □

5.3 Racines d'un polynôme

5.3.1 Fonctions polynomiales

Définition 5.3.1
Soit $P \in \mathbb{K}[X]$. On appelle *fonction polynomiale associée à* P, notée $\tilde{P}$, l'application

$$\begin{aligned}\tilde{P} : \mathbb{K} &\longrightarrow \mathbb{K} \\ x &\longmapsto \sum_{n=0}^{\infty} P_n x^n\end{aligned}$$

Théorème 5.3.2
L'application $F : \begin{aligned}\mathbb{K}[X] &\longrightarrow \mathbb{K}^{\mathbb{K}} \\ P &\longmapsto \tilde{P}\end{aligned}$ *est linéaire et multiplicative, c'est-à-dire que*

$$\forall (P,Q) \in \mathbb{K}[X] \qquad F(PQ) = F(P)F(Q)$$

Preuve : Soient P et Q deux polynômes, soit λ un scalaire. On a

$$\lambda P + Q = \sum_{n=0}^{\infty} (\lambda P + Q)_n X^n = \sum_{n=0}^{\infty} (\lambda P_n + Q_n) X^n$$

donc
$$\begin{aligned}\forall x \in \mathbb{K} \qquad F(\lambda P + Q)(x) &= \sum_{n=0}^{\infty} (\lambda P_n + Q_n)(x) \\ &= \lambda \sum_{n=0}^{\infty} P_n x^n + \sum_{n=0}^{\infty} Q_n x^n = \lambda F(P)(x) + F(Q)(x)\end{aligned}$$

et
$$F(\lambda P + Q) = \lambda F(P) + F(Q)$$

Vérifions maintenant la multiplicativité. On utilise le **corollaire 1.16** et la linéarité de F :

$$\begin{aligned}\forall x \in \mathbb{K} \qquad F(PQ)(x) &= F\Big(\sum_{n=0}^{\infty} \sum_{m=0}^{\infty} P_n Q_m X^{n+m} \Big) = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} P_n Q_m x^{n+m} \\ &= \Big(\sum_{n=0}^{\infty} P_n x^n \Big) \Big(\sum_{m=0}^{\infty} Q_m x^m \Big) = F(P)(x) \times F(Q)(x)\end{aligned}$$

d'où
$$F(PQ) = F(P)F(Q)$$ □

5.3.2 Racines d'un polynôme

Définition 5.3.3
Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On dit que *a est racine de* P si et seulement si $\tilde{P}(a) = 0$.

Voici le théorème fondamental caractérisant les racines d'un polynôme :

Théorème 5.3.4
Soient $P \in \mathbb{K}[X]$ *et* $a \in \mathbb{K}$. *a est racine de* P *si et seulement si* $(X - a) | P$.

Preuve : D'après le théorème de division euclidienne, il existe des polynômes Q et R tels que

$$P = (X - a)Q + R \qquad \text{avec} \qquad \deg R < \deg(X - a) = 1$$

Donc R est en fait un polynôme constant, c'est-à-dire qu'il existe $\lambda \in \mathbb{K}$ tel que $R = \lambda$. On a donc

$$P = (X - a)Q + \lambda$$

D'après la linéarité et la multiplicativité de F,

$$F(P) = F(X - a) \times F(Q) + \lambda F(1)$$

d'où
$$\tilde{P}(a) = \lambda$$

Par suite, a est racine de P si et seulement si $\lambda = 0$, c'est-à-dire que le reste de la division euclidienne de P par $X - a$ est nul. Ce qui est équivalent à dire que $(X-a)|P$. □

Corollaire 5.3.5
Soit $P \in \mathbb{K}[X]$. *Soient* $n \in \mathbb{N}^\star$ *et* $a_1, \dots, a_n \in \mathbb{K}$ *des racines distinctes de* P. *Alors*

$$(X-a_1)\cdots(X-a_n)|P$$

Preuve : On démontre ceci par récurrence. Pour tout entier p, on definit la propriété $\mathscr{P}(p)$: « Soit P un polynôme de degré P. Soient $n \in \mathbb{N}^\star$ et $a_1, \dots, a_n \in \mathbb{K}$ des racines de P. Alors $(X-a_1)\dots(X-a_n)$ divise P. »

- **$\mathscr{P}(1)$ est vraie :** soit P un polynôme de degré 1. On sait qu'il admet une et une seule racine, qu'on note a. Et le **théorème 3.4** nous dit que $X-a$ divise P.
- **$\mathscr{P}(p) \Longrightarrow \mathscr{P}(p+1)$** : soit p un entier, tel que $\mathscr{P}(p)$ soit vraie. On se donne un polynôme P, de degré $p+1$. Soient n un entier, et $a_1, \dots, a_n$ des racines de P, distinctes.
  D'après le **théorème 3.4**, $(X-a_n)|P$ donc il existe un polynôme Q tel que $P = (X-a_n)Q$. Il découle du **théorème 3.2** que

  $$\tilde{P} = F(X-a_n)\tilde{Q}$$

  c'est-à-dire $\qquad \forall x \in \mathbb{K} \qquad \tilde{P}(x) = (x-a_n)\tilde{Q}(x)$

  Puisque $a_1, \dots, a_{n-1}$ sont des racines de P, distinctes deux-à-deux et différentes de a_n, on obtient que ces nombres sont aussi des racines que Q. Mais Q est de degré p. D'après $\mathscr{P}(p)$, $(X-a_1)\cdots(X-a_{n-1})$ divise Q. Donc il existe un polynôme R tel que

  $$Q = (X-a_1)\cdots(X-a_{n-1})R$$

  d'où $\qquad P = (X-a_n)Q = (X-a_1)\cdots(X-a_n)R$

  ce qui établit $\mathscr{P}(p+1)$.
- **Conclusion :** $\mathscr{P}(p)$ est vraie pour tout entier p, ce qui achève la démonstration. □

Corollaire 5.3.6
Soit P *un polynôme de degré* $p \in \mathbb{N}$. *Il admet au plus* p *racines distinctes.*

Preuve : On sait déjà que les polynômes de degré 0 n'admettent aucune racine, ce qui prouve le théorème pour $p = 0$.

Si p n'est pas nul, on se donne $n \in \mathbb{N}$ tel qu'il existe au moins n racines distinctes $a_1, \dots, a_n$ de P. D'après le **corollaire 3.5**, $(X-a_1)\cdots(X-a_n)$ divise P donc

$$p = \deg P \geqslant \deg\big((X-a_1)\cdots(X-a_n)\big) = n$$

Donc P admet moins de p racines distinctes. □

Corollaire 5.3.7
Si $\mathbb{K}$ *est infini, l'application* F *est injective.*

Preuve : On sait que F est linéaire, donc il suffit d'en étudier le noyau. Soit $P \in \operatorname{Ker} F$. Cela signifie que $\tilde{P}$ est l'application nulle. Donc tout élément de $\mathbb{K}$ est racine. Cela nous fait une infinité de racines. Hmmm... C'est impossible, à moins que P soit le polynôme nul. Donc F est injective. □

Ce théorème nous assure donc qu'il y a une correspondance bijective entre polynômes et fonctions polynomiales sur $\mathbb{R}$ ou $\mathbb{C}$. Comme on peut le constater, ce résultat est loin d'être trivial puisqu'il résulte de toute une chaîne de théorèmes et du fait que $\mathbb{R}$ et $\mathbb{C}$ sont infinis.

5.4 Dérivation et racines multiples

Dans toute la suite, on suppose que $\mathbb{K}$ est un corps dans lequel pour tout entier $n \in \mathbb{N}$, n n'est pas nul.

5.4.1 Dérivation

Théorème 5.4.1
Il existe un unique endomorphisme de $\mathbb{K}[X]$*, noté* D*, tel que*

$$\forall n \in \mathbb{N}^\star \qquad D(X^n) = nX^{n-1} \qquad \textit{et} \qquad D(1) = 0$$

Preuve : Un tel endomorphisme existe : il suffit de poser

$$\forall P \in \mathbb{K}[X] \qquad D(P) = \sum_{n=1}^{\infty} nP_nX^{n-1} = \sum_{n=0}^{\infty} (n+1)P_{n+1}X^n$$

qui est clairement linéaire d'après la définition de la structure d'espace vectoriel sur $\mathbb{K}[X]$, et qui transforme les polynômes en polynômes.

Réciproquement, soit D un endomorphisme de $\mathbb{K}[X]$ tel que

$$\forall n \in \mathbb{N}^\star \qquad D(X^n) = nX^{n-1} \qquad \text{et} \qquad D(1) = 0$$

Si P est un polynôme quelconque, dans la mesure où D est linéaire, on a

$$D(P) = D\Big(\sum_{n=0}^{\infty} P_nX^n\Big) = \sum_{n=0}^{\infty} P_nD(X^n) = \sum_{n=1}^{\infty} nP_nX^{n-1}$$

qui est bien l'endomorphisme de $\mathbb{K}[X]$ décrit plus haut. □

Définition 5.4.2
L'endomorphisme D donné par le **théorème 4.1** est appelé *dérivation*. On notera

$$\forall P \in \mathbb{K}[X] \qquad P' = D(P)$$

et

$$\forall n \in \mathbb{N} \quad \forall P \in \mathbb{K}[X] \qquad P^{(n)} = D^n(P)$$

Théorème 5.4.3
La dérivation est un endomorphisme de $\mathbb{K}[X]$ *tel que*

$$\forall (P,Q) \in \mathbb{K}[X] \qquad D(PQ) = P'Q + Q'P$$

Preuve : On vérifie d'abord la propriété pour les monômes unitaires :

$$\begin{aligned} \forall (n,m) \in \mathbb{N} \qquad D(X^nX^m) &= D(X^{n+m}) = (n+m)X^{n+m-1} \\ &= nX^{n-1}X^m + mX^{m-1}X^n \\ D(X^nX^m) &= D(X^n)X^m + D(X^m)X^n \end{aligned}$$

À présent, si P et Q sont deux polynômes quelconques, on sait que

$$PQ = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} P_n Q_m X^n X^m$$

Comme D est linéaire,

$$\begin{aligned} D(PQ) &= \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} P_n Q_m D(X^n X^m) = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} P_n D(X^n) Q_m X^m + \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} P_n X^n Q_m D(X^m) \\ &= D(P)Q + PD(Q) \end{aligned}$$

□

Théorème 5.4.4 (Formule de Leibniz)
Soient P *et* Q *deux polynômes, soit n un entier. On a*

$$D^n(PQ) = \sum_{k=0}^{n} C_n^k P^{(k)} Q^{(n-k)}$$

Preuve : On peut faire cela par récurrence, par exemple. La formule marche clairement pour $n = 0$. On suppose qu'elle est vraie pour un entier n. On a alors

$$D^{n+1}(PQ) = D\big(D^n(PQ)\big) = D\Big(\sum_{k=0}^{n} C_n^k P^{(k)} Q^{(n-k)}\Big)$$

On utilise la linéarité de la dérivation

$$D^{n+1}(PQ) = \sum_{k=0}^{n} C_n^k D(P^{(k)} Q^{(n-k)})$$

puis la formule de dérivation d'un produit et on sépare les sommes :

$$\begin{aligned} D^{n+1}(PQ) &= \sum_{k=0}^{n} C_n^k (P^{(k+1)} Q^{(n-k)} + P^{(k)} Q^{(n-k+1)}) \\ &= \sum_{k=0}^{n} C_n^k P^{(k+1)} Q^{(n-k)} + \sum_{k=0}^{n} C_n^k P^{(k)} Q^{(n-k+1)} \end{aligned}$$

On procède à un décalage d'indice $k \leftarrow k+1$ dans la première somme puis on regroupe les sommes en utilisant la relation de Pascal :

$$\begin{aligned} D^{n+1}(PQ) &= \sum_{k=1}^{n+1} C_n^{k-1} P^{(k)} Q^{(n-k+1)} + \sum_{k=0}^{n} C_n^k P^{(k)} Q^{(n-k+1)} \\ &= P^{(n+1)} Q^{(0)} + \sum_{k=1}^{n} C_{n+1}^k P^{(k)} Q^{(n+1-k)} + P^{(0)} Q^{(n+1)} \\ D^{n+1}(PQ) &= \sum_{k=0}^{n+1} C_{n+1}^k P^{(k)} Q^{(n+1-k)} \end{aligned}$$

Par récurrence, la formule est donc vraie pour tout entier n. □

Théorème 5.4.5 (Formule de Taylor)

$$\forall P \in \mathbb{K}[X] \qquad P = \sum_{k=0}^{\infty} \frac{P^{(k)}(a)}{k!} (X-a)^k$$

Preuve : On vérifie d'abord la formule pour les monômes. Soit n un entier. Il est aisé de vérifier par récurrence que

$$\forall k \in \mathbb{N} \qquad D^k(X^n) = \begin{cases} n(n-1)\cdots(n-k+1)X^{n-k} \text{ si } k \leqslant n \\ 0 \text{ si } k \geqslant n+1 \end{cases}$$

donc $$\sum_{k=0}^{\infty} \frac{\mathrm{D}^k(\mathrm{X}^n)(a)}{k!}(\mathrm{X}-a)^k = \sum_{k=0}^{n} \mathrm{C}_n^k a^{n-k}(\mathrm{X}-a)^k = (\mathrm{X}-a+a)^n = \mathrm{X}^n$$

d'après la formule du binôme de Newton.

Maintenant, si $\mathrm{P} \in \mathbb{K}[\mathrm{X}]$, on a

$$\begin{aligned}
\mathrm{P} &= \sum_{n=0}^{\infty} \mathrm{P}_n \mathrm{X}^n = \sum_{n=0}^{\infty} \mathrm{P}_n \sum_{k=0}^{\infty} \frac{\mathrm{D}^k(\mathrm{X}^n)(a)}{k!}(\mathrm{X}-a)^k = \sum_{k=0}^{\infty}\sum_{n=0}^{\infty} \mathrm{P}_n \mathrm{D}^k(\mathrm{X}^n)(a)\frac{(\mathrm{X}-a)^k}{k!} \\
&= \sum_{k=0}^{\infty} \mathrm{D}^k\Big(\sum_{n=0}^{\infty} \mathrm{P}_n \mathrm{X}^n\Big)(a)\,\frac{(\mathrm{X}-a)^k}{k!} \\
\mathrm{P} &= \sum_{k=0}^{\infty} \frac{\mathrm{P}^{(k)}(a)}{k!}(\mathrm{X}-a)^k
\end{aligned}$$

□

5.4.2 Racines multiples

Définition 5.4.6
Soient P un polynôme, $a \in \mathbb{K}$ et $m \in \mathbb{N}^\star$. On dit que a est *racine multiple de* P, de *multiplicité* m, si et seulement si $(\mathrm{X}-a)^m$ divise P, mais $(\mathrm{X}-a)^{m+1}$ ne divise pas P.

Théorème 5.4.7
Soient P *un polynôme,* $a \in \mathbb{K}$ *et* $m \in \mathbb{N}^\star$. *a est racine de* P*, de multiplicité m, si et seulement si*

$$\mathrm{P}(a) = \mathrm{P}'(a) = \cdots = \mathrm{P}^{(m-1)}(a) = 0 \qquad \textit{et} \qquad \mathrm{P}^{(m)}(a) \neq 0$$

Preuve : On utilise la formule de Taylor et on casse la somme au m-ème terme :

$$\mathrm{P} = \sum_{k=0}^{m-1} \frac{\mathrm{P}^{(k)}(a)}{k!}(\mathrm{X}-a)^k + \frac{\mathrm{P}^{(m)}(a)}{m!}(\mathrm{X}-a)^m + \sum_{k=m+1}^{\infty} \frac{\mathrm{P}^{(k)}(a)}{k!}(\mathrm{X}-a)^k$$

et on met en facteur $(\mathrm{X}-a)^m$:

$$\mathrm{P} = \sum_{k=0}^{m-1} \frac{\mathrm{P}^{(k)}(a)}{k!}(\mathrm{X}-a)^k + (\mathrm{X}-a)^m\Big(\frac{\mathrm{P}^{(m)}(a)}{m!} + \sum_{k=m+1}^{\infty} \frac{\mathrm{P}^{(k)}(a)}{k!}(\mathrm{X}-a)^{k-m}\Big)$$

Si on pose

$$\mathrm{R} = \sum_{k=0}^{m-1} \frac{\mathrm{P}^{(k)}(a)}{k!}(\mathrm{X}-a)^k \qquad \text{et} \qquad \mathrm{Q} = \frac{\mathrm{P}^{(m)}(a)}{m!} + \sum_{k=m+1}^{\infty} \frac{\mathrm{P}^{(k)}(a)}{k!}(\mathrm{X}-a)^{k-m}$$

on observe que $$\mathrm{P} = (\mathrm{X}-a)^m\mathrm{Q} + \mathrm{R} \qquad \text{avec} \qquad \deg \mathrm{R} < m$$

donc Q et R sont le quotient et le reste de la division euclidienne de P par $(\mathrm{X}-a)^m$.

Supposons que a est racine d'ordre m de P. Cela signifie que $(\mathrm{X}-a)^m$ divise P, donc que $\mathrm{R} = 0$. D'où $\mathrm{P} = (\mathrm{X}-a)^m\mathrm{Q}$. Et comme $(\mathrm{X}-a)^{m+1}$ ne divise pas P, il est exclu que a soit racine de Q. Donc $\mathrm{Q}(a) \neq 0$. Or,

$$\mathrm{Q}(a) = \frac{\mathrm{P}^{(m)}(a)}{m!} + \sum_{k=m+1}^{\infty} \frac{\mathrm{P}^{(k)}(a)}{k!}(a-a)^{k-m} = \frac{\mathrm{P}^{(m)}(a)}{m!}$$

et on en déduit $$\mathrm{P}^{(m)}(a) \neq 0$$

Il reste à montrer que les autres dérivées de P sont nulles. Comme on sait que R est le polynôme nul, le polynôme $\mathrm{R}(\mathrm{X}+a)$ est nul également. Donc

$$0 = R(X+a) = \sum_{k=0}^{m-1} \frac{P^{(k)}(a)}{k!}(X+a-a)^k = \sum_{k=0}^{m-1} \frac{P^{(k)}(a)}{k!}X^k$$

Un polynôme est nul si et seulement si tous ses coefficients sont nuls donc

$$\forall k \in [\![0\,;m-1]\!] \qquad P^{(k)}(a) = 0$$

Ceci démontre la première partie de notre equivalence.

Réciproquement, supposons que $P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0$ mais que $P^{(m)}(a) \neq 0$. On a automatiquement que $R = 0$, donc $(X-a)^m$ divise P. Et comme

$$Q(a) = \frac{P^{(m)}(a)}{m!} \neq 0$$

on voit que $(X-a)$ ne divise pas Q. Et $(X-a)^{m+1}$ ne divise donc pas P. □

5.5 Polynômes scindés

5.5.1 Le théorème de d'Alembert

Définition 5.5.1
Soit $P \in \mathbb{K}[X]$, de degré $n \in \mathbb{N}$. On dit qu'il est *scindé* si, et seulement si, il existe $\lambda, a_1, \ldots, a_n \in \mathbb{K}$, tels que

$$P = \lambda \prod_{k=1}^{n} (X - a_k)$$

Théorème 5.5.2 (Théorème de d'Alembert)
Tout polynôme non constant dans $\mathbb{C}[X]$ *est scindé.*

Preuve : Hors-programme. □

Le théorème de d'Alembert nous dit donc que tout polynôme à coefficients complexes, non constant admet autant de racines complexes (en comptant les racines multiples avec leur multiplicité) que son degré. C'est un résultat très fort (et difficile) : pour s'en convaincre, rappelons-nous que la situation dans $\mathbb{R}[X]$ est plus compliquée. Il y a des polynômes qui n'admettent pas de racines réelles, comme X^2+1. Ou n'importe quel polynôme de degré 2, de discriminant négatif.

Ce théorème a d'importantes conséquences, comme la détermination précise des irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$.

Corollaire 5.5.3
Les polynômes irréductibles de $\mathbb{C}[X]$ *sont les polynômes de degré 1.*

Preuve : Les polynômes de degré 1 sont évidemment irréductibles : si $\deg P = 1$ et si Q et R sont tels que $P = QR$, on a

$$1 = \deg P = \deg Q + \deg R \qquad \text{avec} \qquad \deg Q, \deg R \geqslant 0$$

Donc l'un des polynômes Q ou R doit être de degré 0. Ce qui montre que P est irréductible.

Réciproquement, soit P un polynôme irréductible. Puisqu'il n'est pas constant, on a $\deg P \geqslant 1$. D'après le **théorème de d'Alembert**, P admet au moins une racine complexe, qu'on note a. Donc $(X-a)|P$ et il existe $Q \in \mathbb{C}[X]$ tel que

$$P = (X - a)Q$$

Mais P est irréductible et $(X - a)$ n'est pas constant ; donc Q doit être constant. Et P est bien de degré 1. □

Pour déterminer les irréductibles de $\mathbb{R}[X]$, nous aurons besoin du théorème suivant :

Théorème 5.5.4
Soit $P \in \mathbb{R}[X]$. *Soit* a *une racine complexe de* P. *Alors* $\overline{a}$ *est aussi racine complexe de* P.

Preuve : Puisque a est racine de P, on a

$$0 = P(a) = \sum_{n=0}^{\infty} P_n a^n$$

Il suffit de prendre le conjugué de cette expression, en se rappelant que les coefficients de P sont réels :

$$0 = \overline{\sum_{n=0}^{\infty} P_n a^n} = \sum_{n=0}^{\infty} P_n \overline{a}^n$$

donc $\overline{a}$ est racine de P. □

Théorème 5.5.5
Les irréductibles de $\mathbb{R}[X]$ *sont*

- *Les polynômes de degré 1 ;*
- *les polynômes de degré 2, dont les discriminant est négatif.*

Preuve : Les polynômes de degré 1 de $\mathbb{R}[X]$ sont irréductibles (la preuve est la même que pour $\mathbb{C}[X]$).

Soit maintenant P, de degré 2, de discriminant négatif. Si Q et R sont dans $\mathbb{R}[X]$, tels que $P = QR$, on a

$$2 = \deg P = \deg Q + \deg R$$

donc $\begin{cases} \deg Q = 0 \\ \deg R = 2 \end{cases}$ ou $\begin{cases} \deg Q = 1 \\ \deg R = 1 \end{cases}$ ou $\begin{cases} \deg Q = 2 \\ \deg R = 0 \end{cases}$

Si on est dans le premier ou le troisième cas, on obtient que P est irréductible. Supposons qu'on soit dans le deuxième cas ; alors Q est de la forme $\lambda(X - a)$ et P admet une racine. C'est une contradiction. Donc P est bien irréductible.

Réciproquement, soit P un polynôme de $\mathbb{R}[X]$, irréductible. On suppose $\deg P \geqslant 2$, puisqu'on sait déjà que tout polynôme de degré 1 est irréductible. Alors P n'admet aucune racine réelle : s'il en admettait, il serait divisible par un polynôme de la forme $(X - a)$, avec $a \in \mathbb{R}$, ce qui nierait l'irréductibilité son irréductibilité.

En revanche, il admet des racines complexes, d'après le **théorème de d'Alembert**. Soit a l'une d'elle ; on sait donc que a n'est pas réel, et que $\overline{a}$ est aussi racine de P. Donc $(X - a)(X - \overline{a})$ divise P dans $\mathbb{C}[X]$: il existe $Q \in \mathbb{C}[X]$, tel que

$$P = (X - a)(X - \overline{a})Q = (X^2 - 2X\mathrm{Re}\, a + |a|^2)Q \qquad (\mathbf{1})$$

Montrons que Q appartient en fait à $\mathbb{R}[X]$. Le polynôme $X^2 - 2X\mathrm{Re}\, a + |a|^2$ est à coefficients réels donc on peut procéder à la division euclidienne de P par $X^2 - 2X\mathrm{Re}\, a + |a|^2$.

$$\exists S, R \in \mathbb{R}[X] \qquad P = (X^2 - 2X\mathrm{Re}\, a + |a|^2)S + R \qquad \text{avec} \qquad \deg R \leqslant 1$$

Puisque S et R sont à coefficients réels, *a fortiori* complexes, on en déduit qu'ils sont aussi le quotient et le reste de cette division euclidienne dans $\mathbb{C}[X]$. D'après (**1**), R = 0 (et S = Q, accessoirement). En résumé,

$$P = (X^2 - 2X\mathrm{Re}\, a + |a|^2)S \qquad \text{avec} \qquad S \in \mathbb{R}[X]$$

Comme P est irréductible, S est un polynôme constant. Donc P est de degré 2, à discriminant négatif puisque

$$4(\mathrm{Re}\, a)^2 - 4|a|^2 = 4((\mathrm{Re}\, a)^2 - |a|^2) < 0$$ □

Corollaire 5.5.6
Tout polynôme à coefficients réels, de degré impair, admet au moins une racine réelle.

Preuve : Soit P un polynôme à coefficients réels, n'admettant aucune racine réelle. La décomposition de P en produit d'irréductibles ne contient aucun terme de degré 1. Donc il s'agit uniquement de termes de degré 2 (de discriminant négatif), d'après la détermination des irréductibles de $\mathbb{R}[X]$ qui vient d'être faite. Le degré de P est donc pair.

Par contre-apposée, si le degré de P est impair, P admet des racines réelles. □

5.5.2 Relations entre coefficients et racines d'un polynôme scindé

Le but de ce paragraphe est d'exprimer les coefficients d'un polynôme à l'aide de ses racines. On commence par une définition :

Définition 5.5.7 (Fonctions symétriques élémentaires)
Soient $n \in \mathbb{N}^\star$ et $k \in [\![1\,;n]\!]$. On appelle k-ème *fonction symétrique élémentaire d'ordre n* la fonction $\sigma_k^n : \mathbb{K}^n \longrightarrow \mathbb{K}$ définie par :

$$\forall (x_1, \ldots, x_n) \in \mathbb{K}^n \qquad \sigma_k^n(x_1, \ldots, x_n) = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} x_{i_1} \cdots x_{i_k}$$

Exemple 5.5.8
Oui, ce n'est pas très beau. Mais comme toujours, il suffit de faire quelques exemples pour voir ce que sont ces objets. Supposons par exemple que $n = 4$ et donnons-nous x_1, x_2, x_3 et x_4 dans $\mathbb{K}$. Pour simplifier l'écriture, on note simplement σ_k au lieu de $\sigma_k^4(x_1, x_2, x_3, x_4)$. Par définition,

$$\sigma_1 = \sum_{1 \leqslant i_1 \leqslant 4} x_{i_1} = x_1 + x_2 + x_3 + x_4$$

Jusque là, c'est simple. Ensuite,

$$\sigma_2 = \sum_{1 \leqslant i_1 < i_2 \leqslant 4} x_{i_1} x_{i_2}$$

On réfléchit un peu : i_1 ne peut prendre que les valeurs 1, 2 et 3 puisqu'il doit être strictement inférieur à i_2. Si i_1 vaut 1, alors i_2 prend les valeurs 2, 3 et 4. Quand i_1 vaut 2, i_2 prend les valeurs 3 et 4. Et enfin, quand i_1 vaut 3, i_2 ne peut valoir que 4. Donc

$$\sigma_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$$

De la même manière, $$\sigma_3 = x_1x_2x_3 + x_1x_3x_4 + x_2x_3x_4$$

et enfin, $$\sigma_4 = x_1x_2x_3x_4$$

Fixons $n \in \mathbb{N}^\star$ et $x_1, \dots, x_n \in \mathbb{K}$. Il y a deux fonctions symétriques élémentaires qui sont faciles à imaginer :

$$\sigma_1^n(x_1, \dots, x_n) = \sum_{1 \leqslant i_1 \leqslant n} x_{i_1} = \sum_{i=1}^{n} x_i$$

Il s'agit simplement de la somme de tous les termes de la suite $(x_i)_{1 \leqslant i \leqslant n}$. On a aussi

$$\sigma_n^n(x_1, \dots, x_n) = \sum_{1 \leqslant i_1 < \cdots < i_n \leqslant n} x_{i_1} \cdots x_{i_n}$$

Si $i_1, \dots, i_n$ sont des entiers donnés, tels que $1 \leqslant i_1 < \cdots < i_n \leqslant n$, l'application $j \longmapsto i_j$ est injective de $[\![1 ; n]\!]$ sur lui-même donc $\{i_1, \dots, i_n\} = [\![1 ; n]\!]$. Et on a montré qu'il existe une seule manière d'ordonner une partie finie de $\mathbb{N}$ donc

$$\forall\, j \in [\![1 ; n]\!] \qquad i_j = j$$

Donc la somme qui définit $\sigma_n^n(x_1, \dots, x_n)$ ne comporte qu'un seul terme. D'où

$$\sigma_n^n(x_1, \dots, x_n) = x_1 \cdots x_n$$

C'est simplement le produit des termes de la suite $(x_i)_{1 \leqslant i \leqslant n}$.

Lemme 5.5.9 (Relations entre fonctions symétriques)
Soient $n \geqslant 2$ un entier, $k \in [\![1 ; n-1]\!]$ et $x_1, \dots, x_{n+1} \in \mathbb{K}$. Alors

$$\sigma_{k+1}^n(x_1, \dots, x_n) + x_{n+1}\sigma_k^n(x_1, \dots, x_n) = \sigma_{k+1}^{n+1}(x_1, \dots, x_{n+1})$$

et

$$x_{n+1}\sigma_n^n(x_1, \dots, x_n) = \sigma_{n+1}^{n+1}(x_1, \dots, x_{n+1})$$

Preuve : Pour simplifier l'écriture, on se contentera d'écrire σ_k^n ou σ_k^{n+1} au lieu de

$$\sigma_k^n(x_1, \dots, x_n) \qquad \text{ou} \qquad \sigma_k^{n+1}(x_1, \dots, x_{n+1})$$

La deuxième relation est claire, puisqu'on a expliqué que

$$\sigma_{n+1}^{n+1} = x_1 \cdots x_{n+1} = x_{n+1} \times x_1 \cdots x_n = x_{n+1}\,\sigma_n^n$$

Pour la première, on fixe $k \in [\![1 ; n-1]\!]$ et on considère les ensembles :

$$\mathrm{A} = \{(i_1, \dots, i_{k+1}) \in [\![1 ; n+1]\!]^{k+1} \mid 1 \leqslant i_1 < \cdots < i_{k+1} \leqslant n+1\}$$

$$\mathrm{B} = \{(i_1, \dots, i_{k+1}) \in [\![1 ; n+1]\!]^{k+1} \mid 1 \leqslant i_1 < \cdots < i_{k+1} \leqslant n\}$$

et

$$\mathrm{C} = \{(i_1, \dots, i_{k+1}) \in [\![1 ; n+1]\!]^{k+1} \mid 1 \leqslant i_1 < \cdots < i_k \leqslant n \quad \text{et} \quad i_{k+1} = n+1\}$$

On observe alors, simplement d'après leur définition que

$$\mathrm{A} = \mathrm{B} \cup \mathrm{C} \qquad \mathrm{B} \cap \mathrm{C} = \emptyset$$

et

$$\mathrm{B} = \{(i_1, \dots, i_{k+1}) \in [\![1 ; n]\!]^{k+1} \mid 1 \leqslant i_1 < \cdots < i_{k+1} \leqslant n\}$$

Alors

$$\sigma_{k+1}^n = \sum_{(i_1, \dots, i_{k+1}) \in \mathrm{B}} x_{i_1} \cdots x_{i_{k+1}}$$

et

$$x_{k+1}\,\sigma_k^n = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} x_{i_1} \cdots x_{i_k} x_{n+1} = \sum_{(i_1, \dots, i_{k+1}) \in \mathrm{C}} x_{i_1} \cdots x_{i_k} \underbrace{x_{i_{k+1}}}_{= x_{n+1}}$$

Par suite,

$$\sigma_{k+1}^n + x_{n+1}\sigma_k^n = \sum_{\mathrm{B}} x_{i_1} \cdots x_{i_{k+1}} + \sum_{\mathrm{C}} x_{i_1} \cdots x_{i_{n+1}}$$

et comme B et C sont disjoints, de réunion A, on peut regrouper ces sommes pour conclure. □

Corollaire 5.5.10 (Relations coefficients racines)
Soit $P \in \mathbb{K}[X]$ *un polynôme scindé de degré n, dont on note* λ *le coefficient dominant et* $a_1, \dots, a_n$ *les racines comptées avec multiplicités. Alors*

$$\forall k \in [\![0\,;n-1]\!] \qquad P_k = (-1)^{n-k}\lambda\sigma_{n-k}(a_1,\dots,a_n)$$

Preuve : On vérifie que la proposition est vraie pour $n = 1$. Si P est de degré 1, de coefficient dominant λ et avec pour racine a_1, on a

$$P = P_0 + P_1X = \lambda(X - a_1) = \lambda X - \lambda a_1$$

Deux polynômes sont égaux si, et seulement si, ils ont les mêmes coefficients donc

$$P_0 = -\lambda a_1 = (-1)^{1-0}\lambda\sigma^1_{1-0}$$

On le vérifie également pour $n = 2$: si P est de degré 2, de coefficient dominant λ et de racines a_1, a_2, on a

$$P = P_0 + P_1X + P_2X^2 = \lambda(X - a_1)(X - a_2) = \lambda X^2 - \lambda(a_1 + a_2)X + \lambda a_1 a_2$$

donc $$P_0 = \lambda a_1 a_2 = (-1)^{2-0}\lambda\sigma^2_{2-2}$$

et $$P_1 = -\lambda(a_1 + a_2) = (-1)^{2-1}\lambda\sigma^2_{2-1}$$

On suppose maintenant la formule établie pour tout polynôme de degré $n \geqslant 2$. On se donne $P \in \mathbb{K}[X]$, scindé, de degré $n+1$, de racines $a_1, \dots, a_{n+1}$ et de coefficient dominant λ. On a donc

$$P = \lambda \prod_{k=1}^{n+1}(X - a_k) = \lambda(X - a_{n+1}) \times \prod_{k=1}^{n}(X - a_k)$$

D'après l'hypothèse de récurrence,

$$\prod_{k=1}^{n}(X - a_k) = X^n + \sum_{k=0}^{n-1}(-1)^{n-k}\sigma^n_{n-k}X^k$$

d'où
$$\begin{aligned}\frac{P}{\lambda} &= (X - a_{n+1})\left(X^n + \sum_{k=0}^{n-1}(-1)^{n-k}\sigma^n_{n-k}X^k\right)\\ &= X^{n+1} - a_{n+1}X^n + \sum_{k=0}^{n-1}(-1)^{n-k}\sigma^n_{n-k}X^{k+1} - \sum_{k=0}^{n-1}(-1)^{n-k}a_{n+1}\sigma^n_{n-k}X^k\end{aligned}$$

On fait un changement d'indice $k \leftarrow k+1$ dans la première somme puis on regroupe :

$$\begin{aligned}\frac{P}{\lambda} &= X^{n+1} - a_{n+1}X^n + \sum_{k=1}^{n}(-1)^{n+1-k}\sigma_{n+1-k}X^k + \sum_{k=0}^{n-1}(-1)^{n+1-k}a_{n+1}\,\sigma^n_{n-k}X^k\\ &= X^{n+1} - \underbrace{(a_{n+1} + \sigma^n_1)}_{\sigma^{n+1}_1}X^n + (-1)^{n+1}a_{n+1}\sigma^n_n + \sum_{k=1}^{n-1}(-1)^{n+1-k}\underbrace{(\sigma^n_{n+1-k} + a_{n+1}\sigma^n_{n-k})}_{=\sigma^{n+1}_{n+1-k}}X^k\\ \frac{P}{\lambda} &= X^{n+1} + \sum_{k=0}^{n-1}(-1)^{n+1-k}\sigma^{n+1}_{n+1-k}X^k\end{aligned}$$

On a utilisé le **lemme 5.9** pour la dernière étape. Il ne reste plus qu'à multiplier par λ et utiliser le fait que deux polynômes sont égaux si, et seulement si, ils ont les mêmes coefficients, pour conclure que le théorème est vrai pour les polynômes de degré $n+1$. □

Ce qui suit n'est qu'un cas particulier de ce qui précède, mais est suffisamment important pour qu'on l'évoque :

Corollaire 5.5.11
Soient $n \in \mathbb{N}^\star$, *et* P *scindé, de degré* n *et de coefficient dominant* λ.

- *La somme des racines de* P *(comptées avec multiplicités) vaut* $-\frac{P_{n-1}}{\lambda}$.
- *Le produit des racines de* P *(comptées avec multiplicités) vaut* $(-1)^n \frac{P_0}{\lambda}$.

5.6 Arithmétique des polynômes

Il s'agit de faire le même travail que dans $\mathbb{Z}$ en observant que l'on, dans $\mathbb{K}[X]$ comme dans $\mathbb{Z}$, un théorème de division euclidienne. Il devrait donc être possible de décrire un algorithme d'Euclide pour les calculs de PGCD et de PPCM, et de démontrer l'unicité de la décomposition en produit d'irréductibles dont l'existence a été établie au **théorème 2.6**.

5.6.1 PGCD et PPCM

Le lemme suivant sera fondamental pour définir le PGCD de deux polynômes :

Lemme 5.6.1
Soient A *et* B *deux polynômes, avec* $B \neq 0$. *On note* R *le reste de la division euclidienne de* A *par* B. *Alors*

$$\{D \in \mathbb{K}[X] \mid D|A \text{ et } D|B\} = \{D \in \mathbb{K}[X] \mid D|R \text{ et } D|B\}$$

Preuve : On note Q le quotient de cette division euclidienne, de manière à avoir $A = BQ + R$. Il est alors clair que si D est un diviseur commun à B et Q, il divise aussi A et B.

Mais on a aussi $R = A - BQ$: tout diviseur commun à A et B est un diviseur commun à B et R. □

Théorème 5.6.2 (Définition du PGCD)
Soient A *et* B *deux polynômes, avec* $B \neq 0$. *Il existe un unique polynôme* D, *unitaire, tel que*

1. D *est un diviseur commun à* A *et* B *;*
2. *tout diviseur commun à* A *et* B *divise* D.

D *est alors appelé le plus grand diviseur commun à* A *et* B, *noté pgcd*(A, B). *De plus, il existe deux polynômes* U *et* V *tels que* $D = AU + BV$.

Preuve : On démontre l'existence de D par récurrence sur le degré du polynôme B : on note, pour tout entier n, $\mathscr{P}(n)$ la propriété suivante :

> « Soient A et B dans $\mathbb{K}[X]$, avec $\deg B = n$. Il existe $D \in \mathbb{K}[X]$, unitaire, diviseur commun à A et B, tel que tout diviseur commun à A et B divise D. Il existe aussi des polynômes U et V tels que $AU + BV = D$. »

Si B est un polynôme constant, alors 1 convient ; donc $\mathscr{P}(0)$ est vraie.

Soit n un entier tel que $\mathscr{P}(n)$ soit vraie. On se donne deux polynômes A et B, avec $\deg B = n+1$. En notant Q et R le quotient et le reste de la division euclidienne de A par B, on sait d'après le **lemme 6.1**, que

$$\{D \in \mathbb{K}[X] \mid D|A \text{ et } D|B\} = \{D \in \mathbb{K}[X] \mid D|R \text{ et } D|B\}$$

D'après l'hypothèse de récurrence et puisque $\deg R < \deg B = n+1$, il existe $D \in \mathbb{K}[X]$, unitaire, diviseur commun à B et R (donc à A et B) et tel que tout diviseur commun à B et R (donc à A et B) divise D.

De plus, il existe des polynômes U et V tels que $BU + VR = D$. Mais

$$A = BQ + R \qquad \text{donc} \qquad R = A - BQ$$

et finalement $$D = BU + VR = BU + V(A - BQ) = B(U - Q) + AV$$

Ce qui achève de démontrer $\mathscr{P}(n+1)$.

L'existence de D est donc assurée, par récurrence. Reste à établir l'unicité. On suppose avoir trouvé D_1 et D_2, unitaires, diviseurs communs à A et B, tels que tout diviseur commun à A et B divise D_1 et D_2. En particulier, $D_1 | D_2$ et $D_2 | D_1$; d'après la **proposition 2.4**, il existe $\lambda \in \mathbb{K}^\star$ tel que $D_2 = \lambda D_1$. Mais D_1 et D_2 sont unitaires donc $\lambda = 1$ et $D_2 = D_1$. □

On adoptera la convention suivante : le PGCD de 0 et 0 est 0.

Exemple 5.6.3

On n'a, pour l'instant, pas décrit d'algorithme efficace de calcul du PGCD. Donc la seule méthode disponible consiste à lister tous les diviseurs communs unitaires à A et B pour choisir celui divisible par tous les autres.

C'est pourquoi on s'en tiendra à un exemple simple où A et B sont déjà factorisés. Prenons

$$A = 2(X-3)^2(X+4)^2 \qquad B = 3(X-1)^2(X-3)(X+4)^3$$

A a 9 diviseurs unitaires ; B en a 24. Théoriquement, il faudrait tous les lister pour être sûr de ne pas en oublier, puis comparer les listes. Pour en déduire la liste de diviseurs unitaires communs

$$1 \quad X-3 \quad X+4 \quad (X+4)^2 \quad (X-3)(X+4) \quad (X-3)(X+4)^2$$

Celui qui est divisible par tous les autres est $(X-3)(X+4)^2$: c'est le PGCD de A et B.

Cette stratégie, décrite dans l'exemple, est loin d'être optimale ; si A et B étaient plus compliqués, ou même non factorisés, comment aurait-on fait ? En fait, l'existence du PGCD ne nous apprend pas comment le calculer. C'est la preuve de son existence qui explique la marche à suivre. Il suffit d'appliquer l'algorithme suivant :

```
Algorithme d'Euclide :
Calculer le reste R de la division de A par B.
Si R=0, alors pgcd(A,B)=B/x o\'u x est le coefficient dominant de B.
Sinon, recommencer avec A=B et B=R.
```

C'est exactement le même algorithme que celui décrit pour les calculs de PGCD dans $\mathbb{Z}$, et on ne rentrera donc pas dans les détails de son fonctionnement. L'exemple suivant illustre sa mise en œuvre, pour calculer non seulement le PGCD de deux polynômes A et B, mais aussi obtenir des polynômes U et V tels que $AU + BV = \text{pgcd}(A, B)$.

Exemple 5.6.4

On prend les polynômes $A = X^4 + 1$ et $B = X^3 - 1$. On trouve successivement

$$X^4 + 1 = X(X^3 - 1) + (X + 1)$$

$$X^3 - 1 = (X^2 - X + 1)(X + 1) - 2$$

$$X + 1 = -\frac{X+1}{2} \times 2$$

Le PGCD de A et B est donc 1. On trouve U et V tels que AU + BV = −2 (le dernier reste non nul) :

Quotient	α	β
	0	1
X	1	0
X^2-X+1	$-X$	1
$-\frac{X+1}{2}$	X^3-X^2+X+1	$-X^2+X-1$

On vérifie bien que $(X^3-X^2+X+1)(X^3-1)+(-X^2+X-1)(X^4+1)=-2$

d'où $$\frac{-X^3+X^2-X-1}{2}(X^3-1)+\frac{X^2-X+1}{2}(X^4+1)=1$$

Proposition 5.6.5 (Définition du PPCM)
Soient A *et* B *dans* $\mathbb{K}[X]$*, non nuls. Il existe un unique polynôme* M*, unitaire, tel que*

1. M *est un multiple commun à* A *et* B *;*
2. *tout multiple commun à* A *et* B *est divisible par* M.

M *est alors appelé le plus petit multiple commun à* A *et* B*, noté ppcm*(A, B).

Preuve : L'ensemble des multiples communs à A et B n'est pas vide, puisqu'il contient AB. Donc $\{\deg P \mid A|P \text{ et } B|P\}$ est une partie non vide de $\mathbb{N}$, qui admet un plus petit élément noté m. Soit M un multiple commun à A et B, avec $\deg M = m$. On peut supposer M unitaire, en le divisant par son coefficient dominant.

Soit P un autre multiple commun à A et B. On effectue la division euclidienne de P par M :

$$P = QM + R \qquad \text{avec} \qquad \deg R < m$$

Alors R = P − QM ; comme A et B divisent P et M, ils divisent aussi R. Donc R est un multiple commun à A et B. Mais si $R \neq 0$, on peut le diviser par son coefficient dominant pour obtenir un multiple commun à A et B, unitaire, de degré strictement plus petit que m ; ce qui contredit la définition de m. Ainsi, R = 0 et M divise tous les multiples communs à A et B.

Si N est un autre polynôme avec ces propriétés, on a N|M et M|N donc M et N sont proportionnels. Mais comme ils sont unitaires, ils sont en fait égaux. □

Définition 5.6.6 (Polynômes premiers entre eux)
Soient A et B dans $\mathbb{K}[X]$. On dit qu'ils sont premiers entre eux si leur PGCD est 1.

Théorème 5.6.7 (Théorème de Bezout)
Soient A *et* B *dans* $\mathbb{K}[X]$*. Ils sont premiers entre eux si, et seulement si, il existe* U *et* V *dans* $\mathbb{K}[X]$*, tels que* AU + BV = 1.

Preuve : C'est évident, compte tenu de la **définition 6.6** et du **théorème 6.2**. □

Théorème 5.6.8 (Propriétés du PGCD et du PPCM)
Soient A *et* B *dans* $\mathbb{K}[X]$*, non nuls.*

1. *pour tous scalaires* λ *et* μ *non nuls,*

$$pgcd(\lambda A, \mu B) = pgcd(A, B) \qquad et \qquad ppcm(\lambda A, \mu B) = ppcm(A, B)$$

2. *Si* A *et* B *sont premiers entre eux et unitaires, alors* $ppcm(A,B) = AB$.
3. *Les polynômes* $\dfrac{A}{pgcd(A,B)}$ *et* $\dfrac{B}{pgcd(A,B)}$ *sont premiers entre eux.*
4. *Si* $P \in \mathbb{K}[X]$ *est unitaire, alors*
$$pgcd(PA,PB) = P \times pgcd(A,B) \qquad et \qquad ppcm(PA,PB) = P \times ppcm(A,B)$$
5. *Si* A *et* B *sont unitaires, leur PPCM est* $\dfrac{AB}{pgcd(A,B)}$.

Preuve : Dans toute la démonstration, on notera D et M les PGCD et PPCM de A et B. On y va, dans l'ordre :

1. Soient λ et μ dans $\mathbb{K}$, non nuls. On a
$$A|\lambda A \qquad \text{et} \qquad B|\mu B$$
donc D divise λA et μB. Par suite, D divise $\text{pgcd}(\lambda A, \mu B)$.
Réciproquement, $A = \dfrac{1}{\lambda} \times \lambda A$ et $B = \dfrac{1}{\mu} \times \mu B$
car λ et μ ne sont pas nuls. Donc $\text{pgcd}(\lambda A, \mu B)$ divise A et B ; par conséquent, il divise D.
D'après la **proposition 2.4**, D et $\text{pgcd}(\lambda A, \mu B)$ sont proportionnels. Mais comme ils sont unitaires, ils sont égaux.
2. Supposons A et B premiers entre eux. Puisque AB est un multiple commun à A et B, on a M|AB. Réciproquement, on sait d'après Bezout qu'il existe des polynômes U et V tels que $AU + BV = 1$. Donc $AMU + BVM = M$. Mais
$$\begin{cases} B|M \\ A|M \end{cases} \qquad \text{donc} \qquad \begin{cases} AB|AM \\ AB|BM \end{cases}$$
Par conséquent, AB|M. Mais AB et M sont unitaires. Donc ils sont égaux.
3. D'après Bezout, il existe U et V tels que $AU + BV = D$. Donc
$$\frac{A}{D}U + \frac{B}{D}V = 1$$
et Bezout assure alors que $\dfrac{A}{D}$ et $\dfrac{B}{D}$ sont premiers entre eux.
4. Soit $P \in \mathbb{K}[X]$, unitaire. On note $S = \text{pgcd}(PA, PB)$. Comme D|A et D|B, on a PD|PA et PD|PB. Donc PD|S.
En particulier, P|S donc on peut parler du polynôme $\frac{S}{P}$. Comme S|PA et S|PB, on voit que $\frac{S}{P}$ divise à la fois A et B. Donc $\frac{S}{P}|D$ et finalement, S|PD.
Comme S et PD sont unitaires, ils sont égaux.
Pour le PPCM, c'est exactement la même chose.
5. Supposons A et B unitaires. Alors $\frac{A}{D}$ et $\frac{B}{D}$ sont premiers entre eux (point *3*) donc leur PPCM vaut $\frac{AB}{D^2}$ (point *2*). Mais
$$A = D \times \frac{A}{D} \qquad \text{et} \qquad B = D \times \frac{A}{D}$$

Comme D est unitaire, on a (*point 4*) :

$$\text{ppcm}(A,B) = D \times \text{ppcm}\left(\frac{A}{D}, \frac{B}{D}\right) = \frac{AB}{D}$$

Ce dernier théorème montre comment on peut calculer le PPCM de deux polynômes A et B :
- On les divise chacun par leur coefficient dominant, pour les rendre unitaires. Cela ne change pas le PPCM, d'après le point *1*.
- On calcule leur PGCD par l'algorithme d'Euclide, par exemple.
- On calcule enfin $\frac{AB}{\text{pgcd}(A,B)}$, ce qui donne le PPCM.

5.6.2 Les théorèmes de Gauss

Théorème 5.6.9 (Théorème de Gauss 1)
Soient A *et* B *dans* $\mathbb{K}[X]$, *premiers entre eux. Soit* $P \in \mathbb{K}[X]$. *Si* A|PB, *alors* A|P.

Preuve : Supposons que A|PB. Comme A et B sont premiers entre eux, il existe U et V dans $\mathbb{K}[X]$ tels que AU + BV = 1. Alors

$$P = APU + BPV$$

Mais A|APU et A|PBV donc A|P. □

Théorème 5.6.10 (Théorème de Gauss 2)
Soient A *et* B *dans* $\mathbb{K}[X]$, *premiers entre eux. Soit* $P \in \mathbb{K}[X]$. *Si* A|P *et* B|P, *alors* AB|P.

Preuve : La preuve repose encore sur Bezout : soient U et V deux polynômes tels que AU + BV = 1. On multiplie cette relation par P pour obtenir AUP + BVP = P. Puisque A|P et B|P, on a AB|BVP et AB|AUP. Donc AB|P. □

On utilise ces résultats pour achever la preuve du **théorème 2.6**. Commençons par observer

Lemme 5.6.11
Soient A *et* B *dans* $\mathbb{K}[X]$, *premiers entre eux. Soient m et n deux entiers non nuls. Alors* A^m *et* B^n *sont premiers entre eux.*

Preuve : D'après Bezout, il existe U et V dans $\mathbb{K}[X]$ tels que AU + BV = 1. On élève cette relation à la puissance $m+n+1$:

$$\begin{aligned} 1 = (AU+BV)^{m+n} &= \sum_{k=0}^{m+n} C_{m+n}^k U^k V^{m+n-k} A^k B^{m+n-k} \\ &= \sum_{k=0}^{m} C_{m+n}^k U^k V^{m+n-k} A^k B^{m+n-k} + \sum_{k=m+1}^{m+n} C_{m+n}^k U^k V^{m+n-k} A^k B^{m+n-k} \end{aligned}$$

Mais on observe que

$$\forall k \in [\![0\,;m]\!] \qquad m-k \geqslant 0$$

et

$$\forall k \in [\![m+1\,;m+n]\!] \qquad k-m \geqslant 1 \geqslant 0$$

On peut mettre B^n en facteur dans la première somme, et A^m en facteur dans la deuxième pour obtenir une relation de Bezout entre A^m et B^n. Ce qui prouve que ces polynômes sont premiers entre eux. □

Lemme 5.6.12
Soient A *et* B *dans* $\mathbb{K}[X]$, *avec* A *irréductible. Alors* A|B *ou bien pgcd*$(A,B) = 1$.

Preuve : Diviser A par son coefficient dominant ne change pas le PGCD de A et B, donc on peut supposer A unitaire.

On note $D = \text{pgcd}(A,B)$, de sorte que D|A et D|B. Mais A est irréductible, donc $D \in \mathbb{K}[X]^\star$ ou bien D est proportionnel à A. Étudions ces deux possibilités :

- Si $D \in \mathbb{K}[X]^\star$, c'est que D est constant ; mais il est unitaire donc $1 = D = \text{pgcd}(A,B)$.
- Si D est proportionnel à A, comme ces deux polynômes sont unitaires, c'est que D = A. Mais D|B donc A|B.

Corollaire 5.6.13
Soient A *et* B *dans* $\mathbb{K}[X]$, *irréductibles, unitaires, distincts. Alors pgcd*$(A,B) = 1$.

Preuve : Supposons que A|B. Comme B est irréductible, c'est que A est constant ou proportionnel à B.

- Dans le premier cas, comme A est unitaire, c'est que A = 1. Donc $\text{pgcd}(A,B) = 1$.
- Dans le deuxième cas, on a en fait A = B puisque A et B sont unitaires ; ce qui est contradictoire avec le fait que $A \neq B$. Ce cas-là ne se produit donc pas.

En résumé, si A|B, on a bien $\text{pgcd}(A,B) = 1$.

Si A ne divise pas B, le **lemme 6.12** assure que $\text{pgcd}(A,B) = 1$. □

5.6.3 Preuve du théorème 2.6

On est enfin en mesure de démontrer l'unicité de la décomposition d'un polynôme en produit d'irréductibles unitaires ; celle-ci avait été annoncée au **théorème 2.6**.

On peut reprendre la preuve analogue du cours d'arithmétique sur $\mathbb{Z}$: cela fonctionne de la même manière dans $\mathbb{K}[X]$.

Voici une autre ébauche de démonstration, qui devrait normalement faire appel à une récurrence. On se donne un polynôme unitaire P, ainsi que des polynômes irréductibles unitaires non constants $P_1,\dots,P_n$ distincts deux-à-deux, et $Q_1,\dots,Q_k$ distincts deux-à-deux et des entiers non nuls $\alpha_1,\dots,\alpha_n$ et $\beta_1,\dots,\beta_k$, tels que

$$P = P_1^{\alpha_1}\cdots P_n^{\alpha} = Q_1^{\beta_1}\cdots Q_k^{\beta_k}$$

Supposons que P_1 n'est pas l'un des polynômes $Q_1,\dots,Q_k$. D'après le **corollaire 6.12**, P_1 et Q_1 sont premiers entre eux ; le **lemme 6.11** nous dit alors que $P_1^{\alpha_1}$ et $Q_1^{\beta_1}$ sont premiers entre eux. D'après le **théorème de Gauss 1**, c'est que

$$P_1^{\alpha_1} | Q_2^{\beta_2}\cdots Q_k^{\beta_k}$$

On peut recommencer plusieurs fois (récurrence...) ce raisonnement, pour arriver au fait que $P_1^{\alpha_1} | Q_k^{\beta_k}$, ce qui est absurde d'après le **lemme 6.12** et le fait que P_1 n'est pas constant. Donc P_1 est l'un des polynômes $Q_1,\dots,Q_k$.

De la même manière, on montre en fait que chaque $(P_i)_{1\leqslant i\leqslant n}$ est l'un des $(Q_j)_{1\leqslant j\leqslant k}$. Autrement dit,

$$\{P_1,\dots,P_n\}\subset\{Q_1,\dots,Q_k\}$$

En échangeant les rôles des P et des Q, on montre aussi que

$$\{Q_1,\dots,Q_k\}\subset\{P_1,\dots,P_k\}$$

Ces ensembles sont donc égaux. Mais comme ils ont n et k éléments (on a supposé les P distincts deux-à-deux, ainsi que les Q), il vient $n=k$.

Quitte à renommer nos polynômes, on peut supposer que

$$P_1=Q_1 \qquad P_2=Q_2 \qquad \cdots \qquad P_n=Q_n$$

de sorte que
$$P=P_1^{\alpha_1}\cdots P_n^{\alpha_n}=P_1^{\beta_1}\cdots P_n^{\beta_n}$$

Supposons $\alpha_1<\beta_1$. Alors, en divisant par $P_1^{\alpha_1}$, il vient

$$P_2^{\alpha_1}\cdots P_n^{\alpha_n}=P_1^{\beta_1-\alpha_1}Q_2^{\beta_2}\cdots Q_n^{\beta_n}$$

Le même raisonnement qu'au-dessus montre que P_1 est l'un des polynômes $P_2,\dots,P_n$, ce qui est absurde. Donc $\alpha_1\geqslant\beta_1$. Et de la même manière, on montre qu'il est impossible que $\alpha_1>\beta_1$. Donc $\alpha_1=\beta_1$ et on se retrouve avec

$$P_2^{\alpha_2}\cdots P_n^{\alpha_n}=P_2^{\beta_2}\cdots P_n^{\beta_n}$$

On montre alors de proche-en-proche que

$$\alpha_2=\beta_2 \qquad \cdots \qquad \alpha_n=\beta_n$$

ce qui démontre bien l'unicité de la décomposition de P en produit d'irréductibles unitaires.

Chapitre 6

Fractions Rationnelles

Dans ce chapitre, $\mathbb{K}$ est un corps commutatif. On a vu, dans le chapitre sur les structures algébriques, une méthode très générale pour, étant donné un anneau intègre A, construire un corps contenant A et qu'on avait appelé *corps des fractions de* A.

Puisque $\mathbb{K}[X]$ est un anneau intègre, on peut construire son corps des fractions, qu'on notera $\mathbb{K}(X)$. Son étude fait l'objet de ce chapitre et on en déduira un théorème de structure pour $\mathbb{K}(X)$, qui débouche sur une méthode de calcul de primitives.

6.1 Le corps $\mathbb{K}(X)$

6.1.1 Rappels

Définition 6.1.1
Le corps des fractions de l'anneau intègre $\mathbb{K}[X]$ est appelé *corps des fractions rationnelles sur* $\mathbb{K}$. On le note $\mathbb{K}(X)$.

On rappelle que $\mathbb{K}(X)$ est le quotient de l'ensemble $\mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$ par la relation d'équivalence

$$\forall (P,Q),(R,S) \in \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\}) \qquad (P,Q) \sim (R,S) \iff PS - QR = 0$$

Si $(P,Q) \in \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$, sa classe d'equivalence modulo $\sim$ est notée $\frac{P}{Q}$. De sorte qu'on a la « règle des produits en croix » :

$$\frac{P}{Q} = \frac{R}{S} \iff PS = QR$$

On a défini sur $\mathbb{K}(X)$ deux opérations, l'addition et la multiplication, de la manière suivante :

$$\forall \frac{P}{Q}, \frac{R}{S} \in \mathbb{K}(X) \qquad \frac{P}{Q} + \frac{R}{S} = \frac{PS+QR}{QS} \qquad \text{et} \qquad \frac{P}{Q} \times \frac{R}{S} = \frac{PR}{QS}$$

Enfin, si $P \in \mathbb{K}[X]$, on identifie P et la fraction $\frac{P}{1}$ de sorte que $\mathbb{K}[X]$ est inclus dans $\mathbb{K}(X)$.

6.1.2 Degré d'une fraction rationnelle

Lemme 6.1.2
Soient $\frac{P}{Q}$ *et* $\frac{R}{S}$ *dans* $\mathbb{K}(X)$. *Si* $\frac{P}{Q} = \frac{R}{S}$, *alors* $deg P - deg Q = deg R - deg S$.

Preuve : Puisque $\frac{P}{Q} = \frac{R}{S}$, on sait que $PS = QR$. Par suite,

$$\deg P + \deg S = \deg Q + \deg R$$

d'où $$\deg P - \deg Q = \deg R - \deg S$$ □

Définition 6.1.3 (Degré d'une fraction rationnelle)
Soit $F = \frac{P}{Q} \in \mathbb{K}(X)$. On appelle *degré de* F, noté $\deg F$, la quantité $\deg F = \deg P - \deg Q$.

Le lemme précédent montre que l'application $\deg : \mathbb{K}(X) \longmapsto \mathbb{Z} \cup \{-\infty\}$ est bien définie, puisque $\deg F$ ne dépend pas du représentant de F dans $\mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$.

Observons également que si $P \in \mathbb{K}[X]$, le degré de P en tant que polynôme et en tant que fraction rationnelle sont le même, puisque $P = \frac{P}{1}$ et $\deg 1 = 0$. La définition du degré sur $\mathbb{K}(X)$ prolonge donc celle sur $\mathbb{K}[X]$. Mais ses autres propriétés sont également maintenues puisque :

Proposition 6.1.4
Soient F *et* G *dans* $\mathbb{K}(X)$. *Alors*

$$deg(F+G) \leqslant Max(deg F, deg G) \qquad et \qquad deg(FG) = deg F + deg G$$

Preuve : Soient P, Q, R et S des polynômes, avec Q et S non nuls, tels que

$$F = \frac{P}{Q} \qquad \text{et} \qquad G = \frac{R}{S}$$

Alors $$F + G = \frac{PS + QR}{QS} \qquad \text{et} \qquad FG = \frac{PR}{QS}$$

D'après les propriétés du degré sur $\mathbb{K}[X]$, on a tout de suite

$$\deg(FG) = \deg(PR) - \deg(QS) = \deg P + \deg R - \deg Q - \deg S = \deg F + \deg G$$

Pour le cas de la somme $F + G$, supposons par exemple que $\deg F \geqslant \deg G$, de sorte que

$$\deg P - \deg Q \geqslant \deg R - \deg S$$

ou encore $$\deg P + \deg S \geqslant \deg R + \deg Q$$

c'est-à-dire $$\deg PS \geqslant \deg RQ$$

On a $$\deg(F+G) = \deg(PS+QR) - \deg(QS)$$

Mais $$\deg(PS+QR) \leqslant \text{Max}(\deg(PS), \deg(RQ)) = \deg PS = \deg P + \deg S$$

d'où $$\deg(F+G) \leqslant \deg P + \deg S - \deg Q - \deg S = \deg F$$

On ferait de même si $\deg G \geqslant \deg F$. Donc on a bien

$$\deg(F+G) \leqslant \text{Max}(\deg F, \deg G)$$ □

6.1.3 Représentation irréductible d'une fraction rationnelle

Une fraction rationnelle $F \in \mathbb{K}(X)$ admet une infinité de représentations possibles : en effet, si $F = \frac{P}{Q}$ avec $P, Q \in \mathbb{K}[X]$ et $Q \neq 0$, alors $F = \frac{PS}{QS}$ pour tout polynôme S non nul. On s'attache donc à trouver un représentant privilégié de la fraction F.

Définition 6.1.5
Soit $F = \frac{P}{Q} \in \mathbb{K}[X]$. On dit que

- $\frac{P}{Q}$ est une représentation irréductible de F si, et seulement si, P et Q sont premiers entre eux.
- $\frac{P}{Q}$ est une représentation irréductible unitaire de F si, et seulement si, c'est une représentation irréductible et Q est unitaire.

Théorème 6.1.6
Soit $F \in \mathbb{K}(X)$.

- F *admet des représentations irréductibles ; de plus, si* $F = \frac{P}{Q} = \frac{R}{S}$ *sont deux représentations irréductibles de* F, *il existe* $\lambda \in \mathbb{K}$ *tel que* $P = \lambda R$ *et* $Q = \lambda S$.
- F *admet une seule représentation irréductible unitaire.*

Preuve : Soit $F = \frac{A}{B} \in \mathbb{K}(X)$. On note D le PGCD de A et B. On sait (voir le chapitre sur les polynômes) que $P = \frac{A}{D}$ et $Q = \frac{B}{D}$ sont premiers entre eux. De plus, $A = DP$ et $B = DQ$ donc

$$AQ = DPQ = DQP = BP$$

et

$$F = \frac{A}{B} = \frac{P}{Q}$$

F admet donc des représentations irréductibles.

Soit $\frac{R}{S}$ une autre représentation irréductible de F. On sait donc que

$$PS = QR \qquad \text{pgcd}(P, Q) = 1 \qquad \text{pgcd}(R, S) = 1$$

On voit que R|PS ; mais R et S sont premiers entre eux donc (**théorème de Gauss**) R|P. De la même manière, P|R. On sait donc que P et R sont proportionnels : il existe $\lambda \in \mathbb{K}$ tel que $R = \lambda P$. Par suite, $PS = \lambda QP$ donc $S = \lambda Q$. La première partie du théorème est établie.

La seconde partie est simple : si $F = \frac{A}{B}$ est une représentation irréductible et si $\lambda \neq 0$ est le coefficient dominant de B, on note

$$P = \frac{1}{\lambda} A \qquad Q = \frac{1}{\lambda} B$$

de sorte que $F = \frac{P}{Q}$, ce qui fournit une représentation irréductible unitaire de F.

Enfin, si on se donne $F = \frac{R}{S}$ une autre représentation irréductible unitaire de F, on sait, d'après la partie précédente qu'il existe un scalaire μ tel que

$$R = \mu P \qquad \text{et} \qquad S = \mu Q$$

Mais Q et S sont unitaires donc $\mu = 1$, $R = P$ et $S = Q$. □

Exemple 6.1.7

1. Prenons $F = \frac{X^2 - 2X + 1}{2X^2 - 3X + 1}$. On a

$$\text{pgcd}(X^2 - 2X + 1, 2X^2 - 3X + 1) = X - 1$$

L'algorithme de division euclidienne permet d'obtenir

$$X^2-2X+1=(X-1)(X-1) \qquad \text{et} \qquad 2X^2-3X+1=(X-1)(2X-1)$$

donc $F=\frac{X-1}{2X-1}$ est une représentation irréductible de F. Toutes les représentations irréductibles de F sont de la forme $F=\frac{\lambda X-\lambda}{2\lambda X-\lambda}$.

La représentation irréductible unitaire de F est $F=\dfrac{\frac{X}{2}-\frac{1}{2}}{X-\frac{1}{2}}$.

2. Si $F=0$, les représentations possibles de F sont $F=\frac{0}{Q}$ pour tout polynôme Q non nul. Mais comme le PGCD de 0 et Q est Q, les seules représentations irréductibles de F sont $\frac{0}{\lambda}$ avec $\lambda\in\mathbb{K}^\star$.
La représentation irréductible unitaire de F est $F=\frac{0}{1}$.

6.1.4 Zéros et pôles

Définition 6.1.8
Soit $F\in\mathbb{K}(X)$, de représentation irréductible $F=\frac{P}{Q}$. Soit $a\in\mathbb{K}$.

- On dit que *a est un zéro de* F *dans* $\mathbb{K}$ si, et seulement si, a est une racine de P dans $\mathbb{K}$. Dans ce cas, si $F\neq 0$, on appelle *multiplicité de a* (en tant que zéro de F) l'ordre de multiplicité de a en tant que racine de P.
- On dit que *a est un pôle de* F *dans* $\mathbb{K}$ si, et seulement si, a est une racine de Q dans $\mathbb{K}$. Dans ce cas, on appelle *multiplicité de a* (en tant que pôle de F) l'ordre de multiplicité de a en tant que racine de Q.

Exemple 6.1.9

1. La fraction $F=\frac{X(X-1)^2}{(X-2)(X^3+1)^2}$ est dans $\mathbb{R}(X)$ et cette représentation est irréductible. F admet
   - 0 pour zéro d'ordre 1 dans $\mathbb{R}$;
   - 1 pour zéro d'ordre 2 dans $\mathbb{R}$;
   - 2 pour pôle d'ordre 1 dans $\mathbb{R}$;
   - -1 pour pôle d'ordre 2 dans $\mathbb{R}$.
2. Mais cette même fraction se trouve aussi dans $\mathbb{C}(X)$. Outre les zéros et pôles réels listés précédemment, qui sont également des zéros et pôles complexes de F, on trouve aussi $e^{i\pi/3}$ et $e^{-i\pi/3}$, qui sont chacun pôle complexe d'ordre 2.

Théorème 6.1.10
Soit $F\in\mathbb{K}(X)$ *une fraction rationnelle non nulle. L'ensembles des zéros et l'ensemble des pôles de* F *sont chacun fini.*

Preuve : C'est une conséquence immédiate du fait qu'un polynôme admet au plus autant de racines que son degré. □

Définition 6.1.11 (Fonction rationnelle)
Soit $F\in\mathbb{K}(X)$ une fraction rationnelle, de représentation irréductible $F=\frac{P}{Q}$. On note A l'ensemble des pôles de F. On appelle *fonction rationnelle associée à* F la fonction $\widetilde{F}$ définie sur $\mathbb{K}\setminus A$ par :

$$\forall x\in\mathbb{K}\setminus A \qquad \widetilde{F}(x)=\frac{\widetilde{P}(x)}{\widetilde{Q}(x)}$$

Remarquons que si $A = \mathbb{K}$, la fonction rationnelle associée à F n'existe pas, tout simplement (son graphe est vide). Cette remarque peut paraître bizarre : comment serait-il possible que l'ensemble des pôles de F soit égal à $\mathbb{K}$? La réponse est simple : il existe des corps finis, bien que nous n'en ayons pas encore rencontrés. Si $\mathbb{K}$ est fini et si F a pour pôles tous les éléments de $\mathbb{K}$, par exemple si $Q = \prod_{k\in\mathbb{K}} (X - k)$, on ne peut associer de fonction rationnelle à F.

Théorème 6.1.12
On suppose $\mathbb{K}$ infini. L'application

$$\begin{array}{ccc} \mathbb{K}(X) & \longrightarrow & \mathscr{F}(\mathbb{K},\mathbb{K}) \\ F & \longmapsto & \widetilde{F} \end{array}$$

est injective.

Remarque : On rappelle que $\mathscr{F}(\mathbb{K},\mathbb{K})$ est l'ensemble des fonctions de $\mathbb{K}$ dans lui-même. Ce n'est pas un anneau, à cause des problèmes d'ensembles de définition des fonctions. On rappelle que si f et g sont deux fonctions de $\mathbb{K}$ dans $\mathbb{K}$, avec pour domaine de définition $\mathscr{D}_f$ et $\mathscr{D}_g$, alors on définit

$$\forall x \in \mathscr{D}_f \cap \mathscr{D}_g \qquad (f+g)(x) = f(x) + g(x) \quad \text{et} \quad (fg)(x) = f(x)g(x)$$

Ces lois sont associatives, et les *applications* constantes $x \longmapsto 0$ et $x \longmapsto 1$ sont neutres pour ces lois. Mais on n'a pas l'existence d'inverse pour l'additions.

Par exemple, $f : x \longmapsto \frac{1}{x-1}$ est une fonction de $\mathbb{R}$ dans $\mathbb{R}$ et son domaine de définition est $\mathbb{R} \setminus \{1\}$. Mais elle n'a pas d'inverse pour l'addition : si g est un inverse pour l'addition, alors $f+g$ est seulement définie sur $\mathscr{D}_f \cap \mathscr{D}_g$. Elle n'est pas définie sur $\mathbb{R}$, et ne peut donc pas être égale à 0 sur $\mathbb{R}$ tout entier.

Preuve : Soient $F, G \in \mathbb{K}(X)$ de représentations irréductibles $F = \frac{P}{Q}$, $G = \frac{R}{S}$, telles que $\widetilde{F} = \widetilde{G}$. Ces deux fonctions ont le même domaine de définition, donc Q et S ont les mêmes racines. Cet ensemble (fini) des racines de Q et S est noté A. On a

$$\forall x \in \mathbb{K} \setminus A \qquad \widetilde{F}(x) = \widetilde{G}(x)$$

donc

$$\forall x \in \mathbb{K} \setminus A \qquad \frac{P(x)}{Q(x)} = \frac{R(x)}{S(x)}$$

Par suite,

$$\forall x \in \mathbb{K} \setminus A \qquad P(x)S(x) = Q(x)R(x)$$

ou encore

$$\forall x \in \mathbb{K} \setminus A \qquad (PS)(x) = (QR)(x)$$

Mais $\mathbb{K} \setminus A$ est infini, donc P admet une infinité de racines : $P = 0$ et il s'ensuit que $F = 0$. □

Ainsi, lorsque $\mathbb{K}$ est infini, on peut identifier fonctions rationnelles et fractions rationnelles, puisqu'une fonction rationnelle ne peut provenir que d'une seule fraction rationnelle.

6.1.5 Composition

On étend la définition de la composition de $\mathbb{K}[X]$ à $\mathbb{K}(X)$. Pour cela, on constate que si $F \in \mathbb{K}(X)$ est une fraction rationnelle, représentée par $\frac{P}{Q}$ et $\frac{R}{S}$, si $T \in \mathbb{K}[X]$ n'est pas constant, on a $\frac{P\circ T}{Q\circ T} = \frac{R\circ T}{S\circ T}$. En effet on sait que $PS = QR$; de plus, la composition dans $\mathbb{K}[X]$ est distributive à droite sur la multiplication, comme on l'a vu dans le cours sur les polynômes. Donc

$$(P\circ T)(S\circ T) = (R\circ T)(S\circ T)$$

Ceci permet de poser la définition suivante :

Définition 6.1.13 (Composition)
Soient $F = \frac{P}{Q} \in \mathbb{K}(X)$ et $R \in \mathbb{K}[X]$ un polynôme non constant. On appelle *fraction composée de* F *par* G la fraction

$$F\circ R = \frac{P\circ R}{Q\circ R}$$

Proposition 6.1.14 (Propriétés de la composition)
La composition a les propriétés suivantes :

1. $\forall F \in \mathbb{K}(X) \quad \forall R,S \in \mathbb{K}[X] \qquad F\circ(R\circ S) = (F\circ Q)\circ S$
2. $\forall F,G \in \mathbb{K}(X) \quad \forall R \in \mathbb{K}[X] \qquad (F+G)\circ R = (F\circ R) + (G\circ R)$
3. $\forall F,G \in \mathbb{K}(X) \quad \forall R \in \mathbb{K}[X] \qquad (FG)\circ R = (F\circ R)(G\circ R)$

Preuve : Ces propriétés sont des conséquences immédiates des propriétés analogues de la composition entre polynômes. □

Définition 6.1.15
Une fraction rationnelle F est dite *paire* si, et seulement si, $F(-X) = F$. Elle est dite *impaire* si, et seulement si $F(-X) = -F$.

6.1.6 Conjugaison

Définition 6.1.16 (Conjugaison des polynômes complexes)
Soit $P = \sum_{k=0}^{\infty} P_k X^k \in \mathbb{C}[X]$. On appelle *polynôme conjugué de* P le polynôme $\overline{P} = \sum_{k=0}^{\infty} \overline{P_k} X^k$.

Il est clair compte-tenu des propriétés de la conjugaison dans $\mathbb{C}$, que la conjugaison sur $\mathbb{C}[X]$ est un isomorphisme d'anneaux.

Si $F \in \mathbb{C}(X)$ est une fraction rationnelle, représentée par $\frac{P}{Q}$ et $\frac{R}{S}$, on a $PS = RQ$. Par suite, $\overline{P}\,\overline{S} = \overline{R}\,\overline{Q}$ de sorte que $\frac{\overline{P}}{\overline{Q}} = \frac{\overline{R}}{\overline{S}}$. Ceci permet de définir

Définition 6.1.17 (Conjugaison des fractions rationnelles complexes)
Soit $F = \frac{P}{Q} \in \mathbb{C}(X)$. On appelle *fraction conjuguée de* F la fraction rationnelle $\overline{F} = \frac{\overline{P}}{\overline{Q}}$.

Proposition 6.1.18 (Propriétés de la conjugaison)
La conjugaison est un automorphisme involutif du corps $\mathbb{C}(X)$*, c'est-à-dire que*

$$\forall F,G \in \mathbb{C}(X) \qquad \overline{F+G} = \overline{F} + \overline{G} \qquad \textit{et} \qquad \overline{FG} = \overline{F}\,\overline{G}$$

et $$\forall F \in \mathbb{C}(X) \qquad \overline{\overline{F}} = F$$

Preuve : C'est évident, compte-tenu des propriétés de la conjugaison des polynômes. □

6.2 Décomposition en éléments simples

Cette partie constitue le cœur de ce chapitre. Elle s'attache à montrer que toute fraction rationnelle peut être décomposée en somme de « fractions élémentaires. » Ce résultat a une application immédiate, dans le cas du corps $\mathbb{R}$, au calcul d'intégrales puisque ces « fractions élémentaires » seront faciles à primitiver.

6.2.1 Division suivant les puissances croissantes

On aura besoin, avant de commencer, de l'outil théorique suivant :

Théorème 6.2.1 (Division suivant les puissances croissantes)
Soient $n \in \mathbb{N}$, A *et* B *dans* $\mathbb{K}[X]$, *avec* $\text{val}\, B = 0$. *Il existe un unique couple* $(Q,R) \in \mathbb{K}[X]$, *tel que*

$$A = BQ + X^{n+1}R \qquad \textit{et} \qquad \textit{deg}\, Q \leqslant n$$

Q *et* R *sont appelés quotient et reste de la division suivant les puissances croissantes à l'ordre* n *de* A *par* B.

Preuve : On procède par récurrence sur l'entier n, en posant :

$$\mathscr{P}(n) : \forall A, B \in \mathbb{K}[X] \quad \text{avec} \quad \text{val}\, B = 0 \quad \exists (Q,R) \in \mathbb{K}[X] \qquad A = BQ + X^{n+1}R \quad \text{et} \quad \deg Q \leqslant n$$

- $\mathscr{P}$**(0) est vraie** : Notons $p = \deg A$ et $r = \deg B$ et

  $$A = \sum_{k=0}^{p} A_k X^k \qquad B = \sum_{k=0}^{q} B_k X^k$$

  L'hypothèse sur la valuation de B implique que $B_0 \neq 0$. On pose

  $$Q = \frac{A_0}{B_0} \qquad \text{et} \qquad R_1 = A - BQ$$

  de sorte que $$\deg Q = 0 \qquad \text{et} \qquad A = BQ + R_1$$

  On remarque que $$R_1(0) = A(0) - B(0)Q(0) = A_0 - B_0 \frac{A_0}{B_0} = 0$$

  donc 0 est racine de R_1 d'où $X | R_1$. Soit $R \in \mathbb{K}[X]$ tel que $R_1 = XR$. On a bien

  $$A = BQ + XR \qquad \text{avec} \qquad \deg Q = 0$$

- $\mathscr{P}(n) \Longrightarrow \mathscr{P}(n+1)$: Soit $n \in \mathbb{N}$ tel que $\mathscr{P}(n)$ soit vraie. Comme on l'a vu en montrant $\mathscr{P}(0)$, il existe des polynômes Q_1 et R_1 tels que

  $$A = BQ_1 + XR_1 \qquad \text{et} \qquad \deg Q_1 = 0$$

  D'après la propriété $\mathscr{P}(n)$, on peut effectuer la division suivant les puissances croissantes à l'ordre n de R_1 par B puisque $\text{val}\, B = 0$. Ce qui fournit des polynômes Q_2 et R_2 tels que

  $$R_1 = BQ_2 + X^{n+1}R_2 \qquad \text{avec} \qquad \deg Q_2 \leqslant n$$

Alors $A = BQ_1 + XR_1 = BQ_1 + X(BQ_2 + X^{n+1}R_2) = B(Q_1 + XQ_2) + X^{n+2}R_2$

ce qui achève de démontrer $\mathscr{P}(n+1)$ puisque $\deg(Q_1 + XQ_2) \leqslant n+1$.

- **Conclusion** : $\mathscr{P}(n)$ est vraie pour tout entier n.

Reste à montrer l'unicité du quotient et du reste. Soit $n \in \mathbb{N}$, soient A et B dans $\mathbb{K}[X]$ avec B de valuation nulle. On suppose avoir trouvé des polynômes Q_1, Q_2, R_1, R_2 tels que

$$A = BQ_1 + X^{n+1}R_1 = BQ_2 + X^{n+1}R_2 \qquad \text{avec} \qquad \deg Q_1 \text{ et } \deg Q_2 \leqslant n$$

Alors $$B(Q_1 - Q_2) = X^{n+1}(R_2 - R_1)$$

On voit que X^{n+1} divise $B(Q_1 - Q_2)$. Mais X^{n+1} et B sont premiers entre eux, puisque 0 n'est pas racine de B. D'après le **théorème de Gauss**, $X^{n+1} | (Q_1 - Q_2)$. Mais $Q_1 - Q_2$ est de degré au plus n. Donc c'est le polynôme nul : $Q_1 = Q_2$. Par suite, $X^{n+1}(R_2 - R_1) = 0$; mais $\mathbb{K}[X]$ est intègre donc $R_1 = R_2$. □

Exemple 6.2.2

La démonstration du théorème nous dit en pratique comment faire la division suivant les puissances croissantes d'un polynôme A par un polynôme B de valuation non nulle.

Prenons par exemple $A = X + 2$ et $B = X^2 - 3X + 1$ et supposons qu'on veuille faire la division puissances croissantes de A par B à l'ordre 2. On commence (voir initialisation de la récurrence) par poser

$$R_1 = A - 2B = -2X^2 + 7X$$

de sorte que $$A = 2B + R_1 = 2B + X(-2X + 7)$$

On a alors besoin de faire la division puissances croissantes de $-2X+7$ par B à l'ordre 1 (voir démonstration de l'hérédité). Pour ce faire, on pose

$$R_2 = -2X + 7 - 7B = -7X^2 + 19X$$

de sorte que $$-2X + 7 = 7B + R_2 = 7B + X(-7X + 19)$$

et $$A = 2B + X(7B + X(-7X + 19)) = (2 + 7X)B + X^2(-7X + 19)$$

On recommence une dernière fois, en faisant la division puissances croissantes de $-7X+19$ par B à l'ordre 0. On pose donc

$$R_3 = -7X + 19 - 19B = -19X^2 + 50X$$

de sorte que $$-7X + 19 = 19B + R_3 = 19B + X(-19X + 50)$$

et $$A = (2 + 7X)B + X^2(19B + X(-19X + 50)) = (2 + 7X + 19X^2)B + X^3(-19X + 50)$$

Le quotient et le reste de la division puissances croissantes de A par B à l'ordre 2 sont

$$Q = 19X^2 + 7X + 2 \qquad \text{et} \qquad R = -19X + 50$$

Il y a une manière plus agréable de présenter toutes ces opérations dans un même tableau, de manière assez analogue à une division euclidienne :

$$\begin{array}{l|l}
2 + X & 1 - 3X + X^2 \\
\cline{2-2}
2 - 6X + 2X^2 & 2 + 7X + 19X^2 \\
\cline{1-1}
\quad 7X - 2X^2 & \\
\cline{1-1}
\quad 7X - 21X^2 + 7X^3 & \\
\cline{1-1}
\qquad 19X^2 - 7X^3 & \\
\cline{1-1}
\qquad 19X^2 - 57X^3 + 19X^4 & \\
\cline{1-1}
\qquad\qquad 50X^3 - 19X^4 &
\end{array}$$

6.2.2 Étude théorique

Lemme 6.2.3 (Partie entière, partie fractionnaire)
Soit $F = \frac{P}{Q} \in \mathbb{K}(X)$. *Il existe un unique couple* $(E,R) \in \mathbb{K}[X]$ *tel que*

$$F = E + \frac{R}{Q} \qquad \textit{avec} \qquad \textit{deg}\, R < \textit{deg}\, Q$$

E *est alors appelé la partie entière de* F *et* $\frac{R}{S}$ *est la partie fractionnaire.*
En outre si P *et* Q *sont premiers entre eux, alors* R *et* Q *sont premiers entre eux.*

Preuve : On effectue la division euclidienne de P par Q, dont on note E le quotient et R le reste :

$$P = QE + R \qquad \text{avec} \qquad \deg R < \deg Q$$

Alors
$$F = \frac{P}{Q} = E + \frac{R}{Q}$$

On a déjà observé, dans le chapitre sur les polynômes, que $\text{pgcd}(P,Q) = \text{pgcd}(R,Q)$ donc si P et Q sont premiers entre eux, il en est de même de R et Q.

Montrons que cette décomposition est unique. On suppose avoir trouvé des polynômes E_1 et R_1 tels que

$$F = \frac{P}{Q} = E_1 + \frac{R_1}{Q} \qquad \text{avec} \qquad \deg R_1 < \deg Q$$

Alors
$$P = QE_1 + R_1 \qquad \text{avec} \qquad \deg R_1 < \deg Q$$

Donc E_1 et R_1 sont le quotient et le reste de la division euclidienne de P par Q ; ceux-ci sont uniques donc $E = E_1$ et $R = R_1$. □

On sait donc maintenant décomposer une fraction rationnelle en la somme d'un polynôme et d'une fraction de degré strictement négatif. L'opération est assez simple, somme toute : il suffit de mettre en œuvre une division euclidienne.

La partie fractionnaire admet-elle une décomposition plus poussée ? La réponse est oui, mais pour cela, il y a encore du travail. Commençons par

Lemme 6.2.4
Soient $n \in \mathbb{N}^\star$ *et* $Q_0, \dots, Q_n$ *dans* $\mathbb{K}[X]$, *premiers entre eux deux-à-deux. Alors* Q_n *est premier avec* $Q_0 \cdots Q_{n-1}$.

Preuve : Soit $i \in [\![0 ; n-1]\!]$. Puisque Q_n est premier avec Q_i, il existe, d'après le théorème de Bezout, des polynômes U_i et V_i, tels que $U_i Q_n + V_i Q_i = 1$. Autrement dit,

$$\forall i [\![0 ; n-1]\!] \qquad V_i Q_i = 1 - U_i Q_n$$

donc
$$V_0 \cdots V_{n-1} Q_0 \cdots Q_{n-1} = (1 - U_0 Q_n) \cdots (1 - U_{n-1} Q_n)$$

Une récurrence montrerait (mais c'est facile à imaginer) que lorsqu'on développe ce produit, on trouve quelque chose de la forme

$$1 + Q_n P_1 + \cdots + Q_n^n P_n \qquad \text{avec} \qquad P_1, \dots, P_n \in \mathbb{K}[X]$$

d'où
$$V_0 \cdots V_{n-1} Q_0 \cdots Q_{n-1} - Q_n (P_1 + \cdots + P_n Q_n^{n-1}) = 1$$

D'après Bezout, Q_n et $Q_0 \cdots Q_{n-1}$ sont premiers entre eux. □

Lemme 6.2.5
Soient $P \in \mathbb{K}[X]$, $n \in \mathbb{N}^\star$ *et des polynômes* $Q_1, \dots, Q_n \in \mathbb{K}[X]$, *premiers entre eux deux-à-deux. On note*

$$F = \frac{P}{Q_1 \cdots Q_n}$$

et on suppose F *de degré strictement négatif. Il existe un unique n-uplet* $(R_1, \dots, R_n) \in (\mathbb{K}[X])^n$ *tel que*

$$F = \frac{R_1}{Q_1} + \cdots + \frac{R_n}{Q_n} \qquad \textit{avec} \qquad \forall i \in [\![1 ; n]\!] \qquad \deg R_i < \deg Q_i$$

Preuve : On procède par récurrence sur n. On note $\mathscr{P}(n)$ l'énoncé du lemme à l'ordre n et on observe que $\mathscr{P}(1)$ est une trivialité.

Soit $n \in \mathbb{N}^\star$ et supposons $\mathscr{P}(n)$ vraie. On se donne $P \in \mathbb{K}[X]$ et des polynômes $Q_1, \dots, Q_n$ et Q_{n+1}, premiers entre eux deux-à-deux, tels que

$$\deg P < \deg Q_1 + \cdots + \deg Q_n + \deg Q_{n+1}$$

Comme Q_{n+1} est premier avec $Q_1 \cdots Q_n$ d'après le **lemme 2.4**, il existe des polynômes U et V tels que

$$UQ_{n+1} + VQ_1 \cdots Q_n = 1$$

De sorte que
$$P = PUQ_{n+1} + PVQ_1 \cdots Q_n$$

et
$$F = \frac{PUQ_{n+1} + PVQ_1 \cdots Q_n}{Q_1 \cdots Q_n Q_{n+1}} = \frac{PU}{Q_1 \cdots Q_n} + \frac{PV}{Q_{n+1}}$$

D'après l'hypothèse de récurrence, il existe $S_1, \dots, S_n \in \mathbb{K}[X]$ tels que

$$\frac{PU}{Q_1 \cdots Q_n} = \frac{S_1}{Q_1} + \cdots + \frac{S_n}{Q_n}$$

Et d'après le **lemme 2.3**, il existe des polynômes $E_1, \dots, E_n, R_1, \dots, R_n$ tels que

$$\forall i \in [\![1 ; n]\!] \qquad \frac{S_i}{Q_i} = E_i + \frac{R_i}{Q_i} \qquad \text{avec} \qquad \deg R_i < \deg Q_i$$

Il existe aussi des polynômes E_{n+1} et R_{n+1} tels que

$$\frac{PV}{Q_{n+1}} = E_{n+1} + \frac{R_{n+1}}{Q_{n+1}} \qquad \text{avec} \qquad \deg R_{n+1} < \deg Q_{n+1}$$

d'où
$$F = E_1 + \cdots + E_n + E_{n+1} + \frac{R_1}{Q_1} + \cdots + \frac{R_n}{Q_n} + \frac{R_{n+1}}{Q_{n+1}}$$

On a
$$\deg\left(\frac{R_1}{Q_1} + \cdots + \frac{R_n}{Q_n} + \frac{R_{n+1}}{Q_{n+1}}\right) < \operatorname{Max}\left(\deg\frac{R_1}{Q_1}, \cdots, \deg\frac{R_{n+1}}{Q_{n+1}}\right) < 0$$

donc la partie entière de F est $E_1 + \cdots + E_{n+1}$. Mais comme $\deg F < 0$, c'est que sa partie entière est nulle. Donc en fait,

$$F = \frac{R_1}{Q_1} + \cdots + \frac{R_{n+1}}{Q_{n+1}} \qquad \text{avec} \qquad \forall i \in [\![1 ; n+1]\!] \qquad \deg R_i < \deg Q_i$$

On a fait la moitié du travail. Reste à établir l'unicité de cette décomposition.

Supposons avoir trouvé des polynômes $A_1, \dots, A_{n+1}$ tels que

$$F = \frac{A_1}{Q_1} + \cdots + \frac{A_{n+1}}{Q_{n+1}} \qquad \text{avec} \qquad \forall i \in [\![1 ; n+1]\!] \qquad \deg A_{n+1} < \deg Q_{n+1}$$

On note $$F_1 = \frac{R_1}{Q_1} + \cdots + \frac{R_n}{Q_n} \qquad \text{et} \qquad F_2 = \frac{A_1}{Q_1} + \cdots + \frac{A_{n+1}}{Q_{n+1}}$$

On peut d'ailleurs observer que $Q_1 \cdots Q_n F_1$ et $Q_1 \cdots Q_n F_2$ sont des polynômes, qu'on note P_1 et P_2, de sorte que

$$F = \frac{P_1}{Q_1 \cdots Q_n} + \frac{R_{n+1}}{Q_{n+1}} = \frac{P_2}{Q_1 \cdots Q_n} + \frac{A_{n+1}}{Q_{n+1}}$$

Alors $$\frac{P_1 - P_2}{Q_1 \cdots Q_n} = \frac{A_{n+1} - R_{n+1}}{Q_{n+1}}$$

et $$(P_1 - P_2)Q_{n+1} = (A_{n+1} - R_{n+1})Q_1 \cdots Q_n$$

Puisque Q_{n+1} et $Q_1 \cdots Q_n$ sont premiers entre eux, le **théorème de Gauss** assure que Q_{n+1} divise $A_{n+1} - R_{n+1}$. Mais $A_{n+1} - R_{n+1}$ est de degré strictement inférieur au degré de Q_{n+1}. Donc $A_{n+1} - R_{n+1} = 0$. On a donc

$$F = F_1 + \frac{R_{n+1}}{Q_{n+1}} = F_2 + \frac{R_{n+1}}{Q_{n+1}}$$

d'où $$F_1 = F_2$$

ou encore $$\frac{R_1}{Q_1} + \cdots + \frac{R_n}{Q_n} = \frac{A_1}{Q_1} + \cdots + \frac{A_n}{Q_n} \qquad \text{avec} \qquad \forall i \in [\![1\,;n]\!] \qquad \deg A_i \text{ et } \deg R_i < \deg Q_i$$

L'hypothèse de récurrence assure alors que

$$\forall i \in [\![1\,;n]\!] \qquad R_i = A_i$$

Ce qui établit l'unicité de la décomposition de F sous la forme

$$F = \frac{R_1}{Q_1} + \cdots + \frac{R_{n+1}}{Q_{n+1}} \qquad \text{avec} \qquad \forall i \in [\![1\,;n+1]\!] \qquad \deg R_i < \deg Q_i$$

Le lemme est établi à l'ordre $n+1$, et par récurrence pour tout entier n. □

On peut alors combiner les **lemmes 2.5** et **2.3** pour obtenir immédiatement le

Lemme 6.2.6
Soient $n \in \mathbb{N}^\star$, $P \in \mathbb{K}[X]$ et des polynômes $Q_1, \ldots, Q_n \in \mathbb{K}[X]$ premiers entre eux deux-à-deux. Il existe un unique $(E, R_1, \ldots, R_n) \in (\mathbb{K}[X])^{n+1}$ tel que

$$\frac{A}{Q_1 \cdots Q_n} = E + \frac{R_1}{Q_1} + \cdots + \frac{R_n}{Q_n} \qquad \textit{avec} \qquad \forall i \in [\![1\,;n]\!] \qquad \textit{deg}\, R_i < \textit{deg}\, Q_i$$

À ce stade, on a déjà bien avancé mais la preuve du **lemme 2.5** est tellement complexe qu'elle n'aide pas à trouver ces polynômes $R_1, \ldots, R_n$. Quoique... Je mens un peu. Si l'on a bien suivi, il « suffit » d'appliquer l'algorithme d'Euclide à n reprises et l'on doit s'en sortir. Ça fait beaucoup de travail.

Exemple 6.2.7
Illustrons sur un exemple la forme de la décomposition que nous garantit le **lemme 2.5**. Prenons

$$F = \frac{X^3 + 1}{(X-1)^2 (X+2)^3 (X^2 + X + 1)}$$

La partie entière de F est nulle puisque F est de degré -2. Les polynômes $(X-1)^2$, $(X+2)^3$ et $X^2 + X + 1$ sont premiers entre eux deux-à-deux, sur $\mathbb{R}$ ou sur $\mathbb{C}$, donc on peut écrire

$$F = \frac{R_1}{(X-1)^2} + \frac{R_2}{(X+2)^3} + \frac{R_3}{X^2+X+1}$$

avec $\deg R_1 < 2$ $\deg R_2 < 3$ et $\deg R_3 < 1$

Cette décomposition est valable sur $\mathbb{R}$ ou sur $\mathbb{C}$. Mais on peut la pousser plus loin sur $\mathbb{C}$, puisque $X^2+X+1 = (X-j)(X-j^2)$ et les polynômes

$$(X-1)^2 \qquad (X+2)^3 \qquad (X-j) \qquad (X-j^2)$$

sont premiers entre eux deux-à-deux. La décomposition sur $\mathbb{C}$ assurée par le **lemme 2.5** est de la forme

$$F = \frac{S_1}{(X-1)^2} + \frac{S_2}{(X+2)^3} + \frac{S_3}{X-j} + \frac{S_4}{X-j^2}$$

avec $\deg S_1 < 2$ $\deg S_2 < 3$ $\deg S_3 < 1$ et $\deg S_4 < 1$

Mais... Ce qui précède n'indique pas encore comment trouver les R ou les S.

Poussons la décomposition un cran plus loin :

Lemme 6.2.8
Soient $n \in \mathbb{N}^\star$, $P, Q \in \mathbb{K}[X]$ avec $\deg Q \geqslant 1$ et $\deg P < \deg Q^n$. Il existe un unique $(R_1, \dots, R_n) \in \mathbb{K}[X]^n$ tel que

$$\frac{P}{Q^n} = \frac{R_1}{Q} + \cdots + \frac{R_n}{Q^n} \qquad \text{et} \qquad \forall i \in [\![1\,;n]\!] \qquad \deg R_i < \deg Q$$

Preuve : Comme précédemment, on fait une récurrence. On note $\mathscr{P}(n)$ l'énoncé du lemme à l'ordre n et on remarque que $\mathscr{P}(1)$ est trivialement vrai.

Soit $n \in \mathbb{N}^\star$ et supposons $\mathscr{P}(n)$ vrai. On se donne des polynômes P et Q tels que

$$\deg Q \geqslant 1 \qquad \text{et} \qquad \deg P < \deg Q$$

On considère la fraction $F = \frac{P}{Q^{n+1}}$. Alors $QF = \frac{P}{Q^n}$ avec $\deg P < \deg Q^{n+1}$. On sait (**lemme 2.4**) qu'il existe des polynômes R_1 et R tels que

$$QF = R_1 + \frac{R}{Q^n} \qquad \text{avec} \qquad \deg R < \deg Q^n$$

D'après $\mathscr{P}(n)$, il existe des polynômes $R_2, \dots, R_{n+1}$ tels que

$$\frac{R}{Q^n} = \frac{R_2}{Q} + \cdots + \frac{R_{n+1}}{Q^n} \qquad \text{avec} \qquad \forall i \in [\![2\,;n+1]\!] \qquad \deg R_i < \deg Q$$

d'où $$QF = R_1 + \frac{R_2}{Q} + \cdots + \frac{R_{n+1}}{Q^n}$$

et $$F = \frac{R_1}{Q} + \frac{R_2}{Q^2} + \cdots + \frac{R_{n+1}}{Q^{n+1}}$$

Mais $$\frac{R_1}{Q} = F - \frac{R_2}{Q^2} - \cdots - \frac{R_{n+1}}{Q^{n+1}}$$

et toutes les fractions dans le membre de droite sont de degré strictement négatif. Donc $\frac{R_1}{Q}$ l'est aussi, d'où $\deg R_1 < \deg Q$. L'existence de la décomposition de F est établie.

Montrons l'unicité. On suppose avoir trouvé des polynômes $S_1, \dots, S_{n+1}$ tels que

$$F = \frac{S_1}{Q} + \cdots + \frac{S_{n+1}}{Q^{n+1}} \qquad \text{avec} \qquad \forall i \in [\![1\,;n+1]\!] \qquad \deg S_i < \deg Q$$

Alors $$QF = S_1 + \frac{S_2}{Q} + \cdots + \frac{S_{n+1}}{Q^n}$$

Mais $$\deg\left(\frac{S_2}{Q} + \cdots + \frac{S_{n+1}}{Q^n}\right) < 0$$

donc S_1 est la partie entière de QF. Donc $S_1 = R_1$. On a alors

$$\frac{S_2}{Q} + \cdots + \frac{S_{n+1}}{Q^n} = \frac{R_2}{Q} + \cdots + \frac{R_{n+1}}{Q^n}$$

Ces deux fractions sont de degré strictement négatif et peuvent donc être représentées sous la forme $\frac{A}{Q^n}$ avec $\deg A < \deg Q^n$. D'après $\mathscr{P}(n)$, les deux décompositions ci-dessus peuvent être identifiées :

$$\forall i \in [\![2\,;n+1]\!] \qquad R_i = S_i$$

Ce qui achève de démontrer $\mathscr{P}(n+1)$. □

À l'aide des **lemmes 2.3**, **2.5** et **2.6**, il vient le fameux

Théorème 6.2.9 (Théorème de la décomposition en éléments simples)
Soit $n \in \mathbb{N}^\star$. On se donne

- *un polynôme* P ;
- *des polynômes irréductibles* $Q_1, \ldots, Q_n$ *distincts deux-à-deux ;*
- *des entiers* $\alpha_1, \ldots, \alpha_n$ *non nuls.*

Il existe une unique famille de polynômes :

$$E, P_{1,1}, \ldots, P_{1,\alpha_1}, P_{2,1}, \ldots, P_{2,\alpha_2}, \ldots, \ldots, P_{n,1}, \ldots, P_{n,\alpha_n}$$

tels que
$$\frac{P}{Q_1^{\alpha_1} \cdots Q_n^{\alpha_n}} = E + \sum_{k=1}^{n} \sum_{j=1}^{\alpha_k} \frac{P_{k,j}}{Q_k^j}$$

avec $$\forall k \in [\![1\,;n]\!] \quad \forall j \in [\![1\,;\alpha_k]\!] \qquad deg P_{k,j} < deg Q_k$$

Cette expression est appelée décomposition en éléments simples de la fraction $\frac{P}{Q_1^{\alpha_1} \cdots Q_n^{\alpha_n}}$.

Pour chaque $k \in [\![1\,;n]\!]$, la fraction

$$\sum_{j=1}^{\alpha_k} \frac{P_{k,j}}{Q_k^j}$$

est appelée partie polaire de F *relativement à* Q_K.

Exemple 6.2.10
Ok... J'admets, ce théorème peut faire peur. On reprend l'exemple de

$$F = \frac{X^3+1}{(X-1)^2(X+2)^3(X^2+X+1)} \in \mathbb{R}[X]$$

C'est-à-dire qu'on prend

$$P = X^3+1 \qquad Q_1 = X-1 \qquad Q_2 = X+2 \qquad Q_3 = X^2+X+1 \qquad (\alpha_1, \alpha_2, \alpha_3) = (2,3,1)$$

Le théorème assure l'existence de

- $E \in \mathbb{K}[X]$, sans condition particulière ;
- $P_{1,1}, P_{1,2} \in \mathbb{K}[X]$, chacun de degré 0 ;
- $P_{2,1}, P_{2,2}, P_{2,3} \in \mathbb{K}[X]$, chacun de degré 0 ;
- $P_{3,1} \in \mathbb{K}[X]$, de degré 0 ou 1

tels que
$$F = E + \frac{P_{1,1}}{X-1} + \frac{P_{1,2}}{(X-1)^2} + \frac{P_{2,1}}{X+2} + \frac{P_{2,2}}{(X+2)^2} + \frac{P_{2,3}}{(X+2)^3} + \frac{P_{3,1}}{X^2+X+1}$$

Mais les précisions sur les degrés nous disent en fait qu'il existe des réels tels que

$$F = E + \frac{a}{X-1} + \frac{b}{(X-1)^2} + \frac{c}{X+2} + \frac{d}{(X+2)^2} + \frac{e}{(X+2)^3} + \frac{fX+g}{X^2+X+1}$$

Si on arrive à identifier $E, a, \dots, f$, on a trouvé la décomposition en éléments simples de F sur $\mathbb{R}$. On sait déjà que E est la partie entière de F ; une simple division euclidienne (ou l'observation que F est de degré strictement négatif) fournissent $E = 0$.

Si on travaille sur $\mathbb{C}$, alors

$$F = \frac{X^3+1}{(X-1)^2(X+2)^3(X-j)(X-j^2)}$$

et sa décomposition en éléments simples dans $\mathbb{C}(X)$ a la forme

$$F = \frac{a'}{X-1} + \frac{b'}{(X-1)^2} + \frac{c'}{X+2} + \frac{d'}{(X+2)^2} + \frac{e'}{(X+2)^3} + \frac{f'}{X-j} + \frac{g'}{X-j^2}$$

À noter que les coefficients $a', \dots, g'$ sont maintenant complexes. Bien évidemment, il y aura des relations entre les coefficients des décompositions dans $\mathbb{R}$ et $\mathbb{C}$ de F ; mais celles-ci ne sont pas encore établies.

Enfin, illustrons la notion de partie polaire de F. La partie polaire de F relativement à $X-1$ (ou plus simplement, relative au pôle 1) est

$$\frac{a}{X-1} + \frac{b}{(X-1)^2} \qquad \text{sur } \mathbb{R}$$

et
$$\frac{a'}{X-1} + \frac{b'}{(X-1)^2} \qquad \text{sur } \mathbb{C}$$

F a une partie polaire relativement à X^2+X+1 sur $\mathbb{R}$, qui est $\frac{fX+g}{X^2+X+1}$. Elle n'en a pas sur $\mathbb{C}$, puisque X^2+X+1 n'est pas irréductible sur $\mathbb{C}$.

En revanche, sur $\mathbb{C}$, F admet des parties polaires relativement à j et j^2, qui sont respectivement

$$\frac{f'}{X-j} \qquad \text{et} \qquad \frac{g'}{X-j^2}$$

6.2.3 Pratique de la décomposition sur $\mathbb{C}$

En pratique, on aura à décomposer des fractions rationnelles sur $\mathbb{R}$ ou $\mathbb{C}$. Commençons par le cas de $\mathbb{C}$, qui est le plus simple (ou plutôt le moins compliqué) grâce au théorème de d'Alembert et son corollaire : les irréductibles non triviaux de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Soit $F = \frac{P}{Q}$ une fraction rationnelle sur $\mathbb{C}$. On suppose qu'elle a été mise sous forme irréductible unitaire et que Q a été factorisé ; on note $a_1, \dots, a_n$ les racines de Q, de multiplicités respectives $\alpha_1, \dots, \alpha_n$.

Puisque les parties entière et fractionnaire de F sont faciles à obtenir par division euclidienne de P par Q, on peut supposer que $\deg F < 0$. La décomposition en éléments simples de F ressemble donc à

$$F = \frac{P}{(X-a_1)^{\alpha_1}\cdots(X-a_n)^{\alpha_n}} = \sum_{k=1}^{n}\sum_{j=1}^{\alpha_k}\frac{\beta_{k,j}}{(X-a_k)^j}$$

Tous les β sont des nombres complexes et pour tout $k \in [\![1\,;n]\!]$, la partie polaire de F relativement à a_k est

$$F_k = \frac{\beta_{k,1}}{X-a_k} + \cdots + \frac{\beta_{k,n}}{(X-a_k)^{\alpha_k}}$$

de sorte que $$F = F_1 + \cdots + F_n$$

Recherche de $\beta_{1,\alpha_1},\ldots,\beta_{n,\alpha_n}$

Il est possible d'identifier assez aisément, dans chaque F_k, le coefficient de plus petit degré β_{k,α_k}. On observe en effet que si l'on multiplie F par $(X-a_k)^{\alpha_k}$, on obtient une nouvelle fraction rationnelle qui n'a plus a_k pour pôle. Pour simplifier les expressions, prenons $k=1$:

$$(X-a_1)^{\alpha_1}F = \frac{P}{(X-a_2)^{\alpha_2}\cdots(X-a_n)^{\alpha_n}} = (X-a_1)^{\alpha_1}F_1 + (X-a_1)^{\alpha_1}(F_2+\cdots+F_n)$$

La fraction rationnelle $F_2+\cdots+F_n$ peut être évaluée en a_1 puisqu'elle n'a pas a_1 pour pôle. Donc

$$\big[(X-a_1)^{\alpha_1}(F_2+\cdots+F_n)\big](a_1) = (a_1-a_1)^{\alpha_1}(F_2(a_1)+\cdots+F_n(a_1)) = 0$$

Observons aussi que $$(X-a_1)^{\alpha_1}F_1 = \sum_{j=1}^{\alpha_1}\beta_{1,j}(X-a_1)^{\alpha_1-j}$$

donc $$\big[(X-a_1)^{\alpha_1}F_1\big](a_1) = \sum_{j=1}^{\alpha_1}\beta_{1,j}(X-a_1)^{\alpha_1-j}$$

Tous les termes de cette somme pour lesquels $\alpha_1 > j$ sont nuls ; et celui correspondant à $j=\alpha_1$ vaut β_{1,α_1}. Donc

$$\frac{P(a_1)}{(a_1-a_2)^{\alpha_2}\cdots(a_1-a_n)^{\alpha_n}} = \beta_{1,\alpha_1}$$

On a obtenu β_{1,α_1}, par une simple évaluation en a_1 de la fraction $(X-a_1)^{\alpha_1}F$.

Le même travail peut être accompli pour chaque pôle. Et l'on a, en général :

$$\forall k \in [\![1\,;n]\!] \qquad \beta_{k,\alpha_k} = \big[(X-a_k)^{\alpha_k}F\big](a_k)$$

Exemple 6.2.11

On illustre ceci sur notre exemple

$$F = \frac{X^3+1}{(X-1)^2(X+2)^3(X-j)(X-j^2)} = \frac{a'}{X-1} + \frac{b'}{(X-1)^2} + \frac{c'}{X+2} + \frac{d'}{(X+2)^2} + \frac{e'}{(X+2)^3} + \frac{f'}{X-j} + \frac{g'}{X-j^2}$$

La méthode précédente permet de calculer les coefficients b', e', f' et g' :

$$b' = \big[(X-1)^2F\big](1) = \left(\frac{X^3+1}{(X+2)^3(X^2+X+1)}\right)(1) = \frac{2}{3^3\times 3} = \frac{2}{81}$$

$$e' = \big[(X+2)^3F\big](-2) = \left(\frac{X^3+1}{(X-1)^2(X^2+X+1)}\right)(-2) = \frac{-7}{9\times 3} = -\frac{7}{27}$$

Tous calculs faits $$f' = \frac{j^3+1}{(j-1)^2(j+2)^3(j-j^2)} = -\frac{3+i\sqrt{3}}{27}$$

et
$$g' = \frac{j^6+1}{(j^2-1)^2(j^2+2)^3(j^2-j)} = \overline{f'} = -\frac{3-i\sqrt{3}}{27}$$

On a remarqué, au passage, que $g' = \overline{f'}$ car j^2 est le conjugué de j. Cela nous a fait économiser le calcul d'un coefficient, ce qui est toujours agréable. Ceci n'est pas un hasard et est dû, comme nous le verrons, au fait que F est à la fois dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

Ces calculs étaient peu douloureux, à l'exception de celui pour f' peut-être. Le temps total qui y a été passé (sans prendre en compte les explications) ne dépasse pas cinq minutes. On a donc :

$$F = \frac{a'}{X-1} + \frac{2}{81}\frac{1}{(X-1)^2} + \frac{c'}{X+2} + \frac{d'}{(X+2)^2} - \frac{7}{27}\frac{1}{(X+2)^3} - \frac{3+i\sqrt{3}}{27}\frac{1}{X-j} - \frac{3-i\sqrt{3}}{27}\frac{1}{X-j^2}$$

Sur 7 coefficients inconnus, 4 ont été trouvés et il en reste 3.

Observons également que si tous les pôles de notre fraction sont simples, alors cette méthode donne immédiatement la décomposition. Par exemple, en moins d'une minute, on peut montrer que

$$\frac{3X+4}{(X-1)(X+1)(X-2)} = -\frac{7}{2}\frac{1}{X-1} + \frac{1}{6}\frac{1}{X+1} + \frac{10}{3}\frac{1}{X-2}$$

Ceci fournit, par exemple, une primitive de la fonction rationnelle associée à notre fraction :

$$x \longmapsto -\frac{7}{2}\ln|x-1| + \frac{1}{6}\ln|x+1| + \frac{10}{3}\ln|x-2|$$

Évaluations au hasard

S'il reste peu de coefficients à déterminer, on peut évaluer F en quelques points de $\mathbb{C}$ pour obtenir des équations satisfaites par nos coefficients inconnus.

Exemple 6.2.12
Prenons $F = \frac{2X+1}{(X-1)^2(X-i)}$. La décomposition ressemble à

$$F = \frac{a}{X-1} + \frac{b}{(X-1)^2} + \frac{c}{X-i}$$

La méthode précédente fournit immédiatement b et c :

$$b = \frac{3}{1-i} = \frac{3+3i}{2} \qquad \text{et} \qquad c = \frac{2i+1}{(i-1)^2} = \frac{-2+i}{2}$$

donc
$$\frac{2X+1}{(X-1)^2(X-i)} = \frac{a}{X-1} + \frac{3+3i}{2}\frac{1}{(X-1)^2} + \frac{-2+i}{2}\frac{1}{X-i}$$

On peut par exemple évaluer ces deux expressions en 0 pour obtenir :

$$i = -a + \frac{3+3i}{2} - \frac{1+2i}{2} = -a + \frac{2+i}{2}$$

d'où l'on déduit
$$a = \frac{2+i}{2} - i = \frac{2-i}{2}$$

Finalement,
$$F = \frac{2-i}{2}\frac{1}{X-1} + \frac{3+3i}{2}\frac{1}{(X-1)^2} + \frac{-2+i}{2}\frac{1}{X-i}$$

Utilisation de la division suivant les puissances croissantes

Il s'agit de la méthode qui marchera à tous les coups. Mais suivant les situations, il sera peut-être plus rapide de combiner les méthodes précédentes. Elle est surtout efficace pour trouver la partie polaire pour un pôle d'ordre élevé. Rappelons que

$$F = \frac{P}{(X-a_1)^{\alpha_1}\cdots(X-a_n)^{\alpha_n}}$$

On va déterminer la partie polaire relative à a_1. On pose $Y = X - a_1$ de sorte que $X = Y + a_1$ et

$$F = \frac{P(Y+a_1)}{Y^{\alpha_1}(Y+a_1-a_2)^{\alpha_2}\cdots(Y+a_1-a_n)^{\alpha_n}}$$

On note $$B = (Y+a_1-a_2)^{\alpha_2}\cdots(Y+a_1-a_n)^{\alpha_n} \in \mathbb{K}[Y]$$

et l'on effectue la division suivant les puissances croissantes à l'ordre $\alpha_1 - 1$ de $P(Y+a_1)$ par B dans $\mathbb{K}[Y]$. Cela fournit des polynômes Q et R tels que

$$P(Y+a_1) = B(Y)Q(Y) + Y^{\alpha_1}R(Y) \qquad \text{avec} \qquad \deg Q \leqslant \alpha_1 - 1$$

de sorte que $$P(X) = B(X-a_1)Q(X-a_1) + (X-a_1)^{\alpha_1}R(X-a_1)$$

d'où $$\frac{P}{(X-a_2)^{\alpha_2}\cdots(X-a_n)^{\alpha_n}} = Q(X-a_1) + (X-a_1)^{\alpha_1}\frac{R(X-a_1)}{(X-a_2)^{\alpha_2}\cdots(X-a_n)^{\alpha_n}}$$

et $$F = \frac{P}{(X-a_1)^{\alpha_1}\cdots(X-a_n)^{\alpha_n}} = \frac{Q(X-a_1)}{(X-a_1)^{\alpha_1}} + \frac{R(X-a_1)}{(X-a_2)^{\alpha_2}\cdots(X-a_n)^{\alpha_n}}$$

Notons $$Q(Y) = \sum_{k=0}^{\alpha_1-1} Q_k Y^k$$

Alors $$Q(X-a_1) = \sum_{k=0}^{\alpha_1-1} Q_k (X-a_1)^k$$

et $$F = \sum_{k=0}^{\alpha_1-1} \frac{Q_k}{(X-a_1)^{\alpha_1-k}} + \frac{R(X-a_1)}{(X-a_2)^{\alpha_2}\cdots(X-a_n)^{\alpha_n}}$$

On peut réarranger les indices dans la somme pour bien voir qu'on a trouvé la partie polaire relative à a_1, en posant $k \leftarrow \alpha_1 - k$:

$$F = \sum_{k=1}^{\alpha_1} \frac{Q_{\alpha_1-k}}{(X-a_1)^k} + \frac{R(X-a_1)}{(X-a_2)^{\alpha_2}\cdots(X-a_n)^{\alpha_n}}$$

La deuxième fraction ne présente pas a_1 comme pôle ; l'unicité de la décomposition en éléments simples annoncée par le **théorème 2.9** assure alors que la somme constitue la partie polaire de F relative à a_1.

Exemple 6.2.13
On reprend notre fraction $F = \dfrac{X^3+1}{(X-1)^2(X+2)^3(X^2+X+1)}$ et on cherche sa partie polaire relative à -2. Pour cela, on pose $Y = X+2$ de sorte que $X = Y-2$ donc

$$F(X) = \frac{(Y-2)^3+1}{Y^3(Y-3)^2((Y-2)^2+(Y-2)+1)} = \frac{Y^3-6Y^2+12Y-7}{Y^3(Y^4-9Y^3+30Y^2-45Y+27)}$$

On effectue la division puissances croissantes à l'ordre 2 du numérateur par $Y^4-9Y^3+30Y^2-45Y+27$. Tous calculs faits,

$$(Y-2)^3+1 = (Y-3)^2((Y-2)^2+(Y-2)+1)\times\left(\frac{7}{81}Y^2+\frac{1}{81}Y-\frac{7}{27}\right)+Y^3R(Y)$$

On remplace Y par $X+2$:

$$X^3+1=(X-1)^2(X^2+X+1)\times\left(\frac{7}{81}(X+2)^2+\frac{1}{81}(X+2)-\frac{7}{27}\right)+(X+2)^3R(X+2)$$

d'où $$\frac{X^3+1}{(X-2)^3(X-1)^2(X^2+X+1)}=\frac{7}{81}\frac{1}{X+2}+\frac{1}{81}\frac{1}{(X+2)^2}-\frac{7}{27}\frac{1}{(X+2)^3}+\frac{R(X+2)}{(X-1)^2(X^2+X+1)}$$

Évidemment, il est très probable que mes calculs soient faux.

Remarquons qu'on se moque de savoir ce que vaut précisément le polynôme R : en effet, cette méthode fournit la partie polaire de F relative à -2, on ne demande pas plus. Cette observation est assez intéressante : toute personne ayant tenté ce calcul par elle-même a pu voir à quel point il est fastidieux. Mais, à partir du moment où l'on a remarqué que toutes les puissances de Y supérieures à 3 dans le reste de la division puissances croissantes ne nous servent à rien, on augmente son efficacité : il suffit d'ignorer, au cours de ce calcul, toutes les puissances supérieures à 3.

Observons qu'à l'aide de cette méthode et de la première décrite dans cette partie, on a trouvé 6 des 7 coefficients de la décomposition de F. On peut trouver le dernier, celui correspondant à $X-1$, par exemple avec une évaluation au hasard.

Si la fraction est à coefficients réels

Supposons que $F=\dfrac{P}{Q}\in\mathbb{R}(X)$ de sorte que P et Q sont à coefficients réels. On suppose comme précédemment que F n'a pas de partie entière puisque trouver celle-ci ne pose aucun problème.

On sait que si a est une racine complexe non réelle de Q, alors $\overline{a}$ est aussi racine de Q, de même multiplicité que a. Supposons que ce soit le cas ; on note α la multiplicité commune des racines a et $\overline{a}$ dans Q de sorte que

$$Q=(X-a)^\alpha(X-\overline{a})^\alpha Q_1 \qquad \text{avec} \qquad Q_1\in\mathbb{R}[X]$$

En outre, a et $\overline{a}$ ne sont pas racines de Q_1 donc Q_1 est premier avec $(X-a)^\alpha$ et $(X-\overline{a})^\alpha$. On sait que la décomposition en éléments simples de F est de la forme

$$F=\frac{b_1}{X-a}+\cdots+\frac{b_\alpha}{(X-a)^\alpha}+\frac{c_1}{X-\overline{a}}+\cdots+\frac{c_\alpha}{(X-a)^\alpha}+\frac{A}{Q_1} \qquad \text{avec} \qquad A\in\mathbb{R}[X]$$

Alors, comme F, A et Q_1 sont dans $\mathbb{R}(X)$,

$$F=\overline{F}=\frac{\overline{b_1}}{X-\overline{a}}+\cdots+\frac{\overline{b_\alpha}}{(X-\overline{a})^\alpha}+\frac{\overline{c_1}}{X-a}+\cdots+\frac{\overline{c_\alpha}}{(X-a)^\alpha}+\frac{A}{Q_1}$$

Mais le **théorème 2.9** annonce l'unicité de la décomposition de F sur $\mathbb{C}$. Ce qui permet d'assurer que

$$\overline{b_1}=c_1 \quad \overline{b_2}=c_2 \quad \cdots \quad \overline{b_\alpha}=c_\alpha$$

Autrement dit, il suffit de trouver les b ; les c sont simplement leurs conjugués.

Il est important de rappeler qu'on s'est ici fortement appuyé sur le fait que $F\in\mathbb{R}(X)$. On ne peut rien conclure si ce n'est pas le cas !

6.2.4 Pratique de la décomposition sur $\mathbb{R}$

Malheureusement, les choses peuvent devenir très compliquées si la fraction est dans $\mathbb{R}[X]$ et qu'elle a au dénominateur des puissances élevées d'irréductibles de degré 2.

La méthode généralement donnée consiste à d'abord décomposer la fraction sur $\mathbb{C}$, puis regrouper les termes conjugués. Et ensuite utiliser une méthode de divisions euclidiennes successives. Cela serait lourd à expliquer ici. En outre, suivant la situation, on peut ruser, mais tout se fait au cas par cas.

Il est à noter que pour une machine, ces calculs ne posent pas de problème.

Chapitre 7

Espaces Vectoriels de Dimension Finie

Comme toujours, $\mathbb{K}$ est un corps commutatif et E est un $\mathbb{K}$-espace vectoriel.

7.1 Notion de dépendance linéaire

7.1.1 Rappel : sous-espace engendré

On rappelle que si E un $\mathbb{K}$-espace vectoriel et si A est une partie de E, le sous-espace engendré par A, noté VectA, est le plus petit sous-espace vectoriel de E contenant A.

C'est aussi l'ensemble de toutes les combinaisons linéaires finies d'éléments de A. Par suite, si A est une famille finie non vide $A = \{e_1, \dots, e_n\}$ de vecteurs de E, on a

$$\mathrm{Vect}\,A = \left\{ \sum_{k=1}^{n} \lambda_k e_k \mid (\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n \right\} \tag{1}$$

L'objet de ce chapitre est d'étudier les espaces vectoriels qui peuvent être engendrés par une partie finie. Ceux-ci sont particulièrement intéressants puisque, d'après la relation (**1**), leurs éléments peuvent être décrits à partir d'un nombre fini de vecteurs.

Une première chose à faire est de voir comment on peut affiner cette description. Par exemple, il est clair que si A contient le vecteur nul, ce dernier ne contribue rien à VectA. Ou bien, si e_1 et e_2 sont dans A, alors $B = A \cup \{e_1 + e_2\}$ va engendrer le même sous-espace que A.

7.1.2 Familles libres et liées

Définition 7.1.1

Soit $\mathscr{F} = (e_1, \dots, e_n)$ une famille non vide de E. On dit que $\mathscr{F}$ est *libre*, ou encore que $e_1, \dots, e_n$ *sont linéairement indépendants*, si et seulement si

$$\forall (\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n \qquad \left(\sum_{k=1}^{n} \lambda_k e_k = 0 \implies \lambda_1 = \cdots = \lambda_n = 0 \right)$$

On dira que $\mathscr{F}$ est *liée*, ou encore que $e_1, \dots, e_n$ *sont linéairement dépendants*, si et seulement si elle n'est pas libre :

$$\exists (\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n \setminus \{0\} \qquad \sum_{k=1}^{n} \lambda_k e_k = 0$$

Exemple 7.1.2

1. Soit $\mathscr{F} = (e_1, \dots, e_n)$ une famille de vecteurs de E. On suppose qu'elle contient le vecteur nul, c'est-à-dire qu'il existe $i \in [\![1\,;n]\!]$ tel que $e_i = 0$. Alors $\mathscr{F}$ est liée : en effet, posons
$$\forall k \in [\![1\,;n]\!] \qquad \lambda_k = \begin{cases} 0 \text{ si } k \neq i \\ 26.92 \text{ si } k = i \end{cases}$$
Alors
$$\sum_{k=1}^{n} \lambda_k e_k = \lambda_i e_i = 0$$
tandis que $(\lambda_1, \dots, \lambda_n) \neq 0$.
2. Dans $\mathbb{R}[X]$, la famille $(1, X, \dots, X^n)$ est libre. En effet, soit $(\lambda_0, \dots, \lambda_n) \in \mathbb{K}^{n+1}$ tel que
$$\sum_{k=0}^{n} \lambda_k X^k = 0$$
Un polynôme est nul si et seulement si tous ses coefficients sont nuls. Donc
$$\lambda_0 = \cdots = \lambda_n = 0$$
3. Toute base de $\overrightarrow{\mathscr{E}}$ est libre. En effet, soit $(\overrightarrow{u}, \overrightarrow{v}, \overrightarrow{w})$ une famille de 3 vecteurs de $\overrightarrow{\mathscr{E}}$.
On suppose cette famille liée. Il existe des réels α, β et γ, non tous nuls, tels que
$$\alpha\overrightarrow{u} + \beta\overrightarrow{v} + \gamma\overrightarrow{w} = \overrightarrow{0}$$
On peut suppose que c'est γ qui n'est pas nul. De sorte qu'on ait
$$\overrightarrow{w} = -\frac{\alpha}{\gamma}\overrightarrow{u} - \frac{\beta}{\gamma}\overrightarrow{v}$$
On voit que $\overrightarrow{w}$ est combinaison linéaire de $\overrightarrow{u}$ et $\overrightarrow{v}$: $\overrightarrow{u}, \overrightarrow{v}, \overrightarrow{w}$ sont coplanaires et ne constituent donc pas une base.
4. Soit (e_1, e_2) une famille de deux vecteurs de E. Si elle est liée, il existe des scalaires λ_1 et λ_2 dont l'un des deux (par exemple λ_1) n'est pas nul tels que
$$\lambda_1 e_1 + \lambda_2 e_2 = 0$$
d'où
$$e_1 = -\frac{\lambda_2}{\lambda_1} e_2$$
On voit donc que e_1 et e_2 sont proportionnels.

Les exemples 3 et 4 nous amènent à dire que deux vecteurs liés sont *colinéaires* et que trois vecteurs liés sont *coplanaires*.

Le théorème suivant est fondamental pour la suite : il nous confirme qu'une famille liée comporte des vecteurs redondants dans la description du sous-espace vectoriel qu'elle engendre : qu'ils soient là ou qu'on les retire, le sous-espace engendré sera le même. On en profite pour ajouter des propriétés élémentaires de ces nouvelles notions de dépendance linéaire.

Théorème 7.1.3

1. *Soit $\mathscr{F}$ une famille liée de vecteurs de* E. *Alors l'un des vecteurs qui la composent est combinaison linéaire des autres, c'est-à-dire que*
$$\exists e \in \mathrm{F} \qquad e \in \mathit{Vect}(\mathscr{F} \setminus \{e\})$$
De plus, $\mathscr{F}$ et $\mathscr{F} \setminus \{e\}$ engendrent le même sous-espace vectoriel de E.

2. *Soient $\mathscr{F}$ une famille libre et $e \in E$. La famille $\mathscr{F} \cup \{e\}$ est libre si et seulement si e n'est pas dans le sous-espace engendré par $\mathscr{F}$.*
3. *Toute sous-famille d'une famille libre est libre.*

Preuve : Traitons les points un par un :

1. Puisque $\mathscr{F}$ est finie, on peut énumérer ses éléments : $\mathscr{F} = (e_1, \dots, e_n)$. Comme elle est liée, il existe des scalaires $\lambda_1, \dots, \lambda_n$, non tous nuls, tels que
$$\sum_{k=1}^{n} \lambda_k e_k = 0$$
Il existe i tel que $\lambda_i \neq 0$ et on a donc
$$e_i = -\sum_{\substack{k=1 \\ k\neq i}}^{n} \frac{\lambda_k}{\lambda_i} e_k \tag{2}$$
e_i est une combinaison linéaire des autres vecteurs de $\mathscr{F}$.
Comme $\mathscr{F} \setminus \{e_i\}$ est inclus dans $\mathscr{F}$, on a déjà
$$\text{Vect}\,(\mathscr{F} \setminus \{e_i\}) \subset \text{Vect}\,\mathscr{F}$$
Maintenant, si on se donne $x \in \text{Vect}\,\mathscr{F}$, on sait que x est combinaison linéaire des vecteurs de $\mathscr{F}$. Donc il existe des scalaires $x_1, \dots, x_n$ tels que
$$x = \sum_{k=1}^{n} x_k e_k$$
Mais on sait qu'on peut remplacer e_i par l'expression (**2**) donc
$$x = x_i e_i + \sum_{\substack{k=1 \\ k\neq i}}^{n} x_k e_k = \sum_{\substack{k=1 \\ k\neq i}}^{n} \left(x_k - \frac{x_i \lambda_k}{\lambda_i}\right) e_k$$
et on voit que $x \in \text{Vect}\,(\mathscr{F} \setminus \{e_i\})$.
2. Soient $\mathscr{F} = (e_1, \dots, e_n)$ une famille libre et $e \in E$. On suppose d'abord que e se trouve dans le sous-espace engendré par $\mathscr{F}$. Alors e est combinaison linéaire des vecteurs de $\mathscr{F}$:
$$\exists (\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n \qquad e = \sum_{k=1}^{n} \lambda_k e_k$$
Par suite, $\mathscr{F} \cup \{e\}$ est liée puisqu'on a une combinaison linéaire à coefficients non tous nuls :
$$e - \sum_{k=1}^{n} \lambda_k e_k = 0$$
Réciproquement, supposons que $\mathscr{F} \cup \{e\}$ est liée. Alors
$$\exists (\lambda_1, \dots, \lambda_n, \lambda) \in \mathbb{K}^{n+1} \setminus \{0\} \qquad \lambda e + \sum_{k=1}^{n} \lambda_k e_k = 0$$
Il est exclu que λ soit nul : en effet, si c'était le cas, la liberté de $\mathscr{F}$ impliquerait que $\lambda_1, \dots, \lambda_n$ sont également nuls ce qui contredit la ligne précédente. Comme $\lambda \neq 0$, on peut écrire
$$e = -\sum_{k=0}^{n} \frac{\lambda_k}{\lambda} e_k \in \text{Vect}\,(\mathscr{F})$$
On a donc montré que $\mathscr{F} \cup \{e\}$ est liée si et seulement si e appartient à $\text{Vect}\,\mathscr{F}$. C'est la contre-apposée de notre proposition.
3. C'est trivial. □

7.1.3 Bases

Définition 7.1.4
Soit $\mathscr{B} = (e_1, \dots, e_n)$ une famille de vecteurs de E. On dit que c'est une base de E si et seulement si elle est libre et génératrice de E.

Théorème 7.1.5
Soit $(e_1, \dots, e_n)$ une famille libre de vecteurs de E. *C'est une base de l'espace vectoriel qu'elle engendre.*

Preuve : Notons $F = \text{Vect}(e_1, \dots, e_n)$. Cet espace est engendré par la famille libre $(e_1, \dots, e_n)$; d'après la **définition 1.4**, c'est une base de F. □

Théorème 7.1.6
Soit $\mathscr{F} = (e_1, \dots, e_n)$ une famille de vecteurs de E. *Elle est libre si et seulement si*

$$\begin{aligned} f : \quad & \mathbb{K}^n \longrightarrow \mathrm{E} \\ & (\lambda_1, \dots, \lambda_n) \longmapsto \sum_{k=1}^{n} \lambda_k e_k \end{aligned} \qquad \textit{est injective}$$

Preuve : f est clairement linéaire. On sait alors qu'elle est injective si et seulement si son noyau est réduit à $\{0\}$. Donc on étudie $\text{Ker}\, f$:

$$\begin{aligned} \text{Ker}\, f &= \left\{(\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n \mid f(\lambda_1, \dots, \lambda_n) = 0\right\} \\ &= \left\{(\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n \mid \sum_{k=1}^{n} \lambda_k e_k = 0\right\} \end{aligned}$$

D'après la **définition 1.1**, $\text{Ker}\, f = \{0\}$ si et seulement si $\mathscr{F}$ est libre. □

Théorème 7.1.7
Soit $\mathscr{F} = (e_1, \dots, e_n)$ une famille de vecteurs de E. *Elle engendre* E *si et seulement si*

$$\begin{aligned} f : \quad & \mathbb{K}^n \longrightarrow \mathrm{E} \\ & (\lambda_1, \dots, \lambda_n) \longmapsto \sum_{k=1}^{n} \lambda_k e_k \end{aligned}$$

est surjective.

Preuve : C'est une conséquence immédiate du fait que le sous-espace engendré par $\mathscr{F}$ est l'ensemble des combinaisons linéaires de vecteurs de cette famille. □

Corollaire 7.1.8
Soit $\mathscr{F} = (e_1, \dots, e_n)$ une famille de vecteurs de E. *C'est une base de* E *si et seulement si*

$$\begin{aligned} f : \quad & \mathbb{K}^n \longrightarrow \mathrm{E} \\ & (\lambda_1, \dots, \lambda_n) \longmapsto \sum_{k=1}^{n} \lambda_k e_k \end{aligned}$$

est un isomorphisme d'espaces vectoriels.

Preuve : f est clairement linéaire. Et d'après les **théorèmes 1.6** et **1.7**, elle est bijective si et seulement $\mathscr{F}$ est libre et génératrice. □

Voici une propriété des bases que nous avons déjà rencontrée dans les cours de géométrie du plan et de l'espace.

Corollaire 7.1.9
Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de E. *Tout vecteur de* E *s'écrit de manière unique comme combinaison linéaire des $(e_i)_{1 \leqslant i \leqslant n}$.*

Preuve : Soit $x \in$ E. Comme l'application f du **corollaire 1.8** est bijective, il existe un unique $(x_1, \dots, x_n) \in \mathbb{K}^n$, tel que

$$x = \sum_{k=1}^{n} x_k e_k$$

Donc x se décompose de manière unique comme combinaison linéaire des $(e_i)_{1 \leqslant i \leqslant n}$. □

Définition 7.1.10
Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de E. Si $x \in$ E, l'unique $(x_1, \dots, x_n) \in \mathbb{K}^n$ tel que

$$x = \sum_{k=1}^{n} x_k e_k$$

est appelé *système de coordonnées de x dans la base $\mathscr{B}$* et on note

$$[x]_{\mathscr{B}} = (x_1, \dots, x_n)$$

Corollaire 7.1.11
Soit $\mathscr{B}$ une base de E. *L'application*

$$\begin{aligned} g : \ \mathrm{E} &\longrightarrow \mathbb{K}^n \\ x &\longmapsto [x]_{\mathscr{B}} \end{aligned}$$

est un isomorphisme d'espaces vectoriels.

Preuve : g est la bijection réciproque de l'application f définie au **corollaire 1.8**. C'est donc un isomorphisme d'espaces vectoriels, puisqu'on sait du cours d'introduction à l'algèbre linéaire que la réciproque d'un isomorphisme est linéaire. □

Exemple 7.1.12
Si $\mathscr{B} = (e_1, \dots, e_n)$ est une base de E et $i \in [\![1 ; n]\!]$, on observe que e_i est égal à une fois lui-même, plus zéro fois les autres vecteurs de $\mathscr{B}$. Donc

$$\forall i \in [\![1 ; n]\!] \qquad [e_i]_{\mathscr{B}} = (0, \dots, 0, \underset{\substack{\uparrow \\ i\text{-ème position}}}{1}, 0, \dots, 0)$$

Théorème 7.1.13
Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de E. *Soit* F *un autre $\mathbb{K}$-espace vectoriel, soit $(f_1, \dots, f_n)$ une famille de vecteurs de* F. *Il existe un unique $u \in \mathscr{L}(\mathrm{E}, \mathrm{F})$ tel que*

$$\forall i \in [\![1 ; n]\!] \qquad u e_i = f_i$$

Preuve : Si x est un vecteur quelconque de E, on convient de noter $(x_1, \dots, x_n)$ ses coordonnées dans la base $\mathscr{B}$. On définit alors

$$\forall x \in \mathrm{E} \qquad u(x) = \sum_{k=1}^{n} x_k f_k$$

D'après l'**exemple 1.12**, pour tout i compris entre 1 et n, $[e_i]_{\mathscr{B}}$ a toutes ses coordonnées nulles sauf la i-ème qui vaut 1. Donc

$$u(e_i) = f_i$$

Montrons que u est linéaire. Soient x, y dans E et λ dans $\mathbb{K}$. D'après le **corollaire 1.11**,

$$\begin{aligned}[\lambda x + y]_{\mathscr{B}} &= \lambda [x]_{\mathscr{B}} + [y]_{\mathscr{B}} = (\lambda x_1, \ldots, \lambda x_n) + (y_1, \ldots, y_n) \\ &= (\lambda x_1 + y_1, \ldots, \lambda x_n + y_n)\end{aligned}$$

donc $$u(\lambda x + y) = \sum_{k=1}^{n} (\lambda x_k + y_k) f_k = \lambda \sum_{k=1}^{n} x_k f_k + \sum_{k=1}^{n} y_k f_k = \lambda u(x) + u(y)$$

ce qui montre que $u \in \mathscr{L}(\mathrm{E}, \mathrm{F})$.

Vérifions maintenant l'unicité de cette application. Soit $v \in \mathscr{L}(\mathrm{E}, \mathrm{F})$, tel que

$$\forall i \in [\![1 ; n]\!] \qquad v(e_i) = f_i$$

Alors $$\forall x \in \mathrm{E} \qquad v(x) = v\Big(\sum_{k=1}^{n} x_k e_k \Big) = \sum_{k=1}^{n} x_k v(e_k) = \sum_{k=1}^{n} x_k f_k = u(x)$$

d'où $$v = u$$ □

7.2 Dimension d'un espace vectoriel

7.2.1 Existence de bases

Définition 7.2.1

Soit E un $\mathbb{K}$-espace vectoriel. On dit qu'il est *de dimension finie* si et seulement si E est engendré par une partie finie.

> Remarquez comme on définit ce que signifie *être de dimension finie*, mais on ne dit pas (du moins pas encore) ce qu'est la dimension d'un tel espace.
>
> *A priori*, on aimerait naïvement dire qu'il s'agit du cardinal d'une partie génératrice finie. Mais on s'aperçoit immédiatement que cette définition n'aurait aucun sens : il y a des tas de parties génératrices de E. Il peut y en avoir une qui comporte 17 éléments et une autre qui en comporte 666. Du coup, dira-t-on que notre espace est de dimension 17 ou 666 ?
>
> Notre stratégie est en fait la suivante. On montre qu'un espace de dimension finie admet des bases. Et que par miracle (les mathématiciens appellent plutôt cela un lemme) toutes ces bases ont le même cardinal. C'est celui-ci qu'on appellera dimension de l'espace.
>
> On rappelle qu'une base est une partie de E, à la fois libre et génératrice. Donc une partie de E n'est pas une base si elle n'est pas libre, ou si elle n'est pas génératrice.

Théorème 7.2.2

Tout espace vectoriel, non réduit à $\{0\}$*, de dimension finie admet des bases.*

Preuve : Soit E un espace vectoriel de dimension finie, n'admettant pas de base.

Comme E est de dimension finie, il admet une partie génératrice finie : il existe $\mathscr{F} \subset$ E, de cardinal $n > 0$, tel que E = Vect $\mathscr{F}$.

On définit, pour tout entier p, la propriété $\mathscr{P}(p)$: « E peut être engendré par $n-p$ vecteurs. »

- $\mathscr{P}$**(0) est vraie** puisque E est engendré par $\mathscr{F}$ qui a pour cardinal $n-0$.
- $\mathscr{P}$ **est héréditaire :** soit p un entier inférieur à $n-2$. On suppose que $\mathscr{P}(p)$ est vraie. Il existe donc $\mathscr{A} \subset$ E, de cardinal $n-p$, engendrant E. Comme E n'admet pas de base, $\mathscr{A}$ est liée. D'après le **théorème 1.3**, il existe $e \in$ A tel que A $\setminus \{e\}$ engendre E. Mais A $\setminus \{e\}$ a pour cardinal $n-p-1 = n-(p+1)$. Donc $\mathscr{P}(p+1)$ est vraie.
- **Conclusion :** $\mathscr{P}(p)$ est vraie pour tout $p \in [\![0\,;n-1]\!]$.

Puisque $\mathscr{P}(n-1)$ est vraie, E peut être engendré par un seul vecteur. Donnons-nous un vecteur générateur x de E. Comme la famille constituée seulement de x n'est pas une base, elle est liée. Donc il existe $\lambda \neq 0$, tel que $\lambda x = 0$. Donc $x = 0$ et

$$\mathrm{E} = \mathrm{Vect}\,(0) = \{0\}$$

Par contre-apposée, un espace vectoriel de dimension finie, non réduit à $\{0\}$, admet des bases. □

7.2.2 Le lemme fondamental

Lemme 7.2.3

Soient n et p deux entiers non nuls. Soient $\mathscr{A}$ et $\mathscr{B}$ deux familles de vecteurs de E*, de cardinaux respectifs $n+p$ et n. Si tout vecteur de $\mathscr{A}$ est combinaison linéaire des vecteurs de $\mathscr{B}$, alors $\mathscr{A}$ est liée.*

Preuve : On démontre cela par récurrence. On définit, pour tout entier n non nul, la propriété $\mathscr{P}(n)$: « Soient $\mathscr{A}$ et $\mathscr{B}$ deux parties de E, de cardinaux respectifs $n+1$ et n, telles que tout vecteur de $\mathscr{A}$ est combinaison linéaire des vecteurs de $\mathscr{B}$. Alors $\mathscr{A}$ est liée. »

- $\mathscr{P}$**(1) est vraie :** on se donne $\mathscr{A} = \{e_1, e_2\}$ et $\mathscr{B} = \{u\}$ deux parties de E, de cardinaux respectifs 2 et 1. Et on suppose que e_1 et e_2 sont tous deux combinaison linéaire de u : il existe des scalaires λ_1 et λ_2 tels que

  $$e_1 = \lambda_1 u \qquad \text{et} \qquad e_2 = \lambda_2 u$$

  Évidemment, si λ_1 ou λ_2 est nul, $\mathscr{A}$ est liée puisqu'elle contient le vecteur nul. Donc on suppose ces scalaires non nuls et on a

  $$\lambda_2 e_1 - \lambda_1 e_2 = 0$$

  ce qui montre que $\mathscr{A}$ est liée.
- $\mathscr{P}(n) \Longrightarrow \mathscr{P}(n+1)$ **:** Soit n un entier non nul, tel que $\mathscr{P}(n)$ soit vraie. On se donne

  $$\mathscr{A} = \{e_1, \ldots, e_{n+2}\} \qquad \text{et} \qquad \mathscr{B} = \{u_1, \ldots, u_{n+1}\}$$

  deux parties de E, de cardinaux respectifs $n+2$ et $n+1$, telles que tout vecteur de $\mathscr{A}$ soit combinaison linéaire des vecteurs de $\mathscr{B}$. Donc

  $$\forall i \in [\![1\,;n+2]\!] \quad \exists (\lambda_{i,1}, \ldots, \lambda_{i,n+1}) \in \mathbb{K}^{n+1} \qquad e_i = \sum_{j=1}^{n+2} \lambda_{i,j} u_j$$

  Si tous les scalaires $\lambda_{1,n+1}, \ldots, \lambda_{n+2,n+1}$ sont nuls, alors $e_1, \ldots, e_{n+2}$ sont en fait, chacun, combinaison linéaire de $u_1, \ldots, u_n$. D'après $\mathscr{P}(n)$, $(e_1, \ldots, e_{n+1})$ est liée et par suite $\mathscr{A}$ est liée aussi.

Ce cas ayant été traité, on suppose maintenant qu'un de ces scalaires n'est pas nul. Quitte à renommer tous nos vecteurs, on peut supposer que $\lambda_{n+2,n+1} \neq 0$. Et on a donc

$$\forall i \in [\![1\,;n+1]\!] \qquad e_i - \frac{\lambda_{i,n+2}}{\lambda_{n+1,n+2}}\,e_{n+2} = \sum_{j=1}^{n+2} \lambda_{i,j}\,u_j - \sum_{j=1}^{n+2} \frac{\lambda_{n+2,j}\,\lambda_{i,n+2}}{\lambda_{n+1,n+2}}\,u_j$$
$$= \sum_{j=1}^{n+2} \frac{\lambda_{i,j}\,\lambda_{n+1,n+2} - \lambda_{n+2,j}\,\lambda_{i,n+2}}{\lambda_{n+1,n+2}}\,u_j$$

On remarque en particulier que le $n+2$-ème terme de cette somme est nul d'où

$$\forall i \in [\![1\,;n+1]\!] \qquad e_i - \frac{\lambda_{i,n+2}}{\lambda_{n+1,n+2}}\,e_{n+2} = \sum_{j=1}^{n+1} \frac{\lambda_{i,j}\,\lambda_{n+1,n+2} - \lambda_{n+2,j}\,\lambda_{i,n+2}}{\lambda_{n+1,n+2}}\,u_j$$

Les vecteurs du membre de gauche sont au nombre de $n+1$; et ils sont, chacun, combinaison linéaire des n vecteurs $u_1,\dots,u_n$. D'après $\mathscr{P}(n)$, ils sont liés : il existe des scalaires $\mu_1,\dots,\mu_{n+1}$, non tous nuls, tels que

$$\sum_{i=1}^{n+1} \mu_i \Big(e_i - \frac{\lambda_{i,n+2}}{\lambda_{n+1,n+2}}\,e_{n+1}\Big) = 0$$

Après avoir développé tout cela, il vient

$$\sum_{i=1}^{n+1} \mu_i e_i - \Big(\sum_{i=1}^{n+1} \frac{\mu_i \lambda_{i,n+2}}{\lambda_{n+1,n+2}}\Big) e_{n+1} = 0$$

On obtient une combinaison linéaire nulle des vecteurs de $\mathscr{A}$; et au moins un des coefficients de cette combinaison n'est pas nul, puisque l'un des $(\mu_i)_{1\leqslant i\leqslant n+1}$ n'est pas nul. Donc $\mathscr{A}$ est liée et $\mathscr{P}(n+1)$ est vraie.

- **Conclusion :** $\mathscr{P}(n)$ est vraie pour tout entier n non nul.

Ainsi, si n est un entier, toute famille de $n+1$ vecteurs, qui sont chacun combinaison linéaire de n mêmes vecteurs, sont liés. Le lemme s'en déduit immédiatement. □

7.2.3 Existence de la dimension

Théorème 7.2.4

Soit E *un* $\mathbb{K}$*-espace vectoriel non nul de dimension finie. Toutes les bases de* E *ont le même cardinal.*

Preuve : On sait, d'après le **théorème 2.2**, que E admet des bases. Soit $\mathscr{B}$ l'une d'elles, dont on note n le cardinal. Soit $\mathscr{B}'$ une autre base.

Supposons que $|\mathscr{B}'| > n$. Comme $\mathscr{B}'$ engendre E, les n vecteurs de $\mathscr{B}$ sont, chacun, combinaison linéaire des vecteurs de $\mathscr{B}'$. D'après le **lemme 2.3**, $\mathscr{B}$ est liée et on a une contradiction.

De même, si $|\mathscr{B}'| < n$, c'est $\mathscr{B}'$ qui est liée ce qui contredit le fait que c'est une base.

Par conséquent, $|\mathscr{B}'| = n$: toute base de E a pour cardinal n. □

Définition 7.2.5

Soit E un $\mathbb{K}$-espace vectoriel non nul de dimension finie. Le cardinal commun de toutes les bases de E est appelé *dimension de* E. Par convention, l'espace vectoriel nul est de dimension 0.

Exemple 7.2.6

1. On note $\mathbb{K}_n[X]$ le sous-espace de $\mathbb{K}[X]$ formé des polynômes de degré inférieur à n. Il est donc engendré par $(1,X,\dots,X^n)$. On a vu dans l'**exemple 1.2** que $(1,X,\dots,X^n)$ cette famille est libre. C'est donc une base de cet espace, qui est donc de dimension $n+1$.

2. On considère $\mathbb{K}^n$, dont on sait qu'il s'agit d'un $\mathbb{K}$-espace vectoriel. La famille $(e_i)_{1\leqslant i\leqslant n}$, définie par

$$\forall i \in [\![1\,;n]\!] \qquad e_i = (0,\dots,0,\underset{\substack{\uparrow\\ i\text{-ème position}}}{1},0,\dots,0)$$

est clairement libre et génératrice de $\mathbb{K}^n$. Donc $\mathbb{K}^n$ est un $\mathbb{K}$-espace vectoriel de dimension n. Les $(e_i)_{1\leqslant i\leqslant n}$ sont appelés *base canonique* de $\mathbb{K}^n$.

Théorème 7.2.7
Soit E *un* $\mathbb{K}$*-espace vectoriel de dimension finie n non nulle. Soit* $\mathscr{F}$ *une famille finie de vecteurs de* E*, avec* $|\mathscr{F}| = p$.

Si elle est génératrice, on a $p \geqslant n$*, avec égalité si et seulement si c'est une base de* E.

Si elle est libre, on a $p \leqslant n$*, avec égalité si et seulement si c'est une base de* E.

Preuve : On suppose $\mathscr{F}$ génératrice et on définit

$$\mathrm{A} = \{|\mathscr{F}'| \mid \mathscr{F}' \subset \mathscr{F} \text{ et } \mathscr{F}' \text{ génératrice de E}\}$$

Évidemment, A n'est pas vide puisqu'il contient l'entier p, qui est le cardinal de $\mathscr{F}$, qui est génératrice de E par hypothèse. Toute partie non vide de $\mathbb{N}$ admet un plus petit élément ; posons $q = \mathrm{Min\,A}$. Il existe donc une sous-famille $\mathscr{F}'$ de $\mathscr{F}$, de cardinal q, génératrice de E.

Si $\mathscr{F}'$ est liée, on sait d'après le **théorème 1.3** qu'il existe $e \in \mathscr{F}'$ tel que $\mathscr{F}' \setminus \{e\}$ engendre le même sous-espace que $\mathscr{F}'$, c'est-à-dire E. Ceci implique que $q-1$ appartient à A, ce qui contredit la définition de q. Par suite, $\mathscr{F}'$ est libre et génératrice de E : c'en est une base et on a donc $q = n$, d'après le **théorème 2.4**. Or, $\mathscr{F}' \subset \mathscr{F}$ donc $n = q \leqslant p$.

Si on suppose qu'il y a égalité, $|\mathscr{F}'| = |\mathscr{F}|$; d'après le cours sur les ensembles finis, $\mathscr{F}' = \mathscr{F}$. Donc $\mathscr{F}$ est une base de E.

On passe à la deuxième partie du théorème. Supposons que $\mathscr{F}$ est libre. Si $p > n$, le **lemme 2.3** implique que $\mathscr{F}$ est liée, puisque ses éléments sont, chacun, combinaison linéaire de n vecteurs formant une base de E. D'où $p \leqslant n$.

Enfin, on suppose qu'il y a égalité. Si $\mathscr{F}$ n'est pas génératrice, il existe $x \in$ E qui ne soit pas dans $\mathrm{Vect}\,\mathscr{F}$. D'après le **théorème 1.3**, $\mathscr{F} \cup \{x\}$ est une famille libre, de cardinal $n+1$, ce qui contredit le fait que E est de dimension n. Ainsi, $\mathscr{F}$ est aussi génératrice : c'est une base de E. □

7.2.4 Sous-espaces des espaces de dimension finie

Théorème 7.2.8
Soit E *un* $\mathbb{K}$*-espace vectoriel de dimension finie. Si* F *est un sous-espace vectoriel de* E*, alors* F *est de dimension finie et dim*F $\leqslant$ *dim*E*, avec égalité si et seulement si* F = E.

Preuve : Si E ou F est réduit à $\{0\}$, le théorème est trivial. On suppose donc que E est de dimension $n > 0$ et que F est un sous-espace de E, non réduit à $\{0\}$. Soit $\mathscr{B}$ une base de E.

On considère l'ensemble $\mathscr{F}$ de toutes les familles libres d'éléments de F. D'abord, $\mathscr{F}$ n'est pas vide puisque si x est un élément non nul de F, la famille (x) est libre. Ensuite, si $\mathscr{L}$ est une famille libre d'éléments de F, son cardinal est inférieur à n : en effet, si $|\mathscr{L}| > n$, les vecteurs de $\mathscr{L}$ sont, chacun, combinaison linéaire des vecteurs de $\mathscr{B}$, puisque $\mathscr{B}$ engendre E ; d'après le **lemme 2.3**, $\mathscr{L}$ est liée, ce qui est exclu. On a donc

$$\forall \mathscr{L} \in \mathscr{F} \qquad |\mathscr{L}| \leqslant n$$

Par suite, l'ensemble $\{|\mathscr{L}| \mid \mathscr{L} \in \mathscr{F}\}$ est inclus dans $\mathbb{N}$, non vide, majoré par n. Il admet donc un plus grand élément, qu'on note p. Et par définition de p, il existe une famille libre $\mathscr{L} = (e_1, \ldots, e_p)$ d'éléments de F.

On suppose que $\mathscr{L}$ n'engendre pas F. Alors il existe $x \in$ F, qui ne soit pas combinaison linéaire de $(e_1, \ldots, e_n)$. Mais du coup, la famille $(e_1, \ldots, e_n, x)$ est libre, de cardinal $p+1$ Ce qui contredit la définition de p, comme plus grand cardinal d'une famille libre d'éléments de F : $\mathscr{L}$ engendre F.

Par suite, $\mathscr{L}$ est libre, génératrice de F : c'est une base de F, qui est donc de dimension finie égale à $|\mathscr{L}| = p \leqslant n$.

Maintenant, si on suppose qu'il y a égalité, c'est-à-dire que $p = n$. Comme $\mathscr{L}$ est libre, le **théorème 2.7** implique que c'est une base de E. Comme c'était déjà une base de F, on en déduit que F = E. □

Lemme 7.2.9
Soit E *un* $\mathbb{K}$*-espace vectoriel de dimension finie n, dont une base est* $\mathscr{B} = (e_1, \ldots, e_n)$*. Soit* $(f_1, \ldots, f_p)$ *une famille libre de vecteurs de* E*, avec* $p < n$*. Il existe* $i \in [\![1\,;n]\!]$ *tel que* $(f_1, \ldots, f_p, e_i)$ *soit libre.*

Preuve : C'est trivial. On suppose que ce n'est pas le cas. Alors chaque e_i est combinaison linéaire de $(f_1, \ldots, f_p)$, et le **lemme 2.3** implique que $\mathscr{B}$ est liée : contradiction. □

Lemme 7.2.10
Soit E *un* $\mathbb{K}$*-espace vectoriel. Soient* $\mathscr{F}$ *et* $\mathscr{G}$ *deux familles libres de vecteurs de* E*. Vect*$\mathscr{F}$ *et Vect*$\mathscr{G}$ *sont en somme directe si et seulement si* $\mathscr{F} \cup \mathscr{G}$ *est libre. Dans ce cas,* $\mathscr{F} \cup \mathscr{G}$ *est une base de Vect*$\mathscr{F} \oplus$ *Vect*$\mathscr{G}$ *et* $\mathscr{F} \cap \mathscr{G} = \emptyset$*.*

Preuve : Donnons des noms aux éléments de $\mathscr{F}$ et $\mathscr{G}$ en posant :

$$\mathscr{F} = (f_1, \ldots, f_p) \qquad \text{et} \qquad \mathscr{G} = (f_{p+1}, \ldots, f_m)$$

On note aussi

$$\mathrm{F} = \mathrm{Vect}\,\mathscr{F} \qquad \text{et} \qquad \mathrm{G} = \mathrm{Vect}\,\mathscr{G}$$

Supposons $\mathscr{F} \cup \mathscr{G}$ libre. Soit $x \in \mathrm{F} \cap \mathrm{G}$. Alors

$$\exists (\lambda_1, \ldots, \lambda_p) \in \mathbb{K}^p \qquad x = \sum_{k=1}^{p} \lambda_k f_k$$

et

$$\exists (\lambda_{p+1}, \ldots, \lambda_m) \in \mathbb{K}^{m-p} \qquad x = -\sum_{k=p+1}^{m} \lambda_k f_k$$

d'où

$$\sum_{k=1}^{p} \lambda_k f_k + \sum_{k=p+1}^{m} \lambda_k f_k = 0$$

Mais la famille $(f_1, \ldots, f_m)$ est libre donc les $(\lambda_i)_{1 \leqslant i \leqslant m}$ sont nuls. D'où $x = 0$ et $\mathrm{F} \cap \mathrm{G} = \{0\}$: ces sous-espaces sont en somme directe.

Réciproquement, si $\mathrm{F} \cap \mathrm{G} = \{0\}$, montrons que $\mathscr{F} \cup \mathscr{G}$ est libre. On se donne une combinaison linéaire nulle des éléments de $\mathscr{F} \cup \mathscr{G}$: soit $(\lambda_1, \ldots, \lambda_m) \in \mathbb{K}^m$, tel que

$$\sum_{k=1}^{m} \lambda_k f_k = 0$$

Alors $$\sum_{k=1}^{p} \lambda_k f_k = -\sum_{k=p+1}^{m} \lambda_k f_k$$

Notons x ce vecteur ; d'après l'expression du membre de gauche, x appartient à F. Et d'après celle du membre de droite, x appartient à G. Par conséquent, $x = 0$. D'où

$$\sum_{k=1}^{p} \lambda_k f_k = 0 \qquad \text{et} \qquad \sum_{k=p+1}^{m} \lambda_k f_k = 0$$

Comme $\mathscr{F}$ et $\mathscr{G}$ sont libres, on obtient

$$\forall k \in [\![1 ; p]\!] \qquad \lambda_k = 0 \qquad \text{et} \qquad \forall k \in [\![p+1 ; m]\!] \qquad \lambda_k = 0$$

Donc tous les $(\lambda_i)_{1 \leqslant i \leqslant m}$ sont nuls et $\mathscr{F} \cup \mathscr{G}$ est libre.

Montrons la dernière partie du théorème. On suppose $\mathscr{F} \cup \mathscr{G}$ libre et on note H le sous-espace qu'elle engendre. Il est clair que $F \oplus G$ contient H, puisque H est le plus petit sous-espace de E contenant $\mathscr{F}$ et $\mathscr{G}$.

Et il est également clair que H contient $F \oplus G$. En effet, H est un sous-espace contenant $\mathscr{F}$ donc contient le sous-espace engendré par $\mathscr{F}$; de même, H contient G. Donc H contient $F \cup G$ et contient donc $F \oplus G$. D'où $H = F \oplus G$. Par suite, $\mathscr{F} \cup \mathscr{G}$ est une partie libre, génératrice de $F \oplus G$: c'en est une base. □

Corollaire 7.2.11
Soit E *un* $\mathbb{K}$*-espace vectoriel de dimension finie. Soient* F *et* G *des sous-espaces. Ils sont en somme directe si et seulement si*

$$dim(F + G) = dim F + dim G$$

De plus, si F *et* G *sont supplémentaires dans* E*, on a*

$$dim G = dim E - dim F$$

Preuve : Comme F et G sont de dimensions finies, d'après le **théorème 2.8**, ils admettent chacun des bases. Notons $\mathscr{F}$ et $\mathscr{G}$ des bases de F et G. On a

$$\dim F = |\mathscr{F}| \qquad \text{et} \qquad \dim G = |\mathscr{G}|$$

donc $$\dim F + \dim G = |\mathscr{F}| + |\mathscr{G}|$$

Supposons que F et G sont en somme directe. D'après le **lemme 2.10**, $\mathscr{F} \cup \mathscr{G}$ est une base $F \oplus G$ et $\mathscr{F} \cap \mathscr{G} = \emptyset$. Donc

$$\dim(F \oplus G) = |\mathscr{F} \cup \mathscr{G}| = |\mathscr{F}| + |\mathscr{G}| = \dim F + \dim G$$

Réciproquement, si la relation

$$\dim(F + G) = \dim F + \dim G$$

est satisfaite, on a

$$\dim(F + G) = |\mathscr{F}| + |\mathscr{G}|$$

Or, $\mathscr{F} \cup \mathscr{G}$ engendre $F + G$ donc d'après le **théorème 2.7**,

$$\dim(F + G) \leqslant |\mathscr{F} \cup \mathscr{G}|$$

Donc $$|\mathscr{F}| + |\mathscr{G}| \leqslant |\mathscr{F} \cup \mathscr{G}| = |\mathscr{F}| + |\mathscr{G}| - |\mathscr{F} \cap \mathscr{G}|$$

et il s'ensuit que $|\mathscr{F} \cap \mathscr{G}| = 0$

Donc, finalement $\dim(F+G) = |\mathscr{F} \cup \mathscr{G}|$

Autrement dit, $\mathscr{F} \cup \mathscr{G}$ est une base de F+G ; elle est libre, toujours d'après le **théorème 2.7**. D'après le **lemme 2.10**, F et G sont en somme directe.

Maintenant, si F et G sont supplémentaires dans E, on a $E = F \oplus G$. Donc

$$\dim E = \dim F + \dim G$$

et $\dim G = \dim E - \dim F$ □

> Concrètement, ce théorème nous dit que si F et G sont en somme directe dans un espace de dimension finie, on obtient une base de $F \oplus G$ en réunissant une base de F et une base de G.

Théorème 7.2.12 (Théorème de l'échange)
Soit E *un* $\mathbb{K}$*-espace vectoriel de dimension finie n, dont une base est* $\mathscr{B} = (e_1, \dots, e_n)$*. Soit* F *un sous-espace strict de* E*, de dimension* $p < n$*, dont une base est* $(f_1, \dots, f_p)$*. Il existe* $i_1, \dots, i_{n-p} \in [\![1\,;n]\!]$*, tels que* $(f_1, \dots, f_p, e_{i_1}, \dots, e_{i_{n-p}})$ *soit une base de* E*.*

Preuve : On applique le lemme : il existe $i_1 \in [\![1\,;n]\!]$ tel que $(f_1, \dots, f_p, e_{i_1})$ soit libre. Si $p+1 = n$, cette famille est une base de E et on a fini. Sinon, $p+1 < n$ et d'après le lemme, il existe $i_2 \in [\![1\,;n]\!]$ tel que $(f_1, \dots, f_p, e_{i_1}, e_{i_2})$ soit libre. Si $p+2 = n$, c'est une base de E et on a fini. Sinon, $p+2 < n$ et on recommence. On pourrait montrer par récurrence qu'apès $n-p$ étapes, on obtient une famille libre $(f_1, \dots, f_p, e_{i_1}, \dots, e_{i_{n-p}})$; cette dernière étant de cardinal p, c'est une base de E. □

Corollaire 7.2.13 (Théorème de la base incomplète)
Soit E *un* $\mathbb{K}$*-espace vectoriel de dimension finie n. Soit* F *un sous-espace strict, dont on se donne une base* $(f_1, \dots, f_p)$*. Il existe des vecteurs* $f_{p+1}, \dots, f_n$ *tels que* $(f_1, \dots, f_n)$ *soit une base de* E*.*

Preuve : Conséquence immédiate du **théorème de l'échange**. □

Corollaire 7.2.14 (Existence de supplémentaires)
Soit E *un* $\mathbb{K}$*-espace vectoriel de dimension finie. Tout sous-espace de* E *admet des supplémentaires.*

Preuve : Soit F un sous-espace de E. Si F = E ou F = {0}, le théorème est trivial. Si F est strict, il est de dimension $p < n$. Donnons-nous une base $(f_1, \dots, f_p)$ de F. D'après le **théorème de la base incomplète**, on peut compléter cette famille en une base $(f_1, \dots, f_n)$ de E. Posons

$$\mathscr{F} = \{f_1, \dots, f_p\} \qquad \mathscr{G} = \{f_{p+1}, \dots, f_n\} \qquad \text{et} \qquad G = \text{Vect}\,\mathscr{G}$$

Par définition, F est le sous-espace engendré par $\mathscr{F}$. Comme $\mathscr{F} \cup \mathscr{G}$ est libre, le **lemme 2.10** assure que F et G sont en somme directe. En outre, cette famille engendre $F \oplus G$ donc $E = F \oplus G$: G est un supplémentaire de F. □

Corollaire 7.2.15 (Relation de Grassmann)
Soit E *un* $\mathbb{K}$*-espace vectoriel de dimension finie. Soient* F *et* G *deux sous-espaces. On a*

$$dim(F+G) = dim\,F + dim\,G - dim(F \cap G)$$

Preuve : On sait qu'il existe un supplémentaire S_F de $F \cap G$ dans F :

$$(F \cap G) \oplus S_F = F$$

Montrons que G et S_F sont supplémentaires dans $F + G$.

D'abord, soit $x \in G \cap S_F$. Comme $S_F \subset F$, x est dans $F \cap G$. Or, $F \cap G$ et S_F sont en somme directe, donc $x = 0$. Ce qui établit que G et S_F sont en somme directe.

Ensuite, si x est dans $F + G$, il se décompose comme somme d'un vecteur de F et d'un vecteur de G :

$$\exists x_F \in F \quad \exists x_G \in G \qquad x = x_F + x_G$$

Puisque $F = (F \cap G) \cap S_F$, x_F se décompose lui-même comme somme d'un vecteur de $F \cap G$ et d'un vecteur de S_F :

$$\exists y \in (F \cap G) \quad \exists z \in S_F \qquad x_F = y + z$$

d'où
$$x = x_F + x_G = y + z + x_G = z + \underbrace{y + x_G}_{\in G}$$

donc x est dans $S_F + G$. Ce qui établit la première inclusion

$$F + G \subset S_F \oplus G$$

Pour l'inclusion réciproque, il suffit de constater que $S_F \subset F + G$ (car $F + G$ contient F, qui contient lui-même S_F) et $G \subset F+G$. Donc F+G est un sous-espace de E, contenant $S_F \cup G$; il contient donc $S_F \oplus G$. Par suite,

$$F + G = S_F \oplus G$$

D'après le **corollaire 2.11**,

$$\dim(F + G) = \dim S_F + \dim G$$

Toujours d'après ce **corollaire 2.11** et parce que $F = (F \cap G) \oplus S_F$, on a

$$\dim F = \dim(F \cap G) + \dim S_F \qquad \text{soit} \qquad \dim S_F = \dim F - \dim(F \cap G)$$

d'où
$$\dim(F + G) = \dim F + \dim G - \dim(F \cap G) \qquad \square$$

Pour prouver ce théorème, on aurait aussi pu procéder ainsi : on note

$$p = \dim F \qquad q = \dim G \qquad m = \dim(F \cap G)$$

et on prend une base $(e_1, \ldots, e_m)$ de $F \cap G$. Il existe $(e_1, \ldots, e_m, f_{m+1}, \ldots, f_p)$ base de F et $(e_1, \ldots, e_m, g_{m+1}, \ldots, g_q)$ base de G, obtenues en complétant $(e_1, \ldots, e_m)$. Il suffit de montrer

$$\mathscr{B} = (e_1, \ldots, e_m, f_{m+1}, \ldots, f_p, g_{m+1}, \ldots, g_q)$$

est une base de F+G ; en effet, puisqu'elle a pour cardinal $p+q-m$, la relation de Grassmann s'ensuit.

Comme $\mathscr{B}$ est obtenue en réunissant une base de F et une base de G, elle engendre $F + G$. La seule technicité est la liberté de cette famille. Il faut se donner une combinaison linéaire nulle

$$\sum_{k=1}^{m} \alpha_k e_k + \sum_{k=m+1}^{p} \lambda_k f_k + \sum_{k=m+1}^{q} \mu_k g_k = 0$$

et montrer que tous les coefficients sont nuls. En posant

$$x = \sum_{k=1}^{m} \alpha_k e_k + \sum_{k=m+1}^{p} \lambda_k f_k = -\sum_{k=m+1}^{q} \mu_k g_k$$

on observe que x appartient à la fois à F et à G. Donc $x \in F \cap G$; c'est-à-dire que x est uniquement combinaison linéaire des vecteurs $(e_1, \dots, e_m)$. Ceci implique automatiquement

$$\sum_{k=m+1}^{p} \lambda_k f_k = 0 \qquad \text{et} \qquad \sum_{k=m+1}^{q} \mu_k g_k = 0$$

et par suite,

$$\sum_{k=1}^{m} \alpha_k e_k = 0$$

Comme les familles $(e_1, \dots, e_m)$, $(f_{m+1}, \dots, f_p)$ et $(g_{m+1}, \dots, g_q)$ sont libres, il s'ensuit que les $(\alpha_k)_{1 \leqslant k \leqslant m}$, les $(\lambda_k)_{m+1 \leqslant k \leqslant p}$ et les $(\mu_k)_{m+1 \leqslant k \leqslant q}$ sont nuls. $\mathscr{B}$ est donc libre.

7.2.5 Applications linéaires et espaces de dimension finie

Théorème 7.2.16
Soient E *et* F *deux* $\mathbb{K}$*-espaces vectoriels, avec* E *de dimension finie. Soit* $f \in \mathscr{L}(E)$. *Alors* $\operatorname{Im} f$ *est de dimension finie, inférieur à* $\dim E$. *Il est engendré par l'image d'une base de* E.

Preuve : Donnons-nous une base $(e_1, \dots, e_n)$ de E. On a

$$\begin{aligned} \operatorname{Im} f &= f(E) = \{f(x) \mid x \in E\} \\ &= \left\{ f\left(\sum_{k=1}^{n} x_k e_k \right) \mid (x_1, \dots, x_n) \in \mathbb{K}^n \right\} \\ &= \left\{ \sum_{k=1}^{n} x_k f(e_k) \mid (x_1, \dots, x_n) \in \mathbb{K}^n \right\} \\ \operatorname{Im} f &= \operatorname{Vect}\big(f(e_1), \dots, f(e_n)\big) \end{aligned}$$

On voit donc que $\big(f(e_1), \dots, f(e_n)\big)$ engendre $\operatorname{Im} f$, qui est donc de dimension finie. □

Théorème 7.2.17
Soit n *un entier non nul. Tout espace vectoriel de dimension* n *est isomorphe à* $\mathbb{K}^n$.

Preuve : Soit E un $\mathbb{K}$-espace vectoriel de dimension n. Soit $\mathscr{B}$ une base de E ; elle a pour cardinal n. D'après le **corollaire 1.11**, l'application

$$\begin{aligned} E &\longrightarrow \mathbb{K}^n \\ x &\longmapsto [x]_{\mathscr{B}} \end{aligned}$$

est un isomorphisme d'espaces vectoriels. □

Corollaire 7.2.18
Deux $\mathbb{K}$*-espaces vectoriels de dimensions finies sont isomorphes si, et seulement si, ils sont de même dimension.*

Preuve : Si E et F ont même dimension n, ils sont chacun isomorphes à $\mathbb{K}^n$: il existe des isomorphismes $g : E \longrightarrow \mathbb{K}^n$ et $h : F \longrightarrow \mathbb{K}^n$. Donc $h^{-1} \circ g$ est linéaire, et bijective ; c'est un isomorphisme de E sur F.

Nous pouvons même préciser un tel isomorphisme une fois qu'on s'est donné une base $\mathscr{B}$ de E et une base $\mathscr{C}$ de F. En effet, on sait d'après le **corollaire 1.11** qu'on peut prendre pour g l'unique application linéaire de E dans $\mathbb{K}^n$, qui envoie les vecteurs de $\mathscr{B}$ sur la base canonique de $\mathbb{K}^n$. Tandis que h^{-1} est celle qui envoie la base canonique de $\mathbb{K}^n$ sur les vecteurs de $\mathscr{C}$. Donc $h^{-1} \circ g$ est l'unique application linéaire de E dans F, qui envoie les vecteurs de $\mathscr{B}$ sur ceux de $\mathscr{C}$. Plus précisément, si on développe

$$\mathscr{B} = (e_1, \dots, e_n) \qquad \text{et} \qquad \mathscr{C} = (f_1, \dots, f_n)$$

alors $$\forall (x_1, \dots, x_n) \in \mathbb{K}^n \qquad h^{-1} \circ g\Big(\sum_{k=1}^{n} x_k e_k\Big) = \sum_{k=1}^{n} x_k f_k$$

Réciproquement, supposons que E et F sont isomorphes. Il existe $f \in \mathscr{L}(\mathrm{E}, \mathrm{F})$, bijective. Notons n et m les dimensions respectives de E et F. D'après le **théorème 2.16**,

$$\dim \mathrm{Im}\, f \leqslant n$$

Or, f est surjective donc $\mathrm{Im}\, f = \mathrm{F}$. D'où $m \leqslant n$.

Pour l'inégalité inverse, on utilise f^{-1}, qui est surjective de F dans E. Donc E et F ont même dimension. □

Définition 7.2.19
Soient E et F deux $\mathbb{K}$-espaces vectoriels, avec E de dimension finie. Soit $f \in \mathscr{L}(\mathrm{E}, \mathrm{F})$. On appelle *rang de* f la dimension de $\mathrm{Im}\, f$.

En vue du **théorème 2.16**, si $(e_1, \dots, e_n)$ est une base de E, le rang de f sera la dimension du sous-espace engendré par $(f(e_1), \dots, f(e_n))$.

Théorème 7.2.20 (Théorème du rang)
Soient E *et* F *deux* $\mathbb{K}$*-espaces vectoriels, avec* E *de dimension finie. Soit* $f \in \mathscr{L}(\mathrm{E}, \mathrm{F})$. *Alors*

$$dim\, Ker\, f + rg\, f = dim\, \mathrm{E}$$

Preuve : On sait que $\mathrm{Ker}\, f$ admet des supplémentaires, d'après le **corollaire 2.14**. Soit G l'un d'entre eux. D'après le **corollaire 2.11**,

$$\dim \mathrm{G} + \dim \mathrm{Ker}\, f = \dim \mathrm{E}$$

On a vu dans le cours d'introduction à l'algèbre linéaire que G est isomorphe à $\mathrm{Im}\, f$; donc ces deux sous-espaces ont même dimension. Par suite,

$$\dim \mathrm{Im}\, f + \dim \mathrm{Ker}\, f = \dim \mathrm{E}$$ □

Corollaire 7.2.21
Soient E *et* F *deux* $\mathbb{K}$*-espaces vectoriels de même dimension finie. Soit* $f \in \mathscr{L}(\mathrm{E}, \mathrm{F})$. *Les assertions suivantes sont équivalentes :*

1. *f est injective ;*
2. *f est surjective ;*

3. f est bijective.

Preuve : Conséquence immédiate du **théorème du rang** et du **théorème 2.8**. □

Corollaire 7.2.22
Soit E *un* $\mathbb{K}$*-espace vectoriel de dimension finie n. Les hyperplans de* E *sont ses sous-espaces de dimension* $n-1$.

Preuve : Soit H un sous-espace de E. Si H est un hyperplan, c'est le noyau d'une forme linéaire non nulle f. Or, Im $f = \mathbb{K}$, qui est de dimension 1 donc

$$\dim \mathrm{H} = \dim \mathrm{Ker}\, f = n - \dim \mathrm{Im}\, f = n-1$$

Réciproquement, si H est de dimension $n-1$, il admet une base $(e_1,\dots,e_{n-1})$, qu'on peut compléter en une base $(e_1,\dots,e_{n-1},e_n)$ de E. D'après le **théorème 1.13**, il existe $f \in \mathscr{L}(\mathrm{E},\mathbb{K})$, telle que

$$f(e_1) = \cdots = f(e_{n-1}) = 0 \qquad \text{et} \qquad f(e_n) = 1$$

f est une forme linéaire non nulle, dont le noyau contient H. Or, Ker f et H ont même dimension $n-1$ donc sont égaux d'après le **théorème 2.8**. H est un hyperplan. □

Chapitre 8

Matrices

8.1 Les ensembles de matrices

8.1.1 Vocabulaire

Définition 8.1.1
Soient n et p deux entiers strictement positifs. On appelle *matrice de type $n \times p$ à coefficients dans $\mathbb{K}$*, ou *matrice à n lignes et p colonnes à coefficients dans $\mathbb{K}$*, toute application de $[\![1\,;n]\!] \times [\![1\,;p]\!]$ dans $\mathbb{K}$. Leur ensemble est noté $\mathrm{M}_{n,p}(\mathbb{K})$.

Ainsi, si A est une matrice de type $n \times p$, il existe des éléments $(a_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$ de $\mathbb{K}$, tels que

$$\forall (i,j) \in [\![1\,;n]\!] \times [\![1\,;p]\!] \qquad \mathrm{A}(i,j) = a_{i,j}$$

On convient donc de noter indifféremment

$$\mathrm{A} = (a_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}} \qquad \text{ou bien} \qquad \mathrm{A} = \big(\mathrm{A}(i,j)\big)_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$$

Il est également agréable de représenter la matrice A dans un tableau

$$\mathrm{A} = \begin{bmatrix} a_{1,1} & \cdots & a_{1,j} & \cdots & a_{1,p} \\ \vdots & & \vdots & & \vdots \\ a_{i,1} & \cdots & a_{i,j} & \cdots & a_{i,p} \\ \vdots & & \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,j} & \cdots & a_{n,p} \end{bmatrix}$$

Voici maintenant le vocabulaire propre aux matrices :

- Étant donné $(i,j) \in [\![1\,;n]\!] \times [\![1\,;p]\!]$, le scalaire $a_{i,j}$ est appelé *coefficient de* A *situé à la i-ème ligne et j-ème colonne*.
- Le vecteur $(a_{i,1}, \ldots, a_{i,p}) \in \mathbb{K}^p$ est appelé *i-ème ligne de* A.
- Le vecteur $(a_{1,j}, \ldots, a_{n,j}) \in \mathbb{K}^n$ est appelé *j-ème colonne de* A.
- Si $n = 1$, on dit que $\mathrm{A} = [a_{1,1} \ \cdots \ a_{1,p}]$ est une *matrice ligne*.
- Si $p = 1$, on dit que $\mathrm{A} = \begin{bmatrix} a_{1,1} \\ \vdots \\ a_{n,1} \end{bmatrix}$ est une *matrice colonne*.
- Si $n = p$, on dit que A est une *matrice carrée*. L'ensemble des matrices carrées de type $n \times n$ est souvent abrégé en $\mathrm{M}_n(\mathbb{K})$.

- Supposons que A est carrée et que
$$\forall (i,j) \in [\![1\,;n]\!]^2 \qquad (i>j \implies a_{i,j}=0)$$
c'est-à-dire que A est de la forme
$$\mathrm{A}=\begin{bmatrix} a_{1,1} & \cdots & \cdots & a_{1,n} \\ 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{n,n} \end{bmatrix}$$
On dit alors que A est *triangulaire supérieure*.
- Supposons que A est carrée et que
$$\forall (i,j) \in [\![1\,;n]\!]^2 \qquad (i<j \implies a_{i,j}=0)$$
c'est-à-dire que A est de la forme
$$\mathrm{A}=\begin{bmatrix} a_{1,1} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 \\ a_{n,1} & \cdots & \cdots & a_{n,n} \end{bmatrix}$$
On dit alors que A est *triangulaire inférieure*.
- Supposons que A est carrée et que
$$\forall (i,j) \in [\![1\,;n]\!]^2 \qquad (i\neq j \implies a_{i,j}=0)$$
c'est-à-dire que A est de la forme
$$\mathrm{A}=\begin{bmatrix} a_{1,1} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_{n,n} \end{bmatrix}$$
On dit alors que A est *diagonale*. Si de plus tous les coefficients diagonaux sont égaux, on dit que A est *scalaire*. Enfin, remarquons qu'une matrice est diagonale si et seulement si elle est à la fois triangulaire inférieure et triangulaire supérieure.
- On appelle *matrice identité d'ordre n*, notée I_n, la matrice diagonale dans $\mathrm{M}_n(\mathbb{K})$ dont les coefficients diagonaux valent 1.
- On appelle *matrice nulle d'ordre $n\times p$*, notée $0_{n,p}$ ou 0 lorsqu'il n'y a pas d'ambiguïté, la matrice dans $\mathrm{M}_{n,p}(\mathbb{K})$ dont tous les coefficients sont nuls.

8.1.2 L'espace vectoriel $\mathrm{M}_{n,p}(\mathbb{K})$

Dans la mesure où les matrices dans $\mathrm{M}_{n,p}(\mathbb{K})$ sont des applications de $[\![1\,;n]\!]\times[\![1\,;p]\!]$ dans $\mathbb{K}$, cet ensemble est muni de la structure d'espace vectoriel usuelle sur $\mathbb{K}^{[\![1\,;n]\!]\times[\![1\,;p]\!]}$. Nous rappelons comment marchent l'addition matricielle et la multiplication par un scalaire, sous le jour des notations qui ont été définies dans le paragraphe précédent :

Définition 8.1.2
Soient $\mathrm{A}=(a_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$ et $\mathrm{B}=(b_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$ dans $\mathrm{M}_{n,p}(\mathbb{K})$. La *somme* de A et B, notée $\mathrm{A}+\mathrm{B}$ est la matrice définie par

$$A+B=(a_{i,j}+b_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}=\begin{bmatrix}a_{1,1}+b_{1,1} & \cdots & a_{1,p}+b_{1,p}\\ \vdots & & \vdots\\ a_{n,1}+b_{n,1} & \cdots & a_{n,p}+b_{n,p}\end{bmatrix}$$

En d'autres termes, on additionne deux matrices coefficient par coefficient. Évidemment, l'élément neutre pour l'addition est l'application nulle, c'est-à-dire la matrice nulle dans $M_{n,p}(\mathbb{K})$.

Définition 8.1.3
Soient $A=(a_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}\in M_{n,p}(\mathbb{K})$ et $\lambda\in\mathbb{K}$. Le produit de A par λ, noté λA, est la matrice définie par

$$\lambda A=(\lambda a_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}=\begin{bmatrix}\lambda a_{1,1} & \cdots & \lambda a_{1,p}\\ \vdots & & \vdots\\ \lambda a_{n,1} & \cdots & \lambda a_{n,p}\end{bmatrix}$$

Ainsi, on multiplie une matrice par un scalaire en multipliant chaque coefficient de cette matrice par ce scalaire. Comme expliqué en introduction, ces opérations ne sont autres que les opérations usuelles sur $\mathbb{K}^{[\![1;n]\!]\times[\![1;p]\!]}$ qui en font un $\mathbb{K}$-espace vectoriel. Donc

Théorème 8.1.4
$M_{n,p}(\mathbb{K})$, muni des opérations d'addition interne et de la multiplication externe par les éléments de $\mathbb{K}$, est un $\mathbb{K}$-espace vectoriel.

On peut aussi en trouver une base et en calculer la dimension :

Théorème 8.1.5
Les matrices $(E_{k,\ell})_{\substack{1\leqslant k\leqslant n\\1\leqslant \ell\leqslant p}}$ définies par

$$\forall (k,l)\in[\![1;n]\!]\times[\![1;p]\!]\quad\forall(i,j)\in[\![1;n]\!]\times[\![1;p]\!]\qquad (E_{k,\ell})_{i,j}=\begin{cases}1 \text{ si } (i,j)=(k,\ell)\\ 0 \text{ si } (i,j)\neq(k,\ell)\end{cases}$$

forment une base de $M_{n,p}(\mathbb{K})$, appelée base canonique. Cet espace est de dimension np.

Preuve : C'est clair une fois qu'on écrit chacune des matrices $(E_{k,\ell})_{\substack{1\leqslant k\leqslant n\\1\leqslant \ell\leqslant p}}$ sous forme de tableau.
D'après la définition de $E_{k,\ell}$, cette matrice a tous ses coefficients nuls, sauf un seul : celui se trouvant à la k-ème ligne et à la ℓ-ème colonne vaut 1. Sous forme de tableau,

$$E_{k,\ell}=\begin{bmatrix}0 & \cdots & \cdots & \cdots & 0\\ \vdots & & & & \vdots\\ \vdots & & 1 & & \vdots\\ \vdots & & & & \vdots\\ 0 & \cdots & 0 & \cdots & 0\end{bmatrix}\leftarrow k\text{-ème ligne}$$

$$\uparrow$$

ℓ-ème colonne

Compte-tenu du fait que l'addition matricielle et le produit d'une matrice par un scalaire se font coordonnée par coordonnée, on voit que si $A=(a_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$, on a simplement

$$A = \sum_{j=1}^{p} \sum_{i=1}^{n} a_{i,j} E_{i,j}$$

ce qui montre que la famille $(E_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$ engendre $M_{n,p}(\mathbb{K})$.

La liberté est également simple à prouver : on se donne des scalaires $(a_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$ tels que

$$\sum_{j=1}^{p} \sum_{i=1}^{n} a_{i,j} E_{i,j} = 0$$

Ceci implique que la matrice

$$\begin{bmatrix} a_{1,1} & \cdots & a_{1,p} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,p} \end{bmatrix}$$

est nulle. Donc tous ses coefficients sont nuls :

$$\forall (i,j) \in [\![1\,;n]\!] \times [\![1\,;p]\!] \qquad a_{i,j} = 0$$

et la famille $(E_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}}$ est libre. □

8.1.3 Le produit matriciel

On se donne trois entiers strictement positifs n, p et q. Le produit matriciel est une nouvelle opération, externe la plupart du temps, entre les espaces $M_{n,p}(\mathbb{K})$ et $M_{p,q}(\mathbb{K})$. Elle est définie comme suit

Définition 8.1.6
Soient $A = (a_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant p}} \in M_{n,p}(\mathbb{K})$ et $B = (b_{i,j})_{\substack{1\leqslant i\leqslant p\\1\leqslant j\leqslant q}} \in M_{p,q}(\mathbb{K})$. Le *produit de* A *et* B, noté AB, est la matrice de $M_{n,q}(\mathbb{K})$ définie par

$$AB = \left(\sum_{k=1}^{p} a_{i,k} b_{k,j} \right)_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant q}} = \begin{bmatrix} \sum_{k=1}^{p} a_{1,k} b_{k,1} & \cdots & \sum_{k=1}^{p} a_{1,k} b_{k,p} \\ \vdots & & \vdots \\ \sum_{k=1}^{p} a_{n,k} b_{k,1} & \cdots & \sum_{k=1}^{p} a_{n,k} b_{k,p} \end{bmatrix}$$

Prenons le temps d'analyser la formule donnant le terme général du produit AB, de manière à la dédramatiser. Soit $(i,j) \in [\![1\,;n]\!] \times [\![1\,;q]\!]$ et intéressons-nous au coefficient $(AB)_{i,j}$, se situant à la i-ème ligne et j-ème colonne de AB. Par définition, il vaut :

$$(AB)_{i,j} = \sum_{k=1}^{p} a_{i,k} b_{k,j}$$

Il fait donc intervenir les coefficients de la i-ème ligne de A et ceux de la j-ème colonne de B :

$$L_i(A) = [a_{i,1} \cdots a_{i,p}] \qquad \text{et} \qquad C_j(B) = \begin{bmatrix} b_{1,j} \\ \vdots \\ b_{p,j} \end{bmatrix}$$

On voit que $(AB)_{i,j}$ est obtenu simplement en multipliant entre eux :

- le premier coefficient de $L_i(A)$ et le premier coefficient de $C_j(B)$;
- le deuxième coefficient de $L_i(A)$ et le deuxième coefficient de $C_j(B)$;
- $\vdots$;
- le p-ème coefficient de $L_i(A)$ et le p-ème coefficient de $C_j(B)$.

Puis on additionne les nombres calculés, ce qui donne $(AB)_{i,j}$.

Exemple 8.1.7

1. Prenons les matrices

$$A = \begin{bmatrix} 1 & 1 \\ 2 & 3 \\ 1 & 2 \end{bmatrix} \qquad \text{et} \qquad B = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & -3 \end{bmatrix}$$

alors
$$AB = \begin{bmatrix} 1 & 1 \\ 2 & 3 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & -3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & -2 \\ 5 & 8 & -7 \\ 3 & 5 & -5 \end{bmatrix}$$

2. Soit $A \in M_{n,p}(\mathbb{K})$. Dans la mesure où tous les coefficients de la matrice nulle de $M_{p,q}(\mathbb{K})$ sont nuls,

$$\forall (i,j) \in [\![1\,;n]\!] \times [\![1\,;q]\!] \qquad (AB)_{i,j} = \sum_{k=1}^{p} a_{i,k} \underbrace{b_{k,j}}_{=0} = 0$$

donc
$$A \times 0_{p,q} = 0_{n,q}$$

De même,
$$0_{q,n} \times A = 0_{q,p}$$

On voit donc que le produit d'une matrice nulle, que ce soit à gauche ou à droite, par n'importe quelle matrice de dimensions compatibles, est une matrice nulle.

3. Soit $A \in M_{n,p}(\mathbb{K})$. Prenons pour B la matrice I_p, identité d'ordre p. C'est la matrice carée $p \times p$ dont tous les coefficients sont nuls sauf ceux de la diagonale, qui sont égaux à 1. La produit $A \times B$ sera donc une matrice $n \times p$ et

$$\forall (i,j) \in [\![1\,;n]\!] \times [\![1\,;p]\!] \qquad (AB)_{i,j} = \sum_{k=1}^{p} a_{i,k} \underbrace{b_{k,j}}_{=0 \text{ si } k \neq j} = a_{i,j} b_{j,j} = a_{i,j}$$

donc
$$A \times I_p = A$$

De même,
$$I_n \times A = A$$

Le produit de la matrice identité, que ce soit à droite ou à gauche, par une matrice A de dimensions compatibles, est égal à A.

La proposition suivante résume les propriétés élémentaires du produit matriciel :

Proposition 8.1.8

1. $\forall \lambda \in \mathbb{K} \quad \forall A, B \in M_{n,p}(\mathbb{K}) \quad \forall C \in M_{p,q}(\mathbb{K}) \qquad (\lambda A + B)C = \lambda AC + BC$

2. $\forall \lambda \in \mathbb{K} \quad \forall A \in M_{n,p}(\mathbb{K}) \quad \forall (B, C) \in M_{p,q}(\mathbb{K}) \qquad A(\lambda B + C) = \lambda AB + AC$

3. $\forall A \in M_{n,p}(\mathbb{K}) \quad \forall B \in M_{p,q}(\mathbb{K}) \quad \forall C \in M_{q,r}(\mathbb{K}) \qquad A(BC) = (AB)C$

Preuve : Nous ne montrerons que les propriétés 1 et 3 ; la deuxième se démontre de la même manière que la première.

Soient $\lambda \in \mathbb{K}$, A et B dans $\mathrm{M}_{n,p}(\mathbb{K})$ et C dans $\mathrm{M}_{p,q}(\mathbb{K})$. On a

$$\forall (i,j) \in [\![1\,;n]\!] \times [\![1\,;q]\!] \qquad \big((\lambda \mathrm{A}+\mathrm{B})\mathrm{C}\big)_{i,j} = \sum_{k=1}^{p} (\lambda \mathrm{A}+\mathrm{B})_{i,k} c_{k,j}$$

Les opérations d'addition et de multiplication externe dans $\mathrm{M}_{n,p}(\mathbb{K})$ se font coordonnée par coordonnée donc

$$\begin{aligned} \forall (i,j) \in [\![1\,;n]\!] \times [\![1\,;q]\!] \qquad \big((\lambda \mathrm{A}+\mathrm{B})\mathrm{C}\big)_{i,j} &= \sum_{k=1}^{p} (\lambda a_{i,k} + b_{i,k}) c_{k,j} \\ &= \lambda \sum_{k=1}^{p} a_{i,k} c_{k,j} + \sum_{k=1}^{p} b_{i,k} c_{k,j} \\ \big((\lambda \mathrm{A}+\mathrm{B})\mathrm{C}\big)_{i,j} &= \lambda (\mathrm{AC})_{i,j} + (\mathrm{BC})_{i,j} = (\lambda \mathrm{AC} + \mathrm{BC})_{i,j} \end{aligned}$$

La propriété 2 se démontre de la même manière.

Passons à la troisième propriété. Soient $\mathrm{A} \in \mathrm{M}_{n,p}(\mathbb{K})$, $\mathrm{B} \in \mathrm{M}_{p,q}(\mathbb{K})$ et $\mathrm{C} \in \mathrm{M}_{q,r}(\mathbb{K})$. Soit (i,j) dans $[\![1\,;n]\!] \times [\![1\,;r]\!]$; puisque la matrice A est de type $n \times p$ et la matrice BC est de type $p \times r$, on a

$$\big(\mathrm{A}(\mathrm{BC})\big)_{i,j} = \sum_{k=1}^{r} a_{i,k} (\mathrm{BC})_{k,j}$$

D'après la définition du produit BC, on a

$$\forall k \in [\![1\,;r]\!] \qquad (\mathrm{BC})_{k,j} = \sum_{\ell=1}^{q} b_{k,\ell} c_{\ell,j}$$

donc $$\big(\mathrm{A}(\mathrm{BC})\big)_{i,j} = \sum_{k=1}^{r} a_{i,k} \sum_{\ell=1}^{q} b_{k,\ell} c_{\ell,j} = \sum_{k=1}^{r} \sum_{\ell=1}^{q} a_{i,k} b_{k,\ell} c_{\ell,j}$$

On intervertit l'ordre des sommes :

$$\big(\mathrm{A}(\mathrm{BC})\big)_{i,j} = \sum_{\ell=1}^{q} \sum_{k=1}^{r} a_{i,k} b_{k,\ell} c_{\ell,j} = \sum_{\ell=1}^{q} \Big(\sum_{k=1}^{r} a_{i,k} b_{k,\ell} \Big) c_{\ell,j}$$

et on reconnaît, dans la somme intérieure, le coefficient (i,ℓ) de la matrice AB. Donc

$$\big(\mathrm{A}(\mathrm{BC})\big)_{i,j} = \sum_{\ell=1}^{q} (\mathrm{AB})_{i,\ell} c_{\ell,j} = \big((\mathrm{AB})\mathrm{C}\big)_{i,j}$$

donc on a bien $$\mathrm{A}(\mathrm{BC}) = (\mathrm{AB})\mathrm{C}$$ □

Remarquons qu'il n'y a aucune raison d'espérer que le produit matriciel commute. Prenons $\mathrm{A} \in \mathrm{M}_{n,p}(\mathbb{K})$ et $\mathrm{B} \in \mathrm{M}_{p,q}(\mathbb{K})$; le produit AB est parfaitement défini, c'est une matrice de type $n \times q$. En revanche, le produit BA n'aura de sens que si $q = n$. Donc il n'est même pas défini en général.

Mais, même si est dans le cas favorable où les dimensions de A et B sont suffisamment compatibles pour que les deux produits AB et BA aient un sens, il toujours faux en général que $\mathrm{AB} = \mathrm{BA}$. Par exemple, supposons que $\mathrm{A} \in \mathrm{M}_{n,p}(\mathbb{K})$ et $\mathrm{B} \in \mathrm{M}_{p,n}(\mathbb{K})$. Alors $\mathrm{AB} \in \mathrm{M}_n(\mathbb{K})$ tandis que $\mathrm{BA} \in \mathrm{M}_p(\mathbb{K})$: ces deux matrices ne sont pas de même type en général, sauf si $n = p$ et ont très peu de chances d'être égales. Par exemple :

$$A = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

$$AB = \begin{bmatrix} 3 \end{bmatrix} \qquad BA = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

Donc, le seul cas où on peut espérer que, peut être, A et B commutent est le cas où elles sont toutes deux carrées, de même taille. Mais observons l'exemple :

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \qquad B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

$$AB = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \qquad BA = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

8.1.4 La transposition

La transposition est la transformation qui échange lignes et colonnes d'une matrice :

Définition 8.1.9
On appelle *transposition* l'application

$$\begin{array}{ccc} M_{n,p}(\mathbb{K}) & \longrightarrow & M_{p,n}(\mathbb{K}) \\ \begin{bmatrix} a_{1,1} & \cdots & a_{1,p} \\ \vdots & & \vdots \\ a_{n,1} & & a_{n,p} \end{bmatrix} & \longmapsto & \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{1,p} & \cdots & a_{p,n} \end{bmatrix} \end{array}$$

Si $A \in M_{n,p}(\mathbb{K})$, son image par la transposition est appelée sa *transposée* et on la note ${}^tA$.

Exemple 8.1.10
La transposée de $\begin{bmatrix} 1 & 2 \\ 3 & -2 \\ -1 & 6 \end{bmatrix}$ est $\begin{bmatrix} 1 & 3 & -1 \\ 2 & -2 & 6 \end{bmatrix}$.

Théorème 8.1.11
Pour tous entiers non nuls n et p, la transposition est un isomorphisme de $M_{n,p}(\mathbb{K})$.

Preuve : La linéarité est évidente. Et on observe que transposer deux fois une matrice ne change pas cette dernière, donc la transposition sur $M_{n,p}(\mathbb{K})$ est inversible, d'inverse la transposition sur $M_{p,n}(\mathbb{K})$. □

Théorème 8.1.12

$$\forall A \in M_{n,p}(\mathbb{K}) \quad \forall B \in M_{p,q}(\mathbb{K}) \qquad {}^t(AB) = {}^tB\,{}^tA$$

Preuve : Les matrices ${}^tB$ et ${}^tA$ sont respectivement dans $M_{q,p}(\mathbb{K})$ et $M_{p,n}(\mathbb{K})$ donc le produit ${}^tB\,{}^tA$ est dans $M_{q,n}(\mathbb{K})$. Calculons chaque coefficient de cette matrice : si $(i, j) \in [\![1\,;q]\!] \times [\![1\,;n]\!]$, on a

$$({}^t\mathrm{B}\,{}^t\mathrm{A})_{i,j} = \sum_{k=1}^{p} ({}^t\mathrm{B})_{i,k}({}^t\mathrm{A})_{k,j}$$

Or, si $k \in [\![1\,;p]\!]$, le coefficient d'ordre (i,k) de ${}^t\mathrm{B}$ est le coefficient d'ordre (k,i) de B, puisque la transposition échange les rôles des lignes et des colonnes ; de même pour $({}^t\mathrm{A})_{k,j}$, qui vaut $a_{j,k}$. Donc

$$({}^t\mathrm{B}\,{}^t\mathrm{A})_{i,j} = \sum_{k=1}^{p} b_{k,i}a_{j,k} = (\mathrm{AB})_{j,i}$$

et on a bien $$({}^t\mathrm{B}\,{}^t\mathrm{A}) = {}^t(\mathrm{AB})$$ □

8.1.5 L'algèbre $\mathrm{M}_n(\mathbb{K})$

Nous avons pu observer que le produit matriciel, défini plus haut, est en général une opération externe : en général, si A et B sont des matrices de dimensions compatibles pour que le produit AB existe, ce dernier n'est pas dans le même ensemble matriciel que A ou B.

En fait, le seul cas où les matrices A, B et AB vivent dans le même ensemble de matrices se produit lorsque ces matrices sont toutes trois carrées, de même dimension. Cela donne un statut particulier aux ensembles de matrices carrées, puisque ce sont les seuls pour lesquels le produit soit une opération interne.

Les propriétés du produit, obtenues dans le **paragraphe 1.3**, nous donnent :

Proposition 8.1.13
Soit n un entier non nul. L'ensemble $\mathrm{M}_n(\mathbb{K})$, muni de l'addition, du produit externe et du produit matriciel, est une algèbre associative. La matrice I_n est élément neutre pour la multiplication.

Mais on observe également que la transposition sur $\mathrm{M}_n(\mathbb{K})$ est une opération interne : si A est carrée $n \times n$, la matrice ${}^t\mathrm{A}$ est obtenue en échangeant lignes et colonnes de A. Elle est donc $n \times n$ également. On a mieux : puisqu'on a vu que transposer deux fois une matrice nous redonne celle-ci,

Théorème 8.1.14
La transposition est une symétrie sur $\mathrm{M}_n(\mathbb{K})$.

D'après l'étude des symétries dans les espaces vectoriels, on sait que

$$\mathrm{M}_n(\mathbb{K}) = \mathrm{Ker}\,({}^t - \mathrm{I}) \oplus \mathrm{Ker}\,({}^t + \mathrm{I})$$

On a d'ailleurs déterminé explicitement cette décomposition :

$$\forall \mathrm{A} \in \mathrm{M}_n(\mathbb{K}) \qquad \mathrm{A} = \frac{\mathrm{A} + {}^t\mathrm{A}}{2} + \frac{\mathrm{A} - {}^t\mathrm{A}}{2}$$

Définition 8.1.15
Les éléments de $\mathrm{Ker}\,({}^t - \mathrm{I})$ sont appelés *matrices symétriques* ; ce sont les matrices égales à leur transposée, c'est-à-dire de la forme

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{1,2} & a_{2,2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{n-1,n} \\ a_{1,n} & \cdots & a_{n-1,n} & a_{n,n} \end{bmatrix}$$

Les éléments de $\mathrm{Ker}({}^t + \mathrm{I})$ sont appelés *matrices antisymétriques* ; ce sont les matrices opposées à leur transposée, c'est-à-dire de la forme

$$\begin{bmatrix} 0 & a_{1,2} & \cdots & a_{1,n} \\ -a_{1,2} & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{n-1,n} \\ -a_{1,n} & \cdots & -a_{n-1,n} & 0 \end{bmatrix}$$

8.2 Matrices et applications linéaires

Ce paragraphe va nous aider à justifier la raison pour laquelle les opérations sur les matrices (et en particulier le produit) ont été définies de cette manière.

8.2.1 Correspondances entre applications linéaires et matrices

Définition 8.2.1
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n, rapporté à une base $\mathscr{B}$. Si $x \in \mathrm{E}$, on appelle *matrice colonne associée à x relativement à la base $\mathscr{B}$* l'unique $\mathrm{X} \in \mathrm{M}_{n,1}(\mathbb{K})$ formé des composantes de x dans la base $\mathscr{B}$.

Théorème 8.2.2
Soit E *de dimension finie n, rapporté à une base $\mathscr{B}$. L'application qui à un vecteur associe sa matrice colonne relativement à $\mathscr{B}$ est un isomorphisme d'espaces vectoriels entre* E *et* $\mathrm{M}_{n,1}(\mathbb{K})$.

Preuve : Cette application est simplement

$$\begin{array}{ccc} \mathrm{E} & \longrightarrow & \mathrm{M}_{n,1}(\mathbb{K}) \\ x & \longmapsto & {}^t[x]_{\mathscr{B}} \end{array}$$

Il s'agit de la composée de deux isomorphismes d'espaces vectoriels (voir le cours sur les espaces de dimension finie). □

> **Important :** À partir de maintenant, on convient de toujours utiliser des représentations en colonnes pour les composantes des vecteurs. En d'autres termes, on change de notation : jusqu'à présent, $[x]_{\mathscr{B}}$ était la liste des composantes de x dans la base $\mathscr{B}$, présentés sous forme de ligne. Désormais, $[x]_{\mathscr{B}}$ est cette liste en colonnes.
>
> Par exemple, si $\mathrm{P} = 1 + 2\mathrm{X} + 4\mathrm{X}^2$ dans l'espace vectoriel $\mathbb{K}_2[\mathrm{X}]$ rapporté à sa base canonique $\mathscr{B}_c = (1, \mathrm{X}, \mathrm{X}^2)$, on a
>
> $$[\mathrm{P}]_{\mathscr{B}_c} = \begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix}$$

Définition 8.2.3
Soient E et F deux $\mathbb{K}$-espaces vectoriels des espaces vectoriels de dimensions finies respectives n et p. On se donne une base $\mathscr{B} = (e_1, \ldots, e_n)$ de E et une base $\mathscr{C} = (f_1, \ldots, f_p)$ de F. Soit $u \in \mathscr{L}(\mathrm{E}, \mathrm{F})$.

On appelle *matrice de u relativement aux bases $\mathscr{B}$ et $\mathscr{C}$*, notée $\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$, la matrice de type $p \times n$, dont la i-ème colonne est formée des composantes de $u(e_i)$ dans la base $\mathscr{C}$ pour tout $i \in [\![1\,;n]\!]$.

Exemple 8.2.4
On considère les $\mathbb{K}$-espaces vectoriels $\mathbb{K}^2$ et $\mathbb{K}^3$. On note ensuite $\mathscr{B} = (e_1, e_2)$ la base canonique de $\mathbb{K}^2$ et $\mathscr{C} = (f_1, f_2, f_3)$ la base canonique de $\mathbb{K}^3$; rappelons que

$$e_1 = \begin{bmatrix}1\\0\end{bmatrix} \qquad e_2 = \begin{bmatrix}0\\1\end{bmatrix} \qquad f_1 = \begin{bmatrix}1\\0\\0\end{bmatrix} \qquad \begin{bmatrix}0\\1\\0\end{bmatrix} \qquad \begin{bmatrix}0\\0\\1\end{bmatrix}$$

Et considérons l'application linéaire

$$\begin{aligned} u : \mathbb{K}^2 &\longrightarrow \mathbb{K}^3 \\ \begin{bmatrix}x\\y\end{bmatrix} &\longmapsto \begin{bmatrix}2x-3y\\x+y\\-3x+7y\end{bmatrix} \end{aligned}$$

Pour obtenir $\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$, on doit calculer $u(e_1)$ et $u(e_2)$, exprimer leurs coordonnées dans la base $\mathscr{C}$ et grouper ces coordonnées en colonne, dans cet ordre. On calcule donc

$$u(e_1) = \begin{bmatrix}2\\1\\-3\end{bmatrix} = 2f_1 + f_2 - 3f_3 \qquad u(e_2) = \begin{bmatrix}-3\\1\\7\end{bmatrix} = -3f_1 + f_2 + 7f_3$$

Donc
$$\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u) = \begin{bmatrix}2&-3\\1&1\\-3&7\end{bmatrix}$$

Pour qu'il soit bien clair que la matrice d'une application linéaire n'est déterminée qu'au choix d'une base près, prenons le même u, mais des bases différentes dans $\mathbb{K}^2$ et $\mathbb{K}^3$. Par exemple (et pour ne pas faire trop compliqué) :

$$\mathscr{B}' = (e'_1, e'_2) \qquad \text{avec} \qquad e'_1 = \begin{bmatrix}1\\1\end{bmatrix} \qquad \text{et} \qquad e'_2 = \begin{bmatrix}-1\\1\end{bmatrix}$$

et
$$\mathscr{C}' = (f'_1, f'_2, f'_3) \qquad \text{avec} \qquad f'_1 = \begin{bmatrix}0\\1\\0\end{bmatrix} \qquad f'_2 = \begin{bmatrix}1\\0\\0\end{bmatrix} \qquad f'_3 = \begin{bmatrix}0\\0\\1\end{bmatrix}$$

Alors
$$u(e'_1) = \begin{bmatrix}-1\\2\\4\end{bmatrix} = 2f'_1 - f'_2 + 4f'_3 \qquad u(e'_2) = \begin{bmatrix}-5\\0\\10\end{bmatrix} = 0 \times f'_1 - 5f'_2 - 10f'_3$$

Donc
$$\mathrm{Mat}_{\mathscr{B}',\mathscr{C}'}(u) = \begin{bmatrix}2&0\\-1&-5\\4&10\end{bmatrix}$$

Cet exemple, j'espère, illustre bien le fait que cela n'a aucun sens de parler de *la* matrice d'une application linéaire. Il est nécessaire de préciser une base pour l'espace de départ et une base pour l'espace d'arrivée.

Exemple 8.2.5
Un exemple un peu plus abstrait cette fois-ci. Prenons pour E et F le même espace $\mathbb{K}_2[X]$, des polynômes de degré inférieur à 2, munis chacun de la base canonique $\mathscr{B}_c = (1, X, X^2)$. On définit l'endomorphisme suivant :

$$\forall P \in E \qquad u(P) = P(X+1) - P'$$

et on cherche $\mathrm{Mat}_{\mathscr{B}_c,\mathscr{B}_c}(u)$. On doit calculer pour cela $u(1)$, $u(X)$ et $u(X^2)$, et les décomposer dans la base canonique. On a

$$u(1) = 1 \circ (X+1) - 1' = 1$$

$$u(X) = X + 1 - 1 = X$$

et
$$u(X^2) = (X+1)^2 - 2X = X^2 + 1$$

Par suite,
$$\mathrm{Mat}_{\mathscr{B}_c,\mathscr{B}_c}(u) = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Proposition 8.2.6
Soient E *et* F *deux* $\mathbb{K}$*-espaces vectoriels de dimensions finies n et p, rapportés à des bases respectives* $\mathscr{B}$ *et* $\mathscr{C}$*. Soient* $u \in \mathscr{L}(E,F)$*,* $x \in E$ *et* $y \in F$*. Alors* $y = u(x)$ *si et seulement si* $[y]_{\mathscr{C}} = Mat_{\mathscr{B},\mathscr{C}}(u) \times [x]_{\mathscr{B}}$*.*

Preuve : Posons $\mathscr{B} = (e_1, \dots, e_n)$, $\mathscr{C} = (f_1, \dots, f_p)$ et notons $A = (a_{i,j})_{\substack{1 \leqslant i \leqslant p \\ 1 \leqslant j \leqslant n}}$ la matrice de u par rapport aux bases $\mathscr{B}$ et $\mathscr{C}$.

Par définition, la i-ème colonne de A donne les composantes de $u(e_i)$ dans $\mathscr{C}$. Autrement dit

$$\forall i \in [\![1\,;n]\!] \qquad u(e_i) = \sum_{k=1}^{p} a_{k,i} f_k$$

Notons
$$X = [x]_{\mathscr{B}} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in \mathrm{M}_{n,1}(\mathbb{K}) \qquad Y = [y]_{\mathscr{C}} = \begin{bmatrix} y_1 \\ \vdots \\ y_p \end{bmatrix} \in \mathrm{M}_{p,1}(\mathbb{K})$$

de sorte que
$$x = \sum_{i=1}^{n} x_i e_i \qquad \text{et} \qquad y = \sum_{k=1}^{p} y_k f_k$$

Par linéarité de u, on a

$$u(x) = u\Big(\sum_{i=1}^{n} x_i e_i\Big) = \sum_{i=1}^{n} x_i u(e_i) = \sum_{i=1}^{n}\sum_{k=1}^{p} x_i a_{k,i} f_k = \sum_{k=1}^{p}\Big(\sum_{i=1}^{n} a_{k,i} x_i\Big) f_k$$

donc
$$[u(x)]_{\mathscr{C}} = \begin{bmatrix} \sum_{i=1}^{n} a_{1,i} x_i \\ \vdots \\ \sum_{i=1}^{n} a_{p,i} x_i \end{bmatrix} = AX$$

Puisqu'il y a une correspondance bijective entre un vecteur et la colonne de ses coordonnées dans une base donnée, on a

$$y = u(x) \iff Y = [u(x)]_{\mathscr{C}} = AX$$

C'est exactement ce qui était annoncé. □

Proposition 8.2.7
Soient E *et* F *deux* $\mathbb{K}$*-espaces vectoriels de dimensions finies respectives n et p, rapportés à des bases* $\mathscr{B}$ *et* $\mathscr{C}$*. L'application*

$$\begin{aligned}\mathscr{L}(\mathrm{E},\mathrm{F}) &\longrightarrow \mathrm{M}_{p,n}(\mathbb{K})\\ u &\longmapsto Mat_{\mathscr{B},\mathscr{C}}(u)\end{aligned}$$

est un isomorphisme d'espaces vectoriels.

Preuve : Donnons des noms aux vecteurs des bases respectives de E et F :

$$\mathscr{B} = (e_1,\dots,e_n) \qquad \text{et} \qquad \mathscr{C} = (f_1,\dots,f_p)$$

Soient u et v dans $\mathscr{L}(\mathrm{E},\mathrm{F})$, soit $\lambda \in \mathbb{K}$. Notons

$$\mathrm{A} = (a_{i,j})_{\substack{1\leqslant i\leqslant p\\ 1\leqslant j\leqslant n}} = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u) \qquad \text{et} \qquad \mathrm{B} = (b_{i,j})_{\substack{1\leqslant i\leqslant p\\ 1\leqslant j\leqslant n}} = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(v)$$

Par définition de la matrice d'une application linéaire, ceci signifie que

$$\forall i \in [\![1\,;n]\!] \qquad u(e_i) = \sum_{k=1}^{p} a_{k,i} f_k \qquad \text{et} \qquad v(e_i) = \sum_{k=1}^{p} b_{k,i} f_k$$

Par conséquent, $$(\lambda u + v)(e_i) = \lambda u(e_i) + v(e_i) = \sum_{k=1}^{p} (\lambda a_{k,i} + b_{k,i}) f_k$$

et $$\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(\lambda u + v) = \begin{bmatrix} \lambda a_{1,1} + b_{1,1} & \cdots & \lambda a_{1,n} + b_{1,n} \\ \vdots & & \vdots \\ \lambda a_{p,1} + b_{p,1} & \cdots & \lambda a_{p,n} + b_{p,n} \end{bmatrix} = \lambda \mathrm{A} + \mathrm{B}$$

L'application $u \longmapsto \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$ est donc bien linéaire.

Montrons maintenant qu'il sagit d'un isomorphisme. Cela pourrait être fait à la main, mais autant utiliser des résultats déjà établis. Il suffit de montrer que toute matrice dans $\mathrm{M}_{p,n}(\mathbb{K})$ représente une unique application linéaire entre E et F, relativement aux bases $\mathscr{B}$ et $\mathscr{C}$. Soit donc $\mathrm{A} = (a_{i,j})_{\substack{1\leqslant i\leqslant p\\ 1\leqslant j\leqslant n}} \in \mathrm{M}_{p,n}(\mathbb{K})$. Notons

$$\forall i \in [\![1\,;n]\!] \qquad g_i = \sum_{k=1}^{p} a_{k,i} f_k \in \mathrm{F}$$

de sorte que g_i soit représenté dans la base $\mathscr{C}$ par la i-ème colonne de A.

Nous avons vu dans le cours sur les espaces vectoriels de dimension finie qu'une application linéaire sur un espace de dimension finie est entièrement déterminée par l'image des vecteurs de base. Il existe donc un et un seul $u \in \mathscr{L}(\mathrm{E},\mathrm{F})$ tel que

$$\forall i \in [\![1\,;n]\!] \qquad u(e_i) = g_i$$

ce qui est équivalent à dire que $\mathrm{A} = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$. □

Théorème 8.2.8
Soient E *et* F *deux* $\mathbb{K}$*-espaces vectoriels de dimensions finies n et p, rapportés à des bases* $\mathscr{B}$ *et* $\mathscr{C}$*. Soient* $u \in \mathscr{L}(\mathrm{E},\mathrm{F})$ *et* $\mathrm{A} \in \mathrm{M}_{p,n}(\mathbb{K})$*. Alors*

$$\mathrm{A} = Mat_{\mathscr{B},\mathscr{C}}(u) \iff \big(\forall x \in \mathrm{E} \qquad [u(x)]_{\mathscr{C}} = \mathrm{A}[x]_{\mathscr{B}}\big)$$

Preuve : On sait déjà, d'après la **proposition 2.6** que si $A = \text{Mat}_{\mathscr{B},\mathscr{C}}(u)$, alors

$$\forall x \in E \qquad [u(x)]_{\mathscr{C}} = A[x]_{\mathscr{B}}$$

Réciproquement, supposons cette assertion vraie. Donnons des noms aux vecteurs des bases $\mathscr{B}$ et $\mathscr{C}$:

$$\mathscr{B} = (e_1, \dots, e_n) \qquad \text{et} \qquad \mathscr{C} = (f_1, \dots, f_p)$$

Alors $$\forall i \in [\![1\,;n]\!] \qquad [u(e_i)]_{\mathscr{C}} = A[e_i]_{\mathscr{B}} = \begin{bmatrix} a_{1,i} \\ \vdots \\ a_{p,i} \end{bmatrix}$$

Donc pour chaque $i \in [\![1\,;n]\!]$, la i-ème colonne de $\text{Mat}_{\mathscr{B},\mathscr{C}}(u)$ coincide avec la i-ème colonne de A. Ces matrices sont donc égales. □

Théorème 8.2.9
Soient E, F *et* G *trois* $\mathbb{K}$*-espaces vectoriels de dimensions respectives* n, p *et* r, *rapportés chacun à des bases* $\mathscr{B}$, $\mathscr{C}$ *et* $\mathscr{D}$. *Soient* $u \in \mathscr{L}(E,F)$ *et* $v \in \mathscr{L}(F,G)$. *Alors*

$$Mat_{\mathscr{B},\mathscr{D}}(v \circ u) = Mat_{\mathscr{C},\mathscr{D}}(v) \times Mat_{\mathscr{B},\mathscr{C}}(u)$$

Preuve : Remarquons déjà que $\text{Mat}_{\mathscr{B},\mathscr{C}}(u) \in M_{p,n}(\mathbb{K})$ et $\text{Mat}_{\mathscr{C},\mathscr{D}}(v) \in M_{r,p}(\mathbb{K})$: on est sûr que le produit $\text{Mat}_{\mathscr{C},\mathscr{D}}(v) \times \text{Mat}_{\mathscr{B},\mathscr{C}}(u)$ a un sens, ce qui est déjà un bon point.

Soit $x \in E$. D'après la **proposition 2.6**, on a

$$[u(x)]_{\mathscr{C}} = \text{Mat}_{\mathscr{B},\mathscr{C}} \times [x]_{\mathscr{B}}$$

et $$\big[v(u(x))\big]_{\mathscr{D}} = \text{Mat}_{\mathscr{C},\mathscr{D}}(v) \times [u(x)]_{\mathscr{C}} = \text{Mat}_{\mathscr{C},\mathscr{D}} \times (\text{Mat}_{\mathscr{B},\mathscr{C}}(u) \times [x]_{\mathscr{B}})$$

Or, le produit matriciel est « associatif » d'après la **proposition 1.8** donc

$$[v \circ u(x)]_{\mathscr{D}} = (\text{Mat}_{\mathscr{C},\mathscr{D}}(v) \times \text{Mat}_{\mathscr{B},\mathscr{C}}(u)) \times [x]_{\mathscr{B}}$$

Comme ce résultat est vrai pour tout $x \in E$, on en déduit que

$$\text{Mat}_{\mathscr{B},\mathscr{D}}(v \circ u) = \text{Mat}_{\mathscr{C},\mathscr{D}}(v) \times \text{Mat}_{\mathscr{B},\mathscr{C}}(u)$$ □

8.2.2 Matrices inversibles

Définition 8.2.10
Soient n et p deux entiers non nuls, soit $A \in M_{n,p}(\mathbb{K})$. Elle est dite

- *inversible à droite* si, et seulement si, il existe $B \in M_{p,n}(\mathbb{K})$, telle que $AB = I_n$;
- *inversible à gauche* si, et seulement si, il existe $B \in M_{p,n}(\mathbb{K})$ tel que $BA = I_p$.

> Faisons dès maintenant une observation. Si $A \in M_{n,p}(\mathbb{K})$ est une matrice inversible à droite et à gauche, on sait qu'il existe B et C dans $M_{p,n}(\mathbb{K})$ telles que
>
> $$AB = I_n \qquad \text{et} \qquad CA = I_p$$
>
> Par suite, $$C = CI_n = C(AB) = (CA)B = I_pB = B$$
>
> Donc un inverse à droite est aussi inverse à gauche de A et celui-ci est unique.

Proposition 8.2.11
Soient n et p deux entiers non nuls. Soit A *dans* $\mathrm{M}_{n,p}(\mathbb{K})$ *; on note* $u \in \mathscr{L}(\mathbb{K}^p, \mathbb{K}^n)$ *l'application linéaire canoniquement associée à* A. *Alors :*

- A *est inversible à gauche si, et seulement si, u est injective. Dans ce cas, $p \leqslant n$.*
- A *est inversible à droite si, et seulement si, u est surjective. On a alors $n \leqslant p$.*
- A *est inversible à gauche et à droite si, et seulement si, u est bijective. Dans ce cas, $n = p$.*

Preuve : On démontre chaque point dans l'ordre. Dans toute la démonstration, on notera $\mathscr{B}_n = (e_1, \dots, e_n)$ et $\mathscr{B}_p = (f_1, \dots, f_p)$ les bases canoniques de $\mathbb{K}^n$ et $\mathbb{K}^p$. On rappelle que, par définition de u, on a

$$\forall x \in \mathbb{K}^p \qquad u(x) = \mathrm{A}x$$

et que
$$\mathrm{Mat}_{\mathscr{B}_p,\mathscr{B}_n}(u) = \mathrm{A}$$

- Supposons d'abord que A est inversible à gauche. Il existe $\mathrm{B} \in \mathrm{M}_{p,n}(\mathbb{K})$ telle que $\mathrm{BA} = \mathrm{I}_p$. Donc si $x \in \mathrm{Ker}\, u$, on a

  $$0 = u(x) = \mathrm{A}x$$

  donc
  $$0 = \mathrm{B}0 = \mathrm{BA}x = x$$

  ce qui montre que u est injective.
  Réciproquement, si u est injective, on sait que $(u(f_1), \dots, u(f_p))$ est libre dans $\mathbb{K}^n$. Ceci assure en particulier que $p \leqslant n$. Pour simplifier, on pose

  $$\forall i \in [\![1\,;p]\!] \qquad u(f_i) = y_i$$

  On peut compléter la famille $(y_1, \dots, y_p)$ en une base $(y_1, \dots, y_n)$ de $\mathbb{K}^n$. On note v l'unique application linéaire de $\mathbb{K}^n$ dans $\mathbb{K}^p$, telle que

  $$\forall i \in [\![1\,;n]\!] \qquad v(y_i) = \begin{cases} f_i \text{ si } i \leqslant p \\ 0 \text{ sinon} \end{cases}$$

  Alors
  $$\forall i \in [\![1\,;p]\!] \qquad v \circ u(f_i) = v(u(f_i)) = v(y_i) = f_i$$

  Mais $v \circ u \in \mathscr{L}(\mathbb{K}^p)$ et coïncide avec l'identité sur la base $(f_1, \dots, f_p)$. Donc $v \circ u = \mathrm{id}_{\mathbb{K}^p}$. D'après le **théorème 2.9**,

  $$\mathrm{I}_p = \mathrm{Mat}_{\mathscr{B}_p}(v \circ u) = \mathrm{Mat}_{\mathscr{B}_n,\mathscr{B}_p}(v) \times \underbrace{\mathrm{Mat}_{\mathscr{B}_p,\mathscr{B}_n}(u)}_{=\mathrm{A}}$$

  Ceci montre que A est inversible à gauche.
- Supposons maintenant que A est inversible à droite. On prend $\mathrm{B} \in \mathrm{M}_{p,n}(\mathbb{K})$ telle que $\mathrm{AB} = \mathrm{I}_n$ et on montre que u est surjective. On prend $y \in \mathbb{K}^n$; on sait que

  $$y = \mathrm{I}_n y = (\mathrm{AB})\, y = \mathrm{A}(\mathrm{B}y) = u(\mathrm{B}y)$$

  donc u est surjective.
  Réciproquement, supposons u surjective. Chaque vecteur de la base $\mathscr{B}_n$ est atteint par u : il existe donc $x_1, \dots, x_n \in \mathbb{K}^p$ tels que

  $$\forall i \in [\![1\,;n]\!] \qquad u(x_i) = e_i$$

  On note v l'unique application linéaire de $\mathbb{K}^n$ dans $\mathbb{K}^p$, telle que

$$\forall i \in [\![1\,;n]\!] \qquad v(e_i) = x_i$$

et on pose $$\mathrm{B} = \mathrm{Mat}_{\mathscr{B}_n,\mathscr{B}_p}(v)$$

On a $$\forall i \in [\![1\,;n]\!] \qquad u\circ v(e_i) = u(v(e_i)) = u(x_i) = e_i$$

ce qui montre que $u\circ v = \mathrm{id}_{\mathbb{K}^n}$. D'après le **théorème 2.9**, on a $\mathrm{AB} = \mathrm{I}_n$. Donc A est inversible à droite.
Enfin, le théorème du rang montre que

$$\dim(\mathrm{Ker}\,u) + \dim(\mathrm{Im}\,u) = p$$

Comme u est surjective, $\mathrm{Im}\,u = \mathbb{K}^n$ donc on a bien $p \geqslant n$.

- C'est trivial.

Une conséquence immédiate de ce théorème et du **théorème du rang** est :

Corollaire 8.2.12
Soient n un entier strictement positif et $\mathrm{A} \in \mathrm{M}_n(\mathbb{K})$. Les assertions suivantes sont équivalentes :

1. *A est inversible ;*
2. *A est inversible à droite ;*
3. *A est inversible à gauche.*

Définition 8.2.13
Soit n un entier strictement positif. L'ensemble des matrices inversibles dans $\mathrm{M}_n(\mathbb{K})$ est appelé *groupe linéaire d'ordre n* et noté $\mathrm{GL}_n(\mathbb{K})$.

Comment trouver A^{-1} une fois qu'on a A ? Comme toujours, en utilisant le lien entre matrices et applications linéaires.

Si A a été obtenue comme matrice d'un isomorphisme $u : \mathrm{E} \longrightarrow \mathrm{F}$ relativement à des bases $\mathscr{B}$ et $\mathscr{C}$ de E et F, on peut chercher u^{-1} et ensuite écrire $\mathrm{Mat}_{\mathscr{C},\mathscr{B}}(u^{-1})$. Cette matrice est égale à A^{-1}.

Mais si A est simplement une matrice $n \times n$ donnée en tant que telle, on sait qu'elle peut être vue canoniquement comme un endomorphisme de $\mathbb{K}^n$ rapporté à sa base canonique $(e_1,\dots,e_n)$. Pour trouver A^{-1}, il « suffit » (c'est difficile et fastidieux) de trouver ses colonnes. Autrement dit, on doit déterminer $\mathrm{A}^{-1}(e_i)$ pour tout $i \in [\![1\,;n]\!]$. Ce vecteur vérifie $\mathrm{A}(\mathrm{A}^{-1}e_i) = e_i$: c'est l'unique vecteur de $\mathbb{K}^n$ qui est solution de l'équation

$$\mathrm{AX} = e_i$$

qui s'écrit

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n = 0 \\ \qquad\vdots \qquad\qquad\quad \vdots\,\vdots \\ a_{i,1}x_1 + \cdots + a_{i,n}x_n = 1 \\ \qquad\vdots \qquad\qquad\quad \vdots\,\vdots \\ a_{n,1}x_1 + \cdots + a_{n,n}x_n = 0 \end{cases}$$

Bref, trouver A^{-1}, c'est aussi facile que résoudre n systèmes de n équations à n inconnues. Youpi !

Théorème 8.2.14
Soit $\mathrm{A} \in \mathrm{M}_n(\mathbb{K})$. A est inversible si et seulement si ${}^t\mathrm{A}$ l'est. Dans ce cas, $({}^t\mathrm{A})^{-1} = {}^t(\mathrm{A}^{-1})$.

Preuve : Supposons A inversible. Alors $AA^{-1} = I_n$ donc

$$ {}^tI_n = I_n = {}^t(AA^{-1}) = {}^t(A^{-1}){}^tA $$

et on voit que ${}^tA$ est inversible à droite. Donc inversible tout court, d'après le **corollaire 2.12**. Et son inverse est la transposée de l'inverse de A.

Réciproquement, si ${}^tA$ est inversible, alors $A = {}^t({}^tA)$ l'est aussi d'après ce qui précède. Gagné.□

Théorème 8.2.15
Soient A *et* B *dans* $M_n(\mathbb{K})$. *Le produit* AB *est inversible si et seulement si* A *et* B *sont inversibles. Dans ce cas,* $(AB)^{-1} = B^{-1}A^{-1}$.

Preuve : Supposons d'abord que A et B sont inversibles. Alors

$$ (B^{-1}A^{-1})(AB) = B^{-1}(\underbrace{A^{-1}A}_{=I_n})B = B^{-1}B = I_n $$

et on voit que AB est inversible à gauche. Donc inversible tout court, d'inverse $B^{-1}A^{-1}$.

Réciproquement, supposons que AB est inversible. Alors

$$ I_n = (AB)^{-1}(AB) = \big((AB)^{-1}A\big)B $$

B est inversible à gauche et donc inversible tout court. De même,

$$ I_n = (AB)(AB)^{-1} = A\big(B(AB)^{-1}\big) $$

A est inversible à droite, donc inversible. □

8.2.3 Changements de bases

Comme on l'a vu dans le paragraphe précédent, étant donnés des espaces vectoriels E et F de dimensions finies n et p, $\mathscr{L}(E,F)$ et $M_{p,n}(\mathbb{K})$ sont isomorphes. Mais il y au moins autant de manières de construire un tel isomorphisme qu'il y a de bases de E et F. Enfonçons le clou : l'isomorphisme qu'on a construit à la **proposition 2.7** dépend du choix d'une base pour E et d'une base pour F. L'**exemple 2.4** le montre bien.

Du coup se pose la question : disons qu'on ait

- deux bases $\mathscr{B} = (e_1, \dots, e_n)$ et $\mathscr{B}' = (e'_1, \dots, e'_n)$ de E ;
- deux bases $\mathscr{C} = (f_1, \dots, f_p)$ et $\mathscr{C}' = (f'_1, \dots, f'_p)$ de F ;
- une application linéaire $u \in \mathscr{L}(E,F)$.

Notons $A = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$ et $A' = \mathrm{Mat}_{\mathscr{B}',\mathscr{C}'}(u)$. Existe-t-il une relation entre A et A' ? Évidemment, la réponse est positive.

Définition 8.2.16
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n. Soient $\mathscr{B} = (e_1, \dots, e_n)$ et $\mathscr{B}' = (e'_1, \dots, e'_n)$ deux bases de E. On appelle matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$ la matrice

$$ P_{\mathscr{B}}^{\mathscr{B}'} = \begin{bmatrix} [e'_1]_{\mathscr{B}} & \cdots & [e'_n]_{\mathscr{B}} \end{bmatrix} $$

Exemple 8.2.17
Reprenons les bases

- $\mathscr{B} = (e_1, e_2)$ et $\mathscr{B}' = (e'_1, e'_2)$ de $\mathbb{K}^2$;
- $\mathscr{C} = (f_1, f_2, f_3)$ et $\mathscr{C}' = (f'_1, f'_2, f'_3)$ de $\mathbb{K}^3$

de l'**exemple 2.4**. On a

$$e'_1 = e_1 + e_2 \qquad e'_2 = -e_1 + e_2 \qquad e_1 = \frac{e'_1 - e'_2}{2} \qquad e_2 = \frac{e'_1 + e'_2}{2}$$

donc $$\mathrm{P}_{\mathscr{B}}^{\mathscr{B}'} = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \quad \text{et} \quad \mathrm{P}_{\mathscr{B}'}^{\mathscr{B}} = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$

De même, $$f'_1 = f_2 \qquad f'_2 = f_1 \qquad f'_3 = f_3$$

donc $$\mathrm{P}_{\mathscr{C}}^{\mathscr{C}'} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{et} \quad \mathrm{P}_{\mathscr{C}'}^{\mathscr{C}} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Proposition 8.2.18
Soit E *un* $\mathbb{K}$*-espace vectoriel de dimension finie n. Soient* $\mathscr{B}$ *et* $\mathscr{B}'$ *deux bases de* E. *Les matrices de passage* $\mathrm{P}_{\mathscr{B}}^{\mathscr{B}'}$ *et* $\mathrm{P}_{\mathscr{B}'}^{\mathscr{B}}$ *sont inversibles et inverses l'une de l'autre.*

Preuve : La matrice de l'identité, relativement aux bases $\mathscr{B}'$ et $\mathscr{B}$ est obtenue en plaçant en colonnes les coordonnées, dans la base $\mathscr{B}$, des vecteurs de $\mathscr{B}'$; autrement dit, il s'agit de $\mathrm{P}_{\mathscr{B}}^{\mathscr{B}'}$:

$$\mathrm{P}_{\mathscr{B}}^{\mathscr{B}'} = \mathrm{Mat}_{\mathscr{B}',\mathscr{B}}(\mathrm{I})$$

De la même manière, $$\mathrm{P}_{\mathscr{B}'}^{\mathscr{B}} = \mathrm{Mat}_{\mathscr{B},\mathscr{B}'}(\mathrm{I})$$

En utilisant le **théorème 2.9**,

$$\mathrm{P}_{\mathscr{B}}^{\mathscr{B}'}\mathrm{P}_{\mathscr{B}'}^{\mathscr{B}} = \mathrm{Mat}_{\mathscr{B}',\mathscr{B}}(\mathrm{I})\,\mathrm{Mar}_{\mathscr{B},\mathscr{B}'}(\mathrm{I}) = \mathrm{Mat}_{\mathscr{B},\mathscr{B}}(\mathrm{I}) = \mathrm{I}_n$$ □

Exemple 8.2.19
On peut vérifier ce fait avec les matrices de passage obtenues à l'**exemple 2.18** :

$$\mathrm{P}_{\mathscr{B}}^{\mathscr{B}'}\mathrm{P}_{\mathscr{B}'}^{\mathscr{B}} = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \mathrm{I}_2$$

De même avec les matrices de passages entre les bases $\mathscr{C}$ et $\mathscr{C}'$.

Proposition 8.2.20 (Loi de l'emmerdement maximum)
Soit E *un* $\mathbb{K}$*-espace vectoriel de dimension finie n. Soient* $\mathscr{B}$ *et* $\mathscr{B}'$ *deux bases de* E. *Les coordonnées relativement à chacune de ces bases vérifient la relation :*

$$\forall x \in \mathrm{E} \qquad [x]_{\mathscr{B}} = \mathrm{P}_{\mathscr{B}}^{\mathscr{B}'}[x]_{\mathscr{B}'}$$

Preuve : C'est un simple calcul. Donnons des noms aux vecteurs de $\mathscr{B}$ et $\mathscr{B}'$:

$$\mathscr{B} = (e_1, \ldots, e_n) \qquad \mathscr{B}' = (e'_1, \ldots, e'_n)$$

ainsi qu'aux coefficients de la matrice de passage $\mathrm{P}_{\mathscr{B}}^{\mathscr{B}'}$:

$$\mathrm{P}_{\mathscr{B}}^{\mathscr{B}'} = (p_{i,j})_{1 \leqslant i,j \leqslant n}$$

Ceci signifie que $$\forall j \in [\![1\,;n]\!] \qquad e'_j = \sum_{i=1}^{n} p_{i,j}\, e_i$$

Si x est un vecteur de E, qui se décompose relativement à $\mathscr{B}$ sous la forme

$$x = \sum_{j=1}^{n} x'_j e'_j \qquad \text{c'est-à-dire} \qquad [x]_{\mathscr{B}'} = \begin{bmatrix} x'_1 \\ \vdots \\ x'_n \end{bmatrix}$$

On déroule : $$x = \sum_{j=1}^{n} x'_j e'_j = \sum_{j=1}^{n} x'_j \Big(\sum_{i=1}^{n} p_{i,j} e_i \Big) = \sum_{i=1}^{n} \Big(\sum_{j=1}^{n} p_{i,j} x'_j \Big) e_i$$

donc $$[x]_{\mathscr{B}} = \begin{bmatrix} \sum_{j=1}^{n} p_{1,j} x'_j \\ \vdots \\ \sum_{j=1}^{n} p_{n,j} x'_j \end{bmatrix} = \mathrm{P}_{\mathscr{B}}^{\mathscr{B}'} [x]_{\mathscr{B}'}$$ □

Cette proposition porte ce nom parce que sa conclusion est le contraire de ce qu'on espère : en toute logique, compte-tenu de la dénomination, la matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$ *devrait* nous donner les coordonnées relativement à $\mathscr{B}'$, en fonction des coordonnées relativement à $\mathscr{B}$. Mais en fait, pas du tout.

Remarquons aussi qu'elle aurait pu nous permettre de démontrer que $\mathrm{P}_{\mathscr{B}}^{\mathscr{B}'}$ et $\mathrm{P}_{\mathscr{B}'}^{\mathscr{B}}$ sont inverses l'une de l'autre. En effet,

$$\forall x \in \mathrm{E} \qquad [x]_{\mathscr{B}} = \mathrm{P}_{\mathscr{B}}^{\mathscr{B}'} [x]_{\mathscr{B}'} \qquad \text{et} \qquad [x]_{\mathscr{B}'} = \mathrm{P}_{\mathscr{B}'}^{\mathscr{B}} [x]_{\mathscr{B}}$$

d'où $$\forall x \in \mathrm{E} \qquad [x]_{\mathscr{B}} = \mathrm{P}_{\mathscr{B}}^{\mathscr{B}'} \mathrm{P}_{\mathscr{B}'}^{\mathscr{B}} [x]_{\mathscr{B}}$$

Le **théorème 2.8** implique que $\mathrm{I}_n = \mathrm{P}_{\mathscr{B}}^{\mathscr{B}'} \mathrm{P}_{\mathscr{B}'}^{\mathscr{B}}$.

Théorème 8.2.21
Soient E *et* F *deux* $\mathbb{K}$*-espaces vectoriels de dimensions finies n et p. Soient* $\mathscr{B}$ *et* $\mathscr{B}'$ *deux bases de* E *; soient* $\mathscr{C}$ *et* $\mathscr{C}'$ *deux bases de* F. *Soit* $u \in \mathscr{L}(\mathrm{E}, \mathrm{F})$. *Alors*

$$Mat_{\mathscr{B}',\mathscr{C}'}(u) = \mathrm{P}_{\mathscr{C}}^{\mathscr{C}'-1} Mat_{\mathscr{B},\mathscr{C}}(u) \mathrm{P}_{\mathscr{B}}^{\mathscr{B}'}$$

Preuve : Notons

$$\mathrm{A} = \mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u) \qquad \mathrm{A}' = \mathrm{Mat}_{\mathscr{C},\mathscr{C}'}(u) \qquad \mathrm{P} = \mathrm{P}_{\mathscr{B}}^{\mathscr{B}'} \qquad \mathrm{Q} = \mathrm{P}_{\mathscr{C}}^{\mathscr{C}'}$$

Si $x \in \mathrm{E}$, on pose

$$\mathrm{X} = [x]_{\mathscr{B}} \qquad \mathrm{X}' = [x]_{\mathscr{B}'} \qquad \mathrm{Y} = [u(x)]_{\mathscr{C}} \qquad \mathrm{Y}' = [u(x)]_{\mathscr{C}'}$$

D'après la **proposition 2.6**,

$$\mathrm{Y} = \mathrm{AX} \qquad \text{et} \qquad \mathrm{Y}' = \mathrm{A}'\mathrm{X}'$$

D'après la **loi de l'emmerdement maximum**,

$$\mathrm{X} = \mathrm{PX}' \qquad \text{et} \qquad \mathrm{Y} = \mathrm{QY}'$$

Alors $$\mathrm{Y}' = \mathrm{Q}^{-1}\mathrm{Y} = \mathrm{Q}^{-1}\mathrm{AX} = \mathrm{Q}^{-1}\mathrm{APX}'$$

donc $$\forall x \in \mathrm{E} \qquad [u(x)]_{\mathscr{C}'} = \mathrm{Q}^{-1}\mathrm{AP}[x]_{\mathscr{B}'}$$

Le **théorème 2.8** implique alors que $\mathrm{Mat}_{\mathscr{B}',\mathscr{C}'}(u) = \mathrm{Q}^{-1}\mathrm{AP}$, comme annoncé. □

Exemple 8.2.22
Vérifions la validité de cette formule dans le cadre de l'exemple que nous avons suivi jusqu'ici. Nous avions trouvé

$$\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)=\begin{bmatrix}2&-3\\1&1\\-3&7\end{bmatrix}\qquad \mathrm{Mat}_{\mathscr{B}',\mathscr{C}'}(u)=\begin{bmatrix}2&0\\-1&5\\4&10\end{bmatrix}$$

et les matrices de passages étaient

$$\mathrm{P}_{\mathscr{B}}^{\mathscr{B}'}=\begin{bmatrix}1&-1\\1&1\end{bmatrix}\qquad \mathrm{P}_{\mathscr{B}}^{\mathscr{B}'-1}=\frac{1}{2}\begin{bmatrix}1&1\\-1&1\end{bmatrix}\qquad \mathrm{P}_{\mathscr{C}}^{\mathscr{C}'}=\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}\qquad \mathrm{P}_{\mathscr{C}}^{\mathscr{C}'-1}=\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}$$

Calculons :
$$\begin{aligned}\mathrm{P}_{\mathscr{C}}^{\mathscr{C}'-1}\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)\mathrm{P}_{\mathscr{B}}^{\mathscr{B}'}&=\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}\begin{bmatrix}2&-3\\1&1\\-3&7\end{bmatrix}\begin{bmatrix}1&-1\\1&1\end{bmatrix}\\&=\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}\begin{bmatrix}-1&-5\\2&0\\4&10\end{bmatrix}\\&=\begin{bmatrix}2&0\\-1&5\\4&10\end{bmatrix}=\mathrm{Mat}_{\mathscr{B}',\mathscr{C}'}(u)\end{aligned}$$

8.3 Le rang

On rappelle qu'on a déjà parlé à deux reprises d'une notion appelée « rang » : le rang d'une application linéaire sur un espace de dimension finie et le rang d'une famille de vecteurs.

Si $(x_1,\dots,x_n)$ est une famille finie de vecteurs, son rang est la dimension du sous-espace qu'elle engendre. Tandis que si $f\in\mathscr{L}(\mathrm{E},\mathrm{F})$, avec E de dimension finie, alors $\mathrm{rg}\,f$ est la dimension de $\mathrm{Im}\,f$. C'est aussi le rang de l'image par f d'une base de E.

Nous définissons une troisième notion de rang, sur les matrices cette-fois.

8.3.1 Définitions et première propriétés

Définition 8.3.1
Soit $\mathrm{A}\in\mathrm{M}_{n,p}(\mathbb{K})$. Le *rang* de A, noté rgA, est la dimension du sous-espace de $\mathbb{K}^n$ engendré par les colonnes de A.

Définition 8.3.2
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n, rapporté à une base $\mathscr{B}$. Soient des vecteurs $x_1,\dots,x_p$ dans E. On appelle *matrice de la famille* $(x_1,\dots,x_p)$ *relativement à la base* $\mathscr{B}$ la matrice

$$\mathrm{M}_{\mathscr{B}}(x_1,\dots,x_p)=\begin{bmatrix}[x_1]_{\mathscr{B}}&\cdots&[x_p]_{\mathscr{B}}\end{bmatrix}$$

Théorème 8.3.3
1. *Soit* E *un* $\mathbb{K}$*-espace vectoriel de dimension finie n. Le rang d'une famille finie de vecteurs* $(x_1,\dots,x_p)$ *de* E *est égal au rang de sa matrice relativement à n'importe quelle base :*

$$\forall\mathscr{B}\text{ base de }E\qquad rg(x_1,\dots,x_p)=rg\mathrm{M}_{\mathscr{B}}(x_1,\dots,x_p)$$

2. *Soient* E *et* F *deux* $\mathbb{K}$*-espaces vectoriels de dimensions finies. Soit* $u \in \mathscr{L}(E,F)$. *Le rang de* f *est égal au rang de toute matrice pouvant représenter* f.

Preuve : Soit E de dimension finie, soit $(x_1,\dots,x_p)$ une famille finie de vecteurs de E. Donnons-nous une base $\mathscr{B}$ de E. On sait que l'application

$$\begin{aligned}\Phi : E &\longrightarrow \mathbb{K}^n \\ x &\longmapsto [x]_{\mathscr{B}}\end{aligned}$$

est un isomorphisme d'espaces vectoriels. En particulier, sa restriction au sous-espace engendré par $(x_1,\dots,x_p)$ est injective ; et on a

$$\Phi(\text{Vect}\,(x_1,\dots,x_p)) = \text{Vect}\,([x_1]_{\mathscr{B}},\dots,[x_p]_{\mathscr{B}})$$

D'après le théorème du rang,

$$\dim(\text{Vect}\,(x_1,\dots,x_p)) = \dim(\text{Vect}\,([x_1]_{\mathscr{B}},\dots,[x_p]_{\mathscr{B}}))$$

Or, le membre de gauche est le rang de $(x_1,\dots,x_p)$; tandis que celui de droite est le rang de la matrice $M_{\mathscr{B}}(x_1,\dots,x_p)$. La première proposition est donc démontrée.

Maintenant, donnons-nous E et F deux $\mathbb{K}$-espaces vectoriels de dimensions finies n et p. Soit $u \in \mathscr{L}(E,F)$, soient $\mathscr{B} = (e_1,\dots,e_n)$ et $\mathscr{C} = (f_1,\dots,f_p)$ des bases quelconques de E et F. On sait déjà que

$$\text{rg}\,u = \dim(\text{Vect}\,(u(e_1),\dots,u(e_n))) = \text{rg}\,(u(e_1),\dots,u(e_n))$$

Et d'après la première partie du théorème,

$$\text{rg}\,u = \text{rg}\,M_{\mathscr{C}}(u(e_1),\dots,u(e_n))$$

Mais la matrice $M_{\mathscr{C}}(u(e_1),\dots,u(e_n))$ n'est autre que la matrice de u relativement aux bases $\mathscr{B}$ et $\mathscr{C}$. Ce qui achève la démonstration. □

> Observons (c'est évident) qu'une matrice A carrée $n \times n$ est inversible si et seulement si elle est de rang n. En effet, si u est l'endomorphisme de $\mathbb{K}^n$ qu'elle représente canoniquement, on a $\text{rg}\,u = \text{rg}A = n$. Donc u est surjective et A est inversible.

8.3.2 Rang et transposition

Lemme 8.3.4
Soient A *et* B *deux matrices de type* $n \times p$. *On suppose qu' il existe* $P \in GL_n(\mathbb{K})$ *et* $Q \in GL_p(\mathbb{K})$, *tels que* $B = PAQ$. *Alors* A *et* B *ont le même rang.*

Preuve : Supposons que $B = PAQ$ avec $P \in GL_n(\mathbb{K})$ et $Q \in GL_p(\mathbb{K})$. Notons u l'application linéaire de $\mathbb{K}^p$ dans $\mathbb{K}^n$ dont la matrice relativement aux bases canoniques de ces espaces est A. De sorte que $\text{rg}A = \text{rg}\,u$, d'après le **théorème 3.3**.

On note aussi

- $\mathscr{B}$ la base canonique de $\mathbb{R}^p$;
- $\mathscr{B}'$ la famille libre formée par les colonnes de Q ;
- $\mathscr{C}$ la base canonique de $\mathbb{R}^n$;
- $\mathscr{C}'$ la famille libre des colonnes de P^{-1}.

Compte-tenu de ces notations, Q est la matrice de passage de $\mathscr{B}$ à $\mathscr{B}'$ et P^{-1} est la matrice de passage de $\mathscr{C}$ à $\mathscr{C}'$. D'après le **théorème 2.22**, B = PAQ est la matrice de u relativement aux bases $\mathscr{B}'$ et $\mathscr{C}'$. Donc $\operatorname{rg} u = \operatorname{rg} B$: A et B ont même rang. □

Lemme 8.3.5
Soit A *dans* $M_{n,p}(\mathbb{K})$. *Elle est de rang* r *si et seulement si il existe* $P \in GL_n(\mathbb{K})$ *et* $Q \in GL_p(\mathbb{K})$ *telles que*

$$A = P \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} Q$$

Preuve : Le **lemme 3.4** montre que si

$$A = P \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} Q$$

avec P et Q inversibles, alors

$$\operatorname{rg} A = \operatorname{rg} \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} = r$$

Réciproquement, supposons que A est de rang r. Notons $u \in \mathscr{L}(\mathbb{K}^p, \mathbb{K}^n)$ l'application canoniquement associée à A. On sait d'après le **théorème 3.3** que u est de rang r. Cela signifie que $\operatorname{Im} u$ est de dimension r et $\operatorname{Ker} u$ est de dimension $p - r$.

À l'aide du théorème de la base incomplète, on se donne

- une base $\mathscr{B} = (e_1, \dots, e_p)$ de $\mathbb{K}^p$ telle que les $p - r$ derniers vecteurs de $\mathscr{B}$ forment une base de $\operatorname{Ker} u$;
- une base $\mathscr{C} = (f_1, \dots, f_n)$ de $\mathbb{K}^n$ dont les r premiers vecteurs sont définis par

$$\forall i \in [\![1 ; r]\!] \qquad f_i = u(e_i)$$

Alors
$$\operatorname{Mat}_{\mathscr{B},\mathscr{C}}(u) = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$$

u est donc représenté, par rapport aux bases canoniques, par A ; et relativement aux bases $\mathscr{B}$ et $\mathscr{C}$ par $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$. D'après le **théorème 2.22**, il existe des matrices inversibles $P \in GL_n(\mathbb{K})$ et $Q \in GL_p(\mathbb{K})$ telles que

$$A = P \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} Q$$ □

Corollaire 8.3.6
Une matrice et sa transposée ont même rang.

Preuve : Soit $A \in M_{n,p}(\mathbb{K})$, dont on note r le rang. D'après le **lemme 3.5**, il existe des matrices inversibles $P \in GL_n(\mathbb{K})$ et $Q \in GL_p(\mathbb{K})$ telles que

$$A = P \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} Q$$

Donc
$${}^tA = {}^tQ \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} {}^tP$$

ce qui prouve que ${}^t\mathrm{A}$ est également de rang r, d'après le **lemme 3.5**. □

L'intérêt de ce résultat est clair : si on veut calculer le rang d'une matrice, on peut s'intéresser indifféremment au rang de ses lignes ou au rang de ses colonnes. Si la matrices a plus de colonnes que de lignes, ce sera peut-être plus simple d'étudier le rang de ses lignes.

8.3.3 Rang et opérations élémentaires

Les opérations élémentaires sur une famille de vecteurs ont déjà été brièvement abordées en TDs. Nous faisons une étude plus détaillée dans ce paragraphe ; au passage, nous obtiendrons un algorithme pour déterminer si une matrice est inversible et en calculer un inverse.

Définition 8.3.7
Soit A une matrice. On appelle *opération élémentaire sur les lignes de* A toute transformation du type suivant :

- échange des lignes i et j de A ; cette opération est appelé *permutation* et sera notée $\mathrm{L}_i \leftrightarrow \mathrm{L}_j$.
- multiplication de la ligne i de A par un scalaire α non nul ; cette opération est appelée *dilatation* et sera notée $\mathrm{L}_i \leftarrow \alpha\mathrm{L}_i$.
- ajout de la ligne j, dilatée par un scalaire α, à la ligne i ; cette opération est appelée *transvexion* et sera notée $\mathrm{L}_i \leftarrow \mathrm{L}_i + \alpha\mathrm{L}_j$.

Les opérations correspondantes sur les colonnes sont appelées *opérations élémentaires sur les colonnes de* A et on les note avec des C à la place des L.

Lemme 8.3.8
Soit $\mathrm{A} \in \mathrm{M}_{n,p}(\mathbb{K})$*, soit* $(i,j) \in [\![1\,;n]\!] \times [\![1\,;n]\!]$*. La matrice* $\mathrm{E}_{i,j}\mathrm{A}$ *est la matrice dont toutes les lignes sont nulles, sauf la* i*-ème, qui contient la* j*-ème ligne de* A.

Preuve : Il suffit de faire le calcul. □

Corollaire 8.3.9
Soit $\mathrm{A} \in \mathrm{M}_{n,p}(\mathbb{K})$.

1. *Faire la permutation* $\mathrm{L}_i \leftrightarrow \mathrm{L}_j$ *revient à multiplier* A *à gauche par la matrice inversible* $\mathrm{I}_n - \mathrm{E}_{i,i} - \mathrm{E}_{j,j} + \mathrm{E}_{i,j} + \mathrm{E}_{j,i}$.
2. *Faire subir à* A *la dilatation* $\mathrm{L}_i \leftarrow \alpha\mathrm{L}_i$ *revient à multiplier* A *à gauche par la matrice inversible* $\mathrm{I}_n + (\alpha - 1)\mathrm{E}_{i,i}$.
3. *Faire la transvexion* $\mathrm{L}_i \leftarrow \mathrm{L}_i + \alpha\mathrm{L}_j$ *revient à multiplier* A *à gauche par la matrice inversible* $\mathrm{I}_n + \alpha\mathrm{E}_{i,j}$.

Les opérations élémentaires sur les lignes ne changent pas le rang d'une matrice.

Preuve : Procédons par ordre.

1. L'opération de permutation $\mathrm{L}_i \leftrightarrow \mathrm{L}_j$ peut être décomposée de la manière suivante :
   - On remplace les lignes i et j de A par des zéros. Cela revient à soustraire $\mathrm{E}_{i,i}\mathrm{A} + \mathrm{E}_{j,j}\mathrm{A}$ à A.
   - On ajoute ensuite la j-ème ligne de A en i-ème position et la i-ème ligne en j-ème position. Cela revient à ajouter $\mathrm{E}_{i,j}\mathrm{A} + \mathrm{E}_{j,i}\mathrm{A}$.

La matrice obtenue vaut donc

$$A - E_{i,i}A - E_{j,j}A + E_{i,j}A + E_{j,i}A = (I_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i})A$$

$I_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$ est de rang n donc inversible (il suffit d'écrire cette matrice pour le voir).

2. L'opération de dilatation $L_i \leftarrow \alpha L_i$ peut être décomposée de la manière suivante :
   - On remplace la ligne i de A par des zéros. Cela revient à soustraire $E_{i,i}A$ à A.
   - On ajoute ensuite la i-ème ligne, multipliée par α. Cela revient à ajouter $\alpha E_{i,i}A$ à A.

   La matrice obtenue vaut donc

$$A - E_{i,i}A + \alpha E_{i,i}A = (I_n + (\alpha - 1)E_{i,i})A$$

   $I_n + (\alpha - 1)E_{i,i}$ est de rang n donc inversible.

3. L'opération de transvexion $L_i \leftarrow L_i + \alpha L_j$ fournit la matrice

$$A + \alpha E_{i,j}A = (I_n + \alpha E_{i,j})A$$

   Évidemment, $I_n + \alpha E_{i,j}$ est inversible.

On sait que multiplier une matrice par des matrices inversibles ne change pas son rang. Donc les opérations élémentaires sur les lignes ne changent pas le rang d'une matrice. □

Corollaire 8.3.10
Les opérations élémentaires sur les colonnes ne changent pas le rang d'une matrice.

Preuve : Les opérations élémentaires sur les colonnes de A sont des opérations élémentaires sur les lignes de ${}^tA$. Elles ne changent donc pas le rang de ${}^tA$; mais celui-ci est égal au rang de A donc c'est gagné. □

Donc le rang d'une matrice peut se calculer en procédant à des opérations élémentaires sur ses lignes ou ses colonnes. Le but est de simplifier la matrice suffisamment pour qu'elle ait beaucoup de zéros et que le rang se voie bien à l'œil nu. Au final, la constatation importante est que si $A \in M_{n-1,p-1}(\mathbb{K})$, alors

$$\operatorname{rg}\left[\begin{array}{c|ccc} 1 & ? & \cdots & ? \\ \hline 0 & & & \\ \vdots & & A & \\ 0 & & & \end{array}\right] = 1 + \operatorname{rg} A$$

8.3.4 La méthode du pivot

Dans ce dernier paragraphe, nous démontrons que la méthode du pivot marche. C'est à la fois un outil de calcul du rang, mais nous verrons qu'il nous fournit aussi l'inverse d'une matrice quand celle-ci est inversible.

Théorème 8.3.11
Soit A *une matrice inversible. À l'aide d'opérations élémentaires sur les lignes de* A*, il est possible de transformer* A *en* I_n.

Preuve : Faisons cela par récurrence sur la taille n de la matrice A. Si A est inversible de type 1×1, elle ne contient qu'un élément α, nécessairement non nul ; donc en divisant l'unique ligne de A par α, on obtient la matrice I_1.

Soit $n > 0$ et supposons le résultat vrai pour les matrices inversibles dans $M_n(\mathbb{K})$. Prenons une matrice $A \in GL_{n+1}(\mathbb{K})$. Si sa première colonne était remplie de zéros, son rang serait inférieur à n ce qui contredit son inversibilité. Donc A admet au moins un coefficient non nul dans sa première colonne. À l'aide d'une opération sur les lignes, on peut l'amener en position $(1,1)$, diviser la ligne par ce nombre et se retrouver avec une matrice de la forme

$$A_1 = \left[\begin{array}{c|ccc} 1 & a_{1,2} & \cdots & a_{1,n+1} \\ \hline a_{2,1} & & & \\ \vdots & & B_1 & \\ a_{n+1,1} & & & \end{array}\right]$$

On peut ensuite faire $L_i \leftarrow L_1 - a_{i,1}L_1$ pour $i \in [\![2\,;\,n+1]\!]$ pour se retrouver avec

$$A_2 = \left[\begin{array}{c|ccc} 1 & a_{1,2} & \cdots & a_{1,n+1} \\ \hline 0 & & & \\ \vdots & & B_2 & \\ 0 & & & \end{array}\right]$$

Faire ces manipulations n'a pas changé le rang de la grosse matrice donc

$$1 + \operatorname{rg} B_2 = n+1 \qquad \text{et} \qquad \operatorname{rg} B_2 = n$$

Comme B_2 est de taille $n \times n$, de rang n, elle est inversible. D'après l'hypothèse de récurrence, on peut manipuler ses lignes pour obtenir l'identité. Cela revient à manipuler de la même manière les lignes 2 à $n+1$ de A_2. Après cette opération, on a

$$A_3 = \left[\begin{array}{c|ccc} 1 & a_{1,2} & \cdots & a_{1,n+1} \\ \hline 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \end{array}\right]$$

Enfin, on fait $L_1 \leftarrow L_1 - \sum_{k=2}^{n+1} a_{1,k}L_k$ pour obtenir enfin la matrice I_{n+1}. Ce qui achève la démonstration. □

> On est enfin capable de montrer rigoureusement pourquoi la « technique », décrite en cours pour calculer l'inverse d'une matrice inversible, marche. Voici schématiquement comment elle fonctionne : on a $A \in GL_n(\mathbb{K})$; on colle A à côté de I_n pour former une « matrice augmentée » de taille $n \times 2n$. Et on manipule les lignes de cette grosse matrice de manière à transformer A en I_n :
>
> $$\left[\begin{array}{c|c} A & I_n \end{array}\right] \xrightarrow[\text{opérations sur les lignes}]{} \left[\begin{array}{c|c} I_n & B \end{array}\right]$$
>
> Par quel « miracle » est-ce que B est automatiquement égale à A^{-1} ?
>
> Rappelons-nous que les opérations sur les lignes d'une matrice sont équivalentes à la multiplication à gauche par une matrice inversible, d'après le **corollaire 3.9**. Donc faire toutes nos opérations sur les lignes de A, c'est multiplier A à gauche par une matrice inver-

sible P qui code toutes ces opérations. Dans la mesure où, à la fin du processus, on obtient l'identité, cela signifie que $PA = I_n$, donc $P = A^{-1}$.

Ensuite, répercuter ces opérations sur I_n, c'est simplement multiplier I_n par P. Donc $B = PI_n = P = A^{-1}$.

Chapitre 9

Déterminants

L'objet de ce chapitre est d'introduire la théorie des formes multilinéaires en dimension finie et d'en étudier une en particulier : le déterminant. Il s'agit d'un outil théorique très important en algèbre linéaire, en particulier parce qu'il permet de caractériser l'inversibilité d'une matrice.

Dans tout ce qui suit, $\mathbb{K}$ est corps commutatif dans lequel $2 \neq 0$.

9.1 Propriétés élémentaires du groupe symétrique

On rappelle que le groupe symétrique $\mathfrak{S}_n$ est l'ensemble des bijections de l'ensemble $[\![1\,;n]\!]$ sur lui-même. Ses éléments sont appelés *permutations de* $[\![1\,;n]\!]$. Le but de ce court paragraphe est de montrer une propriété de $\mathfrak{S}_n$, essentielle pour la suite de ce chapitre : toute permutation de $[\![1\,;n]\!]$ peut s'écrire comme produit de transpositions.

Définition 9.1.1 (Invariant d'une permutation)
Soient $n \geqslant 1$ un entier et $\sigma \in \mathfrak{S}_n$. On appelle *invariant* de σ l'ensemble

$$\mathrm{Inv}\,\sigma = \{k \in [\![1\,;n]\!] \mid \sigma(k) = k\}$$

Les éléments de $\mathrm{Inv}\,\sigma$ sont appelés les *points fixes de* σ.

Définition 9.1.2 (Transposition)
Soit $n \geqslant 2$ un entier. On appelle *transposition* tout élément de $\mathfrak{S}_n$ qui a exactement $n-2$ points fixes.

Théorème 9.1.3
Soit $n \geqslant 2$ un entier. Toute permutation de $[\![1\,;n]\!]$ peut s'écrire comme produit de transpositions.

Preuve : La démonstration se fait par récurrence. Pour tout entier n, on note $\mathscr{P}(n)$ la proposition : « toute permutation de $[\![1\,;n]\!]$ est un produit de transpositions. »

- **$\mathscr{P}(2)$ est vraie** : L'ensemble $\mathscr{S}_2$ est de cardinal 2 et contient donc deux éléments qu'il est facile de déterminer :

$$\mathrm{id} \qquad \text{et} \qquad \tau : \begin{cases} 1 \longmapsto 2 \\ 2 \longmapsto 1 \end{cases}$$

  τ est une transposition, puisque $\mathrm{Inv}\,\tau = \emptyset$ qui est de cardinal 0. Et on a $\mathrm{id} = \tau^2$.

- $\mathscr{P}(n) \Longrightarrow \mathscr{P}(n+1)$: Soit $n \geqslant 2$ tel que $\mathscr{P}(n+1)$ soit vraie. Soit σ une permutation de l'ensemble $[\![1\,;n+1]\!]$.
  Si $n+1$ est un point fixe de σ, alors σ est en fait une permutation de $[\![1\,;n]\!]$; d'après $\mathscr{P}(n)$, σ est un produit de transpositions.
  Si $n+1$ n'est pas un point fixe de σ, on a $\sigma(n+1) \neq n+1$ et on le note a. On définit alors :

$$\forall k \in [\![1\,;n+1]\!] \qquad \tau(k) = \begin{cases} k & \text{si } k \notin \{a, n+1\} \\ a & \text{si } k = n+1 \\ n+1 & \text{si } k = a \end{cases}$$

  τ est bien une transposition, puisqu'elle a $n-2$ points fixes qui sont tous les éléments de $[\![1\,;n+1]\!]$ sauf a et $n+1$. Et on a

$$\tau\sigma(n+1) = \tau(\sigma(n+1)) = \tau(a) = n+1$$

  Donc $\tau\sigma$ est une permutation de $[\![1\,;n+1]\!]$ qui fixe $n+1$; c'est donc une permutation de $[\![1\,;n]\!]$. D'après $\mathscr{P}(n)$, il existe des transpositions $\tau_1, \ldots, \tau_k$ telles que

$$\tau\sigma = \tau_1 \cdots \tau_k$$

  d'où
$$\sigma = \tau^{-1}\tau_1 \cdots \tau_k = \tau\tau_1 \cdots \tau_k$$

  puisque $\tau = \tau^{-1}$. Ce qui achève de démontrer $\mathscr{P}(n+1)$.
- **Conclusion** : $\mathscr{P}(n)$ est vraie pour tout $n \geqslant 2$. □

Une transposition de $[\![1\,;n]\!]$ est une permutation qui échange simplement deux éléments de $[\![1\,;n]\!]$. Le théorème dit donc qu'une permutation quelconque de $[\![1\,;n]\!]$ est la composition d'échanges.

Exemple 9.1.4
On prend $n = 4$. Considérons la permutation de $[\![1\,;4]\!]$ suivante :

$$\sigma(1) = 2 \qquad \sigma(2) = 3 \qquad \sigma(3) = 4 \qquad \sigma(4) = 1$$

On suit l'idée de la démonstration du théorème pour réussir à décomposer σ : on introduit la transposition τ_1 qui échange 1 et 4. et fixe 2 et 3. On a alors

$$\tau_1\sigma : \begin{cases} 1 \longmapsto \tau_1(2) = 2 \\ 2 \longmapsto \tau_1(3) = 3 \\ 3 \longmapsto \tau_1(4) = 1 \\ 4 \longmapsto \tau_1(1) = 4 \end{cases}$$

La permutation $\tau_1\sigma$ fixe 4 et permute 1, 2 et 3. On recommence en introduisant la transposition τ_2 qui échange 1 et 3, mais qui fixe 2 et 4. Alors

$$\tau_2\tau_1\sigma : \begin{cases} 1 \longmapsto \tau_2(2) = 2 \\ 2 \longmapsto \tau_2(3) = 1 \\ 3 \longmapsto \tau_2(1) = 3 \\ 4 \longmapsto \tau_2(4) = 4 \end{cases}$$

Et on remarque que $\tau_2\tau_1\sigma$ est une transposition, puisqu'elle fixe 3 et 4. On la note τ_3. On a alors

$$\tau_2\tau_1\sigma = \tau_3$$

d'où
$$\sigma = \tau_1\tau_2\tau_3$$

en composant par τ_2 puis τ_1 à gauche.

Peut-être le schéma suivant sera-t-il encore plus clair :

$$(1,2,3,4) \xrightarrow{\tau_3} (2,1,3,4) \xrightarrow{\tau_2} (2,3,1,4) \xrightarrow{\tau_1} (2,3,4,1)$$

En appliquant successivement τ_3, τ_2 et enfin τ_1, on a bien obtenu σ.

9.2 Formes multilinéaires

9.2.1 Définitions

Définition 9.2.1 (Application partiellement linéaire)
Soient $E_1,\dots,E_n,F$ des $\mathbb{K}$-espaces vectoriels. Soit f une application de $E_1 \times \cdots \times E_n$ dans F. Soit $k \in [\![1\,;n]\!]$. On dit que f est *partiellement linéaire par rapport à la k-ème variable* si, et seulement si, pour tout $(x_1,\dots,x_{k-1},x_{k+1},\dots,x_n) \in E_1 \times \cdots \times E_{k-1} \times E_{k+1} \times \cdots \times E_n$, l'application

$$\begin{aligned} E_k &\longmapsto F \\ x &\longrightarrow f(x_1,\dots,x_{k-1},x,x_{k+1},\dots,x_n) \end{aligned}$$

est linéaire.

En d'autres termes, il s'agit d'une application qui, une fois toutes les variables fixées, sauf la k-ème, devient linéaire par rapport à celle-ci.

Soit f une telle application ; soit $(x_1,\dots,x_{k-1},x_{k+1},\dots,x_n) \in E_1 \times \cdots \times E_{k-1} \times E_{k+1} \times \cdots \times E_n$. La linéarité par rapport à la k-ème variable signifie que, pour tous $x,x' \in E_k$ et tous $\lambda,\mu \in \mathbb{K}$,

$$\begin{aligned} f(x_1,\dots,x_{k-1},\lambda x+\mu x',x_{k+1},\dots,x_n) = \lambda f(x_1,\dots,x_{k-1},x,x_{k+1},\dots,x_n) \\ +\mu f(x_1,\dots,x_{k-1},x',x_{k+1},\dots,x_n) \end{aligned}$$

> Évidemment, il se pose un problème de notation si l'on souhaite parler d'une application sur $E_1 \times \cdots \times E_n$, linéaire par rapport à la première variable, ou par rapport à la n-ème.
>
> En effet, si $k=1$, alors $k-1=0$ et il n'y a pas d'espace E_0 ; si $k=1$, alors $k+1=n+1$ et il n'y a pas d'espace E_{n+1}.
>
> Il n'est pas difficile, cependant, d'imaginer ce que serait la définition rigoureuse dans le cas où $k=1$ par exemple : pour que f soit linéaire par rapport à la première variable, on demande que pour tout $(x_2,\dots,x_n) \in E_2 \times \cdots \times E_n$, l'application
>
> $$\begin{aligned} E_1 &\longrightarrow F \\ x &\longmapsto f(x,x_2,\dots,x_n) \end{aligned}$$
>
> soit linéaire. De la même manière pour une application linéaire par rapport à la dernière variable.
>
> Il est possible de donner une définition peut-être un peu plus rigoureuse, en définissant ce qu'on appelle des opérateurs de projection et d'insertion. Mais les notations deviennent vite incompréhensibles.

Exemple 9.2.2
L'application $\begin{aligned} \mathbb{R}\times\mathbb{R} &\longrightarrow \mathbb{R} \\ (x,y) &\longmapsto x^2y \end{aligned}$ est linéaire par rapport à la deuxième variable. En revanche, elle n'est pas linéaire par rapport à la première.

Définition 9.2.3 (Application multilinéaire)
Soient $E_1,\dots,E_n$ et F des $\mathbb{K}$-espaces vectoriels. Une application de $E_1\times\cdots\times E_n$ dans F est dite *n-linéaire* si, et seulement si, elle est partiellement linéaire par rapport à toutes ses variables.

Si $F=\mathbb{K}$, on dit que *f est une forme n-linéaire*.

Si $E_1,\dots,E_n$ sont un même espace vectoriel E, on dit simplement que *f est n-linéaire sur* E, bien que f soit en fait définie sur E^n.

Définition 9.2.4 (Application alternée)
Soient E et F des $\mathbb{K}$-espaces vectoriels. Soit f une application de E^n dans F. On dit que *f est alternée* si, et seulement si,

$$\forall (x_1,\dots,x_n)\in E^n \quad \forall i,j\in[\![1\,;n]\!] \qquad (i\neq j \text{ et } x_i=x_j) \implies f(x_1,\dots,x_n)=0$$

Définition 9.2.5 (Application antisymétrique)
Soient E et F des $\mathbb{K}$-espaces vectoriels. Soit f une application de E^n dans F. On dit que *f est antisymétrique* si, et seulement si,

$$\forall (x_1,\dots,x_n)\in E^n \quad \forall i<j\in[\![1\,;n]\!]$$
$$f(x_1,\dots,x_{i-1},x_j,x_{i+1},\dots,x_{j-1},x_i,x_{j+1},\dots,x_n)=-f(x_1,\dots,x_n)$$

9.2.2 Propriétés élémentaires

Proposition 9.2.6
Soient E *et* F *des* $\mathbb{K}$*-espaces vectoriels. Une application n-linéaire de* E *dans* F *est antisymétrique si, et seulement si, elle est alternée.*

Preuve : Soit f une application n-linéaire de E dans F.

Supposons d'abord que f est alternée. Soient $(x_1,\dots,x_n)\in E^n$ et $i<j\in[\![0\,;n]\!]$. On a alors

$$f(x_1,\dots,x_{i-1},x_i+x_j,x_{i+1},\dots,x_{j-1},x_i+x_j,x_{j+1},\dots,x_n)=0$$

puisque le même vecteur x_i+x_j est présent aux positions i et j. Mais en utilisant la n-linéarité de f, on trouve aussi que

$$\begin{aligned}0=f(x_1,\dots,x_{i-1},x_i,x_{i+1},\dots,x_{j-1},x_j,x_{j+1},\dots,x_n)&\\ +f(x_1,\dots,x_{i-1},x_i,x_{i+1},\dots,x_{j-1},x_i,x_{j+1},\dots,x_n)&\\ +f(x_1,\dots,x_{i-1},x_j,x_{i+1},\dots,x_{j-1},x_i,x_{j+1},\dots,x_n)&\\ +f(x_1,\dots,x_{i-1},x_j,x_{i+1},\dots,x_{j-1},x_j,x_{j+1},\dots,x_n)&\end{aligned}$$

Comme f est alternée, le deuxième et le quatrième terme de cette somme sont nuls. D'où

$$f(x_1,\dots,x_n)+f(x_1,\dots,x_{i-1},x_j,x_{i+1},\dots,x_{j-1},x_i,x_{j+1},\dots,x_n)=0$$

ce qui démontre que f est antisymétrique.

Réciproquement, supposons que f est antisymétrique. On se donne $(x_1,\dots,x_n)\in E^n$ et i,j dans $[\![1\,;n]\!]$, distincts. On suppose que $x_i=x_j$. Ceci veut dire que x_i se trouve en positions i et j dans la liste $(x_1,\dots,x_n)$. Si l'on échange ces deux termes, cette liste n'est pas changée ; mais comme f est antisymétrique,

$$f(x_1,\dots,x_n)=-f(x_1,\dots,x_n)$$

d'où

$$2f(x_1,\dots,x_n)=0$$

et comme $2 \neq 0$, il est inversible dans $\mathbb{K}$ et il vient $f(x_1,\dots,x_n) = 0$. Ce qui démontre que f est alternée. □

Proposition 9.2.7
Soient E *et* F *des* $\mathbb{K}$*-espaces vectoriels. L'ensemble* $\mathscr{L}^n(\mathrm{E},\mathrm{F})$ *des formes* n*-linéaires alternées de* E *dans* F *est un* $\mathbb{K}$*-espace vectoriel.*

Preuve : On montre que cet ensemble est un sous-espace vectoriel de $\mathrm{F}^{(\mathrm{E}^n)}$. Évidemment, l'application nulle sur E^n est n-linéaire alternée donc $\mathscr{L}^n(\mathrm{E},\mathrm{F})$ n'est pas vide. Soient f et g deux formes n-linéaires alternées ; soit $\lambda \in \mathbb{K}$. On veut montrer que $\lambda f + g$ est n-linéaire alternée.

Soient $(x_1,\dots,x_n) \in \mathrm{E}^n$ et $i, j \in [\![1\,;n]\!]$, distincts. On suppose que $x_i = x_j$. Alors

$$(\lambda f + g)(x_1,\dots,x_n) = \lambda f(x_1,\dots,x_n) + g(x_1,\dots,x_n)$$

Mais comme f et g sont alternées et $x_i = x_j$, chaque terme à droite est nul. Donc $\lambda f + g$ est alternée.

Montrons aussi la linéarité par rapport à chaque variable. Soit $k \in [\![1\,;n]\!]$; on se donne une liste $(x_1,\dots,x_{k-1},x_{k+1},\dots,x_n) \in \mathrm{E}_1 \times \cdots \times \mathrm{E}_{k-1} \times \mathrm{E}_{k+1} \times \cdots \times \mathrm{E}_n$. On sait que les applications

$$u : \begin{array}{ccc} \mathrm{E} & \longrightarrow & \mathrm{F} \\ x & \longmapsto & f(x_1,\dots,x_{k-1},x,x_{k+1},\dots,x_n) \end{array} \quad \text{et} \quad v : \begin{array}{ccc} \mathrm{E} & \longrightarrow & \mathrm{F} \\ x & \longmapsto & g(x_1,\dots,x_{k-1},x,x_{k+1},\dots,x_n) \end{array}$$

sont dans $\mathscr{L}(\mathrm{E},\mathrm{F})$; par suite, $\lambda u + v$ est dans cet espace vectoriel. Ce qui démontre que $\lambda f + g$ est linéaire par rapport à la k-ème variable. □

Lemme 9.2.8
Soit E *un* $\mathbb{K}$*-espace vectoriel de dimension* n*, rapporté à une base* $\mathscr{B} = (e_1,\dots,e_n)$*. Soit* f *une application* p*-linéaire de* E *dans un* $\mathbb{K}$*-espace vectoriel* F*. Enfin, soient* $x_1,\dots,x_p$ *dans* E*, qui se décomposent ainsi dans* $\mathscr{B}$ *:*

$$\forall i \in [\![1\,;p]\!] \qquad x_i = \sum_{j=1}^{n} a_{j,i} e_j$$

Alors
$$f(x_1,\dots,x_p) = \sum_{i_1=1}^{n} \sum_{i_2=1}^{n} \cdots \sum_{i_p=1}^{n} a_{i_1,1} a_{i_2,2} \dots a_{i_p,p} f(e_{i_1}, e_{i_2},\dots,e_{i_p})$$

Preuve : C'est une conséquence simple de la p-linéarité de f. On pourrait faire une récurrence sur p, mais cela rendrait peut-être la preuve plus complexe qu'elle ne l'est. Il suffit de « développer $f(x_1,\dots,x_p)$ p fois à la suite. On commence par utiliser la linéarité par rapport à la première variable :

$$f(x_1,\dots,x_p) = f\Big(\sum_{i_1=1}^{n} a_{i_1,1} e_{i_1}, x_2,\dots,x_p\Big) = \sum_{i_1=1}^{n} a_{i_1,1} f(e_{i_1}, x_2,\dots,x_p)$$

Puis on décompose x_2 dans $\mathscr{B}$:

$$f(x_1,\dots,x_p) = \sum_{i_1=1}^{n} a_{1,i_1} f(e_{i_1}, x_2,\dots,x_p) = \sum_{i_1=1}^{n} a_{i_1,1} f\Big(e_{i_1}, \sum_{i_2=1}^{n} a_{i_2,2} e_{i_2}, x_3,\dots,x_p\Big)$$

Pour chaque i_1 fixé entre 1 et n, on utilise la linéarité de f par rapport à la deuxième variable pour dire que

$$a_{i_1,1} f\Big(e_{i_1}, \sum_{i_2=1}^{n} a_{i_2,2} e_{i_2}, x_3,\dots,x_p\Big) = \sum_{i_2=1}^{n} a_{i_1,1} a_{i_2,2} f(e_{i_1}, e_{i_2}, x_3,\dots,x_p)$$

d'où $$f(x_1,\dots,x_p)=\sum_{i_1=1}^{n}\sum_{i_2=1}^{n}a_{i_1,1}a_{i_2,2}\,f(e_{i_1},e_{i_2},x_3,\dots,x_p)$$

Et l'on continue ainsi, jusqu'à avoir développé par rapport à la p-ème variable. □

Théorème 9.2.9
Soit E *un* $\mathbb{K}$*-espace vectoriel de dimension finie* n*. Soit* f *une forme* n*-linéaire alternée sur* E*, non nulle. Soit* $(x_1,\dots,x_n)$ *une famille de* n *vecteurs de* E*. Elle est libre si, et seulement si,* $f(x_1,\dots,x_n)\neq 0$.

Preuve : Supposons que $(x_1,\dots,x_n)$ est libre et que $f(x_1,\dots,x_n)=0$. C'est une base E car E est de dimension n. Alors, si $(y_1,\dots,y_n)$ est un n-uplet de vecteurs de E, ils peuvent se décomposer dans la base $(x_1,\dots,x_n)$:

$$\forall i\in[\![1\,;n]\!]\qquad y_i=\sum_{j=1}^{n}a_{j,i}x_j$$

d'où $$f(y_1,\dots,y_n)=\sum_{i_1,\dots,i_n=1}^{n}a_{i_1,1}\cdots a_{i_n,n}\,f(x_{i_1},\dots,x_{i_n})$$

On se considère un terme de cette somme : soit $(i_1,\dots,i_n)\in[\![1\,;n]\!]$. Il y a deux possibilités :

- Il existe $k<\ell\in[\![1\,;n]\!]$ tels que $i_k=i_\ell$: autrement dit, deux des indices sont égaux. Alors dans $(x_{i_1},\dots,x_{i_n})$, le vecteur x_{i_k} est répété en k-ème et ℓ-ème position. Comme f est alternée, $f(x_{i_1},\dots,x_{i_k})=0$.
- Les entiers $i_1,\dots,i_n$ sont distincts deux-à-deux : alors $(i_1,\dots,i_n)$ fait apparaître tous les entiers de 1 à n, dans le désordre. Mais f est alternée, donc antisymétrique d'après la **proposition 2.6** ; par suite,

  $$f(x_{i_1},\dots,x_{i_n})=\pm f(x_1,\dots,x_n)=0$$

  En effet, d'après le **théorème 1.3**, on peut transformer la famille $(x_1,\dots,x_n)$ en $(x_{i_1},\dots,x_{i_n})$ en faisant une succession d'échanges de deux vecteurs. Chaque échange change le signe se trouvant devant $f(x_1,\dots,x_n)$.

Par suite, $$f(y_1,\dots,y_n)=0$$

et ceci pour tout $(y_1,\dots,y_n)\in\mathrm{E}^n$. Par suite, f est nulle, ce qui fournit une contradiction. Donc si $(x_1,\dots,x_n)$ est libre, $f(x_1,\dots,x_n)\neq 0$.

Réciproquement, supposons que la famille $(x_1,\dots,x_n)$ est liée. Alors l'un de ces vecteurs est combinaison linéaire des autres. Supposons qu'il s'agit de x_1 : il existe des scalaires $\lambda_2,\dots,\lambda_n$ tels que

$$x_1=\sum_{k=2}^{n}\lambda_k x_k$$

Par suite, $$f(x_1,\dots,x_n)=\sum_{k=2}^{n}\lambda_k\,f(x_k,x_2,\dots,x_n)$$

en utilisant la linéarité de f par rapport à la première variable. Mais dans chaque terme de cette somme, il y a le vecteur x_k qui est répété : il se trouve en première et en k-ème position. Comme f est alternée, tous les termes sont nuls d'où

$$f(x_1,\dots,x_n)=0$$

Si c'est un autre vecteur que x_1 qui est combinaison linéaire des autres, on l'amène en première position en l'échangeant avec x_1 ; ceci change uniquement le signe de f car f est antisymétrique. Et on utilise ce qui précède pour trouver que $f(x_1,\dots,x_n)=0$. □

Corollaire 9.2.10
Soit E *un* $\mathbb{K}$*-espace vectoriel de dimension finie* n*. L'espace vectoriel* $\mathscr{L}^n(\mathrm{E},\mathbb{K})$ *est de dimension 0 ou 1.*

Preuve : On montre que deux formes n-linéaires alternées sur E forment une famille liée. Soit $(e_1,\dots,e_n)$ une base de E ; soient f et g deux formes n-linéaires alternées sur E. Alors

$$f(e_1,\dots,e_n)\in\mathbb{K} \qquad \text{et} \qquad g(e_1,\dots,e_n)\in\mathbb{K}$$

donc il existe des scalaires λ et μ tels que

$$\lambda f(e_1,\dots,e_n)+\mu g(e_1,\dots,e_n)=0$$

D'après la **proposition 2.7**, $\lambda f+\mu g$ est une forme n-linéaire alternée sur E. Mais elle s'annule sur $(e_1,\dots,e_n)$ qui est libre. Donc $\lambda f+\mu g$ est la forme n-linéaire alternée nulle. □

> Ce théorème nous dit donc qu'il y a deux possibilités : soit il n'existe pas de forme n-linéaire alternée sur E de dimension n, sauf la forme nulle ; ou bien il y en a une et alors $\mathscr{L}^n(\mathrm{E},\mathbb{K})$ est de dimension 1.
>
> L'objectif de la prochaine section est de montrer qu'il existe une forme n-linéaire alternée non nulle sur E, en la construisant.

9.3 Le déterminant

9.3.1 Mineures d'une matrice carrée

Définition 9.3.1 (Matrice mineure)
Soit $n\geqslant 2$ un entier. Soient $\mathrm{A}\in\mathscr{M}_n(\mathbb{K})$ et $(i,j)\in[\![1\,;n]\!]^2$. On appelle *matrice mineure d'ordre* (i,j) *de* A, notée $\mathrm{A}^{(i,j)}$ ou encore $m_{i,j}(\mathrm{A})$, la matrice carrée de taille $n-1$ obtenue en supprimant, dans A, la i-ème ligne et la j-ème colonne.

Autrement dit, si $\mathrm{A}=(a_{k,\ell})_{1\leqslant k,\ell\leqslant n}$, on a

$$\forall k,\ell\in[\![1\,;n-1]\!] \qquad \mathrm{A}^{(i,j)}_{k,\ell}=\begin{cases}\mathrm{A}_{k,\ell} & \text{si} \quad k\leqslant i-1 \quad \text{et} \quad \ell\leqslant j-1\\ \mathrm{A}_{k+1,\ell} & \text{si} \quad k\geqslant i \quad \text{et} \quad \ell\leqslant j-1\\ \mathrm{A}_{k,\ell+1} & \text{si} \quad k\leqslant i-1 \quad \text{et} \quad \ell\geqslant j\\ \mathrm{A}_{k+1,\ell+1} & \text{si} \quad k\geqslant i \quad \text{et} \quad \ell\geqslant j\end{cases}$$

Observons que si $j=1$, alors les deux premières conditions ci-dessus ne peuvent pas se produire. Cette remarque est utile pour la démonstration du

Lemme 9.3.2
Soient $n\in\mathbb{N}$ *et* $\mathrm{A}\in\mathrm{M}_{n+2}(\mathbb{K})$*. On se donne* $i\in[\![1\,;n+2]\!]$ *et* $j\in[\![1\,;n+1]\!]$*. Alors*

$$(\mathrm{A}^{(i,1)})^{(j,1)}=\begin{cases}(\mathrm{A}^{(j,1)})^{(i-1,1)} & si \quad j\leqslant i-1\\ (\mathrm{A}^{(j+1,1)})^{(i,1)} & si \quad j\geqslant i\end{cases}$$

Preuve : Démontrer ce résultat est un vrai bonheur. On peut s'en tirer avec un dessin commenté, mais il est très difficile de donner des explications claires dans un texte écrit. On commence par calculer le terme général de la matrice $(A^{(i,1)})^{(j,1)}$, qui est carrée de taille n, puisqu'elle est obtenue à partir de A par deux extractions de mineures successives.

Soient $k,\ell \in [\![1\,;n]\!]$. On a

$$(A^{(i,1)})^{(j,1)}_{k,\ell} = \begin{cases} A^{(i,1)}_{k,\ell+1} & \text{si} \quad k \leqslant j-1 \\ A^{(i,1)}_{k+1,\ell+1} & \text{si} \quad k \geqslant j \end{cases}$$

puis
$$(A^{(i,1)})^{(j,1)}_{k,\ell} = \begin{cases} A_{k,\ell+2} & \text{si} \quad k \leqslant i-1 \quad \text{et} \quad k \leqslant j-1 & (\mathbf{1}) \\ A_{k+1,\ell+2} & \text{si} \quad k \geqslant i \quad \text{et} \quad k \leqslant j-1 & (\mathbf{2}) \\ A_{k+1,\ell+2} & \text{si} \quad k+1 \leqslant i-1 \quad \text{et} \quad k \geqslant j & (\mathbf{3}) \\ A_{k+2,\ell+2} & \text{si} \quad k+1 \geqslant i \quad \text{et} \quad k \geqslant j & (\mathbf{4}) \end{cases}$$

- **Supposons que $j \leqslant i-1$** : On peut déjà observer que la condition (**2**) est impossible. On calcule ensuite

$$(A^{(j,1)})^{(i-1,1)}_{k,\ell} = \begin{cases} A^{(j,1)}_{k,\ell+1} & \text{si} \quad k \leqslant i-2 \\ A^{(j,1)}_{k+1,\ell+1} & \text{si} \quad k \geqslant i-1 \end{cases}$$

puis
$$(A^{(j,1)})^{(i-1,1)}_{k,\ell} = \begin{cases} A_{k,\ell+2} & \text{si} \quad k \leqslant i-2 \quad \text{et} \quad k \leqslant j-1 & (\mathbf{a}) \\ A_{k+1,\ell+2} & \text{si} \quad k \leqslant i-2 \quad \text{et} \quad k \geqslant j & (\mathbf{b}) \\ A_{k+1,\ell+2} & \text{si} \quad k \geqslant i-1 \quad \text{et} \quad k+1 \leqslant j-1 & (\mathbf{c}) \\ A_{k+2,\ell+2} & \text{si} \quad k \geqslant i-1 \quad \text{et} \quad k+1 \geqslant j & (\mathbf{d}) \end{cases}$$

On remarque que la condition (**c**) est impossible. De plus,
  - Si $k \leqslant j-1$, alors $k \leqslant i-2 \leqslant i-1$ donc les condition (**1**) et (**a**) sont équivalentes.
  - La condition (**b**) est équivalente à la condition (**3**).
  - Si $k+1 \geqslant i$ (qui est la même chose que $k \geqslant i-1$), alors $k+1 \geqslant j$ et $k \geqslant j$ puisqu'on a supposé que $j \leqslant i-1$. Donc les conditions (**4**) et (**d**) sont équivalentes.

  Ceci montre que $\forall k,\ell \in [\![1\,;n]\!] \qquad (A^{(i,1)})^{(j,1)}_{k,\ell} = (A^{(j,1)})^{(i-1,1)}_{k,\ell}$

  Les deux matrices sont égales, comme annoncé.
- **Si $j \geqslant i$** : on fait exactement le même travail et tout marche bien. □

9.3.2 Déterminant d'une matrice carrée

Définition 9.3.3 (Déterminant d'une matrice carrée)
Soit $A \in M_2(\mathbb{K})$. On appelle *déterminant de* A le scalaire

$$\det A = A_{1,1}A_{2,2} - A_{1,2}A_{2,1}$$

Soit $n \geqslant 2$ un entier. On suppose construite une application déterminant sur tous les espaces $M_2(\mathbb{K}),\ldots,M_n(\mathbb{K})$. On pose alors

$$\forall A \in M_{n+1}(\mathbb{K}) \qquad \det A = \sum_{i=1}^{n+1} (-1)^{i+1} A_{i,1} \det A^{(i,1)}$$

Ceci définit une application sur $M_{n+1}(\mathbb{K})$, qu'on appelle déterminant.

On utilise donc le théorème de récurrence forte pour définir le déterminant sur chacun des espaces $M_n(\mathbb{K})$ pour $n \geqslant 2$. D'après la définition, pour calculer le déterminant d'une matrice carrée

de taille $n+1$, on doit calculer les déterminants de toutes les matrice mineures $A^{(1,1)},\dots,A^{(n+1,1)}$ (qui sont carrées de taille n donc pour lesquelles le déterminant est déjà défini). Pour chaque $i \in [\![1 ; n+1]\!]$, le déterminant de la mineure $A^{(i,1)}$ est multiplié par $(-1)^{i+1}$ et par le coefficient $A_{i,1}$ qui se trouve justement sur la ligne et la colonne de A qu'on efface pour obtenir $A^{(i,1)}$. Et on ajoute tout. C'est ce qu'on appelle *développer le déterminant de* A *par rapport à la première colonne*.

Évidemment, les déterminants des mineures $A^{(1,1)},\dots,A^{(n+1,1)}$ se calculent eux-même par une formule similaire. Etc, jusqu'à arriver à des matrices 2×2 dont le déterminant se calcule par la formule donnée au début de la définition **3.3**.

Illustrons ceci sur le calcul d'un déterminant 3×3. Soit $A \in M_3(\mathbb{K})$. On a, par définition :

$$\begin{aligned}\det A &= \det\begin{bmatrix} A_{1,1} & A_{1,2} & A_{1,3} \\ A_{2,1} & A_{2,2} & A_{2,3} \\ A_{3,1} & A_{3,2} & A_{3,3}\end{bmatrix} \\ &= A_{1,1}\det\begin{bmatrix} A_{2,2} & A_{2,3} \\ A_{3,2} & A_{3,3}\end{bmatrix} - A_{2,1}\det\begin{bmatrix} A_{1,2} & A_{1,3} \\ A_{3,2} & A_{3,3}\end{bmatrix} + A_{3,1}\det\begin{bmatrix} A_{1,2} & A_{1,3} \\ A_{2,2} & A_{2,3}\end{bmatrix}\end{aligned}$$

$$\det A = A_{1,1}(A_{2,2}A_{3,3} - A_{3,2}A_{2,3}) - A_{2,1}(A_{1,2}A_{3,3} - A_{3,2}A_{1,3}) + A_{3,1}(A_{1,2}A_{2,3} - A_{2,2}A_{1,3})$$

On s'arrête là : la brutalité du calcul est probablement bien illustrée. Maintenant qu'on sait développer un déterminant 3×3, on peut développer un déterminant 4×4 : pour ce faire, il faut développer quatre déterminants 3×3 qui sont les déterminants des quatre mineurs associés à la première colonne de la matrice considérée. Et ainsi de suite.

Proposition 9.3.4
Soit $n \geqslant 2$. Alors det$I_n = 1$.

Preuve : Un simple calcul montre que

$$\det I_2 = 1\times 1 - 0\times 0 = 1$$

On suppose la formule vraie pour $n \geqslant 2$. Les coefficients de la première colonne de I_{n+1} sont tous nuls, sauf le premier. Donc

$$\det I_{n+1} = (-1)^{1+1}\times 1\times \det I_{n+1}^{(1,1)} = \det I_{n+1}^{(1,1)}$$

Mais la mineure $I_{n+1}^{(1,1)}$ n'est autre que I_n donc

$$\det I_{n+1} = \det I_n = 1$$

Le théorème est donc établi par récurrence. □

On en arrive au point important de cette partie :

Lemme 9.3.5
Soit $n \geqslant 2$ un entier. Soit $A \in M_n(\mathbb{K})$. *Si les deux premières colonnes de* A *sont égales, alors det*$A = 0$.

Preuve : On pose $N = n-2$ de sorte que $n = N+2$. On va devoir accomplir l'exploit de développer deux fois de suite le déterminant de A. On développe une première fois :

$$\det A = \sum_{i=1}^{N+2} (-1)^{i+1} A_{i,1} \det A^{(i,1)}$$

Une deuxième fois : $$\det A = \sum_{i=1}^{N+2} (-1)^{i+1} A_{i,1} \sum_{j=1}^{N+1} (-1)^{j+1} A_{j,1}^{(i,1)} \det\left((A^{(i,1)})^{(j,1)}\right)$$

Les calculs qui suivent sont très désagréables, et je ne parviens pas à les présenter de manière compréhensible. Ils seront faits en détail en cours et il faudra s'en contenter.

Mais en pratique, on utilise le **lemme 3.2**, on fait de grosses manipulations de sommes doubles, on utilise le fait que les deux premières colonnes de A sont égales et on trouve que $\det A = 0$. □

Lemme 9.3.6
Soit $n \geqslant 3$ un entier. Soient $A \in M_n(\mathbb{K})$ et $i < j \in [\![2\,;n]\!]$ tels que les colonnes i et j de A sont égales. Alors $\det A = 0$

Preuve : Il suffit de faire l'observation suivante : si $k \in [\![1\,;n]\!]$, la matrice mineure $A^{(k,1)}$ a également deux colonnes égales, qui sont les colonnes $i-1$ et $j-1$. Donc une récurrence immédiate prouve le résultat, après avoir remarqué qu'une matrice 2×2 dont les deux dernière colonnes sont égales a un déterminant nul :

$$\det\begin{bmatrix} a & a \\ b & b \end{bmatrix} = ab - ab = 0$$ □

9.3.3 Déterminant dans $\mathbb{K}^n$

Définition 9.3.7
Soit $n \geqslant 2$ un entier. On appelle *déterminant* sur $\mathbb{K}^n$ l'application définie par

$$\forall (x_1,\dots,x_n) \in (\mathbb{K}^n)^n \qquad \det(x_1,\dots,x_n) = \det[x_1\ \cdots\ x_n] = \det\begin{bmatrix} x_{1,1} & \cdots & x_{1,n} \\ \vdots & & \vdots \\ x_{n,1} & \cdots & x_{n,n} \end{bmatrix}$$

Théorème 9.3.8
Soit $n \geqslant 2$ un entier. Le déterminant est une forme n-linéaire alternée sur $\mathbb{K}^n$. Si l'on note $(e_1,\dots,e_n)$ la base canonique de $\mathbb{K}^n$, on a $\det(e_1,\dots,e_n) = 1$.

Preuve : On montre le théorème par récurrence, en notant $\mathscr{P}(n)$ la proposition : « Le déterminant sur $\mathbb{K}^n$ est une forme n-linéaire alternée sur $\mathbb{K}^n$. »

- Le fait que $\mathscr{P}(2)$ est vraie est un simple calcul. Soient $x_1, x_2 \in \mathbb{K}^2$; alors

  $$\det(x_1,x_2) = \det\begin{bmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{bmatrix} = x_{1,1}\,x_{2,2} - x_{1,2}\,x_{2,1}$$

  Il est clair que si $x_1 = x_2$, ces deux termes se simplifient ce qui montre que le déterminant est alterné. La linéarité partielle par rapport aux deux variables est également l'affaire d'une simple vérification.
- Soit $n \geqslant 2$ tel que $\mathscr{P}(n)$ soit vraie. On se donne $x_1,\dots,x_{n+1} \in \mathbb{K}^{n+1}$ et $i < j \in [\![1\,;n+1]\!]$, tels que $x_i = x_j$. Si $i \geqslant 2$, le **lemme 3.6** montre que $\det(x_1,\dots,x_{n+1}) = 0$ puisque la matrice $[x_1\ \cdots\ x_{n+1}]$ a ses colonnes i et j égales.
  On suppose donc maintenant que $i = 1$. Si $j = 2$, le **lemme 3.5** montre que $(x_1,\dots,x_{n+1})$ a un déterminant nul : la matrice $[x_1\ \cdots\ x_{n+1}]$ a ses deux premières colonnes égales.
  Il reste donc à régler le cas où $i = 1$ et $j > 2$. Pour chaque $k,\ell \in [\![1\,;n+1]\!]$, on note $x_k^{(\ell)}$ le vecteur x_k dont on a retiré la ℓ-ème ligne. Alors par définition,

$$\begin{aligned}\det(x_1,\dots,x_{n+1}) &= \det[x_1 \ \cdots \ x_{n+1}] = \sum_{\ell=1}^{n+1}(-1)^{\ell+1}x_{\ell,1}\det[x_2^{(\ell)} \ \cdots x_{n+1}^{(\ell)}]\\ &= \sum_{\ell=1}^{n+1}(-1)^{\ell+1}x_{\ell,1}\det(x_2^{(\ell)},\dots,x_{n+1}^{(\ell)})\end{aligned}$$

Il s'agit dans cette somme de l'application déterminant sur $\mathbb{K}^n$, dont on sait qu'elle est n-linéaire alternée d'après $\mathscr{P}(n)$. Elle est donc antisymétrique et l'on peut échanger les vecteurs $x_2^{(\ell)}$ et $x_j^{(\ell)}$, ce qui a pour effet de changer le signe du déterminant :

$$\begin{aligned}\det(x_1,\dots,x_{n+1}) &= -\sum_{\ell=1}^{n+1}(-1)^{\ell+1}x_{\ell,1}\det(x_j^{(\ell)},x_3^{(\ell)},\dots,x_{j-1}^{(\ell)},x_2^{(\ell)},x_{j+1}^{(\ell)},\dots,x_{n+1}^{(\ell)})\\ &= -\det(x_1,x_j,x_3,\dots,x_{j-1},x_2,x_{j+1},\dots,x_{n+1})\end{aligned}$$

Ce dernier déterminant est nul puisque les deux premiers vecteurs sont égaux.
Reste à montrer la n-linéarité. Commençons par la linéarité par rapport à la première variable. C'est simple, compte-tenu de la définition du déterminant : soient $x,y,x_2,\dots,x_{n+1}$ dans $\mathbb{K}^{n+1}$ et $\lambda\in\mathbb{K}$. On a

$$\begin{aligned}\det(\lambda x+y,x_2,\dots,x_{n+1}) &= \sum_{\ell=1}^{n+1}(-1)^{\ell+1}(\lambda x_{\ell,1}+y_{\ell,1})\det(x_2,\dots,x_{n+1})\\ &= \lambda\sum_{\ell=1}^{n+1}(-1)^{\ell+1}x_{\ell,1}\det(x_2,\dots,x_{n+1})+\sum_{\ell=1}^{n+1}(-1)^{\ell+1}y_{\ell,1}\det(x_2,\dots,x_{n+1})\\ \det(\lambda x+y,x_2,\dots,x_{n+1}) &= \lambda\det(x,x_2,\dots,x_{n+1})+\det(y,x_2,\dots,x_{n+1})\end{aligned}$$

Enfin, si $j\in[\![2;n]\!]$, on montre la linéarité par rapport à la j-ème variable. Soient des vecteurs $x,y,x_2,\dots,x_{j-1},x_{j+1},\dots,x_{n+1}\in\mathbb{K}^{n+1}$. On a

$$\begin{aligned}&\det(x_1,\dots,x_{j-1},\lambda x+y,x_{j+1},\dots,x_{n+1})\\ &\qquad= \sum_{\ell=1}^{n+1}(-1)^{\ell+1}x_{\ell,1}\det(x_2^{(\ell)},\dots,x_{j-1}^{(\ell)},(\lambda x+y)^{(\ell)},x_{j+1},\dots,x_{n+1})\\ &\qquad= \sum_{\ell=1}^{n+1}(-1)^{\ell+1}x_{\ell,1}\det(x_2^{(\ell)},\dots,x_{j-1}^{(\ell)},\lambda x^{(\ell)}+y^{(\ell)},x_{j+1}^{(\ell)},\dots,x_{n+1}^{(\ell)})\end{aligned}$$

Mais d'après $\mathscr{P}(n)$, le déterminant sur $\mathbb{K}^n$ est linéaire par rapport à la $j-1$-ème variable donc

$$\begin{aligned}&\det(x_1,\dots,x_{j-1},\lambda x+y,x_{j+1},\dots,x_{n+1})\\ &\qquad= \lambda\sum_{\ell=1}^{n+1}(-1)^{\ell+1}x_{\ell,1}\det(x_2^{(\ell)},\dots,x_{j-1}^{(\ell)},x^{(\ell)},x_{j+1}^{(\ell)},\dots,x_{n+1}^{(\ell)})\\ &\qquad\quad+\sum_{\ell=1}^{n+1}(-1)^{\ell+1}x_{\ell,1}\det(x_2^{(\ell)},\dots,x_{j-1}^{(\ell)},y^{(\ell)},x_{j+1}^{(\ell)},\dots,x_{n+1}^{(\ell)})\\ &\qquad\qquad= \lambda\det(x_1,\dots,x_{j-1},x,x_{j+1},\dots,x_{n+1})\\ &\qquad\qquad\quad+\det(x_1,\dots,x_{j-1},y,x_{j+1},\dots,x_{n+1})\end{aligned}$$

Ce qui achève de démontrer $\mathscr{P}(n+1)$.

- **Conclusion** : $\mathscr{P}(n)$ est vraie pour tout $n\geqslant 2$.

Enfin, si l'on note $(e_1,\dots,e_n)$ la base canonique de $\mathbb{K}^n$, on a simplement

$$\det(e_1,\dots,e_n)=\det I_n=1$$

d'après la **proposition 3.4**. □

Corollaire 9.3.9 (Propriété fondamentale)
Soit E *un* $\mathbb{K}$*-espace vectoriel de dimension finie* $n \geqslant 2$*. Une famille de* n *vecteurs de* E *est libre si, et seulement si, son déterminant relatif à n'importe quelle base n'est pas nul.*

9.3.4 Déterminant dans un espace vectoriel de dimension finie

Définition 9.3.10
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \geqslant 2$. On se donne une base $\mathscr{B}$ de E. On appelle *déterminant relativement à la base* $\mathscr{B}$ l'application

$$\begin{aligned} \det_{\mathscr{B}} : \quad & \mathrm{E}^n \longrightarrow \mathbb{K} \\ & (x_1,\dots,x_n) \longmapsto \det\big(\mathrm{Mat}_{\mathscr{B}}(x_1,\dots,x_n)\big) = \det\big([[x_1]_{\mathscr{B}},\dots,[x_n]_{\mathscr{B}}]\big) \end{aligned}$$

Théorème 9.3.11
Soit $n \geqslant 2$ *un entier. Soit* E *un* $\mathbb{K}$*-espace vectoriel de dimension rapporté à une base* $\mathscr{B}$*. L'application* $det_{\mathscr{B}}$ *est une forme* n*-linéaire alternée sur* E *et* $det_{\mathscr{B}}(\mathscr{B}) = 1$

Preuve : C'est une conséquence immédiate du **théorème 3.8**, et du fait que l'application

$$\begin{aligned} \mathrm{E} &\longrightarrow \mathbb{K}^n \\ x &\longmapsto [x]_{\mathscr{B}} \end{aligned}$$

est linéaire. □

Corollaire 9.3.12
Soit E *un* $\mathbb{K}$*-espace vectoriel de dimension finie* $n \geqslant 2$*. L'espace* $\mathscr{L}^n(\mathrm{E},\mathbb{K})$ *est de dimension 1.*

Preuve : On a montré qu'il existe des formes n-linéaires alternées sur E : le déterminant par rapport à n'importe quelle base fait l'affaire. D'après le **corollaire 2.10**, $\mathscr{L}^n(\mathrm{E},\mathbb{K})$ est de dimension 1. □

Corollaire 9.3.13
Soit E *un* $\mathbb{K}$*-espace vectoriel de dimension finie* $n \geqslant 2$*. Soient* $\mathscr{B}$ *est* $\mathscr{C}$ *deux bases de* E*. Alors*

$$\forall x_1,\dots,x_n \in \mathrm{E} \qquad det_{\mathscr{B}}(x_1,\dots,x_n) = det_{\mathscr{B}}(\mathscr{C})\, det_{\mathscr{C}}(x_1,\dots,x_n)$$

et

$$det_{\mathscr{B}}(\mathscr{C})\, det_{\mathscr{C}}(\mathscr{B}) = 1$$

Preuve : Les applications $\det_{\mathscr{B}}$ et $\det_{\mathscr{C}}$ sont proportionnelles puisque $\mathscr{L}^n(\mathrm{E},\mathbb{K})$ est de dimension 1. Donc il existe $\lambda \in \mathbb{K}$ tel que

$$\forall x_1,\dots,x_n \in \mathrm{E} \qquad \det_{\mathscr{B}}(x_1,\dots,x_n) = \lambda \det_{\mathscr{C}}(x_1,\dots,x_n)$$

En particulier,

$$\det_{\mathscr{B}}(\mathscr{C}) = \lambda \det_{\mathscr{C}}(\mathscr{C}) = \lambda$$

d'où

$$\forall x_1,\dots,x_n \in \mathrm{E} \qquad \det_{\mathscr{B}}(x_1,\dots,x_n) = \det_{\mathscr{B}}(\mathscr{C}) \det_{\mathscr{C}}(x_1,\dots,x_n)$$

Il suffit d'évaluer cette relation sur la famille $\mathscr{B}$ pour avoir la deuxième formule. □

9.4 Calculs de déterminants

Évidemment, en l'état actuel des choses, un déterminant est loin d'être facile à calculer. Pour des matrices 3×3 ou 4×4, les calculs sont acceptables. Mais au-delà, le calcul direct devient indécent. De plus, nous voudrons l'année prochaine calculer des déterminants de matrices dont les coefficients sont des indéterminées et si possible les factoriser ; un calcul direct ne permet pas cela. Ce paragraphe établit donc des règles de calcul pratique.

Les premiers théorèmes sont donnés sans preuve, puisqu'ils sont des conséquences immédiates des **théorèmes 3.8 et 2.9**.

Théorème 9.4.1
Soit $n\geqslant 2$ un entier. Soit $A\in M_n(\mathbb{K})$, dont on note les colonnes $C_1,\dots,C_n$. Alors

- $\forall i<j\in[\![1\,;n]\!]\qquad det A=-det[C_1\ \cdots\ C_{i-1}\ C_j\ C_{i+1}\ \cdots\ C_{j-1}\ C_i\ C_{j+1}\ \cdots\ C_n]$
  Autrement dit, si on échange deux colonnes d'une matrice, on change le signe du déterminant.
- $\forall i\in[\![1\,;n]\!]\quad\forall\lambda\in\mathbb{K}\qquad \lambda det A=det[C_1\ \cdots\ C_{i-1}\ \lambda C_i\ C_{i+1}\ \cdots\ C_n]$
  Multiplier une colonne par λ multiplie le déterminant de A par λ.
- $\forall\lambda\in\mathbb{K}\qquad det(\lambda A)=\lambda^n det A$
  Multiplier A par λ multiplie le déterminant par λ^n.
- $\forall i\in[\![1\,;n]\!]\quad\forall\lambda_1,\dots,\lambda_n\in\mathbb{K}^n\qquad \lambda_i det A=det[C_1\ \cdots C_{i-1}\ \big(\sum_{k=1}^{n}\lambda_k C_k\big)\ C_{i+1}\ \cdots\ C_n]$
  Remplacer la i-ème colonne par une combinaison linéaire des colonnes de A multiplie simplement le déterminant de A par le coefficient affecté à la i-ème colonne.
  *En particulier, **ajouter** à une colonne une combinaison linéaire des autres ne change pas le déterminant.*
- *A est inversible si, et seulement si, son déterminant n'est pas nul.*
- $\forall i\in[\![1\,;n]\!]\qquad det A=\sum_{j=1}^{n}(-1)^{i+j}A_{j,i}\,det A^{(j,i)}$
  Un déterminant peut être développé par rapport à n'importe quelle colonne.

Exemple 9.4.2
Donnons-nous trois scalaires a,b,c et tentons de calculer le déterminant

$$D=\begin{vmatrix}1&1&1&1\\1&a&b&c\\1&a^2&b^2&c^2\\1&a^3&b^3&c^3\end{vmatrix}$$

Un calcul direct, en développant par rapport à la première colonne, par exemple, fournit une superbe expression que je n'ai pas le courage d'écrire. Mais si l'on s'y prend avec méthode, on peut obtenir directement une formule factorisée. Effectuons dans l'ordre :

$$C_4\leftarrow C_4-C_3\qquad C_3\leftarrow C_3-C_2\qquad C_2\leftarrow C_2-C_1$$

Ces opérations ne changent pas le déterminant donc

$$D=\begin{vmatrix}1&0&0&0\\1&a-1&b-a&c-b\\1&a^2-1&b^2-a^2&c^2-b^2\\1&a^3-1&b^3-a^3&c^3-b^3\end{vmatrix}$$

On peut voir que $a-1$ se met en facteur dans la première colonne ; $b-a$ dans la deuxième et $c-b$ dans la troisième :

$$\mathrm{D} = (a-1)(b-a)(c-b)\begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & a+1 & b+a & c+b \\ 1 & a^2+a+1 & b^2+ab+a^2 & c^2+bc+b^2 \end{vmatrix}$$

On effectue alors les opérations suivantes, qui ne changent pas le déterminant :

$$\mathrm{C}_4 \leftarrow \mathrm{C}_4 - \mathrm{C}_3 \qquad \mathrm{C}_3 \leftarrow \mathrm{C}_3 - \mathrm{C}_2$$

et il vient $$\mathrm{D} = (a-1)(b-a)(c-b)\begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & a+1 & b-1 & c-a \\ 1 & a^2+a+1 & b^2+ab-a-1 & c^2+bc-ab-a^2 \end{vmatrix}$$

On remarque que $$b^2+ab-a-1 = (b-1)(b+1)+a(b-1) = (b-1)(a+b+1)$$

et de même $$c^2+bc-ab-a^2 = (c-a)(c+a)+b(c-a) = (c-a)(a+b+c)$$

ce qui permet de factoriser $b-1$ dans la troisième colonne et $c-a$ dans la dernière :

$$\mathrm{D} = (a-1)(b-1)(b-a)(c-a)(c-b)\begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & a+1 & 1 & 1 \\ 1 & a^2+a+1 & a+b+1 & a+b+c \end{vmatrix}$$

Et la dernière modification de colonne est $\mathrm{C}_4 \leftarrow \mathrm{C}_4 - \mathrm{C}_3$:

$$\mathrm{D} = (a-1)(b-1)(b-a)(c-a)(c-b)\begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & a+1 & 1 & 0 \\ 1 & a^2+a+1 & a+b+c & c-1 \end{vmatrix}$$

On factorise le $c-1$ de la dernière colonne :

$$\mathrm{D} = (a-1)(b-1)(c-1)(b-a)(c-a)(c-b)\begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & a+1 & 1 & 0 \\ 1 & a^2+a+1 & a+b+c & 1 \end{vmatrix}$$

Ce dernier déterminant se développe sans le moindre problème par rapport à la dernière colonne, qui est bien remplie de zéros. Quelques secondes plus tard, il vient

$$\mathrm{D} = (a-1)(b-1)(c-1)(b-a)(c-a)(c-b)$$

Mais on peut faire bien mieux. Il faut cependant travailler un peu plus :

Théorème 9.4.3
Soit $n \geqslant 2$ un entier. Alors

$$\forall \mathrm{A}, \mathrm{B} \in \mathrm{M}_n(\mathbb{K}) \qquad det(\mathrm{BA}) = (det\mathrm{B})(det\mathrm{A})$$

Preuve : On définit $$\forall x_1, \ldots, x_n \in \mathbb{K}^n \qquad f(x_1, \ldots, x_n) = \det(\mathrm{B}x_1, \ldots, \mathrm{B}x_n)$$

Il est évident que f est une forme n-linéaire alternée sur $\mathbb{K}^n$ puisque le produit matriciel est distributif sur l'addition vectorielle. D'après le **corollaire 3.12**, f est proportionnelle au déterminant sur $\mathbb{K}^n$: il existe $\lambda \in \mathbb{K}^n$ tel que

$$\forall x_1,\dots,x_n \in \mathbb{K}^n \qquad \det(Bx_1,\dots,Bx_n) = \lambda \det(x_1,\dots,x_n)$$

On trouve λ en evaluant cette expression sur la base canonique de $\mathbb{K}^n$, sur laquelle le déterminant vaut 1. Et il vient que $\lambda = \det B$:

$$\forall x_1,\dots,x_n \in \mathbb{K}^n \qquad \det(Bx_1,\dots,Bx_n) = \det B \times \det(x_1,\dots,x_n)$$

Enfin, on prend pour $x_1,\dots,x_n$ les colonnes de A, dans l'ordre et il vient

$$\det(BA) = (\det B)(\det A)$$ □

Corollaire 9.4.4
Soit $n \geqslant 2$ un entier. Alors

$$\forall A \in M_n(\mathbb{K}) \qquad det A = det({}^tA)$$

Preuve : On vérifie sans aucun mal que le résultat est vrai pour les matrices d'opérations élémentaires introduites dans le chapitre sur les matrices. Mais toute matrice $A \in GL_n(\mathbb{K})$ peut s'écrire sous la forme

$$A = E_1 \cdots E_p$$

où $p \in \mathbb{N}^\star$ et $E_1,\dots,E_p$ sont des matrices élémentaires. Par suite,

$${}^tA = {}^tE_p \cdots {}^tE_1$$

d'où $$\det {}^tA = (\det {}^tE_p)\cdots(\det {}^tE_1) = (\det E_p)\cdots(\det E_1) = \det A$$

Si A n'est pas inversible, alors ${}^tA$ n'est pas inversible également car ces deux matrices ont le même rang. Par conséquent, leurs déterminants sont égaux, tous les deux, à zéro. □

Corollaire 9.4.5
*Dans le **théorème 4.1**, on peut remplacer le mot « colonne » par « ligne. »*

Théorème 9.4.6
Soient n et p deux entiers non nuls. Soient $A \in M_n(\mathbb{K})$, $B \in M_p(\mathbb{K})$ et $C \in M_{n,p}(\mathbb{K})$. Alors

$$\begin{vmatrix} A & C \\ 0 & B \end{vmatrix} = (det A)(det B)$$

Preuve : On note

- $A_1,\dots,A_n \in \mathbb{K}^n$ les colonnes de A ;
- $C_1,\dots,C_p \in \mathbb{K}^n$ les colonnes de C ;
- $B_1,\dots,B_p \in \mathbb{K}^p$ les colonnes de B.
- 0_p le vecteur nul dans $\mathbb{K}^p$.

et on définit $$\forall x_1,\dots,x_n \in \mathbb{K}^n \qquad f(x_1,\dots,x_n) = \det\left(\begin{bmatrix} x_1 \\ 0_p \end{bmatrix},\dots,\begin{bmatrix} x_n \\ 0_p \end{bmatrix},\begin{bmatrix} C_1 \\ B_1 \end{bmatrix},\dots,\begin{bmatrix} C_p \\ B_p \end{bmatrix}\right)$$

Il est évident que f est une forme n-linéaire alternée sur $\mathbb{K}^n$ donc il existe $\lambda \in \mathbb{K}$ tel que

$$\forall x_1,\dots,x_n \in \mathbb{K}^n \qquad f(x_1,\dots,x_n) = \lambda \det(x_1,\dots,x_n)$$

On évalue cette expression sur la base canonique de $\mathbb{K}^n$. Il vient immédiatement que

$$\det \mathrm{B} = \lambda$$

donc $$\forall x_1,\dots,x_n \in \mathbb{K}^n \qquad f(x_1,\dots,x_n) = (\det \mathrm{B}) \det(x_1,\dots,x_n)$$

En particulier, $$f(\mathrm{A}_1,\dots,\mathrm{A}_n) = (\det \mathrm{B}) \det(\mathrm{A}_1,\dots,\mathrm{A}_n) = (\det \mathrm{B})(\det \mathrm{A})$$

C'est exactement la formule recherchée. □

9.5 Allons plus loin

9.5.1 Déterminant d'un endomorphisme

Théorème 9.5.1
Soient $n \geqslant 2$ et E *un* $\mathbb{K}$*-espace vectoriel de dimension finie. Soit $f \in \mathscr{L}(\mathrm{E})$. Toutes les matrices représentatives de f ont le même déterminant.*

Preuve : Il suffit de montrer que le déterminant d'une matrice associée à f ne dépend pas du choix de la base. On se donne donc deux bases $\mathscr{B}$ et $\mathscr{C}$ de E. On note B et C les matrices de f relativement aux bases $\mathscr{B}$ et $\mathscr{C}$ respectivement, et P la matrice de passage de $\mathscr{B}$ à $\mathscr{C}$. On sait que $\mathrm{C} = \mathrm{PBP}^{-1}$ donc

$$\det \mathrm{C} = \det(\mathrm{PBP}^{-1}) = (\det \mathrm{P})(\det \mathrm{B})(\det \mathrm{P}^{-1}) = (\det \mathrm{PP}^{-1})(\det \mathrm{B}) = \det \mathrm{B}$$ □

Définition 9.5.2
Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \geqslant 2$ rapporté à une base $\mathscr{B}$. Si $f \in \mathscr{L}(\mathrm{E})$, on appelle *déterminant de f* le déterminant de $\mathrm{Mat}_{\mathscr{B}} f$. Celui-ci ne dépend pas de la base choisie.

L'intérêt de cette notion est évident : on peut calculer le déterminant d'un endomorphisme de E dans n'importe quelle base. Si l'on trouve une base « sympathique », dans laquelle f a une matrice avec beaucoup de zéros, on s'empressera de travailler dessus pour calculer le déterminant de f. Le théorème suivant est trivial, compte-tenu de la définition précédente :

Corollaire 9.5.3
Soient E *de dimension finie $n \geqslant 2$ et $f \in \mathscr{L}(\mathrm{E})$. Alors f est un automorphisme de* E *si, et seulement si, $\det f \neq 0$.*

9.5.2 Formule de la comatrice

Définition 9.5.4
Soit $n \geqslant 2$ un entier. Soit $\mathrm{A} \in \mathrm{M}_n(\mathbb{K})$. Les déterminants des mineurs de A sont appelés *cofacteurs de* A. La matrice ComA, définie par

$$\forall i,j \in [\![1\,;n]\!] \qquad (\mathrm{Com}\,\mathrm{A})_{i,j} = (-1)^{i+j} \det \mathrm{A}^{(i,j)}$$

est appelée *comatrice de* A.

Théorème 9.5.5 (Formule de la comatrice)
Soit $n \geqslant 2$ un entier. Soit $A \in M_n(\mathbb{K})$. On a

$$({}^t Com A)\, A = (det A)\, I_n$$

En particulier, $$\forall A \in GL_n(\mathbb{K}) \qquad A^{-1} = \frac{{}^t Com A}{det A}$$

Preuve : On se donne $i, j \in [\![1\,;n]\!]$ et on calcule le coefficient i, j de $({}^t\mathrm{Com}A)A$. D'abord, on rappelle que

$$\forall k \in [\![1\,;n]\!] \qquad ({}^t\mathrm{Com}A)_{i,k} = (\mathrm{Com}A)_{k,i} = (-1)^{k+i} \det A^{(k,i)}$$

donc $$\left(({}^t\mathrm{Com}A)A\right)_{i,j} = \sum_{k=1}^{n} (-1)^{k+i} A_{k,j} \det A^{(k,i)}$$

Si $i = j$, on reconnaît le développement de $\det A$ par rapport à la i-ème colonne. Si $i \neq j$, on reconnaît le développement du déterminant de la matrice A dans laquelle on a remplacé la i-ème colonne par la j-ème ; cette matrice a deux colonnes identiques (la i-ème et la j-ème) donc ce déterminant est nul. Par suite,

$$\forall i, j \in [\![1\,;n]\!] \qquad \left(({}^t\mathrm{Com}A)A\right)_{i,j} = \begin{cases} 0 & \text{si } i \neq j \\ \det A & \text{si } i = j \end{cases}$$

Autrement dit, $$({}^t\mathrm{Com}A)A = (\det A)\, I_n$$ □

Cette formule paraît très intéressante pour calculer l'inverse d'une matrice inversible. Mais... numériquement, elle est inutilisable. En effet, un calcul de déterminant $n \times n$ requiert aux alentours de $n!$ opérations. Cela prend un temps ridicule si n est grand. En revanche, pour les matrices $n = 2, 3$ ou 4, il peut être intéressant d'utiliser la comatrice. Il ne faut, bien sûr, pas se tromper avec l'alternance des signes quand on calcule les cofacteurs.

La formule de la comatrice a donc un intérêt purement théorique, et elle a effectivement des applications importantes.

9.5.3 Les formules de Cramer

Les formules de Cramer « permettent » théoriquement de calculer les solutions d'un système linéaire (carré) inversible.

Théorème 9.5.6 (Formules de Cramer)
Soient $n \geqslant 2$ un entier et $A \in GL_n(\mathbb{K})$, dont on note les colonnes $A_1, \ldots, A_n$. Soient $B \in \mathbb{K}^n$ et $X = A^{-1}B$ l'unique solution du système linéaire $AX = B$. Alors

$$\forall i \in [\![1\,;n]\!] \qquad x_i = \frac{det[A_1 \cdots A_{i-1}\, B\, A_{i+1} \cdots A_n]}{det A}$$

Preuve : Puisque $AX = B$, on a $\sum_{k=1}^{n} x_k A_k = B$. Donc si $i \in [\![1\,;n]\!]$, on a par linéarité du déterminant par rapport à la i-ème variable :

$$\det[A_1 \cdots A_{i-1}\, B\, A_{i+1} \cdots A_n] = \sum_{k=1}^{n} x_k \det[A_1 \cdots A_{i-1}\, A_k\, A_{i+1} \cdots A_n]$$

Mais si $k \neq i$ dans cette somme, la matrice dont on calcule le déterminant a deux colonnes identiques : la i-ème et la k-ème. Donc

$$\det[\mathrm{A}_1 \ \cdots \ \mathrm{A}_{i-1} \ \mathrm{B} \ \mathrm{A}_{i+1} \ \cdots \ \mathrm{A}_n] = x_i \det[\mathrm{A}_1 \ \cdots \ \mathrm{A}_{i-1} \ \mathrm{A}_i \ \mathrm{A}_{i+1} \ \cdots \ \mathrm{A}_n] = x_i \det \mathrm{A}$$

donc $$\forall i \in [\![1 ; n]\!] \qquad x_i = \frac{\det[\mathrm{A}_1 \ \cdots \ \mathrm{A}_{i-1} \ \mathrm{B} \ \mathrm{A}_{i+1} \ \cdots \ \mathrm{A}_n]}{\det \mathrm{A}}$$ □

À nouveau, il s'agit d'une formule dont l'intérêt est purement theorique. Sauf pour la résolution de systèmes 2×2 ou 3×3, la méthode du pivot est beaucoup plus efficace.

Chapitre 10

Fondements de l'Analyse Réelle

Il s'agit pour nous dans ce chapitre de nous donner une base solide pour pouvoir faire de l'analyse rigoureuse. Nous allons ainsi développer les propriétés fondamentales de $\mathbb{R}$. En revanche, construire $\mathbb{R}$ rigoureusement est hors de question, puisqu'il s'agit d'un travail très difficile et il nous faudra donc admettre quelques petites choses.

On prendra donc pour acquis le fait que $\mathbb{R}$ est un ensemble de nombres, contenant strictement $\mathbb{Q}$, muni d'une addition, et d'une multiplication distributive sur l'addition. Dans $\mathbb{R}$ on peut toujours soustraire deux nombres et on peut diviser par un nombre non nul. Un produit de deux réels est positif si et seulement si ces nombres sont de même signe.

10.1 Propriété de la borne supérieure

10.1.1 Ordre dans $\mathbb{R}$

Définition 10.1.1
Soient a et b deux nombres réels. On dira que *a est inférieur à b*, ou bien que *b est supérieur à a*, si et seulement si $a-b$ est négatif. On notera $a \leqslant b$ ou $b \geqslant a$.

On dira que *a est strictement inférieur à b*, ou que *b est strictement supérieur à a*, si et seulement si $a \leqslant b$ et $a \neq b$. On notera alors $a < b$.

Proposition 10.1.2
Voici les propriétés de l'ordre dans $\mathbb{R}$:

1. ***Réflexivité :*** $\forall x \in \mathbb{R} \qquad x \leqslant x$;
2. ***Antisymétrie :*** $\forall (x,y) \in \mathbb{R}^2 \qquad \big(x \leqslant y \quad et \quad y \leqslant x\big) \Longrightarrow x = y$;
3. ***Transitivité :*** $\forall (x,y,z) \in \mathbb{R}^3 \qquad \big(x \leqslant y \quad et \quad y \leqslant z\big) \Longrightarrow x \leqslant z$;
4. ***Totalité :*** $\forall (x,y) \in \mathbb{R}^2 \qquad (x \leqslant y \quad ou\ bien \quad y \leqslant x)$;
5. ***Compatibilité avec l'addition :***
$$\forall (x,y,z,t) \in \mathbb{R}^4 \qquad (x \leqslant y \quad et \quad z \leqslant t) \Longrightarrow x+z \leqslant y+t$$
6. ***Compatibilité avec la multiplication :***
$$\forall (x,y,z,t) \in \mathbb{R}_+^4 \qquad (x \leqslant y \quad et \quad z \leqslant t) \Longrightarrow xz \leqslant xt \leqslant yt$$

Preuve : Conséquence triviale de la **définition 1.1**. □

Exemple 10.1.3
Supposons qu'on ait quatre réels x, y, z et t tels que

$$x \leqslant y \qquad z \leqslant t \qquad \text{et} \qquad x+z = y+t$$

On sait que $x \leqslant x$ et $z \leqslant t$ donc $x+z \leqslant x+t$

Puis $x \leqslant y$ et $t \leqslant t$ donc $x+t \leqslant y+t = x+z$

D'après la propriété d'antisymétrie, on obtient $x+z = x+t$ donc $z = t$. Et par suite $x = y$.

Définition 10.1.4
Soient $\mathrm{A} \subset \mathbb{R}$ une partie non vide de $\mathbb{R}$ et $x \in \mathbb{R}$.

- On dit que x *est un majorant de* A si et seulement si
$$\forall a \in \mathrm{A} \qquad a \leqslant x$$
Si de plus, x appartient à A, on dit que x *est un plus grand élément de* A et on note $x = \mathrm{Max A}$.
- On dit que x *est un minorant de* A si et seulement si
$$\forall a \in \mathrm{A} \qquad x \leqslant a$$
Si de plus, x appartient à A, on dit que x *est un plus petit élément de* A et on note $x = \mathrm{Min A}$.
- Si A admet un majorant, on dit que A *est majoré*.
- Si A admet un minorant, on dit que A *est minoré*.
- Si A est majoré et minoré, on dit que A *est borné*.

Par convention, n'importe quel réel majore et minore l'ensemble vide, qui est donc borné.

Exemple 10.1.5
L'ensemble des majorants de $]-1\,;1[$ est $[1\,;+\infty[$; l'ensemble de ses minorants est $]-\infty\,;-1]$.

Proposition 10.1.6
Si un sous-ensemble $\mathbb{R}$ admet un plus grand élément, celui-ci est unique. S'il admet un plus petit élément, celui-ci est unique.

Preuve : La même que pour la proposition analogue dans $\mathbb{N}$. □

Proposition 10.1.7
Toute partie finie non vide de $\mathbb{R}$ admet un plus petit élément et un plus grand élément.

Preuve : On démontre ceci par récurrence. Le résultat est trivial pour un ensemble à un élément.

Si n est un entier, on suppose que toute partie de $\mathbb{R}$ à n éléments admet un plus grand élément. Puis on se donne $\mathrm{A} \subset \mathbb{R}$, fini, de cardinal $n+1$. On pioche au hasard un élément $a \in \mathrm{A}$. L'ensemble $\mathrm{A} \setminus \{a\}$ est de cardinal n donc admet un plus grand élément x. Comme l'ordre dans $\mathbb{R}$ est total (**proposition 1.2, point 4**), on a

$$a \leqslant x \qquad \text{ou} \qquad x \leqslant a$$

Dans le premier cas, x est le plus grand élément de A, puisqu'il majore $\mathrm{A} \setminus \{a\}$ ainsi que a. Dans le second cas, d'après les propriétés de transitivité et réflexivité de l'ordre dans $\mathbb{R}$, on a

$$\forall z \in \mathrm{A} \setminus \{a\} \qquad z \leqslant x \leqslant a \qquad \text{et} \qquad a \leqslant a$$

Donc a majore A ; c'en est donc le plus grand élément. Ce qui prouve l'hérédité.

On a donc montré par récurrence que toute partie finie de $\mathbb{R}$ admet un plus grand élément.

On passe au problème du plus petit élément. On pourrait refaire une récurrence. Mais on peut aussi utiliser ce qu'on vient d'établir. Soit A une partie finie de $\mathbb{R}$. L'ensemble $B = -A = \{-x \mid x \in A\}$ donc il admet un plus grand élément, noté $-a$ avec $a \in A$:

$$\forall b \in A \qquad -b \leqslant -a$$

Ainsi, $$\forall b \in A \qquad a \leqslant b$$

et a est le plus petit élément de A. □

10.1.2 Bornes supérieure et inférieure

Définition 10.1.8 (Borne supérieure)
Soit A une partie de $\mathbb{R}$. Si l'ensemble des majorants de A admet un plus petit élément a, on dit que *la borne supérieure de* A *est* a, ou bien que a *est le supremum de* A. On notera alors $a = \text{Sup}\, A$.

Par convention, $\emptyset$ admet une borne supérieure, qui est $-\infty$.

> Remarquons d'abord que la définition du *s*upremum*e*st bien posée. En effet, si l'ensemble des majorants de A admet un plus petit élément, celui-ci est unique d'après la **proposition 1.6**. Il n'y a donc pas d'ambiguïté sur qui est la borne supérieure de A : c'est le plus petit des majorants de A.
>
> Il également est important de bien voir la distinction entre *supremum* et plus grand élément. Une partie de $\mathbb{R}$ peut très bien admettre un *s*upremum, sans avoir de plus grand élément. Voir l'exemple qui suit de l'intervalle $]-1\,;1[$.
>
> En revanche, si A admet un plus grand élément, celui-ci est automatiquement la borne supérieure de A.

Exemple 10.1.9

1. Reprenons l'exemple de l'intervalle $]-1\,;1[$. On a vu que l'ensemble de ses majorants est $[1\,;+\infty[$. Ce dernier admet un plus petit élément : 1. Donc $1 = \text{Sup}\,]-1\,;1[$.

   Remarquons que dans ce cas, le supremum de $]-1\,;1[$ n'appartient pas à cet ensemble.
2. En revanche, l'intervalle $]-1\,;1]$ admet pour ensemble de majorants $[1\,;+\infty[$, dont le plus petit élément est 1. Donc $1 = \text{Sup}\,]-1\,;1]$; et on voit que $]-1\,;1]$ contient sa borne supérieure.
3. L'ensemble des majorants de $\mathbb{R}_-$ est $[0\,;+\infty[$. Ce dernier admet un plus petit élément, qui est 0. Donc $0 = \text{Sup}\,\mathbb{R}_-$ et $\mathbb{R}_-$ contient sa borne supérieure.
4. L'ensemble des majorants de $\mathbb{R}_-^\star$ est $[0\,;+\infty[$. Donc $0 = \text{Sup}\,\mathbb{R}_-^\star$ et $\mathbb{R}_-^\star$ ne contient pas sa borne supérieure.

Théorème 10.1.10 (Propriété de la borne supérieure)
Toute partie non vide, majorée, de $\mathbb{R}$ *admet une borne supérieure.*

Preuve : Admis. □

> Ce résultat est indémontrable compte-tenu de l'approche de $\mathbb{R}$ imposée par le programme de CPGE. Il nous faudrait en effet construire $\mathbb{R}$ proprement pour être en mesure de démon-

trer la propriété de la borne supérieure. Je me contenterai de dire que cette construction est très difficile.

Définition 10.1.11
Soit A une partie de $\mathbb{R}$. Si l'ensemble des minorants de A admet un plus grand élément a, on dit que *la borne inférieure de* A *est* a, ou bien que a *est l'infimum de* A. On notera alors $a = \text{Inf}\,\text{A}$. Par convention, $\emptyset$ admet une borne inférieure, qui est $+\infty$.

Corollaire 10.1.12 (Propriété de la borne inférieure)
Toute partie non vide, minorée, de $\mathbb{R}$ *admet une borne inférieure.*

Preuve : Soit A une partie de $\mathbb{R}$, non vide, minorée. On note B l'ensemble des minorants de A, c'est-à-dire que

$$\text{B} = \{x \in \mathbb{R} \mid \forall a \in \text{A} \quad x \leqslant a\}$$

et on définit les ensembles

$$\text{A}' = \{-x \mid x \in \text{A}\} \qquad \text{et} \qquad \text{B}' = \{-x \mid x \in \text{B}\}$$

Dans la mesure où A n'est pas vide par hypothèse, A′ n'est pas vide non plus. Ensuite,

$$\begin{aligned} \forall x \in \mathbb{R} \qquad x \in \text{B}' &\iff -x \in \text{B} \\ &\iff \forall a \in \text{A} \qquad -x \leqslant a \\ &\iff \forall a \in \text{A} \qquad -a \leqslant x \\ &\iff \forall a' \in \text{A}' \qquad a' \leqslant x \\ x \in \text{B}' &\iff x \text{ est un majorant de A}' \end{aligned}$$

Par suite, B′ est l'ensemble des majorants de A′.

D'après la **propriété de la borne supérieure**, B′ admet un plus petit élément, que l'on note b'. Montrons que $b = -b'$ est le plus grand élément de B. C'est simple : si x appartient à B, $-x$ appartient à B′ donc $b' \leqslant -x$. Par suite, $x \leqslant b$ et b est bien le plus grand élément de B.

L'ensemble des minorants de A a un plus grand élément. Donc A admet une borne inférieure. □

La preuve précédente établit au passage que, si A est non vide minoré, alors

$$\text{Inf}\,\text{A} = -\text{Sup}\,\{-x \mid x \in \text{A}\}$$

Ces deux propriétés de la borne inférieure et de la borne supérieure sont absolument fondamentales en analyse réelles, car elles assurent l'existence de nombres satisfaisant une certaine propriété.

Exemple 10.1.13
Par exemple, c'est ainsi qu'on montre que $\sqrt{2}$ existe en tant que nombre réel. On considère l'ensemble

$$\text{A} = \{x > 0 \mid x^2 \leqslant 2\}$$

A n'est pas vide, puisqu'il contient 1. Et A est majoré par 2, par exemple. En effet, si x appartient à A, on a

$$x^2 \leqslant 2 \leqslant 4 \qquad \text{et} \qquad x > 0$$

donc $$(x-2)(x+2) \leqslant 0 \qquad \text{et} \qquad x > 0$$

Comme $x+2>0$, c'est que $x-2<0$, donc $x \leqslant 2$. D'après la **propriété de la borne supérieure**, A admet une borne supérieure qu'on note a. Remarquons tout de suite que $a \geqslant 1$; en effet, a majore A, qui contient 1. Puis montrons que $a^2 = 2$.

- On suppose que $a^2 > 2$, de sorte que $a^2 - 2$ est un nombre réel strictement positif qu'on note ε :

  $$a^2 - 2 = \varepsilon > 0$$

  On note h le plus petit des deux nombres 1 et $\varepsilon/2a$. De sorte que l'on ait à la fois

  $$\begin{cases} a-h \geqslant 0 & \text{car } a \geqslant 1 \text{ et } h \leqslant 1 \\ 2ah \leqslant \varepsilon & \text{car } h \leqslant \dfrac{\varepsilon}{2a} \end{cases}$$

  $$(a-h)^2 = a^2 - 2ah + h^2 = 2 + \underbrace{\varepsilon - 2ah}_{\geqslant 0} + \underbrace{h^2}_{\geqslant 0} \geqslant 2$$

  Par suite, si x appartient à A, on a

  $$x^2 \leqslant 2 \leqslant (a-h)^2$$

  donc $$0 \leqslant (a-h)^2 - x^2 = (a-h-x)(a-h+x)$$

  Puisque $a-h+x$ est positif, $a-h-x$ doit aussi être positif d'où

  $$\forall x \in \text{A} \qquad x \leqslant a-h$$

  Donc $a-h$ majore A. C'est absurde, puisque a est le plus petit des majorants de A. Donc $a^2 \leqslant 2$.
- On suppose que $a^2 < 2$, de sorte que $2 - a^2$ est un nombre réel strictement positif qu'on note ε :

  $$2 - a^2 = \varepsilon > 0$$

  On note h le plus petit des deux nombres 1 et $\varepsilon/(2a+1)$. Ainsi,

  $$\begin{cases} h^2 \leqslant h & \text{car } 0 \leqslant h \leqslant 1 \\ (2a+1)h \leqslant \varepsilon & \text{car } h \leqslant \dfrac{\varepsilon}{2a+1} \end{cases}$$

  et du coup $$\begin{aligned} (a+h)^2 &= a^2 + 2ah + h^2 = 2 - \varepsilon + 2ah + h^2 \\ &\leqslant 2 - \varepsilon + (2a+1)h \leqslant 2 \end{aligned}$$

  ce qui montre que $a+h$ appartient à A. Ce qui est absurde, puisque a est censé majorer $a+h$. Donc $a^2 \geqslant 2$.

On conclut bien que $a^2 = 2$ et on voit que a n'est autre que la racine carrée de 2.

> On conclut aussi que ce type de preuve, utilisant uniquement les bases de l'analyse réelle est extrêmement fastidieux. L'un des buts du cours d'analyse est donc de développer une théorie rigoureuse (donc partant des bases), mais suffisamment souple et puissante pour éviter le recours systématique aux bases.

10.1.3 Caractérisation

Théorème 10.1.14

Soit A *une partie de* $\mathbb{R}$*, non vide, majorée. Soit* $a \in \mathbb{R}$*. On a*

$$a = Sup\text{A} \iff \begin{cases} \forall x \in \text{A} & x \leqslant a \\ \forall \varepsilon > 0 & \exists x \in \text{A} \qquad a - \varepsilon \leqslant x \end{cases}$$

Preuve : Supposons que $a = \text{Sup}\,\text{A}$, qui existe puisque A est non vide et majoré. Alors a est un majorant de A :

$$\forall x \in \text{A} \qquad x \leqslant a \tag{1}$$

De plus, si ε est un nombre strictement positif donné, $a - \varepsilon < a$. Comme a est le plus petit des majorants de A, $a - \varepsilon$ n'est pas un majorant de A. Donc

$$\exists x \in \text{A} \qquad a - \varepsilon \leqslant x \tag{2}$$

Réciproquement, supposons que (**1**) et (**2**) sont satisfaites. Comme A est non vide, majoré, il admet une borne supérieure qu'on note a'. La propriété (**1**) nous dit que a est un majorant de A. Comme a' est le plus petit des majorants de A, on a $a' \leqslant a$.

Supposons que $a' \neq a$; alors l'inégalité est stricte et $a - a'$ est un nombre réel strictement positif. Posons

$$\varepsilon = \frac{a - a'}{2} > 0$$

D'après la propriété (**2**), il existe x dans A tel que

$$x \geqslant a - \varepsilon = a - \frac{a - a'}{2} = \frac{a' + a}{2} > a'$$

Ceci contredit le fait que a' majore A. Donc $a = a' = \text{Sup}\,\text{A}$. □

On a une caractérisation similaire de la borne inférieure :

Théorème 10.1.15
Soit A *une partie de* $\mathbb{R}$*, non vide, minorée. Soit* $a \in \mathbb{R}$*. On a*

$$a = Inf\text{A} \iff \begin{cases} \forall x \in \text{A} & a \leqslant x \\ \forall \varepsilon > 0 & \exists x \in \text{A} \qquad x \leqslant a + \varepsilon \end{cases}$$

Théorème 10.1.16
Un réel x *est nul si et seulement si*

$$\forall \varepsilon > 0 \qquad |x| \leqslant \varepsilon$$

Preuve : Si $x = 0$, on a

$$\forall \varepsilon > 0 \qquad |x| = 0 \leqslant \varepsilon$$

Réciproquement, supposons que

$$\forall \varepsilon > 0 \qquad |x| \leqslant \varepsilon$$

Alors en particulier,

$$\forall \varepsilon > 0 \qquad x \leqslant \varepsilon$$

donc x minore $\mathbb{R}_+$. Donc x est inférieur au plus petit minorant de $\mathbb{R}_+$, qui est 0. De même, on montre que $x \geqslant 0$. D'où $x = 0$. □

> Cette équivalence semble être une manière compliquée de dire qu'un réel est nul. Mais elle est en fait extrêmement utile, et nous en userons et abuserons en analyse. En effet, il est très rare qu'on ait affaire à des égalités tout au long d'un travail d'analyse. Au mieux, on

n'est souvent capable de faire que des estimations. Et si celles-ci sont suffisamment fines, on peut espérer montrer par exemple qu'une quantité qu'on considère est arbitrairement proche de 0 ; pour en déduire, à l'aide du **théorème 1.16**, que cette quantité est nulle.

10.2 Conséquences

10.2.1 La propriété d'Archimède

Proposition 10.2.1
Soient x et y deux nombres réels avec $x > 0$. Il existe un entier naturel n tel que $nx \geqslant y$.

Preuve : Supposons la conclusion fausse :

$$\forall n \in \mathbb{N} \qquad nx < y$$

L'ensemble $\{nx \mid n \in \mathbb{N}\}$ de tous les multiples entiers de x est donc majoré par y. Il n'est évidemment pas vide. D'après la **propriété de la borne supérieure**, l'ensemble de ses majorants admet un plus petit élément a. On a

$$\forall n \in \mathbb{N} \qquad (n+1)x \leqslant a$$

donc
$$\forall n \in \mathbb{N} \qquad nx \leqslant a - x < a$$

et $a - x$ est un majorant de $\{nx \mid n \in \mathbb{N}\}$ strictement inférieur à a : on a une contradiction avec le fait que a est le plus majorant de cet ensemble. □

Corollaire 10.2.2
Soient x et y deux entiers avec $x > 1$. Il existe un entier n tel que $x^n \geqslant y$.

Preuve : On écrit la formule du binôme

$$\forall n \in \mathbb{N} \qquad x^n = (1 + (x-1))^n = \sum_{k=0}^{n} \mathrm{C}_n^k (x-1)^k$$

Tous les termes de cette somme sont positifs donc

$$\forall n \in \mathbb{N} \qquad x^n \geqslant 1 + n(x-1)$$

D'après la propriété d'archimède, comme $x - 1 > 0$, il existe un entier n tel que

$$n(x-1) \geqslant y - 1$$

Donc
$$x^n \geqslant 1 + n(x-1) \geqslant y$$ □

10.2.2 La partie entière

Proposition 10.2.3
Soit x un nombre réel. Il existe un unique entier relatif, noté $\mathrm{E}(x)$ *ou* $[x]$*, tel que*

$$\mathrm{E}(x) \leqslant x < \mathrm{E}(x) + 1$$

$\mathrm{E}(x)$ *est appelé partie entière de x.*

Preuve : Considérons l'ensemble $\mathrm{E} = \{n \in \mathbb{Z} \mid n \leqslant x\}$. Il n'est pas vide puisque d'après la propriété d'Archimède,

$$\exists n \in \mathbb{N} \qquad n \geqslant -x \qquad \text{c'est-à-dire} \qquad -n \leqslant x$$

Toujours d'après la propriété d'Archimède, il existe un entier N tel que $x \leqslant \mathrm{N}$. De sorte que

$$\forall n \in \mathrm{E} \qquad n \leqslant x \leqslant \mathrm{N}$$

et E est une partie de $\mathbb{Z}$, non vide, majorée par N. Elle admet donc un plus grand élément, qu'on note n_0. De sorte que $n_0 + 1$ ne puisse se trouver dans E puisqu'il est supérieur strictement à n_0. Par conséquent,

$$n_0 \leqslant x < n_0 + 1$$

Montrons qu'en fait, cet entier est uniquement déterminé par cette relation. Soit $n_1 \in \mathbb{Z}$ tel que

$$n_1 \leqslant x < n_1 + 1$$

Alors $$n_0 \leqslant x < n_1 + 1 \qquad \text{et} \qquad n_1 - n_0 > -1$$

Comme $n_1 - n_0$ est entier relatif, il s'ensuit que $n_1 - n_0 \geqslant 0$. De la même manière, on montre que $n_0 - n_1 \leqslant 0$. D'où $n_0 = n_1$. □

10.2.3 Développement décimal d'un nombre réel

Théorème 10.2.4
Soit x un nombre réel. Il existe une suite $(a_n)_{n\in\mathbb{N}}$ d'entiers tels que

$$\forall n \in \mathbb{N}^\star \qquad a_n \in [\![0\,;9]\!]$$

et $$\forall n \in \mathbb{N} \qquad \sum_{k=0}^{n} \frac{a_k}{10^k} \leqslant x < \frac{1}{10^n} + \sum_{k=0}^{n} \frac{a_k}{10^k}$$

Ces entiers sont déterminés de manière unique et appelés termes du développement décimal de x.

Preuve : Il suffit de définir cette suite par récurrence. On souhaite que $a_0 \leqslant x < a_0 + 1$ donc on prend $a_0 = [x]$, qui est l'unique nombre vérifiant cette relation.

Ensuite, on veut que

$$a_0 + \frac{a_1}{10} \leqslant x < \frac{1}{10} + a_0 + \frac{a_1}{10}$$

ou de manière équivalente, après multiplication par 10 des deux membres des cette égalité :

$$a_1 \leqslant 10(x - a_0) < a_1 + 1$$

On sait que $[10(x - a_0)]$ est l'unique entier vérifiant cette relation. Et dans la mesure où

$$0 \leqslant x - a_0 < 1$$

il vient $$0 \leqslant 10(x - a_0) < 10$$

d'où $$a_1 = [10(x - a_0)] \in [\![0\,;9]\!]$$

On se donne maintenant un entier $n > 0$ et on suppose les n premiers termes du développement décimal de x construits. On prend alors

$$a_{n+1} = \left[10^{n+1}\left(x - \sum_{k=0}^{n} \frac{a_k}{10^k}\right)\right]$$

On a $$a_{n+1} \leqslant 10^{n+1}\left(x - \sum_{k=0}^{n} \frac{a_k}{10^k}\right) < a_{n+1} + 1$$

d'où $$\sum_{k=0}^{n+1} \frac{a_k}{10^k} \leqslant x < \frac{1}{10^{n+1}} + \sum_{k=0}^{n+1} \frac{a_k}{10^k}$$

Ce qui établit qu'on peut construire le $(n+1)$-ème du développement décimal. □

Corollaire 10.2.5
$\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$ sont denses dans $\mathbb{R}$, c'est-à-dire que tout intervalle ouvert non vide contient des rationnels et des irrationnels.

Preuve : Soit $]a\,;\,b[$ un intervalle ouvert non vide de $\mathbb{R}$, c'est-à-dire que $a < b$. Notons $\epsilon = b - a$. D'après le **corollaire 2.2**, il existe un entier N tel que

$$10^{\mathrm{N}} > \frac{1}{\epsilon} \qquad \text{ou encore} \qquad \frac{1}{10^{\mathrm{N}}} < \epsilon$$

Notons $(a_n)_{n\in\mathbb{N}}$ les termes du développement décimal de a. On a en particulier

$$\sum_{k=0}^{\mathrm{N}} \frac{a_k}{10^k} \leqslant a < \frac{1}{10^{\mathrm{N}}} + \sum_{k=0}^{\mathrm{N}} \frac{a_k}{10^k}$$

Par conséquent, $$a < \frac{1}{10^{\mathrm{N}}} + \sum_{k=0}^{\mathrm{N}} \frac{a_k}{10^k} \leqslant \frac{1}{10^k} + a < a + \epsilon < b$$

et on a bien un rationnel dans $]a\,;\,b[$.

Du coup, l'intervalle $]a+\sqrt{2}\,;\,b+\sqrt{2}[$ contient un rationnel r. Et $r - \sqrt{2}$ est irrationnel et se trouve dans $]a\,;\,b[$. □

Chapitre 11

Suites

11.1 Premières définitions

11.1.1 Rappels

On rappelle qu'une suite u à valeurs réelles est une application $u : \mathbb{N} \longrightarrow \mathbb{R}$. Pour tout entier n, pour exprimer la valeur prise en n par la suite u, on utilise généralement la notation indicielle u_n plutôt que la notation fonctionnelle $u(n)$. Mais ces deux notations sont strictement équivalentes, au choix de l'utilisateur. u_n est alors appelé terme d'indice n de la suite u ; remarquons qu'il s'agit du $n+1$-ème terme de la suite si celle-ci part de 0.

Exemple 11.1.1
u_0 est le premier terme de la suite u ; c'est aussi le terme d'indice 0. u_1 est le deuxième terme, et le terme d'indice 1.

> Une bonne raison pour laquelle on souhaiterait utiliser la notation fonctionnelle peut être trouvée lorsqu'on travaille avec une famille de suites. Par exemple, supposons qu'on étudie 23432 suites en même temps (ou même une infinité de suites) ; on n'a pas envie d'utiliser 23432 symboles différents pour nommer chacune de ces suites. Et du coup, on les appelle u_1, u_2, …, jusqu'à u_{23432}.
>
> Lorsqu'on veut exprimer le terme d'indice n de la suite u_p (avec $1 \leqslant p \leqslant 23432$), on peut écrire $u_{p,n}$ ou bien $u_p(n)$. Cette deuxième notation est plus agréable, dans ce cas, que celle à double indice.

Nous avons déjà vu au moins deux manières de définir une suite :

- **explicitement**, c'est-à-dire que la valeur de u_n est accessible facilement connaissant n ; par exemple,
$$\forall n \in \mathbb{N} \qquad u_n = \frac{1}{n^2+1}$$
- **par récurrence**, c'est-à-dire que chaque terme de la suite est donné en fonction de ses prédécesseurs. Nous avons déjà démontré, dans le cours sur les récurrences, qu'une définition du type
$$\begin{cases} u_0 = a \\ u_{n+1} = f(u_n) \end{cases}$$

est bien posée pour peu que f soit une application de domaine $\mathscr{D}$ telle que $f(\mathscr{D}) \subset \mathscr{D}$.
Ce type de définition ne permet pas en général d'obtenir rapidement les valeurs de u à un indice donné. En effet, pour calculer u_{27}, on doit d'abord calculer u_1 en fonction de u_0, puis u_2 en fonction de u_1, etc.

Il y a d'autres manières de définir des suites, que nous aurons l'occasion de voir en exercice.

Voici maintenant quelques points de vocabulaire :

Définition 11.1.2
Soit $a \in \mathbb{R}$. La suite définie par

$$\forall n \in \mathbb{N} \qquad u_n = a$$

est appelée *suite constante égale à* a.

Définition 11.1.3
Une suite u est dite *positive* si et seulement si tous ses termes sont positifs, c'est-à-dire

$$\forall n \in \mathbb{N} \qquad u_n \geqslant 0$$

Elle est dite *négative* si et seulement si tous ses termes sont négatifs :

$$\forall n \in \mathbb{N} \qquad u_n \leqslant 0$$

On définirait de même une suite *strictement positive* ou *strictement négative*.

Définition 11.1.4
On dit qu'une suite u est *croissante* si et seulement si

$$\forall n \in \mathbb{N} \qquad u_n \leqslant u_{n+1}$$

Elle est dite *décroissante* si et seulement si

$$\forall n \in \mathbb{N} \qquad u_n \geqslant u_{n+1}$$

De même, on pourrait définir les suites *strictement croissantes*, *strictement décroissantes*, ou encore *(strictement) croissantes/décroissantes à partir d'un rang* n_0.

> Une remarque évidente : la croissance d'une suite s'étudie donc *a priori* en étudiant le signe de $u_{n+1} - u_n$ pour tout entier n. Si cette grandeur est toujours positive, u est croissante.
>
> De manière équivalente dans le cas où u ne s'annule pas et ne change pas de signe, on peut étudier le rapport $\frac{u_{n+1}}{u_n}$. Si cette grandeur est toujours supérieure à 1, la suite u est croissante.

Dans la mesure où les suites sont simplement des applications de $\mathbb{N}$ dans $\mathbb{R}$, les définitions usuelles des opérations sur les fonctions s'appliquent. Ainsi, étant données deux suites u et v et un réel λ, on peut parler de

- la somme des suites u et v comme étant la suite $u+v$ dont chaque terme est la somme des termes correspondants de u et v :

$$\forall n \in \mathbb{N} \qquad (u+v)_n = u_n + v_n$$

- le produit des suites u et v comme étant la suite uv dont chaque terme est le produit des termes correspondants de u et v :

$$\forall n \in \mathbb{N} \qquad (uv)_n = u_n v_n$$

- le produit de u par λ comme étant la suite λu dont chaque terme est le produit par λ du terme correspondant de u :

$$\forall n \in \mathbb{N} \qquad (\lambda u)_n = \lambda u_n$$

Enfin, une dernière définition qui sent peut-être moins le rappel que les autres :

Définition 11.1.5
Soient u et v deux suites à valeurs réelles. On dit que *v est extraite de u* si et seulement si il existe une application $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ strictement croissante telle que

$$\forall n \in \mathbb{N} \qquad v_n = u_{\varphi(n)}$$

On peut aussi dire que *v est une sous-suite de u*.

Exemple 11.1.6
Les sous-suites les plus classiques d'une suite donnée u sont celle des termes impairs ou pairs de u. Ainsi, en posant

$$\forall n \in \mathbb{N} \qquad v_n = u_{2n}$$

et

$$\forall n \in \mathbb{N} \qquad w_n = u_{2n+1}$$

v et w sont toutes deux des suites extraites de u. La fonction φ strictement croissante est, dans chaque cas respectif, $n \longmapsto 2n$ et $n \longmapsto 2n+1$.

Au passage, profitons-en pour préciser que le terme suivant u_{2n} dans la suite v est $u_{2(n+1)} = u_{2n+2}$ et non pas u_{2n+1}.

Un autre exemple un peu moins trivial : si u est la suite définie par

$$\forall n \in \mathbb{N}^\star \qquad u_n = \frac{1}{n^2 - 2n}$$

alors la suite définie par

$$\forall n \geqslant 2 \qquad v_n = \frac{1}{n^2 - 1}$$

est extraite de u puisque $v_n = u_{n+1}$.

11.1.2 Représentations d'une suite

Voir cours, pas le courage de faire les dessins.

11.2 Limite d'une suite

11.2.1 Suites convergentes

Notre but est d'exprimer rigoureusement le fait que les termes successifs d'une suite « s'approchent de plus en plus » d'une certaine valeur. De manière à pouvoir définir rigoureusement la notion de limite.

Ainsi, supposons que les termes d'une suite u s'agglomèrent autour d'une valeur ℓ de sorte qu'on souhaite dire que la suite tend vers ℓ. Alors certainement, dans un intervalle de longueur 1 centré en ℓ, tous les termes de u se retrouveront coincés à partir d'une certain rang. Mais cela exprime seulement ce qu'on vient de dire et rien d'autre : tous les termes de u à partir d'un certain rang sont à une distance au maximum 1 de ℓ.

Améliorons donc notre précision : certainement, tous les termes de u, au bout d'un moment, doivent se situer à une distance au plus un millionnième de ℓ. Mais cela ne suffit toujours pas à exprimer proprement la convergence : par exemple, la suite de terme général $1+(-1)^n/1000000$ vérifie cette propriété avec $\ell = 1$ et pourtant elle passe son temps à prendre alternativement les valeurs

$$1+\frac{1}{10^6} \qquad \text{et} \qquad 1-\frac{1}{10^6}$$

Nous allons donc poser la définition suivante :

Définition 11.2.1
Soient u une suite et ℓ un nombre réel. On dit que u *converge vers* ℓ si et seulement si

$$\forall \varepsilon > 0 \quad \exists N \in \mathbb{N} \quad \forall n \geqslant N \qquad |u_n - \ell| \leqslant \varepsilon$$

Dans ce cas, on dit que ℓ est une limite de u.

En Français : on requiert que, quelle que soit la taille ε de l'intervalle qu'on considère autour de ℓ, tous les termes de la suite u s'y retrouvent coincés à partir d'un certain rang N (qui dépend évidemment de ε).

Avant de donner des exemples, montrons que ce ℓ, candidat à être une limite, est unique :

Proposition 11.2.2
*Soient u une suite et ℓ, ℓ' deux nombres réels. Si u converge à la fois vers ℓ et ℓ', alors $\ell = \ell'$. On dira alors que ℓ est **la** limite de u, ce qu'on notera*

$$\lim_{n\to\infty} u_n = \ell \qquad \textit{ou bien} \qquad \lim_{\infty} u = \ell \qquad \textit{ou encore} \qquad u_n \xrightarrow[n\to\infty]{} \ell$$

> En d'autres termes, si une suite admet des limites, celles-ci sont égales : il y a une et une seule limite possible pour la suite u.

Preuve : Donnons-nous un nombre réel $\varepsilon > 0$. Comme u converge vers ℓ, on sait qu'il existe un entier N_1 tel que

$$\forall n \geqslant N_1 \qquad |u_n - \ell| \leqslant \frac{\varepsilon}{2}$$

De même, puisque u converge vers ℓ', il existe un entier N_2 tel que

$$\forall n \geqslant N_2 \qquad |u_n - \ell'| \leqslant \frac{\varepsilon}{2}$$

L'entier $N = \text{Max}(N_1, N_2)$ est supérieur à la fois à N_1 et N_2 donc

$$|u_N - \ell| \leqslant \frac{\varepsilon}{2} \qquad \text{et} \qquad |u_N - \ell'| \leqslant \frac{\varepsilon}{2}$$

Par suite, $$|\ell - \ell'| = |\ell - u_N + u_N - \ell'| \leqslant |\ell - u_N| + |u_N - \ell'| \leqslant \varepsilon$$

simplement d'après l'inégalité triangulaire. On a donc démontré que

$$\forall \varepsilon > 0 \qquad |\ell - \ell'| \leqslant \varepsilon$$

D'après un théorème vu dans le cours sur les fondements de l'analyse, on a $\ell - \ell' = 0$, c'est-à-dire $\ell = \ell'$. □

Des exemples simples de démonstration de la convergence de suites à l'aide de la définition seront faits en TDs ; bien évidemment, on aimerait avoir à y recourrir aussi peu souvent que possible et nous allons développer des outils permettant d'assurer simplement la convergence de suites.

11.2.2 Premières propriétés

Proposition 11.2.3
Soient u une suite et ℓ un nombre réel. La suite u converge vers ℓ si et seulement si la suite $u - \ell$ converge vers 0.

Preuve : Trivial. □

Ce premier résultat est trivial, mais utile dans la mesure où il est parfois (souvent ?) plus simple de montrer une convergence vers 0.

Proposition 11.2.4
Soit u une suite convergente de limite ℓ. Toutes les sous-suites de u convergent vers ℓ.

Preuve : Soit φ une application de $\mathbb{N}$ dans lui-même, strictement croissante.

La preuve repose sur le fait que $\varphi(n) \geqslant n$ pour tout entier n. Ceci se démontre aisément par récurrence. En effet, $\varphi(0)$ est entier donc supérieur à 0. Et si on suppose que $\varphi(n) \geqslant n$, alors par croissance stricte de φ, on a $\varphi(n+1) > \varphi(n) \geqslant n$. Comme $\varphi(n+1)$ est un entier, s'il est strictement supérieur à n, c'est qu'il est supérieur à $n+1$. Ainsi, on a montré par récurrence que

$$\forall n \in \mathbb{N} \qquad \varphi(n) \geqslant n$$

Maintenant, passons à la preuve proprement dite. Soit ε un nombre réel strictement positif. Puisque u converge vers ℓ, on sait qu'il existe un entier, qu'on appelle N, tel que

$$\forall n \geqslant \mathrm{N} \qquad |u_n - \ell| \leqslant \varepsilon$$

Par suite, si $n \geqslant \mathrm{N}$, on a $\varphi(n) \geqslant n \geqslant \mathrm{N}$ et on sait donc que $|u_{\varphi(n)} - \ell| \leqslant \varepsilon$. On a donc montré

$$\forall \varepsilon > 0 \quad \exists \mathrm{N} \in \mathbb{N} \quad \forall n \geqslant \mathrm{N} \qquad |u_{\varphi(n)} - \ell| \leqslant \varepsilon$$

La suite extraite $(u_{\varphi(n)})_{n\in\mathbb{N}}$ converge vers ℓ. □

L'utilité de cette proposition réside surtout dans sa contre-apposée : pour montrer qu'une suite ne converge pas, il suffit d'en trouver deux sous-suites qui convergent vers des limites différentes. Ou bien une sous-suite qui ne converge pas.

Exemple 11.2.5
Posons $u_n = (-1)^n$ pour tout entier n. On a alors

$$\forall n \in \mathbb{N} \qquad u_{2n} \qquad \text{et} \qquad u_{2n+1} = -1$$

Les suites extraites $(u_{2n})_{n\in\mathbb{N}}$ et $(u_{2n+1})_{n\in\mathbb{N}}$ convergent vers des limites différentes donc u ne converge pas.

Proposition 11.2.6
Soient u et v deux suites et ℓ un nombre réel. Soit $n_0 \in \mathbb{N}$. On suppose que

$$\forall n \geqslant n_0 \qquad u_n = v_n$$

Alors u converge vers ℓ si et seulement si v converge vers ℓ.

Preuve : C'est très simple. Supposons que u converge vers ℓ. Si ε est un nombre réel strictement positif, on sait qu'il existe N_1 tel que

$$\forall n \geqslant N_1 \qquad |u_n - \ell|$$

Posons alors $N = \text{Max}(N_1, n_0)$ de sorte que

$$\forall n \geqslant N_1 \qquad v_n = u_n$$

et $$\forall n \geqslant N_1 \qquad |u_n - \ell| \leqslant \varepsilon$$

Alors $$\forall n \geqslant N_1 \qquad |v_n - \ell| \leqslant \varepsilon$$

et v converge vers ℓ. De même pour la réciproque. □

Cette propriété démontre le caractère asymptotique de la notion de limite : la convergence d'une suite ne dépend vraiment que des valeurs de celle-ci prises pour de grands indices. Si deux suites ont leurs 17490 premières valeurs qui diffèrent, mais coincident après cela, elles convergeront bien évidemment simultanément.

Théorème 11.2.7
Toute suite convergente est bornée.

Preuve : Soit u une suite convergente, de limite ℓ. Alors il existe un entier N tel que

$$\forall n \geqslant N \qquad |u_n - \ell| \leqslant 1$$

Donc $$\forall n \geqslant N \qquad |u_n| \leqslant 1 + |\ell|$$

Si on note M le maximum de l'ensemble fini $\{u_0, \ldots, u_{N-1}, |\ell| + 1\}$, on a alors d'après ce qui précède

$$\forall n \in \mathbb{N} \qquad |u_n| \leqslant M$$

u est bornée. □

Théorème 11.2.8
Soit u une suite convergente dont la limite est strictement positive. Alors tous les termes de u sont strictement positifs à partir d'un certain rang.

Preuve : Notons $\ell > 0$ la limite de u. D'après la définition de la convergence, il existe un entier N tel que

$$\forall n \geqslant N \qquad |u_n - \ell| \leqslant \frac{\ell}{2}$$

donc $$\forall n \geqslant N \qquad \ell - \frac{\ell}{2} \leqslant u_n \leqslant \ell + \frac{\ell}{2}$$

et en particulier $$\forall n \geqslant N \qquad 0 < \frac{\ell}{2} \leqslant u_n$$

Tous les termes de u au-delà de u_N sont strictement positifs. □

Le théorème suivant régit les « passages à la limite dans les inégalités » :

Théorème 11.2.9
Soient u une suite et M un nombre réel tel que

$$\forall n \in \mathbb{N} \qquad u_n \leqslant M$$

Si u converge, alors $\lim u \leqslant M$.

Preuve : Notons ℓ la limite de u. Soit ε strictement positif fixé. On sait qu'il existe un entier N tel que $|u_N - \ell| \leqslant \varepsilon$. Par suite,

$$\ell - u_N \leqslant \varepsilon$$

et

$$\ell \leqslant \varepsilon + u_N \leqslant \varepsilon + M$$

Comme cela est vrai pour tout $\varepsilon > 0$, on a obtenu que ℓ minore $[M ; +\infty[$. Donc ℓ est inférieur à l'inf de cet ensemble, qui est M. □

11.2.3 Suites tendant vers l'infini

Définition 11.2.10
Soit u une suite. On dit qu'elle tend vers $+\infty$ si et seulement si

$$\forall M > 0 \quad \exists N \in \mathbb{N} \quad \forall n \geqslant N \qquad u_n \geqslant M$$

On dit qu'elle tend vers $-\infty$ si et seulement si

$$\forall M < 0 \quad \exists N \in \mathbb{N} \quad \forall n \geqslant N \qquad u_n \leqslant M$$

Théorème 11.2.11
Toute suite tendant vers $+\infty$ est minorée. Toute suite tendant vers $-\infty$ est majorée.

Preuve : Supposons que u tende vers $+\infty$. On sait qu'il existe un entier N tel que

$$\forall n \geqslant N \qquad u_n \geqslant 26$$

En posant $M = \text{Min}\{u_0, \ldots, u_{N-1}, 26\}$, on voit que M minore u.

De même pour la seconde partie du théorème. □

Théorème 11.2.12
Soient u une suite tendant vers $+\infty$ (resp. $-\infty$) et v une suite minorée (resp. majorée). Alors $u+v$ tend vers $+\infty$ (resp. $-\infty$).

Preuve : Notons α un minorant de v :

$$\forall n \in \mathbb{N} \qquad v_n \geqslant \alpha$$

Soit M un nombre réel strictement positif. Puisque la suite u tend vers $+\infty$, il existe un entier N tel que

$$\forall n \geqslant N \qquad u_n \geqslant M - \alpha$$

Du coup

$$\forall n \geqslant N \qquad u_n + v_n \geqslant M$$

et la suite $u+v$ tend vers $+\infty$. De même pour le cas où $u \longrightarrow -\infty$ et v est majorée. □

Théorème 11.2.13
Soient u une suite tendant vers $+\infty$ et v une suite minorée (resp. majorée) par un nombre strictement positif (resp. négatif). Alors uv tend vers $+\infty$.

Preuve : Soit m un minorant strictement de v :

$$\forall n \in \mathbb{N} \qquad u_n \geqslant m > 0$$

Soit M un nombre réel strictement positif. Comme u tend vers $+\infty$, il existe un entier N tel que

$$\forall n \geqslant \mathrm{N} \qquad u_n \geqslant \frac{\mathrm{M}}{m}$$

Par suite,
$$\forall n \geqslant \mathrm{N} \qquad u_n v_n \geqslant \frac{\mathrm{M}}{m} m = \mathrm{M}$$

et u tend vers $+\infty$. □

Pas grand chose à ajouter ; il est clair que les suites tendant vers l'infini ne sont pas bornées, simplement d'après la définition. Mais la réciproque n'est pas vraie : il y a des suites non bornées qui ne tendent pas $+\infty$ ou $-\infty$. Par exemple, la suite de terme général $(-1)^n n$.

11.3 Calculs de limites

11.3.1 Opérations sur les limites

Plutôt que d'énoncer une batterie de théorèmes, voici plusieurs tableaux résumant les opérations sur les limites.

- **Somme :**

	$\lim u = \ell \in \mathbb{R}$	$\lim u = +\infty$	$\lim u = -\infty$	u bornée
$\lim v = \ell' \in \mathbb{R}$	$\ell + \ell'$	$+\infty$	$-\infty$	??
$\lim v = +\infty$	$+\infty$	$+\infty$	??	$+\infty$
$\lim v = -\infty$	$-\infty$	??	$-\infty$	$-\infty$
v bornée	??	$+\infty$	$-\infty$	??

Tous les cas sont des conséquences immédiates des théorèmes précédents, sauf celui où u converge vers ℓ et v converge vers ℓ'. Dans ce cas, montrons que $u+v$ converge vers $\ell+\ell'$. Soit ε un nombre strictement positif fixé. Comme u et v convergent, on sait qu'il existe des entiers N_1 et N_2 tels que

$$\forall n \geqslant \mathrm{N}_1 \qquad |u_n - \ell| \leqslant \frac{\varepsilon}{2}$$

et
$$\forall n \geqslant \mathrm{N}_2 \qquad |v_n - \ell| \leqslant \frac{\varepsilon}{2}$$

Posons $\mathrm{N} = \mathrm{Max}(\mathrm{N}_1, \mathrm{N}_2)$ de sorte que N soit à la fois supérieur à N_1 et N_2. D'après l'inégalité triangulaire,

$$\forall n \geqslant \mathrm{N} \qquad |u_n + v_n - (\ell + \ell')| \leqslant |u_n - \ell| + |v_n - \ell'| \leqslant \varepsilon$$

Ce qui montre que $u+v$ converge vers $\ell+\ell'$.

- **Produit :**

	$\lim u = \ell \in \mathbb{R}^\star$	$\lim u = 0$	$\lim u = +\infty$	$\lim u = -\infty$
$\lim v = \ell' \in \mathbb{R}^\star$	$\ell\ell'$	0	$\text{sgn}(\ell')\infty$	$-\text{sgn}(\ell')\infty$
$\lim v = 0$	0	0	??	??
$\lim v = +\infty$	$\text{sgn}(\ell)\infty$	??	$+\infty$	$-\infty$
$\lim v = -\infty$	$-\text{sgn}(\ell)\infty$	??	$-\infty$	$+\infty$

La plupart des cas découlent de ce qui a été fait dans les deux derniers paragraphe, sauf ceux où u et v convergent toutes les deux.
Supposons donc que $u_n \xrightarrow[n\to\infty]{} \ell$ et $v_n \xrightarrow[n\to\infty]{} \ell'$. On ne fait aucune supposition quant à la nullité éventuelle de ces limites. On a alors

$$\forall n \in \mathbb{N} \qquad u_n v_n = (u_n - \ell + \ell) v_n = (u_n - \ell) v_n + \ell v_n$$

et donc

$$\forall n \in \mathbb{N} \qquad u_n v_n - \ell\ell' = (u_n - \ell) v_n + \ell(v_n - \ell')$$

La suite v converge donc est bornée ; soit M tel que

$$\forall n \in \mathbb{N} \qquad |v_n| \leqslant \mathrm{M}$$

On a

$$\forall n \in \mathbb{N} \qquad |u_n v_n - \ell\ell'| \leqslant |u_n - \ell|\,\mathrm{M} + |\ell|\,|v_n - \ell'|$$

Fixons $\varepsilon > 0$. Les suites u et v convergent donc il existe des entiers N_1 et N_2 tels que

$$\forall n \geqslant \mathrm{N}_1 \qquad |u_n - \ell| \leqslant \frac{\varepsilon}{2\mathrm{M}}$$

et

$$\forall n \geqslant \mathrm{N}_2 \qquad |v_n - \ell'| \leqslant \frac{\varepsilon}{2(|\ell| + 1)}$$

Posons $\mathrm{N} = \mathrm{Max}(\mathrm{N}_1, \mathrm{N}_2)$, de sorte que N soit supérieur à la fois à N_1 et N_2. Alors

$$\forall n \geqslant \mathrm{N} \qquad |u_n v_n - \ell\ell'| \leqslant \varepsilon$$

ce qui démontre que $u_n v_n \xrightarrow[n\to\infty]{} \ell\ell'$.

- **Rapport :** Nous aurons besoin d'un lemme :

Lemme 11.3.1
Soit u une suite convergente de limite $\ell \neq 0$. Alors les termes de u ne sont pas nuls à partir d'un certain rang n_0 ; de plus, $(1/u_n)_{n \geqslant n_0}$ converge vers $1/\ell$.
Si u converge vers $\pm\infty$, alors les termes de u ne sont pas nuls à partir d'un certain rang n_0 ; de plus, $(1/u_n)_{n \geqslant n_0}$ converge vers 0.

Preuve : Commençons par le cas où u converge vers une limite ℓ non nulle. Alors $|u| - |\ell/2|$ converge vers $|\ell/2| > 0$ et d'après le **théorème 2.8**, les termes de la suite $|u| - |\ell/2|$ sont tous strictement positifs à partir d'un certain rang que l'on note n_0. On a donc

$$\forall n \geqslant n_0 \qquad |u_n| - \frac{|\ell|}{2} > 0$$

donc

$$\forall n \geqslant n_0 \qquad |u_n| > \frac{|\ell|}{2}$$

Le rapport $1/u_n$ est donc parfaitement défini dès que n est supérieur à n_0. Alors

$$\forall n \geqslant n_0 \qquad \left|\frac{1}{u_n} - \frac{1}{\ell}\right| = \frac{|\ell - u_n|}{|\ell u_n|} \leqslant 2|\ell - u_n|$$

et le fait que u converge vers ℓ permet de conclure.
Maintenant, si u tend vers $+\infty$ on sait qu'il existe n_0 tel que

$$\forall n \geqslant n_0 \qquad u_n \geqslant 1$$

donc on peut former le rapport $1/u_n$ à partir du rang n_0. Montrons que $(1/u_n)_{n\geqslant n_0}$ tend vers 0. Soit $\varepsilon > 0$ donné. Comme u tend vers $+\infty$, il existe un entier N tel que

$$\forall n \geqslant \mathrm{N} \qquad u_n \geqslant \frac{1}{\varepsilon} > 0$$

de sorte que

$$\forall n \geqslant \mathrm{N} \qquad 0 \leqslant \frac{1}{u_n} \leqslant \varepsilon$$

ce qui achève la démonstration.
Pour le cas où u tend vers $-\infty$, il suffit d'appliquer le résultat qu'on vient de démontrer à $-u$.
□

On en déduit le tableau qui régit les rapports de suites :

	$\lim u = \ell \in \mathbb{R}$	$\lim u = +\infty$	$\lim u = -\infty$
$\lim v = \ell' \in \mathbb{R}^\star$	$\dfrac{\ell}{\ell'}$	$\mathrm{sgn}(\ell')\infty$	$-\mathrm{sgn}(\ell')\infty$
$\lim v = +\infty$	0	??	??
$\lim v = -\infty$	0	??	??

11.3.2 Composition d'une suite par une fonction

Il y a essentiellement un théorème à connaître. Il est pour l'instant admis, nous le démontrerons dans le chapitre suivant :

Théorème 11.3.2
Soient u une suite et f une fonction. On suppose que u tend vers une limite finie ou infinie, qu'on note ℓ, et que f admet une limite en ℓ. Alors

$$\lim_{n\to\infty} f(u_n) = f(\ell)$$

En particulier, ce théorème nous dit que si u est une suite définie par une relation du type $u_n = f(n)$, et si on sait que f a une limite en $+\infty$, alors u converge vers $\lim\limits_{x\to\infty} f(x)$.

Il est également très utile pour déterminer les limites potentielles des suites récurrentes. Supposons qu'on étudie une suite du type $u_{n+1} = f(u_n)$ où u_0 est donné et f est une fonction qui admet une limite en chaque point. Et supposons qu'on sache que u converge vers un réel ℓ ; d'après le théorème précédent,

$$\lim_{n\to\infty} f(u_n) = f(\ell)$$

mais aussi

$$\lim_{n\to\infty} f(u_n) = \lim_{n\to\infty} u_{n+1} = \ell$$

Donc $f(\ell) = \ell$: les limites possibles de notre suite récurrente sont les points fixes de la fonction f.

11.4 Théorèmes d'existence de limites

11.4.1 Théorème de la limite monotone

Théorème 11.4.1
Toute suite croissante majorée converge. Toute suite décroissante minorée converge.

Preuve : Soit u une suite croissante majorée. Le nombre $\ell = \text{Sup}\{u_n \mid n \in \mathbb{N}\}$ existe, d'après la propriété de la borne supérieure. Et d'après la caractérisation de ℓ vue dans le chapitre précédent, on sait que si ε est un nombre strictement positif donné, il existe un entier N tel que

$$\ell - \varepsilon \leqslant u_N \leqslant \ell$$

Or, la suite u est croissante donc

$$\forall n \geqslant N \qquad \ell - \varepsilon \leqslant u_N \leqslant u_n$$

et u est majorée par ℓ. On a ainsi montré que

$$\forall n \geqslant N \qquad \ell - \varepsilon \leqslant u_n \leqslant \ell$$

donc

$$\forall n \geqslant N \qquad |u_n - \ell| \leqslant \varepsilon$$

Ainsi, u converge vers $\ell = \text{Sup}\{u_n \mid n \in \mathbb{N}\}$.

Si u est décroissante minorée, on montre de même qu'elle converge et que sa limite est $\text{Inf}\{u_n \mid n \in \mathbb{N}\}$. □

11.4.2 Théorème des gendarmes

Théorème 11.4.2
Soient u, v et w trois suites telles que

$$\forall n \in \mathbb{N} \qquad u_n \leqslant v_n \leqslant w_n$$

On suppose de plus que u et w convergent vers la même limite ℓ. Alors v converge vers ℓ.

Preuve : Comme u et w convergent vers ℓ, on sait, étant donné $\varepsilon > 0$ quelconque, qu'il existe deux entiers N_1 et N_2 tels que

$$\forall n \geqslant N_1 \qquad |u_n - \ell| \leqslant \varepsilon$$

et

$$\forall n \geqslant N_2 \qquad |w_n - \ell| \leqslant \varepsilon$$

Si on pose $N = \text{Max}(N_1, N_2)$, de sorte que N soit supérieur à la fois à N_1 et N_2, on a en particulier

$$\forall n \geqslant N \qquad u_n - \ell \geqslant -\varepsilon \qquad \text{et} \qquad w_n - \ell \leqslant \varepsilon$$

d'où

$$\forall n \geqslant N \qquad -\varepsilon \leqslant u\_\ell \leqslant v_n - \ell \leqslant w_n - \ell \leqslant \varepsilon$$

Autrement dit,

$$\forall n \geqslant N \qquad |v_n - \ell| \leqslant \varepsilon$$

ce qui achève la démonstration. □

Corollaire 11.4.3
Le produit d'une suite qui converge vers 0, par une suite bornée, tend vers 0.

Preuve : Soient u et v deux suites, avec u bornée et v tendant vers 0. Comme u est bornée, il existe un réel $M > 0$ tel que

$$\forall n \in \mathbb{N} \qquad |u_n| \leqslant M$$

Par suite, $$\forall n \in \mathbb{N} \qquad |u_n v_n| \leqslant M|v_n|$$

Comme la suite $(Mv_n)_{n\in\mathbb{N}}$ tend vers 0, le théorème des gendarmes permet de conclure que uv tend vers 0. □

11.4.3 Théorème des suites adjacentes

Théorème 11.4.4
Soient u et v deux suites, telles que

1. *u croît ;*
2. *v décroît ;*
3. *$u \leqslant v$;*
4. *$u - v$ tend vers 0.*

Alors u et v convergent vers la même limite.

Des suites qui vérifient les hypothèses de ce théorème sont dites adjacentes.

Preuve : Puisque u croît, on a en particulier

$$\forall n \in \mathbb{N} \qquad u_0 \leqslant u_n \leqslant v_n$$

donc v est minorée. D'après le théorème de la limite monotone, v converge ; notons ℓ' sa limite.

De même, puisque v décroît, on a

$$\forall n \in \mathbb{N} \qquad u_n \leqslant v_n \leqslant v_0$$

donc u est majorée. D'après le théorème de la limite monotone, u converge ; notons ℓ sa limite.

D'après le théorème d'addition des limites, on a

$$0 = \lim_{n\to\infty} (u_n - v_n) = \ell - \ell'$$

donc $\ell = \ell'$: u et v convergent, vers la même limite. □

11.4.4 Théorème de Bolzano-Weiertstraß

Théorème 11.4.5
Toute suite bornée admet des sous-suites convergentes.

Preuve : Soit u une suite bornée ; notons m un minorant. Pour tout entier n, on note A_n l'ensemble des termes de la suite u d'indice supérieur à n :

$$A_n = \{u_k \mid k \geqslant n\}$$

Bien entendu, A_n n'est pas vide ; et il est majoré puisque u est majorée. D'après la propriété de la borne supérieure, A_n admet un supremum, qu'on note v_n :

$$\forall n \in \mathbb{N} \qquad v_n = \operatorname{Sup} A_n = \operatorname*{Sup}_{k \geqslant n} u_k$$

On a évidemment $v_n \geqslant u_n \geqslant m$ et v est donc minorée. De plus, comme $A_n \subset A_{n+1}$, on sait que

$$v_n = \operatorname{Sup} A_n \leqslant \operatorname{Sup} A_{n+1} = v_{n+1}$$

donc la suite v est décroissante. D'après le théorème de la limite monotone, v converge vers une limite qu'on note ℓ.

Montrons que u admet une sous-suite qui converge vers ℓ. Il nous faut construire cette sous-suite et on le fait par récurrence. On pose $\varphi(0) = 0$ et on définit pour tout entier n la propriété $\mathscr{P}(n)$: « Il existe des entiers $\varphi(0) < \varphi(1) < \cdots < \varphi(n)$ tels que

$$\forall k \in [\![1\,;n]\!] \qquad v_{\varphi(k-1)+1} - \frac{1}{k+1} \leqslant u_{\varphi(k)} \leqslant v_{\varphi(k-1)+1}$$ □

$\mathscr{P}(0)$ est vraie : il n'y a rien à prouver dans ce cas-là. Donc on prouve que $\mathscr{P}$ est héréditaire : supposons $\mathscr{P}(n)$ vraie. La seule chose à faire, c'est construire $\varphi(n+1)$ puisque les $n+1$ premières valeurs sont déjà données par $\mathscr{P}(n)$. C'est simple : par définition,

$$v_{\varphi(n)+1} = \operatorname{Sup}\{u_k \mid k \geqslant \varphi(n)+1\}$$

donc d'après la caractérisation de la borne supérieure d'un ensemble, il existe $k \geqslant \varphi(n)+1$, entier, tel que

$$v_{\varphi(n)+1} - \frac{1}{n+2} \leqslant u_k \leqslant v_{\varphi(n)+1}$$

Il suffit de définir $\varphi(n+1)$ comme étant égal à cet entier k et c'est gagné.

Puisque $\mathscr{P}(n)$ est vraie pour tout entier n, on a construit une application $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$, strictement croissante, telle que

$$\forall n \in \mathbb{N}^\star \qquad v_{\varphi(n-1)+1} - \frac{1}{n+1} \leqslant u_{\varphi(n)} \leqslant v_{\varphi(n-1)+1}$$

Or, la suite v converge vers ℓ donc la suite extraite $(v_{\varphi(n-1)+1})_{n\in\mathbb{N}}$ converge aussi vers ℓ. D'après le théorème des gendarmes, $(u_{\varphi(n)})_{n\in\mathbb{N}}$ converge vers ℓ. □

11.5 Comparaison de suites

Le but de ce paragraphe est d'affiner les informations qu'on a sur une suite. Ainsi, si une suite converge vers 0, on aimerait en plus savoir « de quelle manière elle tend vers 0 ». Il est clair que les suites de terme général $1/n$ et $1/2^n$ ne tendent pas vers 0 à la même vitesse. Bref, nous allons donner un cadre rigoureux à la notion intuitive de « vitesse de convergence ».

11.5.1 Négligeabilité

Définition 11.5.1
Soient u et v deux suites. On dit que v *est négligeable devant* u, ce qu'on notera $v = o(u)$, si et seulement si

$$\forall \varepsilon > 0 \quad \exists N \in \mathbb{N} \quad \forall n \geqslant N \qquad |v_n| \leqslant \varepsilon |u_n|$$

Définition 11.5.2
Soient u, v et w trois suites. On notera $u_n = v_n + o(w_n)$ pour dire que

$$u_n - v_n = o(w_n)$$

Théorème 11.5.3
Soient u et v deux suites, avec u à termes non nuls. On a

$$v = o(u) \iff \lim_{n\to\infty} \frac{v_n}{u_n} = 0$$

Preuve : C'est clair au vu de la définition. □

Exemple 11.5.4
Voici des exemples simples :

$$n^3 = o(n^4) \quad \text{puisque} \quad \frac{n^3}{n^4} = \frac{1}{n} \xrightarrow[n\to\infty]{} 0$$

$$\frac{1}{n^3} = o\Big(\frac{1}{n}\Big) \quad \text{puisque} \quad \frac{n}{n^3} = \frac{1}{n^2} \xrightarrow[n\to\infty]{} 0$$

Ces deux relations nous disent en substance que n^3 tend vers l'infini à une vitesse négligeable par rapport à n^4 ; ou bien que $\frac{1}{n}$ tend vers 0 infiniment moins vite que $\frac{1}{n^3}$.

Plus basique maintenant : si u converge vers une limite non nulle, on a $u_n = \ell + o(1)$. Si u converge vers 0, on a $u_n = o(1)$.

Voici une batterie de théorèmes qui régissent les règles d'utilisation des petits « o » ; la preuve est triviale, il suffit d'écrire les définitions et tout marche très bien.

Théorème 11.5.5

1. *Soient u et v deux suites, soit $\lambda \in \mathbb{R}^\star$. On suppose que $u_n = o(v_n)$. Alors $\lambda u_n = o(v_n)$ et $u_n = o(\lambda v_n) = o(v_n)$.*
2. *Soient u, v et w trois suites telles que*

   $$u_n = o(w_n) \quad \text{et} \quad v_n = o(w_n)$$

   Alors $$u_n + v_n = o(v_n)$$
3. *Soient u, v et w trois suites. On suppose que*

   $$u_n = o(v_n) \quad \text{et} \quad v_n = o(w_n)$$

   Alors $$u_n = o(w_n)$$
4. *Soient u, v, w, x quatre suites, telles que*

   $$u_n = o(v_n) \quad \text{et} \quad w_n = o(x_n)$$

   Alors $$u_n w_n = o(v_n x_n)$$
5. *Soient u et v deux suites telles que $u_n = o(v_n)$. Si $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ est strictement croissante, alors $u_{\varphi(n)} = o(v_{\varphi(n)})$.*

En Français, ce théorème nous dit successivement que :

1. Si on a une relation de négligeabilité, multiplier par un nombre réel non nul ne change rien.
2. Si deux suites sont négligeables devant **une même** troisième, leur somme est négligeable devant celle-ci.
3. La négligeabilité se transmet transitivement.
4. Multiplier des relations de négligeabilité membre-à-membre se fait sans problème.
5. « Extraire » une sous-relation d'une relation de négligeabilité ne pose aucun problème.

> En revanche, il est important de ne jamais appliquer le résultat FAUX suivant : « On peut ajouter membre à membre des relations de négligeabilité ».
> Voici un contre-exemple simple. On a
> $$n+1=o(n^2+4) \qquad \text{et} \qquad -n=o(-n^2)$$
> Si la phrase entre guillemets ci-dessus était vraie, on aurait
> $$n+1-n=o(n^2+4-n^2)=o(4)$$
> et ce n'est clairement pas le cas.

Voici enfin les relations de négligeabilité classiques à connaître :

$$\forall \alpha \in \mathbb{R} \quad \forall \beta > 0 \qquad \ln^\alpha n = o(n^\beta)$$

$$\forall \alpha < \beta \qquad n^\alpha = o(n^\beta)$$

$$\forall a, b > 0 \quad \text{avec} \quad a < b \qquad a^n = o(b^n)$$

$$\forall a, \alpha \in \mathbb{R} \quad \text{avec} \quad a > 1 \qquad n^\alpha = o(a^n)$$

$$\forall a > 1 \qquad a^n = o(n!)$$

11.5.2 Équivalents

Définition 11.5.6
Soient u et v deux suites. On dit qu'elles sont *équivalentes*, ce qu'on note $u_n \sim v_n$, si et seulement si

$$\forall \varepsilon > 0 \quad \exists N \in \mathbb{N} \quad \forall n \geqslant N \qquad |u_n - v_n| \leqslant \varepsilon v_n$$

En vue du paragraphe précédent, on voit que si u et v ne s'annulent pas, alors

$$\begin{aligned} u_n \sim v_n &\iff u_n - v_n = o(v_n) \\ &\iff \left(\frac{u_n - v_n}{v_n}\right)_{n\in\mathbb{N}} \text{converge vers } 0 \\ &\iff \left(\frac{u_n}{v_n}\right)_{n\in\mathbb{N}} \text{converge vers } 1 \end{aligned}$$

C'est cette dernière caractérisation qui sera, en pratique, la plus utile pour montrer que deux suites sont équivalentes. On peut aussi pousser notre chaîne d'équivalences un peu plus loin :

$$u_n \sim v_n \iff \lim_{n\to\infty} \frac{u_n}{v_n} = 1 \iff \lim_{n\to\infty} \frac{v_n}{u_n} = 1 \iff v_n \sim u_n$$

On voit ainsi que la terminologie est bien choisie : en effet, on dit « les suites sont équivalentes », ce qui semble impliquer qu'aucune des deux suites ne joue un rôle particulier par rapport à l'autre. C'est bien le cas, puisque $u_n \sim v_n$ est la même chose que $v_n \sim u_n$.

Cette notion signifie intuitivement que les suites u et v se comportent « de la même manière » quand n croît. Ou du moins, de manières suffisamment similaires pour que leur rapport soit environ égal à 1 pour de grandes valeurs de n. Mais cette explication n'est correcte que si les suites u et v ne s'annulent pas. Rendons-la plus précise dans le cas général.

Théorème 11.5.7
Soient u et v deux suites telles que $u \sim v$.

- *On a aussi $v \sim u$.*
- *u converge si et seulement si v converge et leurs limites sont alors égales.*
- *u tend vers $+\infty$ si et seulement v tend vers $+\infty$.*
- *Même chose avec $-\infty$.*
- *u diverge si et seulement si v diverge.*

Preuve : Supposons que $u \sim v$. Soient $\varepsilon \in]0\,;1[$ et $\alpha = \frac{1-\varepsilon}{\varepsilon}$. On a bien $\alpha > 0$ et par suite, il existe $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N \qquad |u_n - v_n| \leqslant \alpha |v_n|$$

donc
$$\forall n \geqslant N \qquad |v_n| - |u_n| \leqslant |u_n - v_n| \leqslant \alpha |v_n|$$

et
$$\forall n \geqslant N \qquad |v_n| \leqslant \frac{|u_n|}{1-\alpha} = \varepsilon |u_n|$$

On a donc prouvé

$$\forall \varepsilon \in]0\,;1[\quad \exists N \in \mathbb{N} \quad \forall n \geqslant N \qquad |u_n - v_n| \leqslant \varepsilon |u_n|$$

ce qui montre que $v \sim u$.

Maintenant, on suppose que u converge vers un $\ell \in \mathbb{R}$. On fixe $\varepsilon > 0$. Puisque $v \sim u$, on sait qu'il existe $N > 0$ tel que

$$\forall n \geqslant N \qquad |u_n - v_n| \leqslant \varepsilon |u_n|$$

et
$$\forall n \geqslant N \qquad |u_n - \ell| \leqslant \varepsilon$$

Alors
$$\forall n \geqslant N \qquad |v_n - \ell| \leqslant |v_n - u_n| + |u_n - \ell| \leqslant \varepsilon + \varepsilon |u_n|$$

Enfin, la suite u est bornée parce qu'elle converge. On note

$$M = \sup_{n\in\mathbb{N}} |u_n|$$

et on a
$$\forall n \geqslant N \qquad |v_n - \ell| \leqslant (1+M)\varepsilon$$

Ceci prouve que v converge vers ℓ.

De la même manière, on prouve que si v converge, alors u converge vers la même limite.

Du coup, par contre-apposée, si u diverge, v diverge ; et vice-versa.

Enfin, par contre-apposée, u diverge si, et seulement si, v diverge. □

Exemple 11.5.8
Quelques exemples simples pour commencer : on a $n^2+3n+1 \sim n^2$ ou bien $\frac{1}{n}+\frac{2}{5n^4} \sim \frac{1}{n}$.

Voici maintenant une liste d'équivalents classiques ; dans ce qui suit, u est une suite qui tend vers 0. Et ces formules sont des conséquences immédiates de formules classiques sur les fonctions usuelles.

$$(1+u_n)^\alpha - 1 \sim \alpha u_n \quad \text{ou bien} \quad (1+u_n)^\alpha = 1+\alpha u_n + o(u_n)$$
$$\ln(1+u_n) \sim u_n \quad \text{ou bien} \quad \ln(1+u_n) = u_n + o(u_n)$$
$$e^{u_n} - 1 \sim u_n \quad \text{ou bien} \quad e^{u_n} = 1 + u_n + o(u_n)$$
$$\sin u_n \sim u_n \quad \text{ou bien} \quad \sin u_n = u_n + o(u_n)$$
$$\cos u_n \sim 1 \quad \text{ou bien} \quad \cos u_n = 1 + o(1)$$
$$1-\cos u_n \sim \frac{u_n^2}{2} \quad \text{ou bien} \quad \cos u_n = 1 - \frac{u_n^2}{2} + o(u_n^2)$$
$$\tan u_n \sim u_n \quad \text{ou bien} \quad \tan u_n = u_n + o(u_n)$$
$$\arcsin u_n \sim u_n \quad \text{ou bien} \quad \arcsin u_n = u_n + o(u_n)$$
$$\arccos u_n \sim \frac{\pi}{2} \quad \text{ou bien} \quad \arccos u_n = \frac{\pi}{2} + o(1)$$
$$\arccos u_n - \frac{\pi}{2} \sim -u_n \quad \text{ou bien} \quad \arccos u_n = \frac{\pi}{2} - u_n + o(u_n)$$
$$\arctan u_n \sim u_n \quad \text{ou bien} \quad \arctan u_n = u_n + o(u_n)$$
$$\operatorname{sh} u_n \sim u_n \quad \text{ou bien} \quad \operatorname{sh} u_n = u_n + o(u_n)$$
$$\operatorname{ch} u_n \sim 1 \quad \text{ou bien} \quad \operatorname{ch} u_n = 1 + o(1)$$
$$\operatorname{ch} u_n - 1 \sim \frac{u_n^2}{2} \quad \text{ou bien} \quad \operatorname{ch} u_n = 1 + \frac{u_n^2}{2} + o(u_n^2)$$
$$\operatorname{th} u_n \sim u_n \quad \text{ou bien} \quad \operatorname{th} u_n = u_n + o(u_n)$$
$$\operatorname{argsh} u_n \sim u_n \quad \text{ou bien} \quad \operatorname{argsh} u_n = u_n + o(u_n)$$
$$\operatorname{argth} u_n \sim u_n \quad \text{ou bien} \quad \operatorname{argth} u_n = u_n + o(u_n)$$

Enfin, la liste des règles de calcul avec les équivalents et les « petits o ». Chacune étant triviale à vérifier :

Théorème 11.5.9

1. *Soit u une suite à termes non nuls. Alors $u_n \sim u_n$.*
2. *Soient u et v deux suites à termes non nuls. Alors $u_n \sim v_n$ si et seulement si $v_n \sim u_n$.*
3. *Soient u, v et w trois suites à termes non nuls. Si $u_n \sim v_n$ et $v_n \sim w_n$, alors $u_n \sim w_n$.*

4. *Soient u, v, u' et v' quatre suites à termes non nuls. On suppose que*

$$u_n = o(v_n) \qquad u_n \sim u'_n \qquad v_n \sim v'_n$$

Alors $$u'_n = o(v'_n)$$

5. *Soient u, v, u' et v' quatre suites à termes non nuls telles que*

$$u_n \sim u'_n \qquad v_n \sim v'_n$$

Alors $$u_n v_n \sim v_n v'_n$$

6. *Soient u et v deux suites à termes non nuls, telles que $u_n \sim v_n$. Alors $\frac{1}{u_n} \sim \frac{1}{v_n}$.*
7. *Soient u et v deux suites à termes strictement positifs telles que $u_n \sim v_n$. Pour tout nombre réel α, $u_n^\alpha \sim v_n^\alpha$.*
8. *Soient u et v deux suites à termes non nuls telles que $u_n \sim v_n$. Si $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ est strictement croissante, $u_{\varphi(n)} \sim v_{\varphi(n)}$.*

Voici, comme dans le paragraphe précédent, la traduction « en Français » de ces propriétés, peut-être plus facile à retenir :

1. Toute suite est équivalent à elle-même.
2. L'équivalence est une relation symétrique : dire que u est équivalente à v ou que v est équivalente à u, c'est la même chose.
3. L'équivalence se transmet : si deux suites sont équivalentes à une même troisième, elles sont équivalentes (entre elles).
4. Lorsqu'on a une relation de négligeabilité, on peut en remplacer les protagonistes par des suites équivalentes.
5. On peut multiplier des équivalents.
6. On peut inverser des équivalents.
7. On peut prendre des puissances d'équivalents.
8. Les équivalents sont conservés par extraction.

> Remarquons qu'il n'y a pas de règle pour la manipulation d'équivalents et de sommes. Pour la simple raison qu'on ne peut pas, en général, additionner les équivalents. Ne le faites **jamais**.
>
> Par exemple, on a $n+1 \sim n$ et $-n \sim 2-n$; si on pouvait additionner les équivalents, on trouverait $1 \sim 2$. Horreur !
>
> Il n'y a également pas de règle de composition des équivalents : ce n'est pas parce que $u_n \sim v_n$ que $f(u_n) \sim f(v_n)$.
>
> Par exemple, on a $n \sim n+1$ mais on n'a certainement pas $e^n \sim e^{n+1}$.
>
> Je répète : **n'additionnez jamais des équivalents et ne les composez jamais par une fonction**.
>
> Si vous souhaitez avoir l'équivalent d'une somme, passez plutôt en notation o et utilisez les règles de calcul avec ceux-ci. Par exemple :

$$n+1 = n+\mathrm{o}(n) \qquad \text{et} \qquad -n = 2-n+\mathrm{o}(n)$$

donc $$1 = 2+\mathrm{o}(n)$$

ce qui est vrai (et peu intéressant) mais n'implique certainement pas que $1 \sim 2$.

De même pour la composition : si vous souhaitez montrer que $\ln(n+1) \sim \ln n$, vous ne pouvez vous contenter de composer la relation $n+1 \sim n$, ce qui constitue une justification fausse. Écrivez plutôt

$$\ln(n+1) = \ln\left(n\left(1+\frac{1}{n}\right)\right) = \ln n + \ln\left(1+\frac{1}{n}\right) = \ln n + \frac{1}{n} + \mathrm{o}\left(\frac{1}{n}\right) = \ln n + \mathrm{o}(\ln n)$$

donc $$\ln(n+1) \sim \ln n$$

Chapitre 12

Fonctions et régularité

12.1 Notions de topologie

Au début de ce chapitre, nous allons formaliser la notion de limite d'une fonction, qui a pour l'instant toujours été considérée comme intuitive. Une fois ceci fait, il nous faudra présenter les règles de calcul avec les limites : addition, soustraction, multiplication, division, composition. Sachant que chacune de ces limites peut être finie ou infinie, et prise en un point ou en l'infini, cela conduirait à trop de cas particuliers à considérer.

Et il nous faut donc présenter quelques notions de topologie, fort utiles pour considérer d'un seul coup toutes les possibilités de limites.

Commençons avec la droite réelle achevée

Définition 12.1.1
On appelle *droite réelle achevée* l'ensemble $\overline{\mathbb{R}}$ constitué de $\mathbb{R}$ auquel on ajoute deux éléments qui ne sont pas réels. On les note respectivement $+\infty$ et $-\infty$.

L'addition et la multiplication prolongent celles sur $\mathbb{R}$. Et on ajoute en plus les opérations suivantes :

$$+\infty + \infty = +\infty \qquad -\infty - \infty = -\infty$$

$$(+\infty) \times (+\infty) = +\infty \qquad (+\infty) \times (-\infty) = -\infty \qquad (-\infty) \times (-\infty) = +\infty$$

$$\forall x > 0 \qquad x \times (+\infty) = +\infty \qquad x \times (-\infty) = -\infty$$

$$\forall x < 0 \qquad x \times (+\infty) = -\infty \qquad x \times (-\infty) = +\infty$$

L'ordre entre les nombres réels reste le même ; on ajoute les conventions suivantes :

$$\forall x \in \overline{\mathbb{R}} \qquad -\infty \leqslant x \leqslant +\infty$$

Vient ensuite la notion de voisinage :

Définition 12.1.2
Soit $a \in \overline{\mathbb{R}}$. On appelle voisinage de a tout ensemble contenant un intervalle ouvert contenant a.

Ainsi, si a appartient à $\mathbb{R}$, un voisinage est un ensemble qui contient un intervalle du type $]c\,;d[$ avec $c < a < d$.

Si $a = +\infty$, un voisinage de a est n'importe quel ensemble qui contient un intervalle du type $]c\,;+\infty[$. Et si $a = -\infty$, un voisinage de a est n'importe quel ensemble qui contient un intervalle du type $]-\infty, c[$.

Grosso-modo, tout ce qu'on réclame de la part d'un voisinage de a, c'est qu'il y ait, dedans, de la place (un intervalle ouvert) autour de a. De manière à ce qu'on puisse approcher a des deux côtés, sans trou.

Voici les propriétés fondamentales des voisinages :

Proposition 12.1.3
Soit $a \in \overline{\mathbb{R}}$.

1. *Tout intervalle ouvert contenant a est un voisinage de a.*
2. *Une intersection finie de voisinages de a est un voisinage de a.*
3. *Une union quelconque de voisinages de a est un voisinage de a.*

Preuve : Évidemment, la première proposition est vraie par définition même d'un voisinage : un intervalle contenant a contient un intervalle contenant a (lui-même).

Donnons-nous n voisinages $V_1, \dots, V_n$ de a. Pour tout $i \in [\![1\,;n]\!]$, V_i contient un intervalle J_i contenant a. Donc $\bigcap_{i=1}^{n} V_i$ contient $\bigcap_{i=1}^{n} J_i$. Comme on l'a vu en exercice au cours du chapitre sur les fondements de l'analyse, une intersection finie d'intervalles ouverts est un intervalle ouvert ; donc $\bigcap_{i=1}^{n} J_i$ est un intervalle ouvert contenant a. Et $\bigcap_{i=1}^{n} V_i$ est un voisinage de a.

Enfin, donnons-nous $(V_j)_{j\in J}$ une famille quelconque de voisinages de a. Chacun d'entre eux contient un intervalle ouvert contenant a ; c'est donc en particulier le cas de $\bigcup_{j\in J} V_j$. □

Définition 12.1.4
Soit I un intervalle. On appelle *adhérence* de I, notée $\overline{I}$, l'ensemble I auquel on ajoute ses bornes. On appelle *intérieur* de I, noté $\overset{\circ}{I}$, l'ensemble I auquel on retire ses bornes.

Définition 12.1.5
Soient f une fonction définie sur un intervalle I et $a \in \overline{I}$. On dit que f vérifie une propriété au voisinage de a si, et seulement si, il existe un voisinage V de a tel que cette propriété soit vérifiée dans $V \cap I$.

Par exemple, la fonction cos est décroissante au voisinage de $\pi/2$; bien qu'elle ne soit pas décroissante (tout court).

12.2 Limites

12.2.1 Limite en un point

Définition 12.2.1
Soit f une fonction définie sur un intervalle I. Soient $a \in \overline{I}$ et $\ell \in \overline{\mathbb{R}}$. On dit que f admet ℓ comme limite en a si et seulement si pour tout voisinage V de ℓ, il existe un voisinage U de a tel que

$$\forall x \in U \cap I \qquad f(x) \in V$$

Cette définition est un poil plus abstraite que celle de la limite d'une suite. Mais elle peut être comprise d'une manière similaire : pour tout voisinage V de ℓ, aussi petit soit-il, il existe un voisinage U de a suffisamment petit (mais pas si petit quand même, puisqu'il contient tout un intervalle) tel que, dès que x appartient à $I \cap U$, $f(x)$ se retrouve coincé dans V.

Les dessins faits en cours aideront, je l'espère, à comprendre concrètement ce que signifie cette notion.

Comme pour les suites, le premier théorème sur les limites est celui d'unicité :

Théorème 12.2.2
Soient f une fonction définie sur un intervalle I *et $\ell, \ell' \in \overline{\mathbb{R}}$. On suppose que f admet ℓ et ℓ' comme limites en a. Alors $\ell = \ell'$.*

De plus, si $a \in$ I, alors $\ell = f(a)$.

Preuve : Supposons que f admet ℓ et ℓ' comme limites en a et que $\ell \neq \ell'$. On choisit alors des intervalles disjoints V_ℓ et $V_{\ell'}$, contenant respectivement ℓ et ℓ'.

Alos V_ℓ est un voisinage de ℓ et $V_{\ell'}$ est un voisinage de ℓ'. Puisque f admet ℓ comme limite en a, il existe un voisinage U de a tel que

$$\forall x \in U \cap I \qquad f(x) \in V_\ell$$

De même, il existe un voisinage U′ de a tel que

$$\forall x \in U' \cap I \qquad f(x) \in V_{\ell'}$$

Or, d'après la **proposition 1.3**, $A = (U \cap I) \cap (U' \cap I)$ est un voisinage de a. Et on a

$$\forall x \in A \qquad f(x) \in V_\ell \qquad \text{et} \qquad f(x) \in V_{\ell'}$$

c'est-à-dire

$$\forall x \in A \qquad f(x) \in V_\ell \cap V_{\ell'}$$

ce qui contredit le fait que V_ℓ et $V_{\ell'}$ sont disjoints. Donc $\ell = \ell'$.

Maintenant, supposons qu'en plus, a appartienne à I. Commençons par montrer que $\ell \in \mathbb{R}$. On suppose que $\ell = +\infty$. Alors $]f(a) ; +\infty[$ est un voisinage de ℓ ; d'après la définition de la limite, il existe U voisinage de a tel que

$$\forall x \in U \qquad f(x) \in]f(a) ; +\infty[$$

Or, $a \in U$ donc $f(a) \in]f(a) ; +\infty[$: contradiction. De même, on montre qu'il est exclu que $\ell = -\infty$ en considérant le voisinage $]-\infty ; f(a)[$ de $-\infty$.

Bref, ℓ est donc un nombre réel. On se donne $\varepsilon > 0$ et on pose $V =]\ell - \varepsilon ; \ell + \varepsilon[$. C'est un voisinage de ℓ et f admet ℓ comme limite en a donc il existe un voisinage U de a tel que

$$\forall x \in U \qquad f(x) \in V$$

c'est-à-dire que

$$\forall x \in U \qquad |f(x) - \ell| \leqslant \varepsilon$$

En particulier, $|f(a) - \ell| \leqslant \varepsilon$. Cette inégalité est valable pour tout $\varepsilon > 0$. Donc $f(a) = \ell$. □

Définition 12.2.3
Soient f une fonction définie sur un intervalle I, $a \in \overline{I}$ et $\ell \in \overline{\mathbb{R}}$ tels que f admette ℓ comme limite en a. Dans la mesure où ℓ est la seule et unique limite possible, on dira que ℓ est **la** *limite de f en a* et on notera :

$$\lim_{x \to a} f(x) = \ell \qquad \lim_{a} f = \ell \qquad \text{ou} \qquad f(x) \xrightarrow[x \to a]{} \ell$$

Notre définition d'une limite, pour abstraite qu'elle puisse paraître, présente l'avantage de traiter tous les cas de limites d'un coup : limites en un point, en $-\infty$ ou en $+\infty$; limites finies ou infinies. Mais dans chacun de ces cas particulier, elle peut être formulée de manière plus concrète.

Proposition 12.2.4
Soient f un fonction définie sur un intervalle I, $a \in \overline{\mathrm{I}}$ *et* $\ell \in \overline{\mathbb{R}}$. ℓ *est la limite de f en a si et seulement si :*

- ***Si*** $a \in \mathbb{R}$ ***et*** $\ell \in \mathbb{R}$ *:*
$$\forall \varepsilon > 0 \quad \exists \eta > 0 \quad \forall x \in \mathrm{I} \qquad (|x-a| \leqslant \eta \implies |f(x)-\ell| \leqslant \varepsilon)$$
- ***Si*** $a \in \mathbb{R}$ ***et*** $\ell = +\infty$ *:*
$$\forall \mathrm{M} > 0 \quad \exists \eta > 0 \quad \forall x \in \mathrm{I} \qquad (|x-a| \leqslant \eta \implies f(x) \geqslant \mathrm{M})$$
Notons que dans ce cas là, a n'est pas dans I, *comme on a pu le voir dans la preuve du* ***théorème 2.2****.*
- ***Si*** $a \in \mathbb{R}$ ***et*** $\ell = -\infty$ *:*
$$\forall \mathrm{M} < 0 \quad \exists \eta > 0 \quad \forall x \in \mathrm{I} \qquad (|x-a| \leqslant \eta \implies f(x) \leqslant \mathrm{M})$$
Même remarque que précédemment : a n'appartient pas à I.
- ***Si*** $a = +\infty$ ***et*** $\ell = +\infty$
$$\forall \mathrm{M} > 0 \quad \exists \alpha > 0 \quad \forall x \in \mathrm{I} \qquad (x \geqslant \alpha \implies f(x) \geqslant \mathrm{M})$$
- ***Si*** $a = +\infty$ ***et*** $\ell = -\infty$
$$\forall \mathrm{M} < 0 \quad \exists \alpha > 0 \quad \forall x \in \mathrm{I} \qquad (x \geqslant \alpha \implies f(x) \leqslant \mathrm{M})$$
- ***Si*** $a = +\infty$ ***et*** $\ell \in \mathbb{R}$
$$\forall \varepsilon > 0 \quad \exists \alpha > 0 \quad \forall x \in \mathrm{I} \qquad (x \geqslant \alpha \implies |f(x)-\ell| \leqslant \varepsilon)$$
- ***Si*** $a = -\infty$ ***et*** $\ell = +\infty$
$$\forall \mathrm{M} > 0 \quad \exists \alpha < 0 \quad \forall x \in \mathrm{I} \qquad (x \leqslant \alpha \implies f(x) \geqslant \mathrm{M})$$
- ***Si*** $a = -\infty$ ***et*** $\ell = -\infty$
$$\forall \mathrm{M} < 0 \quad \exists \alpha < 0 \quad \forall x \in \mathrm{I} \qquad (x \leqslant \alpha \implies f(x) \leqslant \mathrm{M})$$
- ***Si*** $a = +\infty$ ***et*** $\ell \in \mathbb{R}$
$$\forall \varepsilon > 0 \quad \exists \alpha < 0 \quad \forall x \in \mathrm{I} \qquad (x \leqslant \alpha \implies |f(x)-\ell| \leqslant \varepsilon)$$

Bien évidemment, il serait idiot d'apprendre ces relations par cœur. Ce sont de simples traductions de la **définition 2.1** dans chacun des neuf contextes ci-dessus ; et il est important de comprendre pourquoi.

Théorème 12.2.5
Soient f une fonction définie sur un intervalle I, $a \in \overline{\mathrm{I}}$ *et* $\ell \in \overline{\mathbb{R}}$.

- ***Si*** $\ell \in \mathbb{R}$, $\lim\limits_a f = \ell \iff \lim\limits_a (f-\ell) = 0$
- ***Si*** $a \in \mathbb{R}$, $\lim\limits_a f = \ell \iff \lim\limits_{h \to 0} f(a+h) = \ell$

Preuve : Supposons d'abord que $\ell \in \mathbb{R}$, de sorte que la fonction $f-\ell$ soit bien définie. On suppose que $\lim_a f = \ell$. Soit V un voisinage de 0. Alors $V_\ell = \{x+\ell \mid x \in V\}$ est un voisinage de ℓ et il existe un voisinage U de a tel que

$$\forall x \in U \qquad f(x) \in V_\ell$$

c'est-à-dire $$\forall x \in U \quad \exists y \in V \qquad f(x) = y + \ell$$

ou encore $$\forall x \in U \quad \exists y \in V \qquad f(x) - \ell = y$$

donc $$\forall x \in U \qquad (f(x) - \ell) \in V$$

Ce qui montre que $\lim_a (f-\ell) = 0$. La réciproque se montre de la même manière.

Maintenant, supposons que $a \in \mathbb{R}$, c'est-à-dire que a n'est pas $+\infty$ ou $-\infty$. Ainsi, on peut parler sans problème de $f(a+h)$ pour tout réel h tel que $a+h \in I$. Soit V un voisinage de ℓ. Puisque $\lim_a f = \ell$, il existe un voisinage U de a tel que

$$\forall x \in U \qquad f(x) \in V$$

Posons alors $U_0 = \{x-a \mid x \in U\}$: c'est un voisinage de 0. On a alors

$$\forall h \in U_0 \qquad f(\underbrace{a+h}_{\in U}) \in V$$

ce qui montre que $\lim_0 f(a+h) = \ell$. □

Théorème 12.2.6
Soient f une fonction définie sur un intervalle I, $a \in \overline{I}$ et $\ell \in \mathbb{R}$. On suppose que $\lim_a f = \ell$. Alors f est bornée au voisinage de a.

> En Français : une fonction qui admet une limite **finie** en a est bornée tant qu'on ne s'éloigne pas trop de a. Ce n'est pas étonnant : par intuition de ce que signifie l'existence d'une limite, si x est proche de a, $f(x)$ est proche de ℓ. Donc $f(x)$ ne peut pas être trop grand. La preuve est très simple.

Preuve : L'intervalle $V =]\ell-1\,;\,\ell+1[$ est un voisinage de ℓ. Donc il existe un voisinage U de a tel que

$$\forall x \in U \qquad f(x) \in V$$

c'est-à-dire que $$\forall x \in U \qquad \ell - 1 \leqslant f(x) \leqslant \ell + 1$$

f est bien bornée dans un voisinage de a. □

12.2.2 Limites à gauche et à droite

Définition 12.2.7
Soient f une fonction définie sur un intervalle I, $a \in \overline{I}$ et $\ell \in \overline{\mathbb{R}}$.

Si f est définie au voisinage de a, à gauche. On dit que f admet ℓ pour limite à gauche en a si et seulement si la restriction de f à $I \cap]-\infty\,;\,a[$ admet pour limite ℓ. On écrira

$$\ell = \lim_{x \to a^-} f(x) \qquad \ell = \lim_{a^-} f \qquad \text{ou} \qquad f(x) \xrightarrow[x \to a^-]{} \ell$$

Si f est définie au voisinage de a, à droite, on dit que f admet ℓ pour limite à droite en a si et seulement si la restriction de f à $\mathrm{I}\cap]a;+\infty[$ admet pour limite ℓ. On écrira

$$\ell = \lim_{x\to a^+} f(x) \qquad \ell = \lim_{a^+} f \qquad \text{ou} \qquad f(x) \xrightarrow[x\to a^+]{} \ell$$

Comme précédemment, la définition est formulée de manière abstraite, dans un but unificateur. Voici sa traduction dans les différents cas :

Proposition 12.2.8
Soient f une fonction définie sur un intervalle I, $a \in \overline{\mathrm{I}}$ *et* $\ell \in \overline{\mathbb{R}}$. *On suppose f définie dans un voisinage à gauche de a. Alors* $\lim\limits_{x\to a^-} f(x) = \ell$ *si et seulement si*

- ***Si*** $\ell = -\infty$ ***:***

$$\forall \mathrm{M} < 0 \quad \exists \eta > 0 \quad \forall x \in \mathrm{I} \qquad (a - \eta \leqslant x < a \implies f(x) \leqslant \mathrm{M})$$

- ***Si*** $\ell = +\infty$ ***:***

$$\forall \mathrm{M} > 0 \quad \exists \eta > 0 \quad \forall x \in \mathrm{I} \qquad (a - \eta \leqslant x < a \implies f(x) \geqslant \mathrm{M})$$

- ***Si*** $\ell \in \mathbb{R}$ ***:***

$$\forall \varepsilon > 0 \quad \exists \eta > 0 \quad \forall x \in \mathrm{I} \qquad (a - \eta \leqslant x < a \implies |f(x) - \ell| \leqslant \varepsilon)$$

Je vous fais le cadeau des limites à droite. Une des utilités de ces notions est de caractériser l'existence d'une limite pour une fonction. Comme on s'y attend,

Théorème 12.2.9
Soient f une fonction définie sur un intervalle I, $a \in \mathring{\mathrm{I}}$ *et* $\ell \in \mathbb{R}$. *Alors f tend vers ℓ en a si et seulement si les trois propriétés suivantes sont satisfaites :*

1. $f(a) = \ell$;
2. $\lim\limits_{x\to a^-} f(x) = \ell$;
3. $\lim\limits_{x\to a^+} f(x) = \ell$.

Preuve : Supposons que f admet ℓ comme limite en a. Comme a est un point intérieur à I, il appartient à I et le **théorème 2.2** affirme que $f(a) = \ell$. Cela implique automatiquement que ℓ n'est pas infini. On a donc

$$\forall \varepsilon > 0 \quad \exists \eta > 0 \quad \forall x \in \mathrm{I} \qquad (|x - a| \leqslant \eta \implies |f(x) - \ell| \leqslant \varepsilon)$$

En jetant un œil à la **proposition 2.8**, on voit que f tend vers ℓ à gauche en a. Et si on exprimait en quantificateurs la propriété $f(x) \xrightarrow[x\to a^+]{} \ell$, on verrait que f tend vers ℓ en a à droite.

Réciproquement, supposons que les trois propriétés *1, 2* et *3* sont satisfaites. Alors ℓ n'est pas infini et on doit donc montrer que

$$\forall \varepsilon > 0 \quad \exists \eta > 0 \quad \forall x \in \mathrm{I} \qquad (|x - a| \leqslant \eta \implies |f(x) - \ell| \leqslant \varepsilon)$$

Soit $\varepsilon > 0$. Comme on sait que f tend vers ℓ à gauche, il existe $\eta_1 > 0$ tel que

$$\forall x \in \mathrm{I} \qquad (a - \eta \leqslant x < a \implies |f(x) - \ell| \leqslant \varepsilon)$$

De même, comme f tend vers ℓ à droite, il existe $\eta_2 > 0$ tel que

$$\forall x \in \mathrm{I} \qquad (a < x \leqslant a+\eta_2 \implies |f(x)-\ell| \leqslant \varepsilon)$$

Posons alors $\eta = \mathrm{Min}(\eta_1, \eta_2)$. De sorte que

$$a-\eta \geqslant a-\eta_1 \qquad \text{et} \qquad a+\eta \leqslant a+\eta_2$$

Du coup, $\forall x \in \mathrm{I}\setminus\{a\} \qquad (a-\eta \leqslant x \leqslant a+\eta \implies |f(x)-\ell| \leqslant \varepsilon)$

Enfin, si $x = a$, on a $|f(x)-\ell| = |f(a)-f(a)| = 0$ donc au final,

$$\forall x \in \mathrm{I} \qquad (a-\eta \leqslant x \leqslant a+\eta \implies |f(x)-\ell| \leqslant \varepsilon)$$

Ce qui établit que f tend vers ℓ en a. □

12.2.3 Limites et inégalités

Théorème 12.2.10
Soient f une fonction définie sur un intervalle I, $a \in \overline{\mathrm{I}}$ *et* $\ell \in \mathbb{R}$. *On suppose que f est positive au voisinage de a et qu'elle tend vers ℓ en a. Alors $\ell \geqslant 0$.*

Preuve : On suppose que $\ell < 0$. Alors l'intervalle $]\frac{3\ell}{2}\,;\frac{\ell}{2}[$ est un voisinage de ℓ et il existe donc un voisinage U de a tel que

$$\forall x \in \mathrm{U} \qquad \frac{3\ell}{2} \leqslant f(x) \leqslant \frac{\ell}{2} < 0$$

Or, on sait aussi qu'il existe un voisinage U′ de a sur lequel f est positive. Par conséquent, sur $\mathrm{U}\cap\mathrm{U}'$, f est strictement négative et positive à la fois. C'est une contradiction. Du coup, $\ell \geqslant 0$. □

Le corollaire suivant peut être résumé ainsi : les inégalités larges sont conservées par passage à la limite, pour peu qu'on ait vérifié avant que les limites existent.

Corollaire 12.2.11
Soient f, g deux fonctions définies sur un intervalle I, $a \in \overline{\mathrm{I}}$. *On suppose que $f \leqslant g$ au voisinage de a et que f et g admettent chacune une limite finie en a. Alors*

$$\lim_{x\to a} f(x) \leqslant \lim_{x\to a} g(x)$$

En particulier :
- *si f est majorée par un nombre réel* M *au voisinage de a, alors* $\lim\limits_{x\to a} f(x) \leqslant \mathrm{M}$;
- *si g est minorée par un nombre réel m au voisinage de a, alors* $\lim\limits_{x\to a} g(x) \geqslant m$.

12.2.4 Opérations sur les limites

Prenez les tableaux résumant les règles d'addition, multiplication et division de limites de suites ; ce sont les mêmes pour les limites de fonctions.

Faisons maintenant des choses nouvelles. Tout d'abord, comme promis, le théorème de composition d'une fonction par une suite.

Théorème 12.2.12
Soient f une fonction définie sur un intervalle I *et u une suite à valeurs dans* I. *Soient $a \in \overline{\mathrm{I}}$ et $\ell \in \overline{\mathbb{R}}$. On suppose que*

$$\lim_a f = \ell \qquad et \qquad \lim_\infty u = a$$

Alors

$$\lim_\infty f(u_n) = a$$

Preuve : Dire que u converge vers a, c'est dire que pour tout voisinage V de a, il existe un entier N tel que

$$\forall n \geqslant \mathrm{N} \qquad u_n \in \mathrm{V}$$

Soit V un voisinage de ℓ ; comme f tend vers ℓ en a, il existe un voisinage U de a tel que

$$\forall x \in \mathrm{U} \qquad f(x) \in \mathrm{V}$$

Et comme u tend vers a, il existe un entier N tel que

$$\forall n \geqslant \mathrm{N} \qquad u_n \in \mathrm{U}$$

Par suite,

$$\forall n \geqslant \mathrm{N} \qquad f(u_n) \in \mathrm{V}$$

ce qui démontre que $f(u_n) \xrightarrow[n\to\infty]{} \ell$. □

Théorème 12.2.13
Soient f et g deux fonctions, définies respectivement sur des intervalles I *et* J, *telles que $f(\mathrm{I}) \subset \mathrm{J}$ de sorte que $g \circ f$ soit bien définie. Soient*

$$a \in \overline{\mathrm{I}} \qquad b \in \overline{\mathrm{J}} \qquad \ell \in \overline{\mathbb{R}}$$

On suppose que

$$\lim_{x\to a} f(x) = b \qquad \lim_{x\to b} g(x) = \ell$$

Alors

$$\lim_{x\to a} g \circ f(x) = \ell$$

Preuve : Soit V un voisinage de ℓ. On sait qu'il existe un voisinage U de b tel que

$$\forall x \in \mathrm{U} \qquad g(x) \in \mathrm{V}$$

Et comme U est un voisinage de b, qui est la limite de f en a, il existe un voisinage W de a tel que

$$\forall x \in \mathrm{W} \qquad f(x) \in \mathrm{U}$$

Alors

$$\forall x \in \mathrm{W} \qquad g \circ f(x) = g(\underbrace{f(x)}_{\in \mathrm{U}}) \in \mathrm{V}$$

ce qui établit que $\lim_{x\to a} g \circ f(x) = \ell$. □

12.2.5 Théorèmes d'existence

Théorème 12.2.14 (Théorème des gendarmes)
Soient f, g et h trois fonctions définies dans un voisinage I *de $a \in \overline{\mathbb{R}}$ et telles que*

$$\forall x \in \mathrm{V} \qquad f(x) \leqslant g(x) \leqslant h(x)$$

On suppose que f et h admettent chacune la même limite $\ell \in \overline{\mathbb{R}}$ en a. Alors $\lim_{x\to a} g(x)$ existe et vaut ℓ.

Preuve : Supposons dans un premier temps que ℓ est fini. Soit V un voisinage de ℓ ; par définition, V contient un intervalle contenant ℓ. Donc il existe $\varepsilon > 0$ tel que $]\ell-\varepsilon\,;\,\ell+\varepsilon[\subset \mathrm{V}$.

Comme f et h admettent ℓ comme limite en a, il existe voisinages U_1 et U_2 de a, tels que

$$\forall x \in \mathrm{U}_1 \cap \mathrm{I} \qquad f(x) \in \mathrm{V}$$

et

$$\forall x \in \mathrm{U}_2 \cap \mathrm{I} \qquad h(x) \in \mathrm{V}$$

En particulier,

$$\forall x \in \mathrm{U}_1 \cap \mathrm{U}_2 \cap \mathrm{I} \qquad \ell-\varepsilon \leqslant f(x) \leqslant g(x) \leqslant h(x) \leqslant h(x)+\varepsilon$$

donc

$$\forall x \in \mathrm{U}_1 \cap \mathrm{U}_2 \cap \mathrm{I} \qquad g(x) \in]\ell-\varepsilon\,;\,\ell+\varepsilon[\subset \mathrm{V}$$

Comme $\mathrm{U}_1 \cap \mathrm{U}_2 \cap \mathrm{I}$ est un voisinage de a, on a bien montré que g admet une limite en a et que cette limite est ℓ.

Supposons maintenant que $\ell = +\infty$. On sait alors qu'il existe un voisinage I' de a tel que

$$\forall x \in \mathrm{I}' \qquad f(x) > 0$$

donc

$$\forall x \in \mathrm{I}' \qquad 0 \leqslant \frac{1}{g(x)} \leqslant \frac{1}{f(x)}$$

La fonction $1/f$ tend vers 0 en a, puisque f tendent vers $+\infty$. D'après ce qui précède, $1/g$ tend aussi vers 0, par valeurs supérieures, en a. Donc g tend vers $+\infty$.

De même si $\ell = -\infty$. □

Corollaire 12.2.15
Soient f une fonction bornée au voisinage de $a \in \overline{\mathbb{R}}$ et g une fonction de limite nulle en a. Alors $fg \xrightarrow[x\to a]{} 0$.

Théorème 12.2.16 (Théorème de la limite monotone)
Soient f une application définie sur un intervalle I*, croissante, et $a \in \overline{\mathrm{I}}$.*

- ***Si $a \in \overset{\circ}{\mathrm{I}}$** : alors f admet des limites en a à gauche et à droite et on a*
$$\lim_{a^-} f \leqslant f(a) \leqslant \lim_{a^+} f$$
- ***Si $a = \mathrm{Sup}\,\mathrm{I}$** : alors f admet une limite en a. Cette limite est finie si f est majorée, et vaut $+\infty$ sinon.*
- ***Si $a = \mathrm{Inf}\,\mathrm{I}$** : alors f admet une limite en a. Cette limite est finie si f est minorée, et vaut $-\infty$ sinon.*

Preuve : Commençons avec le premier cas. Posons

$$m = \mathrm{Sup}\{f(x) \mid x < a\} \qquad \text{et} \qquad \mathrm{M} = \mathrm{Inf}\{f(x) \mid x > a\}$$

Observons d'abord que, comme f est croissante,

$$\forall x < a \qquad f(x) \leqslant f(a)$$

et

$$\forall x > a \qquad f(x) \geqslant f(a)$$

Donc

$$m \leqslant f(a) \leqslant \mathrm{M}$$

Ensuite, donnons-nous $\varepsilon > 0$. D'après la caractérisation des bornes supérieure et inférieure, il existe $x_0 < a$ et $x_1 > a$ tels que

$$m-\varepsilon < f(x_0) \leqslant m \qquad \text{et} \qquad \mathrm{M} \leqslant f(x_1) < \mathrm{M}+\varepsilon$$

Posons $$\eta_1 = a - x_0 > 0 \qquad \text{et} \qquad \eta_2 = x_1 - a > 0$$

Comme f est croissante, on a

$$\forall x \in]\underbrace{a-\eta_1}_{=x_0}; a[\qquad m-\varepsilon \leqslant f(x_0) \leqslant f(x) \leqslant m$$

et $$\forall x \in]a; \underbrace{a+\eta_2}_{=x_1}[\qquad \mathrm{M} \leqslant f(x) \leqslant f(x_1) \leqslant \mathrm{M}+\varepsilon$$

Ceci montre exactement que

$$\lim_{x\to a^-} f(x) = m \qquad \text{et} \qquad \lim_{x\to a^+} f(x) = \mathrm{M}$$

et achève la preuve de la première assertion.

Pour les deux autres, ça marche de la même manière. □

12.3 Relations de comparaison

De la même manière que pour les suites, nous allons définir des relations de comparaison entre fonctions, dans le but d'étudier plus finement le comportement local de celles-ci.

12.3.1 Négligeabilité

Définition 12.3.1

Soient f et g deux fonctions définies sur un intervalle I, soit $a \in \overline{\mathrm{I}}$. On dit que f est négligeable devant g au voisinage de a si, et seulement si, il existe une fonction ε, définie sur I et tendant vers 0 en a telle que $f = \varepsilon g$ au voisinage de a. On note alors

$$f(x) \underset{x\to a}{=} o(g) \qquad \text{ou bien} \qquad f \underset{a}{=} o(g)$$

Les résultats suivants sont triviaux :

Théorème 12.3.2

1. *Soient f et g deux fonctions définies sur un intervalle* I. *Soient $a \in \overline{\mathrm{I}}$ et $\lambda \in \mathbb{R}^\star$. On suppose que $f \underset{a}{=} o(g)$. Alors*

$$\lambda f = o(g) \qquad et \qquad f = o(\lambda g) = o(g)$$

2. *Soient f, g et h trois fonctions telles que*

$$f \underset{a}{=} o(h) \qquad et \qquad g \underset{a}{=} o(h)$$

Alors $$f + g \underset{a}{=} o(g)$$

3. *Soient f, g et h trois fonctions telles que*

$$f \underset{a}{=} o(g) \qquad et \qquad g \underset{a}{=} o(h)$$

Alors $$f \underset{a}{=} o(h)$$

4. *Soient f, g, h, k quatre fonctions, telles que*
$$f \underset{a}{=} o(g) \qquad et \qquad h \underset{a}{=} o(k)$$
Alors $$fh \underset{a}{=} o(gk)$$
5. *Soient f et g deux fonctions telles que $f \underset{a}{=} o(g)$. Soit φ une application définie au voisinage de b, telle que $\lim_{x\to b} \varphi(x) = b$. Alors*
$$f \circ \varphi \underset{b}{=} o(g \circ \varphi)$$

Les remarques accompagnant ce théorème sont les mêmes que pour les suites :

1. On peut multiplier une relation de négligeabilité par un nombre réel non nul, cela ne change rien.
2. Si deux fonctions sont négligeables devant une même troisième, leur somme est négligeable devant celle-ci.
3. La négligeabilité se transmet transitivement.
4. Multiplier une relation de négligeabilité membre à membre ne pose aucun problème.
5. On peut composer **à droite** une relation de négligeabilité par une fonction.

En revanche, on **ne peut pas ajouter membre à membre** des relations négligeabilité. Par exemple,
$$x+1 \underset{x\to+\infty}{=} o(x^2+4) \qquad \text{et} \qquad -x \underset{x\to+\infty}{=} o(-x^2)$$
Si on ajoute membre à membre ces relations, on obtient
$$1 \underset{x\to+\infty}{=} o(4)$$
ce qui est clairement faux.

Les théorèmes de croissances comparées que nous avons vus au début de l'année se récrivent en termes de « petit o » :
$$\forall \alpha < \beta \qquad x^\beta \underset{x\to 0}{=} o(x^\alpha) \qquad \text{et} \qquad x^\alpha \underset{x\to+\infty}{=} o(x^\beta)$$
$$\forall \beta \in \mathbb{R} \quad \forall \alpha > 0 \qquad \ln^\beta x \underset{x\to+\infty}{=} o(x^\alpha) \qquad \text{et} \qquad x^\alpha \underset{x\to 0}{=} o(|\ln x|^\beta)$$
$$\forall \beta \in \mathbb{R} \quad \forall \alpha > 0 \qquad x^\beta \underset{x\to+\infty}{=} o(e^{\alpha x}) \qquad \text{et} \qquad e^{-\beta x} \underset{x\to-\infty}{=} o(|x|^\alpha)$$
Enfin, le fait qu'une fonction f admette une limite $\ell \in \mathbb{R}$ en a s'écrit $f(x) \underset{x\to a}{=} \ell + o(1)$.

12.4 Continuité

12.4.1 Les théorèmes généraux

Définition 12.4.1

Soit f une fonction définie sur un intervalle I, soit $a \in$ I. On dit que f *est continue en* a si et seulement si f admet une limite en a.

On dit que f *est continue sur* I si et seulement si f est continue en tout point de I.

On dit que f *est continue à gauche en* a si et seulement si $\lim_{x\to a^-} f(x) = f(a)$.

On dit que f *est continue à droite en* a si et seulement si $\lim_{x\to a^+} f(x) = f(a)$.

De manière équivalente, f est continue en a si et seulement si $f(x) \underset{x\to a}{=} f(a) + o(1)$.

Proposition 12.4.2
$\mathscr{C}^0(\mathrm{I})$ *est une algèbre, c'est-à-dire que*

1. *la somme de deux fonctions continues est continue ;*
2. *le produit de deux fonctions continues est continue ;*
3. *le produit d'une fonction continue par un scalaire est continu.*

Preuve : Tous ces résultats sont des conséquences débiles des résultats de manipulations de limites.

Ainsi, supposons par exemple que f et g sont continues sur I. Soit $a \in \mathrm{I}$. Alors $\lim\limits_a f$ et $\lim\limits_a g$ existent et sont finies et on sait alors que $\lim\limits_a (f+g)$ existe et vaut $\lim\limits_a f + \lim\limits_a g$.

De même pour les autres points. □

Ajoutons le théorème de composition :

Théorème 12.4.3
Soient $f \in \mathscr{C}^0(\mathrm{I})$ et $g \in \mathscr{C}^0(\mathrm{J})$, avec $g(\mathrm{J}) \subset \mathrm{I}$. Alors $f \circ g \in \mathscr{C}^0(\mathrm{J})$.

Preuve : Application directe du théorème de composition des limites. □

Définition 12.4.4
Soient I un intervalle et $a \in \mathrm{I}$. Soit $f \in \mathscr{C}(\mathrm{I} \setminus \{a\})$. On dit que f est *prolongeable par continuité en a* si et seulement si $\lim\limits_{x\to a^-} f(x)$ et $\lim\limits_{x\to a^+} f(x)$ existent, sont finies et sont égales à un nombre réel ℓ.

Dans ce cas, la fonction $\overline{f}$ définie par

$$\forall x \in \mathrm{I} \qquad \overline{f}(x) = \begin{cases} f(x) & \text{si } x \neq a \\ \ell & \text{si } x = a \end{cases}$$

est appelée *le prolongement par continuité de f en a.*

12.4.2 Les grands théorèmes

Théorème 12.4.5 (Théorème de bornitude)
Toute fonction continue sur un segment est bornée et atteint ses bornes.

Preuve : Soient $\mathrm{I} = [a\,;b]$ un segment (c'est-à-dire un intervalle fermé) et $f \in \mathscr{C}(\mathrm{I})$.

On suppose $|f|$ non majoré. En d'autres termes,

$$\forall \mathrm{M} > 0 \quad \exists x \in \mathrm{I} \qquad |f(x)| \geqslant \mathrm{M}$$

En particulier, pour chaque entier n, on peut trouver un $x_n \in \mathrm{I}$ tel que $|f(x_n)| \geqslant n$. La suite $(x_n)_{n\in\mathbb{N}}$ est bornée puisque

$$\forall n \in \mathbb{N} \qquad a \leqslant x_n \leqslant b$$

D'après le théorème de **Bolzano-Weierstrass**, elle admet une sous-suite $(x_{\varphi(n)})_{n\in\mathbb{N}}$, convergente vers une limite ℓ. On a

$$\forall n \in \mathbb{N} \qquad a \leqslant x_{\varphi(n)} \leqslant b$$

donc $$a \leqslant \ell \leqslant b$$

en passant à la limite dans l'inégalité. Donc ℓ appartient à I. On a aussi

$$\forall n \in \mathbb{N} \qquad |f(x_{\varphi(n)})| \geqslant \varphi(n)$$

donc $$\lim_{n\to\infty} |f(x_\varphi(n))| = +\infty$$

D'un autre côté, $|f|$ est continue en ℓ donc, d'après le théorème de composition des suites par des fonctions,

$$\lim_{n\to\infty} |f(x_{\varphi(n)})| = |f(\ell)|$$

C'est une contradiction. Donc $|f|$ est majorée. Et f est bornée.

Montrons qu'elle atteint ses bornes. Posons $\mathrm{M} = \mathrm{Sup}\, f$. Par définition,

$$\forall \varepsilon > 0 \quad \exists x \in \mathrm{I} \qquad \mathrm{M} - \varepsilon \leqslant f(x) \leqslant \mathrm{M}$$

En particulier, $$\forall n \in \mathbb{N}^\star \quad \exists x_n \in \mathrm{I} \qquad \mathrm{M} - \frac{1}{n} \leqslant f(x_n) \leqslant \mathrm{M}$$

À l'aide de Bolzano-Weierstrass, on extrait une sous-suite $(x_{\varphi(n)})_{n\in\mathbb{N}}$ qui converge vers une limite ℓ. Comme au-dessus, on a $\ell \in \mathrm{I}$ puisque

$$\forall n \in \mathbb{N}^\star \qquad a \leqslant x_{\varphi(n)} \leqslant b$$

Enfin $$\forall n \in \mathbb{N}^\star \qquad \mathrm{M} - \frac{1}{\varphi(n)} \leqslant f(x_{\varphi(n)}) \leqslant \mathrm{M}$$

D'après le **théorème des gendarmes**,

$$\lim_{n\to\infty} f(x_{\varphi(n)}) = \mathrm{M}$$

Or, f est continue en ℓ donc

$$\lim_{n\to\infty} f(x_{\varphi(n)}) = f(\ell)$$

Par suite, $$f(\ell) = \mathrm{M} = \mathrm{Sup}\, f$$

Le supremum de f est atteint.

De la même manière, on montre que l'infimum est atteint. □

Théorème 12.4.6 (Théorème des valeurs intermédiaires 1)
Soit f continue sur un segment $[a\,;b]$. On suppose que $f(a)$ et $f(b)$ sont de signes opposés. Alors f s'annule au moins une fois sur $[a\,;b]$.

Preuve : Supposons par exemple que $f(a) < 0$ et $f(b) > 0$; si ce n'est pas le cas, il suffit de changer f en $-f$. Considérons l'ensemble

$$\mathrm{A} = \{x \in [a\,;b] \mid f(x) \leqslant 0\}$$

Alors A n'est pas vide (il contient a) et il est majoré par b. Il admet donc une borne supérieure qu'on note y. Par définition de la borne supérieure, pour tout entier n non nul, il existe x_n dans A tel que

$$y - \frac{1}{n} \leqslant x_n \leqslant y$$

D'après le théorème des gendarmes, $x_n \xrightarrow[n\to\infty]{} y$; en outre,

$$\forall n \in \mathbb{N}^\star \qquad a \leqslant x_n \leqslant b$$

donc $$a \leqslant y \leqslant b$$

Comme f est continue sur I, elle admet une limite en y donc $\lim\limits_{n\to\infty} f(x_n) = f(y)$. Or,

$$\forall n \in \mathbb{N}^\star \qquad f(x_n) \leqslant 0$$

donc $$f(y) \leqslant 0$$

Dans la mesure où $f(b) > 0$, y ne peut être égal à b donc $y < b$. Il existe donc un entier N tel que $y + \frac{1}{\mathrm{N}} < b$. Pour tout $n \geqslant \mathrm{N}$, $y + \frac{1}{n}$ majore y qui majore A, donc ne se trouve pas dans A. Par suite,

$$\forall n \geqslant \mathrm{N} \qquad f\left(y + \frac{1}{n}\right) > 0$$

Or $$\lim_{n\to\infty} \left(y + \frac{1}{n}\right) = y$$

donc $$f(y) = \lim_{n\to\infty} f\left(y + \frac{1}{n}\right) \geqslant 0$$

Ce qui achève la démonstration, puisque $f(y) = 0$ □

Voilà voilà... Ce théorème fondamental confirme ce que notre intuition nous dit : le graphe d'une fonction continue ne peut pas passer des y négatifs aux y positifs sans passer au moins une fois par 0.

Théorème 12.4.7 (Théorème des valeurs intermédiaires 2)
Si f est continue sur $[a\,;b]$, elle atteint toutes les valeurs entre $f(a)$ et $f(b)$.

Preuve : Soit $y \in [f(a)\,;f(b)]$. La fonction $g : x \longmapsto f(x) - y$ est continue sur $[a\,;b]$ comme somme de fonctions continues sur $[a\,;b]$ et vérifie

$$g(a) = f(a) - y \leqslant 0 \qquad g(b) = f(b) - y \geqslant 0$$

D'après le **théorème des valeurs intermédiaires 1**, il existe $c \in [a\,;b]$ tel que $g(c) = 0$, c'est-à-dire que $f(c) = y$. □

Théorème 12.4.8 (Théorème des valeurs intermédiaires 3)
L'image continue d'un intervalle est un intervalle.

Preuve : Soient I un intervalle et f continue sur I. On pose $\mathrm{J} = f(\mathrm{I})$ et on se donne $y_1 < y_2$ dans J. Par définition, ces nombres peuvent s'écrire

$$y_1 = f(x_1) \qquad \text{et} \qquad y_2 = f(x_2) \qquad \text{avec} \qquad x_1, x_2 \in \mathrm{I}$$

Pour montrer que J est un intervalle, il suffit de montrer que J contient n'importe quelle valeur comprise entre y_1 et y_2. C'est exactement ce que dit le **théorème des valeurs intermédiaires 2**. □

Corollaire 12.4.9
Soient $a < b$ des nombres réels et f une fonction.

- *Si f est strictement croissante et continue sur $[a;b]$, alors $f([a;b]) = [f(a);f(b)]$.*
- *Si f est strictement croissante et continue sur $[a;b[$, alors $f([a;b[) = [f(a);\lim\limits_{b^-} f[$.*
- *Si f est strictement croissante et continue sur $]a;b]$, alors $f(]a;b]) =]\lim\limits_{a^+} f;f(b)]$.*
- *Si f est strictement croissante et continue sur $]a;b[$, alors $f(]a;b[) =]\lim\limits_{a^+} f;\lim\limits_{b^-} f[$.*
- *Si f est strictement décroissante et continue sur $[a;b]$, alors $f([a;b]) = [f(b);f(a)]$.*
- *Si f est strictement décroissante et continue sur $[a;b[$, alors $f([a;b[) =]\lim\limits_{b^-} f;f(a)]$.*
- *Si f est strictement décroissante et continue sur $]a;b]$, alors $f(]a;b]) = [f(b);\lim\limits_{a^+} f[$.*
- *Si f est strictement décroissante et continue sur $]a;b[$, alors $f(]a;b[) =]\lim\limits_{b^-} f;\lim\limits_{a^+} f[$.*

> Remarquons que l'existence de ces limites (finies ou infinies) est garantie par le **théorème de la limite monotone**. Nous allons nous abstenir de prouver ce théorème car il y a 8 cas à considérer et c'est reloud ; il s'agit simplement de combiner le **théorème de la limite monotone** et le **théorème des valeurs intermédiaires 3**.

Théorème 12.4.10 (Théorème de la bijection)
Soit f une fonction continue sur un intervalle I. *f réalise une injection sur* I *si et seulement si elle est strictement monotone. Dans ce cas, f réalise une bijection de* I *sur f(*I*) ; sa réciproque est continue et du même sens de variation que f.*

Preuve : Supposons d'abord f strictement monotone sur I. Alors si $x \neq y$ sont dans I, on peut comparer $f(x)$ et $f(y)$ avec une inégalité stricte et ils sont donc distincts.

Réciproquement, supposons que f est injective, mais que'elle n'est ni strictement croissante, ni strictement décroissante. Cela signifie qu'il existe $x_1 < y_1$ et $x_2 < y_2$ tels que

$$f(x_1) \geqslant f(y_1) \qquad \text{et} \qquad f(x_2) \leqslant f(y_2)$$

On peut même assurer que ces inégalités sont strictes car f est injective.

On pose alors $\forall \lambda \in [0;1] \qquad g(\lambda) = f(\lambda x_1 + (1-\lambda)x_2) - f(\lambda y_1 + (1-\lambda)y_2)$

Comme somme de composées de fonctions continues, g est continue sur I. De plus,

$$g(0) = f(x_2) - f(y_2) < 0 \qquad \text{et} \qquad g(1) = f(x_1) - f(y_1) > 0$$

D'après le **théorème des valeurs intermédiaires 1**, il existe $\lambda_0 \in [0;1]$ tel que $g(\lambda_0)$ soit nul. C'est-à-dire que

$$f(\lambda_0 x_1 + (1-\lambda_0)x_2) = f(\lambda_0 y_1 + (1-\lambda_0)y_2)$$

Comme f est injective,

$$\lambda_0 x_1 + (1-\lambda_0)x_2 = \lambda_0 y_1 + (1-\lambda_0)y_2$$

d'où

$$\lambda_0(x_1 - y_1) = (1-\lambda_0)(y_2 - x_2)$$

En outre, λ_0 ne peut être 0 ou 1 puisque $g(0) < 0$ et $g(1) > 0$. Donc le membre de gauche est strictement négatif et le membre de droite est strictement positif. C'est impossible. Donc f est soit strictement croissante, soit strictement décroissante.

Supposons maintenant que f est strictement monotone, donc injective sur I. Alors elle atteint toutes les valeurs dans J = f(I) et réalise donc une bijection de I sur J. Notons f^{-1} sa bijection réciproque et montrons qu'elle est continue, de même sens de variation que f.

Pour fixer les idées, supposons f strictement croissante et donnons-nous $y_1 < y_2$ dans J. On suppose que $f^{-1}(y_1) \geqslant f^{-1}(y_2)$. Comme f est croissante, appliquer f ne change pas le sens de l'inégalité donc $y_1 \geqslant y_2$. C'est une contradiction, donc $f^{-1}(y_1) < f^{-1}(y_2)$ et f^{-1} est strictement croissante sur J.

Finalement, supposons que f^{-1} n'est pas continue sur J. Il existe alors $y \in$ J tel que f^{-1} ne soit pas continue en y. Du coup, y ne peut être la borne droite ou la borne gauche de J puisqu'une fonction monotone sur un intervalle admet une limite aux bornes de celui-ci, d'après le **théorème de la limite monotone**. Autrement dit, y est à l'intérieur de J.

Dire que f^{-1} n'est pas continue en y signifie qu'il existe un $\varepsilon > 0$ tel que

$$\forall \eta > 0 \quad \exists y' \in]y-\eta\,;\,y+\eta[\cap \mathrm{J} \qquad |f^{-1}(y) - f^{-1}(y')| > \varepsilon$$

En particulier, si n est un entier non nul fixé, il existe $y_n \in$ J tel que

$$y - \frac{1}{n} \leqslant y_n \leqslant y + \frac{1}{n} \qquad \text{et} \qquad |f^{-1}(y) - f^{-1}(y_n)| > \varepsilon$$

D'après le **théorème des gendarmes** (pour les suites), la suite $(y_n)_{n\in\mathbb{N}}$ converge vers y.

Comme y est à l'intérieur de J, il existe $\alpha > 0$ tel que $]y-\alpha\,;\,y+\alpha[\subset$ J. Et comme $(y_n)_{n\in\mathbb{N}}$ converge vers y, il existe N $\in \mathbb{N}$ tel que

$$\forall n \in \geqslant \mathrm{N} \qquad y_n \in]y-\alpha\,;\,y+\alpha[\subset \mathrm{J}$$

Comme f^{-1} est croissante,

$$\forall n \geqslant \mathrm{N} \qquad f^{-1}(y-\alpha) \leqslant f^{-1}(y_n) \leqslant f^{-1}(y+\alpha)$$

Donc la suite $(f^{-1}(y_n))_{n\in\mathbb{N}^\star}$ est bornée et d'après le **théorème de Bolzano-Weierstrass**, il existe $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$, strictement croissante, telle que $(f^{-1}(y_{\varphi(n)}))_{n\in\mathbb{N}^\star}$ converge vers une limite qu'on note x. Or, f est continue en x donc d'après le **théorème de composition des limites**,

$$\lim_{n\to\infty} \underbrace{f(f^{-1}(y_{\varphi(n)}))}_{=y_{\varphi(n)}} = f(x)$$

et il s'ensuit que $f(x) = y$. Autrement dit, $x = f^{-1}(y)$. Or, on avait

$$\forall n \in \mathbb{N} \qquad |f^{-1}(y_{\varphi(n)}) - f^{-1}(y)| \geqslant \varepsilon$$

ce qui assure

$$|x - f^{-1}(y)| \geqslant \varepsilon > 0$$

par passage à la limite dans l'inégalité. C'est une contradiction. Donc f^{-1} est continue sur J. □

> C'est ce théorème qui garantit la continuité des fonctions réciproques que nous avons étudiées l'année dernière.
>
> Par exemple, cos est continue et strictement décroissante sur $[0\,;\,\pi]$. Elle réalise donc une bijection continue de $[0\,;\,\pi]$ sur $[-1\,;\,1]$; sa bijection réciproque, qu'on appelle arccos, est continue sur $[-1\,;\,1]$.

12.5 Dérivation

12.5.1 Résultats généraux

Définition 12.5.1
Soit f une fonction définie sur un intervalle I. Soit $a \in \mathrm{I}$. On dit que f *est dérivable en* a si, et seulement si, la fonction $\tau_a : x \longmapsto \dfrac{f(x)-f(a)}{x-a}$, définie sur $\mathrm{I}\setminus\{a\}$, peut être prolongée par continuité en a.

Cette définition admet plusieurs formulations équivalentes :

- D'après la définition du prolongement par continuité, f *est dérivable en* a si et seulement si τ_a admet en a une limite à gauche et une limite à droite et celles-ci sont égales.
  Leur valeur commune est appelée *nombre dérivé de* f *en* a et on le note $f'(a)$, $\frac{\mathrm{d}f}{\mathrm{d}x}(a)$ ou encore $\mathrm{D}f(a)$.
  Dans le cas où τ_a admet une limite en a à gauche, on dit que f *est dérivable à gauche en* a ; cette limite est notée $f'_g(a)$ et appelée *nombre dérivé à gauche de* f *en* a.
  Si τ_a admet une limite en a à droite, on dit que f *est dérivable à droite en* a ; cette limite est notée $f'_d(a)$ et appelée *nombre dérivé à droite de* f *en* a.
  Ainsi, f est dérivable en a si et seulement si elle est dérivable à gauche et à droite en a, et les dérivées à gauche et à droite sont égales. C'est cette valeur commune qui est le nombre dérivé de f en a.
- On a successivement

$$\begin{aligned} f \text{ dérivable en } a &\iff \lim_{x\to a} \frac{f(x)-f(a)}{x-a} = f'(a) \\ &\iff \frac{f(x)-f(a)}{x-a} \underset{x\to a}{=} f'(a)+\mathrm{o}(1) \\ f \text{ dérivable en } a &\iff f(x) \underset{x\to a}{=} f(a)+(x-a)f'(a)+\mathrm{o}(x-a) \end{aligned}$$

  À ce stade, on voit (intuitivement) que f est dérivable en a si, et seulement si, la droite d'équation « $y = f(a)+(x-a)f'(a)$ » approche, au voisinage de a, la courbe représentative de f avec une précision négaligeable devant $(x-a)$. La dérivabilité nous permet donc de trouver la meilleure approximation de f par une fonction linéaire, au voisinage de a.
- Puisque le point a, en lequel on étudie la dérivabilité de f, se trouve dans I, on peut aussi dire que

$$\begin{aligned} f \text{ dérivable en } a &\iff \lim_{h\to 0} \frac{f(a+h)-f(a)}{h} = f'(a) \\ &\iff f(a+h) \underset{h\to 0}{=} f(a)+hf'(a)+\mathrm{o}(h) \end{aligned}$$

  C'est cette formulation de la dérivabilité en a que nos manipulerons le plus, car elle se ramène à une étude en 0, toujours plus agréable à faire qu'en un autre point ; et elle a l'avantage d'utiliser la notation « petit o » qui est très souple.
  Ainsi, si on arrive à montrer qu'il existe un nombre réel ℓ tel que $f(a+h) \underset{h\to 0}{=} f(a)+h\ell+\mathrm{o}(h)$, alors f sera dérivable en a et ℓ est le nombre dérivé de f en a.

On constate que

Théorème 12.5.2
Si f est dérivable en a, alors f est continue en a.

Preuve : On sait que $$f(a+h) = f(a) + hf'(a) + o(h)$$

donc en particulier $$f(a+h) = f(a) + o(1)$$

ce qui signifie précisément que f admet une limite en a. Donc f est continue en a. □

N'allez surtout pas imaginer une réciproque à ce théorème : une fonction continue en un point n'a aucune raison d'être dérivable. Par exemple, la fonction $x \longmapsto |x|$ est continue en 0, mais pas dérivable en ce point, puisque les dérivées gauche et droite valent respectivement -1 et 1. Ou encore $x \longmapsto \sqrt{x}$ est continue en 0, mais le taux d'accroissement a une limite infinie en 0.

Voici maintenant les théorèmes généraux sur la dérivabilité :

Théorème 12.5.3
Soient f et g deux fonctions dérivables en a.

- *Leur somme est dérivable en a et $(f+g)'(a) = f'(a) + g'(a)$.*
- *Leur produit est dérivable en a et $(fg)'(a) = f'(a)g(a) + f(a)g'(a)$.*
- *Si g ne s'annule pas dans un voisinage de a, leur rapport est dérivable en a et*

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

Preuve : Supposons f et g dérivables en a. Cela signifie que

$$f(a+h) = f(a) + hf'(a) + o(h) \qquad \text{et} \qquad g(a+h) = g(a) + hg'(a) + o(h)$$

Alors $$(f+g)(a+h) = f(a+h) + g(a+h) = f(a) + g(a) + h(f'(a) + g'(a)) + o(h)$$

ce qui établit la première proposition. Ensuite,

$$(fg)(a+h) = f(a+h)g(a+h) = f(a)g(a) + h(f'(a)g(a) + g(a)f'(a)) + o(h) + \text{termes en } h^2$$

Les termes en h^2 sont négligeables devant h donc fg est dérivable en a et son nombre dérivé en a est $f'(a)g(a) + f(a)g'(a)$.

Enfin, pour le rapport, on a, en supposant $g(a) \neq 0$:

$$\frac{f(a+h)}{g(a+h)} = \frac{f(a) + hf'(a) + o(h)}{g(a) + hg'(a) + o(h)} = \frac{1}{g(a)} \frac{f(a) + hf'(a) + o(h)}{1 + hg'(a)/g(a) + o(h)}$$

On connaît l'approximation $\frac{1}{1+x} \underset{x\to 0}{=} 1 - x + o(x)$ donc

$$\begin{aligned}\frac{f(a+h)}{g(a+h)} &= \frac{1}{g(a)}(f(a) + hf'(a) + o(h))\left(1 - h\frac{g'(a)}{g(a)} + o(h)\right) \\ &= \frac{1}{g(a)}\left(f(a) + h\left(f'(a) - \frac{f(a)g'(a)}{g(a)}\right) + o(h) + \text{termes en } h^2\right)\end{aligned}$$

Les termes en h^2 sont négligeables devant h donc

$$\frac{f(a+h)}{g(a+h)} = \frac{f(a)}{g(a)} + h\frac{f'(a)g(a) - f(a)g'(a)}{g(a)^2} + o(h)$$

ce qui achève la démonstration. □

Théorème 12.5.4 (Dérivation d'une composée)
Soient f et g deux fonctions définies respectivement sur I *et* J*, telles que $f(\mathrm{I}) \subset \mathrm{J}$. On suppose f dérivable en $a \in \mathrm{I}$ et g dérivable en $f(a) \in \mathrm{J}$. Alors $g \circ f$ est dérivable en a et on a*

$$(g \circ f)'(a) = f'(a)\, g'(f(a))$$

Preuve : On sait que

$$f(a+h) = f(a) + hf'(a) + \mathrm{o}(h) \qquad \text{et} \qquad g(f(a)+h) = g(f(a)) + hg'(f(a)) + \mathrm{o}(h)$$

donc
$$\begin{aligned}(g \circ f)(a+h) &= g(f(a+h)) = g(f(a) + hf'(a) + \mathrm{o}(h)) \\ &= g(f(a)) + hg'(f(a))(hf'(a) + \mathrm{o}(h)) + \mathrm{o}(hf'(a) + \mathrm{o}(h)) \\ &= g(f(a)) + hf'(a)g'(f(a)) + \mathrm{o}(h)\end{aligned}$$

Ici, comme d'habitude, on a négligé les termes en h^2 devant h. □

Théorème 12.5.5 (Dérivée de l'inverse d'une bijection)
Soit f continue, bijective de I *sur $f(\mathrm{I})$, dérivable en $a \in \mathrm{I}$. Alors f^{-1} est dérivable en $f(a)$ si et seulement si $f'(a) \neq 0$ et on a*

$$(f^{-1})'(f(a)) = \frac{1}{f'(f(a))}$$

Preuve : Supposons d'abord que f^{-1} est dérivable en a. On sait que $f^{-1} \circ f$ est l'identité sur I donc sa dérivée vaut 1 en a. Mais aussi, d'après le théorème de dérivée d'une composée,

$$1 = (f^{-1} \circ f)'(a) = f'(a)(f^{-1})'(f(a))$$

donc $f'(a)$ n'est pas nul.

Réciproquement, supposons que $f'(a) \neq 0$. Comme f est continue, $\mathrm{J} = f(\mathrm{I})$ est un intervalle contenant $f(a)$ d'après le théorème des valeurs intermédiaires. Il existe donc $m > 0$ tel que l'intervalle $[f(a) - m\,;\, f(a) + m]$ soit inclus dans J.

Si h est un nombre réel tel que $|h| \leqslant m$, $f(a) + h$ appartient à J ; f étant bijective de I sur J, il existe un unique nombre $\mathrm{H}(h)$ tel que $f(a) + h = f(a + \mathrm{H}(h))$. D'ailleurs, on peut exprimer $\mathrm{H}(h)$ à l'aide de f^{-1} puisque :

$$f(a) + h = f(a + \mathrm{H}(h)) \iff \mathrm{H}(h) = f^{-1}(f(a) + h) - a$$

D'après le théorème de composition des limites et parce que f^{-1} est continue en $f(a)$ (théorème de la bijection), H admet une limite en 0 et

$$\lim_{h \to 0} \mathrm{H}(h) = \lim_{h \to 0} (f^{-1}(f(a) + h) - a) = a - a = 0$$

Maintenant qu'on sait que $\lim_0 \mathrm{H} = 0$, on peut écrire, à l'aide de la dérivabilité de f en a,

$$f(a) + h = f(a + \mathrm{H}(h)) = f(a) + \mathrm{H}(h) f'(a) + \mathrm{o}(\mathrm{H}(h))$$

d'où
$$h = \mathrm{H}(h) f'(a) + \mathrm{o}(\mathrm{H}(h))$$

soit encore, puisque $f'(a) \neq 0$, $\mathrm{H}(h) f'(a) \sim h$. Du coup, $\mathrm{H}(h) \sim h / f'(a)$ ce qui permet d'écrire

$$\mathrm{H}(h) = \frac{h}{f'(a)} + \mathrm{o}(h)$$

Il s'ensuit que $$f^{-1}(f(a)+h) = a + \mathrm{H}(h) = a + \frac{h}{f'(a)} + \mathrm{o}(h)$$

ce qui montre que f^{-1} est dérivable en $f(a)$ et donne la dérivée de f^{-1} en ce point. □

C'est ce théorème que nous avons utilisé pour démontrer la dérivabilité de toutes les fonctions réciproques que nous avons construites. Par exemple, la fonction sin est continue bijective de $[-\frac{\pi}{2}\,;\frac{\pi}{2}]$ sur $[-1\,;1]$. Si $a \in]-\frac{\pi}{2}\,;\frac{\pi}{2}[$, on a $\sin' a = \cos a$ qui n'est pas nul. Donc arcsin est dérivable en $\sin a$. C'est-à-dire que arcsin est dérivable sur $]-1\,;1[$.

12.5.2 Les espaces $\mathscr{C}^n$

Reloud.

12.5.3 Le théorème de Rolle et ses conséquences

Commençons par une observation sur les extrema d'une fonction :

Théorème 12.5.6
Soient f définie sur I *et a un point intérieur à* I. *On suppose que f est dérivable en a et qu'elle admet un extremum local en ce point. Alors $f'(a) = 0$.*

Preuve : Quitte à changer f en $-f$, on suppose que f admet un maximum local en a. Cela signifie qu'il existe $h > 0$ tel que $[a-h\,;a+h] \subset \mathrm{I}$ et que

$$\forall x \in [a-h\,;a+h] \qquad f(x) \leqslant f(a)$$

Alors $$\forall x \in [a-h\,;a[\qquad \frac{f(x)-f(a)}{x-a} \geqslant 0$$

et $$\forall x \in]a\,;a+h] \qquad \frac{f(x)-f(a)}{x-a} \leqslant 0$$

Puisque f admet une dérivée en a, les taux d'accroissements ci-dessus tendent vers $f'(a)$ en a et on peut appliquer le théorème de passage à la limite dans les inégalités :

$$f'(a) \geqslant 0 \qquad \text{et} \qquad f'(a) \leqslant 0$$

Par suite, $f'(a) = 0$. □

Ce théorème nous donne donc une condition nécessaire sur les extrema locaux d'une fonction f derivable sur I : ils doivent être cherchés parmi les zéros de f'.

Remarquons aussi qu'il n'y a pas de réciproque : ce n'est pas parce que $f'(a) = 0$ que f admet un extremum local en a. La fonction $x \longmapsto x^3$ est un bon contre-exemple.

Théorème 12.5.7 (Théorème de Rolle)
Soit f continue sur $[a\,;b]$, dérivable sur $]a\,;b[$, telle que $f(a) = f(b)$. Alors il existe $c \in]a\,;b[$ tel que $f'(c) = 0$.

Preuve : Comme f est continue sur $[a\,;b]$, elle est bornée et atteint ses bornes. Donc elle atteint son minimum m et son maximum M en des points c_m et c_{M} respectivement.

Si c_m et c_M ne sont tous deux pas intérieurs à $[a;b]$, c'est qu'ils valent soit a, soit b. Et donc que $f(a) = f(b) = m = M$. Auquel cas,

$$\forall x \in [a;b] \qquad m \leqslant f(x) \leqslant M = m$$

et f est constante. Sa dérivée s'annule en tout point de $]a;b[$ et le théorème est démontré.

Si c_m ou c_M est intérieur à $]a;b[$, le **théorème 5.6** montre que f' s'annule en ce point. □

Corollaire 12.5.8 (Théorème des accroissements finis)
Soit f continue sur $[a;b]$, dérivable sur $]a;b[$. Il existe $c \in]a;b[$ tel que $f(b) - f(a) = (b-a)f'(c)$.

Preuve : Posons $\forall x \in [a;b] \qquad g(x) = (f(b) - f(a))x - (b-a)f'(x)$

g est continue sur $[a;b]$, dérivable sur $]a;b[$ et on constate que

$$g(a) = g(b) = af(b) - bf(a)$$

D'après le **théorème de Rolle**, il existe $c \in]a;b[$ tel que $g'(c) = 0$. La calcul de g' donne alors

$$f(b) - f(a) - (b-a)f'(c) = 0$$ □

Corollaire 12.5.9 (Inégalité des accroissements finis)
Soit f continue sur $[a;b]$, dérivable sur $]a;b[$, telle que f' soit minorée par m et majorée par M sur $]a;b[$. Alors

$$m(b-a) \leqslant f(b) - f(a) \leqslant M(b-a)$$

Preuve : D'après le **théorème des accroissements finis**, il existe $c \in]a;b[$ tel que

$$f(b) - f(a) = (b-a)f'(c)$$

Dans la mesure où $b - a \geqslant 0$ et $m \leqslant f'(c) \leqslant M$, on a bien l'inégalité recherchée. □

Corollaire 12.5.10 (Caractérisation des fonctions constantes sur un intervalle)
Soit f continue et dérivable sur $[a;b]$. Elle est constante sur cet intervalle si et seulement sa dérivée y est identiquement nulle.

Preuve : Si f est constante sur $[a;b]$, sa dérivée y est nulle, on le sait déjà.

Réciproquement, supposons que $f' = 0$ sur $[a;b]$. Soit $x \in]a;b]$. D'après le **théorème des accroissements finis**, il existe $c \in]a;x[$ tel que

$$f(x) - f(a) = (x-a)f'(c) = 0$$

donc $$f(x) = f(a)$$

et f est bien constante sur $[a;b]$. □

Corollaire 12.5.11 (Sens de variation et signe de la dérivée)
Soit f continue sur $[a;b]$, dérivable sur $]a;b[$. Elle est croissante sur $[a;b]$ si et seulement si f' est positive sur $]a\ b[$.

Si f' est strictement positive sur $]a;b[$, alors f est strictement croissante sur $[a;b]$.

Preuve : Supposons f' positive sur $]a;b[$. Soient x et y dans $[a;b]$, tels que $x<y$. D'après le **théorème des accroissements finis**, il existe $c\in]x;y[$ tel que

$$f(y)-f(x)=(y-x)f'(c)\geqslant y-x\geqslant 0$$

donc

$$f(y)\geqslant f(x)$$

et f est croissante. Si on avait supposé f' strictement positive sur $]a;b[$, les inégalités ci-dessus auraient été strictes et on aurait obtenu que f' est strictement croissante.

Réciproquement, supposons f croissante sur $[a;b]$. Soit $x_0\in]a;b[$. On a

$$\forall x\in[a;b]\qquad\begin{cases}x<x_0\implies\dfrac{f(x)-f(x_0)}{x-x_0}\geqslant 0\\ x>x_0\implies\dfrac{f(x)-f(x_0)}{x-x_0}\geqslant 0\end{cases}$$

Dans le premier cas, numérateur et dénominateur sont négatifs ; dans le second, ils sont positifs. Donc, en faisant tendre x vers x_0, on trouve $f'(x_0)\geqslant 0$. □

Corollaire 12.5.12 (Théorème des accroissements finis généralisé)
Soient f et g deux fonctions continues sur $[a;b]$, dérivables sur $]a;b[$. On suppose que g' ne s'annule pas sur $]a;b[$. Alors il existe $c\in]a;b[$ tel que

$$\frac{f(b)-f(a)}{g(b)-g(a)}=\frac{f'(c)}{g'(c)}$$

> Observons que la seule hypothèse « g' ne s'annule pas sur $]a;b[$ » suffit à assurer que $g(b)-g(a)\neq 0$ et autorise donc à former le rapport $\dfrac{f(b)-f(a)}{g(b)-g(a)}$: c'est simplement la contraposée du **théorème de Rolle**.

Preuve : Il suffit de poser

$$\forall x\in[a;b]\qquad h(x)=(f(b)-f(a))g(x)-(g(b)-g(a))f(x)$$

h est continue sur $[a;b]$, dérivable sur $]a;b[$ et prend la même valeur en a et b. Il suffit d'appliquer le **théorème de Rolle**. □

Corollaire 12.5.13 (Théorème de Taylor)
Soit f une fonction de classe $\mathscr{C}^n$ sur $[a;b]$, $n+1$ fois dérivable sur $]a;b[$. Il existe $c\in]a;b[$ tel que

$$f(b)=\sum_{k=0}^{n}\frac{f^{(k)}(a)}{k!}(b-a)^k+\frac{f^{(n+1)}(c)}{(n+1)!}(b-a)^{n+1}$$

Preuve : Posons

$$\forall x\in[a;b]\qquad \mathrm{F}(x)=f(x)-\sum_{k=0}^{n}\frac{f^{(k)}(a)}{k!}(x-a)^k\qquad\text{et}\qquad \mathrm{G}(x)=\frac{(x-a)^{n+1}}{(n+1)!}$$

Les fonctions F et G sont n fois dérivables sur $[a;b]$ et un simple calcul donne leurs dérivées successives :

$$\forall p \in [\![0\,;n]\!] \quad \forall x \in [a\,;b] \qquad \begin{cases} \mathrm{F}^{(p)}(x) = f^{(p)}(x) - \displaystyle\sum_{k=0}^{n-p} \frac{f^{(k+p)}(x)}{k!}(x-a)^k \\ \mathrm{G}^{(p)}(x) = \dfrac{(x-a)^{n+1-p}}{(n+1-p)!} \end{cases}$$

En particulier, $\forall p \in [\![0\,;n]\!] \qquad \begin{cases} \mathrm{F}^{(p)}(a) = f^{(p)}(a) - f^{(p)}(a) = 0 \\ \mathrm{G}^{(p)}(a) = 0 \end{cases}$

Ces calculs étant faits, commençons la preuve proprement dite. F et G sont continues sur $[a\,;b]$, dérivables sur $]a\,;b[$ et G′ ne s'annule pas sur $]a\,;b[$. D'après le **théorème des accroissements finis généralisé**, il existe $c_1 \in]a\,;b[$ tel que

$$\frac{\mathrm{F}(b)-\mathrm{F}(a)}{\mathrm{G}(b)-\mathrm{G}(a)} = \frac{\mathrm{F}'(c_1)}{\mathrm{G}'(c_1)}$$

Comme F, G, F′, G′ s'annulent en a, on peut aussi écrire :

$$\frac{\mathrm{F}(b)}{\mathrm{G}(b)} = \frac{\mathrm{F}'(c_1)-\mathrm{F}'(a)}{\mathrm{G}'(c_1)-\mathrm{G}'(a)}$$

Les fonctions F′ et G′ sont continues sur $[a\,;b]$, dérivables sur $]a\,;b[$ et G″ ne s'annule pas sur $]a\,;b[$. D'après le **théorème des accroissements finis généralisé**, il existe $c_2 \in]a\,;c_1[$ tel que

$$\frac{\mathrm{F}(b)}{\mathrm{G}(b)} = \frac{\mathrm{F}'(c_1)-\mathrm{F}'(a)}{\mathrm{G}'(c_1)-\mathrm{G}'(a)} = \frac{\mathrm{F}''(c_2)}{\mathrm{G}''(c_2)}$$

Mais comme $\mathrm{F}''(a) = \mathrm{G}''(a) = 0$, on a aussi

$$\frac{\mathrm{F}(b)}{\mathrm{G}(b)} = \frac{\mathrm{F}''(c_2)-\mathrm{F}''(a)}{\mathrm{G}''(c_2)-\mathrm{G}''(a)}$$

Et on continue. On trouve de proche-en-proche des réels $c_0 > c_1 > \ldots > c_{n+1} > a$ tels que

$$\frac{\mathrm{F}(b)}{\mathrm{G}(b)} = \frac{\mathrm{F}'(c_1)}{\mathrm{G}'(c_1)} = \cdots = \frac{\mathrm{F}^{(n)}(c_n)}{\mathrm{G}^{(n)}(c_n)} = \frac{\mathrm{F}^{(n+1)}(c_{n+1})}{\mathrm{G}^{(n+1)}(c_{n+1})}$$

Or, $\forall x \in]a\,;b[\qquad \mathrm{F}^{(n+1)}(x) = f^{(n+1)}(x) \qquad \text{et} \qquad \mathrm{G}^{(n+1)}(x) = 1$

donc $$\frac{\mathrm{F}(b)}{\mathrm{G}(b)} = f^{(n+1)}(c_{n+1})$$

soit $$f(b) - \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k = \frac{f^{(n+1)}(c_{n+1})}{(n+1)!}(x-a)^{n+1}$$ □

Corollaire 12.5.14 (Théorème de Taylor-Young)
Soit f une fonction de classe $\mathscr{C}^n$ sur un voisinage de a. Alors

$$f(x) \underset{x\to a}{=} \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k + o((x-a)^n)$$

Preuve : Si $n = 0$, le résultat est clair. Si $n > 0$, f est *a fortiori* de classe $\mathscr{C}^{n-1}$ sur un voisinage V de a, et dérivable n fois dans V. D'après le **théorème de Taylor**, si $x \in \mathrm{V}$, il existe $c(x)$ compris entre a et x tel que

$$f(x) = \sum_{k=0}^{n-1} \frac{f^{(k)}(a)}{k!}(x-a)^k + \frac{f^{(n)}(c(x))}{n!}(x-a)^n$$

donc
$$\frac{f(x) - \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k}{(x-a)^n} = \frac{f^{(n)}(c(x)) - f^{(n)}(a)}{n!}$$

Or,
$$|a - c(x)| \leqslant |a - x|$$

donc $c(x) \xrightarrow[x\to a]{} a$. Comme $f^{(n)}$ est continue en a,

$$\frac{f(x) - \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k}{(x-a)^n} = \frac{f^{(n)}(c(x)) - f^{(n)}(a)}{n!} \xrightarrow[x\to a]{} 0$$

Autrement dit,
$$f(x) \underset{x\to a}{=} \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k + o((x-a)^n)$$ □

Corollaire 12.5.15 (Inégalité de Taylor-Lagrange)
Soit f une fonction de classe $\mathscr{C}^n$ et $n+1$ fois dérivable sur un voisinage V *de a. On suppose $f^{(n+1)}$ bornée sur* V*, par un réel* $M > 0$*. Alors*

$$\forall x \in V \qquad \left| f(x) - \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k \right| \leqslant \frac{M|x-a|^{n+1}}{(n+1)!}$$

Preuve : C'est une simple application du théorème de Taylor : si $x \in V$, il existe c entre a et x tel que

$$\left| f(x) - \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k \right| = \left| \frac{f^{(n+1)}(c)}{(n+1)!}(x-a)^{n+1} \right| \leqslant \frac{M|x-a|^{n+1}}{(n+1)!}$$ □

12.5.4 La méthode de Newton

La méthode de Newton propose un algorithme pour trouver numériquement les zéros d'une fonction. Elle est décrite et étudiée dans un DM.

12.6 Fonctions usuelles

Il s'agit dans ce paragraphe de définir proprement toutes les fonctions élémentaires utilisées en mathématiques. On admet seulement, pour l'instant, le théorème d'existence de primitives pour les fonctions continues sur un intervalle :

Théorème 12.6.1
Soit f une fonction continue sur un intervalle I*. Alors f admet des primitives sur* I*. Deux primitives de f ont une différence constante.*

Preuve : La preuve de l'existence sera faite dans le chapitre d'intégration. Si F et G sont deux primitives de f sur I, alors

$$\forall x \in I \qquad F'(x) = f(x) = G'(x)$$

donc $$\forall x \in I \qquad (F-G)'(x) = 0$$

Comme I est un intervalle, on sait que F – G est constante sur I. □

12.6.1 La fonction inverse

La fonction inverse est la fonction $f : x \longmapsto \frac{1}{x}$. Elle est définie et continue sur $\mathbb{R}^\star$, d'après les théorèmes généraux d'existence de limites. Mais elle est aussi dérivable sur cet intervalle d'après le théorème de dérivation d'un inverse et l'on a

$$\forall x \in \mathbb{R}^\star \qquad f'(x) = -\frac{1}{x^2}$$

Comme la fonction $x \longmapsto x^2$ ne s'annule pas sur $\mathbb{R}^\star$ et est dérivable, on voit que f' est dérivable et

$$\forall x \in \mathbb{R}^\star \qquad f''(x) = -\frac{-2x}{x^4} = \frac{2}{x^3}$$

On voit alors qu'on peut montrer, par une récurrence immédiate, que f est de classe $\mathscr{C}^\infty$ sur $\mathbb{R}^\star$ et

$$\forall n \in \mathbb{N} \quad \forall x \in \mathbb{R}^\star \qquad f^{(n)}(x) = \frac{(-1)^n n!}{x^{n+1}}$$

Ceci permet de calculer en particulier le développement de Taylor de f au voisinage de 1, pour tout entier n :

$$\frac{1}{1-x} = f(1-x) \underset{x=1}{=} \sum_{k=0}^{n} \frac{f^{(k)}(1)}{k!}(-x)^k + o(x^n)$$

d'où $$\boxed{\frac{1}{1-x} \underset{h=0}{=} \sum_{k=0}^{n} x^k + o(x^n)}$$

Il est évidemment naturel de se demander si, pour un x fixé, ce développement converge vers $f(x)$. La réponse est positive si, et seulement si, $|x| < 1$: montrons-le. On se donne un réel x. On a

$$\forall n \in \mathbb{N} \qquad \sum_{k=0}^{n} x^k = \frac{1-x^{n+1}}{1-x} = \frac{1}{1-x} - \frac{x^{n+1}}{1-x}$$

donc $$\forall x \in \mathbb{N} \qquad \left|\frac{1}{1-x} - \sum_{k=0}^{n} x^k\right| = \frac{|x|^{n+1}}{|1-x|}$$

La suite $(|x|^{n+1})_{n\in\mathbb{N}}$ tend vers 0 si, et seulement si, $|x| < 1$. D'où

$$\boxed{\forall x \in]-1\,;1[\qquad \frac{1}{1-x} = \lim_{n\to\infty} \sum_{k=0}^{n} x^k}$$

12.6.2 Le Logarithme Népérien

On a maintenant tous les outils pour définir l'une des fonctions usuelles fondamentales : le logarithme népérien. À l'aide du **Théorème 11.6.1**, on sait que

Définition 12.6.2
Il existe une unique primitive de la fonction $x \longmapsto 1/x$ sur $\mathbb{R}_+^\star$ s'annulant en 1. Cette fonction est appelée logarithme népérien (ou tout simplement logarithme) et on la note ln.

Cette définition est suffisante pour déduire toutes les propriétés connues du logarithme :

Théorème 12.6.3

1. $\forall x \in \mathbb{R}_+^\star \qquad \ln' x = \dfrac{1}{x} \qquad et \qquad \ln 1 = 0$
2. $\forall x \in \mathbb{R}_+^\star \quad \forall y \in \mathbb{R}_+^\star \qquad \ln(xy) = \ln x + \ln y \qquad et \qquad \ln \dfrac{x}{y} = \ln x - \ln y$
3. $\forall x \in \mathbb{R}_+^\star \quad \forall n \in \mathbb{N} \qquad \ln(x^n) = n \ln x$
4. ln *est une fonction strictement croissante sur* $\mathbb{R}_+^\star$.
5. $\lim\limits_{x \to +\infty} \ln x = +\infty \qquad et \qquad \lim\limits_{x \to 0^+} \ln x = -\infty$
6. ln *réalise une bijection de* $\mathbb{R}_+^\star$ *sur* $\mathbb{R}$.
7. *Soit* f *une fonction dérivable, strictement positive, sur un intervalle* I. *La fonction* $\ln \circ f$ *est dérivable sur* I *et*
$$\forall x \in \mathrm{I} \qquad (\ln \circ f)'(x) = \frac{f'(x)}{f(x)}$$

Preuve : On démontre chacune de ces propriétés.

1. Il s'agit simplement de la définition du logarithme : c'est une primitive de $x \longmapsto 1/x$ sur $\mathbb{R}_+^\star$ donc sa dérivée est $x \longmapsto 1/x$ et elle s'annule en 1.
2. On fixe un nombre strictement positif y et on définit la fonction
$$\forall x \in \mathbb{R}_+^\star \qquad g(x) = \ln(xy) - \ln y$$
Alors g est dérivable sur I, comme composée de deux fonctions dérivables. Et on a, d'après le théorème de dérivation d'une composée :
$$\forall x \in \mathbb{R}_+^\star \qquad g'(x) = y \times \frac{1}{xy} = \frac{1}{x}$$
En outre, $$g(1) = \ln y - \ln y = 0$$
Comme ln est l'unique fonction satisfaisant ces deux propriétés,
$$\forall x \in \mathbb{R}_+^\star \qquad \ln x = g(x) = \ln(xy) - \ln y$$
d'où $$\forall x \in \mathbb{R}_+^\star \qquad \ln(xy) = \ln x + \ln y$$
Puisque y a été choisi arbitrairement, la première partie de la proposition est vérifiée.
On s'attaque à présent au calcul de $\ln(x/y)$. Pour cela, il suffit de constater que
$$\forall x \in \mathbb{R}_+^\star \quad \forall y \in \mathbb{R}_+^\star \qquad \ln x = \ln\left(\frac{x}{y} \times y\right) = \ln \frac{x}{y} + \ln y$$
d'où $$\forall x \in \mathbb{R}_+^\star \quad \forall y \in \mathbb{R}_+^\star \qquad \ln \frac{x}{y} = \ln x - \ln y$$
3. La propriété 2 nous dit que le logarithme d'un produit est la somme des logarithmes de chacun des termes de ce produit. Puisque x^n est le produit de n termes égaux à x, on a
$$\forall x \in \mathbb{R}_+^\star \quad \forall n \in \mathbb{N} \qquad \ln(x^n) = \underbrace{\ln x + \cdots + \ln x}_{n \text{ fois}} = n \ln x$$

4. D'après la première propriété, la dérivée de ln est la fonction $x \longmapsto 1/x$, qui est strictement positive sur $\mathbb{R}_+^\star$. Donc ln est strictement croissante sur cet intervalle.
5. Puisque ln est une fonction strictement croissante, on sait qu'elle admet une limite, finie ou infinie, en $+\infty$ d'après le théorème de la limite monotone. On constate alors que le logarithme n'est pas une fonction bornée puisque

$$\forall n \in \mathbb{N} \qquad \ln 2^n = n \ln 2$$

qui peut être rendu aussi grand que l'on veut en choisissant n de plus en plus grand. Par suite,

$$\lim_{x \to +\infty} \ln x = +\infty$$

Intéressons-nous maintenant à la limite en 0^+. On a

$$\forall x > 0 \qquad \ln x = \ln \frac{1}{1/x} = -\ln \frac{1}{x}$$

Or, $$\lim_{x \to 0^+} \frac{1}{x} = +\infty \qquad \text{et} \lim_{x \to +\infty} -\ln x = -\infty$$

donc d'après le théorème de composition des limites,

$$\lim_{x \to 0^+} \ln x = \lim_{x \to 0^+} \left(-\ln \frac{1}{x}\right) = \lim_{x \to +\infty} \left(-\ln x\right) = -\infty$$

6. D'après la propriété de croissance stricte du logarithme, et les valeurs de ses limites en 0^+ et en $+\infty$, elle réalise bien une bijection de $\mathbb{R}_+^\star$ sur $\mathbb{R}$.
7. Soit f une fonction dérivable et strictement positive sur un intervalle I. D'après le théorème de dérivation d'une composée, la fonction $\ln \circ f$ est dérivable sur I et

$$\forall x \in \mathrm{I} \qquad (\ln \circ f)'(x) = f'(x) \ln'\big(f(x)\big) = \frac{f'(x)}{f(x)}$$

Comme pour la fonction inverse, il est toujours bon de s'intéresser à la régularité du logarithme :

Théorème 12.6.4
La fonction ln *est de classe* $\mathscr{C}^\infty$ *sur* $\mathbb{R}_+^\star$. *De plus, pour tout entier* n,

$$\ln(1-x) \underset{x \to 1}{=} -\sum_{k=1}^{n} \frac{x^k}{k} + o(x^n)$$

et $$\forall x \in [-1\,;1[\qquad \ln(1-x) = -\lim_{n \to \infty} \sum_{k=1}^{n} \frac{x^k}{k}$$

Preuve : Comme la dérivée de ln sur $\mathbb{R}_+^\star$ est de classe $\mathscr{C}^\infty$, le logarithme est aussi infiniment dérivable. De plus, les calculs du pargraphe précédent montrent que

$$\forall n \in \mathbb{N}^\star \quad \forall x \in \mathbb{R}_+^\star \qquad \ln^{(n)} x = \frac{(-1)^{n-1}(n-1)!}{x^n}$$

Pour tout entier n, on peut utiliser le théorème de Taylor-Young au voisinage de 1 :

$$\ln(1-x) \underset{x\to 1}{=} \sum_{k=1}^{n} \frac{(-1)^{k-1}(k-1)!}{k!}(-x)^k + o(x^n) = -\sum_{k=1}^{n} \frac{x^k}{k} + o(x^n)$$

Enfin, on fixe $x \in]-1;1[$ et un entier n non nul. On pose

$$\forall y \in [-|x|;|x|] \qquad f(y) = \ln(1-y) + \sum_{k=1}^{n} \frac{y^k}{k}$$

f est dérivable sur $[-|x|;|x|]$ et l'on a

$$\forall y \in [-|x|;|x|] \qquad f'(y) = -\frac{1}{1-y} + \sum_{k=1}^{n} y^{k-1} = -\frac{1}{1-y} + \sum_{k=0}^{n-1} y^k = -\frac{y^n}{1-y}$$

donc $$\forall y \in [-|x|;|x|] \qquad |f'(y)| = \frac{|y|^n}{1-y} \leqslant \frac{|x|^n}{1-|x|}$$

On peut alors appliquer l'inégalité des accroissements finis sur l'intervalle $[0;x]$ ou $[x;0]$, suivant que x est positif ou négatif :

$$|f(x) - f(0)| \leqslant |x| \times \frac{|x|^n}{1-|x|} = \frac{|x|^{n+1}}{1-|x|}$$

On a montré $$\forall n \in \mathbb{N}^\star \qquad \left|\ln(1-x) + \sum_{k=1}^{n} \frac{x^k}{k}\right| \leqslant \frac{|x|^{n+1}}{1-|x|}$$

Mais comme $|x| < 1$, la suite $(|x|^n)_{n\in\mathbb{N}}$ tend vers 0. D'où

$$\forall x \in]-1;1[\qquad \ln(1-x) = -\lim_{n\to\infty} \sum_{k=1}^{n} \frac{x^k}{k}$$

Mais ceci ne suffit par à établir la convergence lorsque $x = -1$. Pour ce faire, on a besoin de l'inégalité de Taylor-Lagrange. On note $g : x \longmapsto \ln(1-x)$, définie sur $[-1;0]$ et infiniment dérivable. Si $k \in \mathbb{N}^\star$ est donné, on sait que

$$\forall x \in [-1;0] \qquad g^{(k)}(x) = -\frac{(n-1)!}{(1-x)^k}$$

donc $$\forall x \in [-1;0] \qquad |g^{(k)}(x)| \leqslant (k-1)!$$

D'après l'inégalité de Taylor-Lagrange appliquée sur $[-1;0]$,

$$\begin{aligned}\forall n \in \mathbb{N}^\star \qquad \left|\ln 2 + \sum_{k=1}^{n} \frac{(-1)^k}{k}\right| &= \left|g(-1) - \sum_{k=1}^{n} \frac{g^{(k)}(0)}{k!}\right| \\ &\leqslant \frac{|-1-0|}{(n+1)!} \sup_{x\in[-1;0]} |g^{(n+1)}(x)| \leqslant \frac{1}{n+1}\end{aligned}$$

Le membre de droite tend vers 0 donc on a gagné. □

12.6.3 L'Exponentielle Népérienne

On vient de voir que le logarithme est une bijection de $\mathbb{R}_+^\star$ sur $\mathbb{R}$. Cette fonction admet donc une réciproque, définie sur $\mathbb{R}$ et à valeurs dans $\mathbb{R}_+^\star$.

Définition 12.6.5
On appelle exponentielle népérienne (ou tout simplement exponentielle) la réciproque du logarithme sur $\mathbb{R}$. Il s'agit d'une fonction définie sur $\mathbb{R}$, à valeurs strictement positives, notée exp.

Théorème 12.6.6

1. $\exp 0 = 1$.
2. *La fonction exponentielle est dérivable sur* $\mathbb{R}$ *et*
$$\forall x \in \mathbb{R} \qquad \exp' x = \exp x$$
3. *La fonction exponentielle est strictement croissante sur* $\mathbb{R}$ *et*
$$\lim_{x\to-\infty} \exp x = 0 \qquad \lim_{x\to+\infty} \exp x = +\infty$$
4. $\forall x \in \mathbb{R} \quad \forall y \in \mathbb{R} \qquad \exp(x+y) = \exp x \times \exp y \qquad et \qquad \exp(x-y) = \dfrac{\exp x}{\exp y}$
5. $\forall x \in \mathbb{R} \quad \forall n \in \mathbb{N} \qquad \exp(nx) = (\exp x)^n$

Preuve :

1. On sait que $\ln 1 = 0$, d'après la définition du logarithme. Or, d'après la **Définition 1.3**, $\exp 0$ est l'unique solution de l'équation $\ln y = 0$. Par suite, $\exp 0 = 1$.
2. On invoque le **Théorème 1.5** : puisque ln est dérivable sur $\mathbb{R}_+^\star$ et sa dérivée ne s'annule jamais sur cet intervalle, exp est derivable sur $\mathbb{R}$. En outre, si $x \in \mathbb{R}$,
$$\exp' x = \frac{1}{\ln'(\exp x)} = \frac{1}{1/\exp x} = \exp x$$
3. Puisque la fonction exp prend ses valeurs dans $\mathbb{R}_+^\star$, elle est strictement positive. Sa dérivée (qui est elle-même) est donc strictement positive et exp est strictement croissante.
   D'après le théorème de la limite monotone, exp admet une limite ℓ en $-\infty$ et une limite L en $+\infty$. D'après le théorème de composition des limites,
$$\left.\begin{array}{l} \lim\limits_{x\to0^+} \ln x = -\infty \\ \lim\limits_{x\to-\infty} \exp x = \ell \end{array}\right\} \quad \text{donc} \quad \ell = \lim_{x\to-\infty} \exp x = \lim_{x\to0^+} \exp(\ln x) = \lim_{x\to0^+} x = 0$$
   De la même manière, on montre que $L = +\infty$.
4. Soient x et y deux nombres réels. Puisque ln et exp sont réciproques l'une de l'autre, en posant
$$x_0 = \exp x \qquad \text{et} \qquad y_0 = \exp y$$
   on a
$$\ln x_0 = x \qquad \text{et} \qquad \ln y_0 = y$$
   Alors
$$\exp(x+y) = \exp(\ln x_0 + \ln y_0) = \exp(\ln x_0 y_0) = x_0 y_0 = \exp x \times \exp y$$
   ce qui établit la première propriété.
   Pour la deuxième, d'après ce qu'on vient de démontrer,
$$\exp(x-y) \times \exp y = \exp(x-y+y) = \exp x$$
   d'où
$$\exp(x-y) = \frac{\exp x}{\exp y}$$

5. On vient de voir que l'exponentielle d'une somme est le produit des exponentielles de chacun des termes de la somme. En particulier, si x est un réel et n un entier,

$$\exp(nx) = \exp\Big(\sum_{k=1}^{n} x\Big) = \prod_{k=1}^{n} \exp x = (\exp x)^n$$ □

Passons aux propriétés de régularité :

Théorème 12.6.7
exp est de classe $\mathscr{C}^\infty$ sur $\mathbb{R}$. De plus, pour tout entier n,

$$exp(x) \underset{x\to 0}{=} \sum_{k=0}^{n} \frac{x^k}{k!} + o(x^n)$$

et

$$\forall x \in \mathbb{R} \qquad exp\, x = \lim_{n\to\infty} \sum_{k=0}^{n} \frac{x^k}{k!}$$

Preuve : Le caractère $\mathscr{C}^\infty$ est évident puisque exp est dérivable et $\exp' = \exp$. Par suite,

$$\forall n \in \mathbb{N} \qquad \exp^{(n)} = \exp \qquad \text{et} \qquad \exp^{(n)}(0) = 1$$

Donc si $n \in \mathbb{N}$ est donné, le théorème de Taylor appliqué au voisinage de 0 donne

$$\exp x \underset{x\to 0}{=} \sum_{k=0}^{n} \frac{x}{k!} + \mathrm{o}\,(x^n)$$

On montre maintenant que le développement de Taylor est convergent. Soient $x \in \mathbb{R}$, non nul et $n \in \mathbb{N}$. On a

$$\forall y \in [-|x|\,;\,|x|] \qquad |\exp^{(n)}(y)| = \exp y \leqslant \exp|x|$$

D'après l'inégalité de Taylor-Lagrange appliquée sur $\mathrm{I} = [0\,;\,x]$ ou $\mathrm{I} = [x\,;\,0]$, suivant que x est positif ou négatif,

$$\Big|\exp x - \sum_{k=0}^{n} \frac{x^k}{k!}\Big| \leqslant \frac{|x|}{(n+1)!} \operatorname*{Sup}_{y\in \mathrm{I}} |\exp^{(n)}(y)| \leqslant \frac{|x| \exp(|x|)}{(n+1)!}$$

Le membre de droite tend vers 0 lorsque n tend vers l'infini, tout est bel et bon. □

12.6.4 Logarithmes et Exponentielles de Base a

Dans toute cette section, on se donne un nombre réel $a > 0$ différent de 1.

Définition 12.6.8
La fonction logarithme de base a, notée $\log_a$, est définie par

$$\forall x \in \mathbb{R}_+^\star \qquad \log_a x = \frac{\ln x}{\ln a}$$

Cette fonction $\log_a$ est proportionnelle au logarithme népérien, donc elle possède les mêmes propriétés à une différence près :

Théorème 12.6.9
1. $\forall x \in \mathbb{R}_+^\star \qquad \log_a' x = \dfrac{1}{x \ln a} \qquad et \qquad \ln 1 = 0$

2. $\forall x \in \mathbb{R}_+^\star \quad \forall y \in \mathbb{R}_+^\star \qquad \log_a(xy) = \log_a x + \log_a y \qquad et \qquad \log_a \dfrac{x}{y} = \log_a x - \log_a y$
3. $\forall x \in \mathbb{R}_+^\star \quad \forall n \in \mathbb{N} \qquad \log_a(x^n) = n \log_a x$
4. $\log_a$ *est une fonction strictement croissante sur* $\mathbb{R}_+^\star$ *si* $a > 1$ *et strictement décroissante si* $a < 1$.
5. $\lim\limits_{x\to+\infty} \log_a x = \begin{cases} +\infty & si\ a > 1 \\ -\infty & si\ 0 < a < 1 \end{cases} \qquad et \qquad \lim\limits_{x\to 0^+} \log_a x = \begin{cases} -\infty & si\ a > 1 \\ +\infty & si\ a < 1 \end{cases}$
6. $\log_a$ *réalise une bijection de* $\mathbb{R}_+^\star$ *sur* $\mathbb{R}$.

Preuve : Toutes les propriétés sont des conséquences directes des propriétés correspondantes pour le logarithme, sauf la 4$^{\text{eme}}$ sur le sens de variation de $\log_a$.

Comme le logarithme est strictement croissant et que $\ln 1 = 0$, il vient

$$\begin{cases} \ln a > 0 & \text{si } a > 1 \\ \ln a < 0 & \text{si } a < 1 \end{cases}$$

Par conséquent $\begin{cases} \log_a \text{ croît} & \text{si } a > 1 \\ \log_a \text{ décroît} & \text{si } a < 1 \end{cases}$ □

Nous allons voir que le logarithme de base a d'un nombre x est la puissance à laquelle il faut élever a pour obtenir x. Mais on ne sait pas encore ce que signifient a^π ou $a^{\sqrt{2}}$. Pour définir ces nouvelles opérations, on étudie les bijections réciproques des fonctions $\log_a$.

Définition 12.6.10
On appelle exponentielle de base a la bijection réciproque de $\log_a$. Il s'agit de l'unique fonction, notée $\exp_a$, définie sur $\mathbb{R}$, à valeurs dans $\mathbb{R}_+^\star$ telle que

$$\forall x \in \mathbb{R} \qquad \log_a(\exp_a x) = x$$

Théorème 12.6.11
1. $\forall x \in \mathbb{R} \qquad \exp_a x = \exp(x \ln a)$
2. $\exp_a 0 = 1 \qquad et \qquad \exp_a 1 = a$
3. *La fonction* $\exp_a$ *est dérivable sur* $\mathbb{R}$ *et*

$$\forall x \in \mathbb{R} \qquad \exp_a' x = \ln a \times \exp_a x$$

4. *Si* $a > 1$ *(resp.* $a < 1$*), la fonction* $\exp_a$ *est strictement croissante (resp. décroissante) sur* $\mathbb{R}$. *En outre,*

$$\lim_{x\to+\infty} \exp_a x = +\infty \ (resp.\ 0) \qquad et \lim_{x\to-\infty} \exp_a x = 0 \ (resp.\ +\infty)$$

5. $\forall x \in \mathbb{R} \quad \forall y \in \mathbb{R} \qquad \exp_a(x+y) = \exp_a x \times \exp_a y \qquad et \qquad \exp_a(x-y) = \dfrac{\exp_a x}{\exp_a y}$
6. $\forall x \in \mathbb{R} \quad \forall n \in \mathbb{N} \qquad \exp_a(nx) = (\exp_a x)^n$

Preuve : Une fois le premier résultat établi, tous les autres en seront des conséquences directes, avec l'aide du **Théorème 2.4** et des théorèmes de manipulations de limites.

Ainsi, soit $x \in \mathbb{R}$. D'après les **Définition 2.3** et **2.1**,

$$x = \log_a(\exp_a x) = \frac{\ln \exp_a x}{\ln a}$$

d'où $$\ln \exp_a x = x \ln a$$

et $$\exp_a x = \exp(x \ln a)$$ □

On constate alors, à l'aide des propriétés 2 et 6 que

$$\forall n \in \mathbb{N} \qquad \exp_a n = (\exp_a 1)^n = a^n$$

C'est-à-dire que $\exp_a$ est définie sur tout $\mathbb{R}$ et prend pour valeur aux entièrs les puissances entières correspondantes de a. Il est donc naturel de définir

Définition 12.6.12
Pour tout réel x, on définit a à la puissance x, noté a^x, comme étant le nombre

$$a^x = \exp_a x = \exp(x \ln a)$$

Si $a = 1$, on pose $a^x = 1$ pour tout réel x. On note $\mathrm{e} = \exp 1$ de sorte que

$$\forall x \in \mathbb{R} \qquad \exp x = \mathrm{e}^x$$

Avec cette nouvelle notation, on garde les propriétés usuelles des puissances entières et on les généralise :

Théorème 12.6.13
$\forall x \in \mathbb{R} \quad \forall y \in \mathbb{R} \qquad a^x a^y = a^{x+y} \qquad a^{x-y} = \dfrac{a^x}{a^y} \qquad et \qquad \left(a^x\right)^y = a^{xy}$

Preuve : Les deux premières propositions ne sont que des récritures de la propriété 5 dans le **Théorème 2.8**, en remplaçant $\exp_a z$ par a^z. Pour la troisième, on prend x et y réels et on a, en déroulant les diverses définitions vues jusqu'à présent :

$$\begin{aligned}(a^x)^y &= \exp_{a^x} y = \exp(y \ln a^x) = \exp(y \ln \exp_a x) \\ &= \exp\left(y \ln \exp(x \ln a)\right) = \exp(xy \ln a) = \exp_a y \\ (a^x)^y &= a^{xy}\end{aligned}$$ □

À ce stade, en partant uniquement de la fonction $x \longmapsto 1/x$ dont on a étudié une primitive ln, on a créé déjà un bon nombre de fonctions fondamentales en analyse et on a généralisé la notion de puissance.

Il nous reste à voir comment ces fonctions se comparent entre elles aux bornes de leurs ensembles de définition.

12.6.5 Croissances Comparées

Tout commence avec le lemme suivant :

Lemme 12.6.14

$$\lim_{x \to +\infty} \frac{\ln x}{x} = 0^+$$

Preuve : Évidemment, cette limite ne s'étudie pas directement à l'aide des théorèmes de manipulation de limites, puisque

$$\lim_{x\to+\infty} \ln x = +\infty \qquad \text{et} \qquad \lim_{x\to+\infty} x = +\infty$$

On ruse en remarquant que

$$\forall x > 1 \qquad 0 \leqslant \frac{1}{x} \leqslant \frac{1}{\sqrt{x}}$$

Par suite $$\forall x > 1 \qquad 0 \leqslant \ln x = \int_1^x \frac{\mathrm{d}t}{t} \leqslant \int_1^x \frac{\mathrm{d}t}{\sqrt{t}} = \left[2\sqrt{t}\right]_1^x = 2\sqrt{x} - 2$$

et $$\forall x > 1 \qquad 0 \leqslant \frac{\ln x}{x} \leqslant \frac{2}{\sqrt{x}} - \frac{2}{x}$$

Il ne reste plus qu'à utiliser le théorème des gendarmes pour conclure. □

Les théorèmes de croissances comparées découlent alors tous de ce lemme :

Théorème 12.6.15
Soient α *et* β *deux nombres réels strictement positifs.*

1. $\lim\limits_{x\to+\infty} \dfrac{\ln^\alpha x}{x^\beta} = 0$
2. $\lim\limits_{x\to 0^+} x^\beta |\ln x|^\alpha = 0$
3. $\lim\limits_{x\to+\infty} \dfrac{x^\alpha}{\exp(\beta x)} = 0$
4. $\lim\limits_{x\to-\infty} |x|^\alpha \exp(\beta x) = 0$

> Remarquons qu'il n'y a pas lieu de s'inquiéter outre mesure de ces valeurs absolues dans les formules 2 et 4. Elles sont juste là car $\ln^\alpha x$ n'a aucun sens lorsque $x < 1$, dans la mesure où $\ln x$ est négatif. En effet, par définition,
>
> $$\ln^\alpha x = \exp(\alpha \ln\ln x)$$
>
> En revanche, $|\ln x|^\alpha$ n'a aucun problème de définition.
>
> De la même manière, x^α ne veut rien dire lorsque $x < 0$.

Preuve :

1. On s'amuse simplement avec les propriétés du logarithme et des puissances :

$$\forall x > 1 \qquad \frac{\ln^\alpha x}{x^\beta} = \left(\frac{\ln x}{x^{\beta/\alpha}}\right)^\alpha$$

Or, $$\forall x > 1 \qquad x = \left(x^{\beta/\alpha}\right)^{\alpha/\beta}$$

d'où $$\forall x > 1 \qquad \ln x = \frac{\alpha}{\beta} \ln x^{\beta/\alpha}$$

et $$\forall x > 1 \qquad \frac{\ln^\alpha x}{x^\beta} = \left(\frac{\alpha}{\beta} \times \frac{\ln x^{\beta/\alpha}}{x^{\beta/\alpha}}\right)$$

Il ne reste plus qu'à appliquer le théorème de composition des limites :

$$\left.\begin{array}{l} \lim\limits_{x\to+\infty} x^{\beta/\alpha} = +\infty \\ \lim\limits_{x\to+\infty} \dfrac{\ln x}{x} = 0^+ \end{array}\right\} \Longrightarrow \lim_{x\to+\infty} \frac{\ln x^{\beta/\alpha}}{x^{\beta/\alpha}} = 0^+$$

ce qui est suffisant pour conclure.

2. Une première manipulation s'impose, pour ramener l'étude en 0^+ en une étude en $+\infty$:

$$\forall x \in]0\,;1[\qquad x^\beta |\ln x|^\alpha = \left(\frac{1}{1/x}\right)^\beta \left|\ln \frac{1}{1/x}\right|^\alpha = \frac{\ln^\alpha 1/x}{(1/x)^\beta}$$

Puis on applique le théorème de composition des limites :

$$\left.\begin{array}{l} \lim\limits_{x\to0^+} \dfrac{1}{x} = +\infty \\ \lim\limits_{x\to+\infty} \dfrac{\ln^\alpha x}{x^\beta} = 0 \end{array}\right\} \Longrightarrow \lim_{x\to0^+} x^\beta |\ln x|^\alpha = 0$$

3. Encore le théorème de composition des limites, avec la propriété 1 :

$$\left.\begin{array}{l} \lim\limits_{x\to+\infty} \exp x = +\infty \\ \lim\limits_{x\to+\infty} \dfrac{\ln^\alpha x}{x^\beta} = 0 \end{array}\right\} \Longrightarrow \lim_{x\to+\infty} \frac{\ln^\alpha(\exp x)}{(\exp x)^\beta} = 0$$

On applique alors les propriétés algébriques du log et de l'exponentielle pour conclure.

4. À nouveau le théorème de composition des limites, avec la propriété 3 :

$$\left.\begin{array}{l} \lim\limits_{x\to-\infty} -x = +\infty \\ \lim\limits_{x\to+\infty} \dfrac{x^\alpha}{\exp\beta x} = 0 \end{array}\right\} \Longrightarrow \lim_{x\to-\infty} \frac{(-x)^\alpha}{\exp(-\beta x)} = 0$$

On conclue avec les propriétés algébriques de l'exponentielle et le fait que lorsque x est négatif, on a $(-x) = |x|$. □

12.6.6 L'exponentielle Complexe

La fonction exponentielle a parfaitement été définie sur $\mathbb{R}$. On va maintenant tenter de la prolonger à $\mathbb{C}$. On définit

$$\forall n \in \mathbb{N} \quad \forall z \in \mathbb{C} \qquad s_n(z) = \sum_{k=0}^{n} \frac{z^k}{k!}$$

On sait déjà (**théorème 6.7**) que pour tout réel x, la suite $(s_n(x))_{n\in\mathbb{N}}$ converge vers $\exp x$.

Proposition 12.6.16
Pour tout nombre complexe z, la suite $(s_n(z))_{n\in\mathbb{N}}$ converge.

Preuve : Soit $z \in \mathbb{C}$. On montre que $(s_n(z))_{n\in\mathbb{N}}$ est de Cauchy. On sait que $(s_n(|z|))_{n\in\mathbb{N}}$ est de Cauchy, puisqu'elle converge vers $\exp(|z|)$. Donc si $\varepsilon > 0$ est donné, il existe $N \in \mathbb{N}$ tel que

$$\forall n \geqslant N \quad \forall p \in \mathbb{N}^\star \qquad |s_n(|z|) - s_{n+p}(|z|)| \leqslant \varepsilon$$

Mais $\forall n \geqslant N \quad \forall p \in \mathbb{N}^\star \qquad |s_n(z) - s_{n+p}(z)| = \left| \sum_{k=n+1}^{n+p} \frac{z^k}{k!} \right| \leqslant \sum_{k=n+1}^{n+p} \frac{|z|^k}{k!} = s_{n+p}(|z|) - s_n(|z|) \leqslant \varepsilon$

Donc $(s_n(z))_{n\in\mathbb{N}}$ est de Cauchy : elle converge. □

Définition 12.6.17 (Exponentielle complexe)
Si $z \in \mathbb{C}$, la limite de la suite $(s_n(z))_{n\in\mathbb{N}}$ est appelée *exponentielle complexe de z* et notée $\exp z$.

Proposition 12.6.18 (Propriétés fondamentales de l'exponentielle complexe)
L'exponentielle complexe possède les propriétés suivantes :

1. *Elle ne s'annule pas sur $\mathbb{C}$.*
2. $\forall z, w \in \mathbb{C} \qquad \exp(z+w) = \exp z \exp w \qquad$ *et* $\qquad \exp(z-w) = \dfrac{\exp z}{\exp w}$
3. $\forall z \in \mathbb{C} \qquad \exp\overline{z} = \overline{\exp z}$
4. $\forall x \in \mathbb{C} \qquad \overline{\exp(ix)} = \exp(-ix) = \dfrac{1}{\exp(ix)} \qquad$ *et* $\qquad |\exp(ix)| = 1$

Preuve : Soient z et w deux nombres complexes. Par définition,

$$\exp z = \lim_{n\to\infty} s_n(z) \qquad \exp w = \lim_{n\to\infty} s_n(w) \qquad \text{et} \qquad \exp(z+w) = \lim_{n\to\infty} s_n(z+w)$$

Fixons un entier n non nul et calculons $s_{2n}(z+w)$:

$$s_{2n}(z+w) = \sum_{k=0}^{2n} \frac{(z+w)^k}{k!} = \sum_{k=0}^{2n} \sum_{\ell=0}^{k} \frac{z^\ell w^{k-\ell}}{\ell!\,(k-\ell)!}$$

On commence par inverser les sommes :

$$s_{2n}(z+w) = \sum_{\ell=0}^{2n} \sum_{k=\ell}^{2n} \frac{z^\ell\, w^{k-\ell}}{\ell!\,(k-\ell)!}$$

et on effectue le changement d'indice $k \leftarrow k-\ell$ dans la somme intérieure :

$$s_{2n}(z+w) = \sum_{\ell=0}^{2n} \sum_{k=0}^{2n-\ell} \frac{z^\ell\, w^k}{\ell! k!}$$

Puis on fait une séparation astucieuse de sommes, pour faire apparaître $s_n(z)\,s_n(w)$:

$$\begin{aligned} s_{2n}(z+w) &= \sum_{\ell=0}^{n}\sum_{k=0}^{n}\frac{z^\ell\,w^k}{\ell!\,k!} + \sum_{\ell=0}^{n}\sum_{k=n+1}^{2n-\ell}\frac{z^\ell\,w^k}{\ell!\,k!} + \sum_{\ell=n+1}^{2n}\sum_{k=0}^{2n-\ell}\frac{z^\ell\,w^k}{\ell!\,k!} \\ &= s_n(z)\,s_n(w) + \sum_{\ell=0}^{n-1}\frac{z^\ell}{\ell!}(s_{2n-\ell}(w)-s_n(w)) + \sum_{\ell=n+1}^{2n}\sum_{k=0}^{2n-\ell}\frac{z^\ell\,w^k}{\ell!\,k!} \end{aligned}$$

On termine par un dernier échange de sommes :

$$\begin{aligned} s_{2n}(z+w)-s_n(z)\,s_n(w) &= \sum_{\ell=0}^{n-1}\frac{z^\ell}{\ell!}(s_{2n-\ell}(w)-s_n(w)) + \sum_{k=0}^{n-1}\sum_{\ell=n+1}^{2n-k}\frac{z^\ell\,w^k}{\ell!\,k!} \\ &= +\sum_{\ell=0}^{n-1}\frac{z^\ell}{\ell!}(s_{2n-\ell}(w)-s_n(w)) + \sum_{k=0}^{n-1}\frac{w^k}{k!}(s_{2n-k}(z)-s_n(z)) \end{aligned}$$

Voilà... Ces calculs sont vrais pour tout n. On fixe un $\varepsilon>0$; comme les suites $s(z)$ et $s(w)$ sont de Cauchy, il existe $\mathrm{N}\in\mathbb{N}$ tel que

$$\forall n,p\geqslant \mathrm{N}\qquad |s_n(z)-s_p(z)|\leqslant\varepsilon\qquad\text{et}\qquad |s_n(w)-s_p(w)|\leqslant\varepsilon$$

On prend alors $n\geqslant \mathrm{N}$, quelconque. On remarque alors que si $\ell\in[\![\,0\,;\,n-1\,]\!]$, alors $2n-\ell\geqslant n+1\geqslant \mathrm{N}$. D'où

$$\forall \ell\in[\![\,0\,;\,n-1\,]\!]\qquad |s_{2n-\ell}(z)-s_n(z)|\leqslant\varepsilon\qquad\text{et}\qquad |s_{2n-\ell}(w)-s_n(w)|\leqslant\varepsilon$$

D'où

$$\begin{aligned} |s_{2n}(z+w)-s_n(z)\,s_n(w)| &\leqslant \varepsilon\sum_{\ell=0}^{n-1}\frac{|z|^\ell}{\ell!}+\varepsilon\sum_{k=0}^{n-1}\frac{|w|^k}{k!} \\ &\leqslant \varepsilon(\exp(|z|)+\exp(|w|) \end{aligned}$$

Cette majoration est vraie pour tout $n\geqslant \mathrm{N}$. Donc on peut passer à la limite (on sait que les suites de gauche convergent) pour obtenir :

$$\forall\varepsilon>0\qquad |\exp(z+w)-\exp z\exp w|\leqslant\varepsilon(\exp(|z|)+\exp(|w|))$$

d'où

$$\exp(z+w)=\exp z\exp w$$

Ce résultat est vrai pour tous z et w dans $\mathbb{C}$. Donc

$$\forall z\in\mathbb{C}\qquad \exp z\exp(-z)=\exp 0=1$$

Donc exp ne s'annule pas, et $\exp(-z)$ est l'inverse de $\exp z$ pour tout $z\in\mathbb{C}$.

Maintenant, prenons un nombre complexe z. Pour tout entier n,

$$s_n(\overline{z})=\sum_{k=0}^{n}\frac{\overline{z}^k}{k!}=\overline{s_n(z)}$$

donc

$$\exp\overline{z}=\overline{\exp z}$$

En particulier, si x est un nombre réel,

$$\overline{\exp(\mathrm{i}x)}=\exp(-\mathrm{i}x)=\frac{1}{\exp(\mathrm{i}x)}\qquad\text{d'où}\qquad |\exp(\mathrm{i}x)|^2=1$$ □

Corollaire 12.6.19 (Dérivation d'une exponentielle complexe)

1. *La fonction $f : x\longmapsto exp(ix)$ est dérivable sur $\mathbb{R}$ et $f'=if$.*

2. *Soit g une fonction définie sur un intervalle* I*, à valeurs complexes, dérivable. Alors $\exp g$ est dérivable sur* I *et* $(\exp g)' = g' \exp g$.

Preuve : Soit $h \in \mathbb{R}^\star$. On a

$$\forall n \in \mathbb{N} \quad n \geqslant 2 \qquad s_n(\mathrm{i}h) = \sum_{k=0}^{n} \frac{(\mathrm{i}h)^k}{k!} = 1 + \mathrm{i}h + \sum_{k=2}^{n} \frac{(\mathrm{i}h)^k}{k!}$$

donc
$$\forall n \in \mathbb{N} \quad n \geqslant 2 \qquad \left| \frac{s_n(\mathrm{i}h) - 1}{h} - \mathrm{i} \right| \leqslant \sum_{k=2}^{n} \frac{|h|^{k-1}}{k!} = \frac{s_n(|h|) - 1}{|h|} - 1$$

Comme les deux membres sont les termes généraux de suites convergentes, on passe à la limite pour obtenir

$$\forall h \in \mathbb{R} \qquad \left| \frac{\exp(\mathrm{i}h) - 1}{h} - \mathrm{i} \right| \leqslant \left| \frac{\exp(|h|) - 1}{h} - 1 \right|$$

Le membre de droite tend vers 0 lorsque h tend vers 0, car l'exponentielle réelle est dérivable en 0. Donc la limite de gauche est nulle et

$$\lim_{h \to 0} \frac{\exp(\mathrm{i}h) - 1}{h} = \mathrm{i}$$

Maintenant, on fixe un $x \in \mathbb{R}$. On a

$$\forall h \in \mathbb{R}^\star \qquad \frac{\exp(\mathrm{i}(x+h)) - \exp \mathrm{i}x}{h} = \exp(\mathrm{i}x) \frac{\exp(\mathrm{i}h) - 1}{h} \xrightarrow[h \to 0]{} \mathrm{i} \exp(\mathrm{i}x)$$

Ce qui montre que f est dérivable en x et $f'(x) = \mathrm{i} f(x)$.

La deuxième partie est un simple calcul : si g est à valeurs complexes, on note g_1 sa partie réelle et g_2 sa partie imaginaire. Alors

$$\exp g = \exp(g_1 + \mathrm{i}g_2) = \exp g_1 \times \underbrace{\exp(\mathrm{i}g_2)}_{= f \circ g_2}$$

D'après les théorèmes généraux, $\exp g$ est dérivable sur I et on utilise les formules de dérivation de produits et de composées. □

12.6.7 Les fonctions circulaires et le nombre π

Définition 12.6.20 (Fonctions cosinus et sinus)
On appelle *fonctions cosinus et sinus* les fonctions définies par

$$\forall z \in \mathbb{C} \qquad \cos x = \frac{\exp(\mathrm{i}z) + \exp(-\mathrm{i}z)}{2} \qquad \text{et} \qquad \sin z = \frac{\exp(\mathrm{i}z) - \exp(-\mathrm{i}z)}{2\mathrm{i}}$$

Théorème 12.6.21
Les fonctions sinus et cosinus satisfont les propriétés suivantes :

1. $\forall x \in \mathbb{R} \qquad \cos x = Re(\exp(ix)) \qquad \sin x = Im(\exp(ix))$
2. $\forall z \in \mathbb{C} \qquad \cos^2 z + \sin^2 z = 1$
3. cos *est impaire et* sin *est paire.*
4. sin *et* cos *sont infiniment dérivables sur* $\mathbb{R}$ *et*

$$\forall x \in \mathbb{R} \qquad \begin{cases} \sin' x = \cos x \\ \cos' x = -\sin x \end{cases}$$

5. $\forall a,b\in\mathbb{C}$ $\begin{cases}\cos(a+b)=\cos a\cos b-\sin a\sin b\\ \sin(a+b)=\sin a\cos b+\cos a\sin b\end{cases}$

6. $\forall z\in\mathbb{R}$ $\begin{cases}\cos z=\lim\limits_{n\to\infty}\sum\limits_{k=0}^{n}(-1)^k\dfrac{z^{2k}}{(2k)!}\\ \sin z=\lim\limits_{n\to\infty}\sum\limits_{k=0}^{n}(-1)^k\dfrac{z^{2k+1}}{(2k+1)!}\end{cases}$

7. $\forall n\in\mathbb{N}$ $\begin{cases}\cos x\underset{x\to0}{=}\sum\limits_{k=0}^{n}(-1)^k\dfrac{x^{2k}}{(2k)!}+o(x^{2n+1})\\ \sin x\underset{x\to0}{=}\sum\limits_{k=0}^{n}(-1)^k\dfrac{x^{2k+1}}{(2k+1)!}+o(x^{2n+2})\end{cases}$

Preuve : L'essentiel du travail a été fait dans le **corollaire 6.19**.

1. La première proposition est une conséquence du fait que $\overline{\exp(\mathrm{i}x)}=\exp(-\mathrm{i}x)$ pour tout $x\in\mathbb{R}$, et que
$$\forall z\in\mathbb{C}\qquad \operatorname{Re}z=\frac{z+\overline{z}}{2}\qquad \operatorname{Im}z=\frac{z-\overline{z}}{2}$$

2. Si $z\in\mathbb{C}$, on a
$$\cos(-z)=\frac{\exp(-\mathrm{i}z)+\exp(\mathrm{i}z)}{2}=\cos z$$
et
$$\sin(-z)=\frac{\exp(-\mathrm{i}z)-\exp(\mathrm{i}z)}{2\mathrm{i}}=-\sin z$$

3. $\forall z\in\mathbb{C}\qquad \cos^2 z+\sin^2 z=(\cos z+\mathrm{i}\sin z)(\cos z-\mathrm{i}\sin z)=\exp(\mathrm{i}z)\exp(-\mathrm{i}z)=1$

4. Comme $x\longmapsto\exp(\mathrm{i}x)$ est infiniment dérivable sur $\mathbb{R}$, on sait que cos et sin le sont aussi d'après les théorèmes généraux. Aussi, d'après les formules de dérivation d'une composée,
$$\forall x\in\mathbb{R}\qquad \cos' x=\frac{\mathrm{i}\exp(\mathrm{i}x)-\mathrm{i}\exp(-\mathrm{i}x)}{2}=-\sin x$$
et de la même manière, $\sin'=\cos$.

5. Les formules d'addition sont également triviales : si a et b sont des complexes,
$$\begin{aligned}\exp(\mathrm{i}(a+b))&=\exp(\mathrm{i}a)\exp(\mathrm{i}b)=(\cos a+\mathrm{i}\sin a)(\cos b+\mathrm{i}\sin b)\\&=(\cos a\cos b-\sin a\sin b)+\mathrm{i}(\sin a\cos b+\cos a\sin b)\end{aligned}$$
et de même $\exp(-\mathrm{i}(a+b))=(\cos a\cos b-\sin a\sin b)-\mathrm{i}(\sin a\cos b+\cos a\sin b)$
D'où
$$\cos(a+b)=\frac{\exp(\mathrm{i}(a+b))+\exp(\mathrm{i}(a-b))}{2}=\cos a\cos b-\sin a\sin b$$
et
$$\sin(a+b)=\frac{\exp(\mathrm{i}(a+b))-\exp(\mathrm{i}(a+b))}{2}=\sin a\cos b+\cos a\sin b$$

6. Si $z \in \mathbb{C}$, on sait que $(s_n(\mathrm{i}z))_{n\in\mathbb{N}}$ et $(s_n(-\mathrm{i}z))_{n\in\mathbb{N}}$ convergent vers $\exp(\mathrm{i}z)$ et $\exp(-\mathrm{i}z)$ respectivement. Toute suite extraite d'une suite convergente converge vers la limite de la suite donc

$$\cos z = \lim_{n\to\infty} \frac{s_{2n}(\mathrm{i}z) + s_{2n}(-\mathrm{i}z)}{2} \qquad \sin z = \lim_{n\to\infty} \frac{s_{2n+1}(\mathrm{i}z) - s_{2n+1}(-\mathrm{i}z)}{2\mathrm{i}}$$

Mais pour tout entier n, en séparant les termes de rangs pair et impair dans $s_{2n}(z)$, on trouve

$$\begin{aligned} s_{2n}(\mathrm{i}z) &= \sum_{k=0}^{2n} \frac{\mathrm{i}^k z^k}{k!} = \sum_{p=0}^{n} \frac{\mathrm{i}^{2p} z^{2p}}{(2p)!} + \sum_{p=0}^{n-1} \frac{\mathrm{i}^{2p+1}}{(2p+1)!} \\ &= \sum_{p=0}^{n} (-1)^p \frac{z^{2p}}{(2p)!} + \mathrm{i} \sum_{p=0}^{n-1} (-1)^p \frac{z^{2p+1}}{(2p+1)!} \end{aligned}$$

et
$$s_{2n}(-\mathrm{i}z) = \sum_{p=0}^{n} (-1)^p \frac{z^{2p}}{(2p)!} - \mathrm{i} \sum_{p=0}^{n-1} (-1)^p \frac{z^{2p+1}}{(2p+1)!}$$

Donc
$$\frac{s_{2n}(\mathrm{i}z) + s_{2n}(-\mathrm{i}z)}{2} = \sum_{p=0}^{n} (-1)^p \frac{z^{2p}}{(2p)!}$$

ce qui donne la première formule en passant à la limite. La deuxième formule s'obtient de la même manière.

7. On commence par observer que

$$\cos 0 = \frac{\exp 0 + \exp 0}{2} = 1 \qquad \sin 0 = \frac{\exp 0 - \exp 0}{2\mathrm{i}} = 0$$

Soit n un entier. On sait que cos est $2n+1$ fois dérivable au voisinage de 0. Le calcul des dérivées de cos et sin permet de montrer, par une récurrence immédiate, que

$$\forall p \in \mathbb{N} \qquad \cos^{(2p)} 0 = (-1)^p \qquad \cos^{(2p+1)} 0 = 0$$

Le théorème de Taylor-Young donne alors à l'ordre $2n+1$

$$\cos x \underset{x\to 0}{=} \sum_{k=0}^{2n+1} \frac{\cos^{(k)} 0}{k!} x^k + \mathrm{o}(x^{2n+1}) = \sum_{k=0}^{n} (-1)^k \frac{x^{2k}}{(2k)!} + \mathrm{o}\left(x^{2n+1}\right)$$

Pour le sinus, c'est la même chose. □

Lemme 12.6.22
Le sinus est strictement positif sur $[0\,;2]$.

Preuve : Soit $x \in [0\,;2]$. On sait que

$$\sin x = \lim_{n\to\infty} \sum_{k=0}^{n} (-1)^k \frac{x^{2k+1}}{(2k+1)!}$$

On pose
$$\forall k \in \mathbb{N} \qquad u_k = \frac{x^{2k+1}}{(2k+1)!}$$

et l'on a $\forall k \in \mathbb{N}$
$$\begin{aligned} u_k - u_{k+1} &= \frac{x^{2k+1}}{(2k+1)!} - \frac{x^{2k+3}}{(2k+3)!} = \frac{x^{2k+1}}{(2k+3)!}\left((2k+3)(2k+2) - x^2\right) \\ &\geqslant \frac{x^{2k+1}}{(2k+3)!}(6 - x^2) \geqslant 0 \end{aligned}$$

Alors $\forall n \in \mathbb{N} \quad \sum_{k=0}^{2n+1} (-1)^k u_k = \sum_{k=0}^{n} u_{2k} - \sum_{k=0}^{n} u_{2n+1} = \sum_{k=0}^{n} \underbrace{(u_{2k} - u_{2k+1})}_{>0}$

$$\geqslant u_0 - u_1$$

En passant à la limite, $\forall x \in [0;2] \qquad \sin x \geqslant u_0 - u_1 > 0$ □

Lemme 12.6.23
La fonction cosinus s'annule une et une seule fois sur $[0;2]$.

Preuve : D'après le **lemme 6.22** et parce que $\cos' = -\sin$, la fonction cosinus est strictement décroissante sur $[0;2]$. De plus, $\cos 0 = 1$; comme cos est continue, il suffit de montrer que $\cos 2 < 0$. On sait que

$$\cos 2 = \lim_{n\to\infty} \sum_{k=0}^{n} (-1)^k \frac{2^{2k}}{(2k!)}$$

On pose $\forall k \in \mathbb{N} \qquad u_k = \dfrac{2^{2k}}{(2k)!}$

Alors $\forall k \in \mathbb{N} \qquad u_k - u_{k+1} = \dfrac{2^{2k}}{(2k)!} - \dfrac{2^{2k+2}}{(2k+2)!} = \dfrac{2^{2k}}{(2k+2)!}\left((2k+2)(2k+1) - 4\right)$

donc $\forall k \in \mathbb{N} \quad k \geqslant 1 \qquad u_k - u_{k+1} > 0$

Par suite, $\forall n \geqslant 3 \qquad \sum_{k=0}^{2n} (-1)^k u_k = u_0 - u_1 + u_2 + \sum_{k=2}^{n} u_{2k} - \sum_{k=3}^{n} u_{2k-1}$

$$= 1 - \frac{4}{2} + \frac{16}{24} + \sum_{k=2}^{n} \underbrace{(u_{2k} - u_{2k-1})}_{\leqslant 0}$$

$$\sum_{k=0}^{2n} (-1)^k u_k \leqslant -\frac{1}{3}$$

En passant à la limite, il vient $\cos 2 \leqslant -\frac{1}{3} < 0$. □

Définition 12.6.24 (Le nombre π)
Soit α l'unique élement de $[0;2]$ tel que $\cos\alpha = 0$. Le réel $2\alpha \in [0;4]$ est noté π.

Ainsi, par définition, $\cos\frac{\pi}{2} = 0$ et cos est strictement positive sur $[0;\frac{\pi}{2}[$. On peut alors en déduire de nombreuses valeurs des fonctions sinus et cosinus. Commençons par

$$\cos^2\frac{\pi}{2} + \sin^2\frac{\pi}{2} = 1 \qquad \text{donc} \qquad \sin\frac{\pi}{2} = \pm 1$$

Mais on a montré que le sinus est strictement positif sur $[0;2]$ donc $\sin\frac{\pi}{2} = 1$. Ensuite, à l'aide des formules d'addition,

$$\sin\pi = 2\sin\frac{\pi}{2}\cos\frac{\pi}{2} = 0$$

et $$\cos\pi = \cos^2\frac{\pi}{2} - \sin^2\frac{\pi}{2} = -1$$

Par suite, $\forall z \in \mathbb{C}$
$$\begin{aligned}
\sin(z+\pi) &= \sin z\cos\pi + \cos z\sin\pi = -\sin z\\
\sin(\pi - z) &= \sin\pi\cos z - \sin z\cos\pi = \sin z\\
\cos(z+\pi) &= \cos z\cos\pi - \sin z\sin\pi = -\cos z\\
\cos(\pi - z) &= \cos z\cos\pi + \sin z\sin\pi = -\cos z\\
\sin\left(\frac{\pi}{2} - z\right) &= \sin\frac{\pi}{2}\cos z - \cos\frac{\pi}{2}\sin z = \cos z\\
\sin\left(\frac{\pi}{2} + z\right) &= \sin\frac{\pi}{2}\cos z + \cos\frac{\pi}{2}\sin z = \cos z
\end{aligned}$$
$$\begin{aligned}
\cos\left(\frac{\pi}{2} - z\right) &= \sin\left(\frac{\pi}{2} - \left(\frac{\pi}{2} - z\right)\right) = \sin z\\
\cos\left(\frac{\pi}{2} + z\right) &= \sin\left(\frac{\pi}{2} + \frac{\pi}{2} + z\right) = \sin(\pi + z) = -\sin z\\
\sin(2\pi + z) &= \sin(\pi + \pi + z) = -\sin(\pi + z) = \sin z\\
\cos(2\pi + z) &= \cos(\pi + \pi + z) = -\cos(\pi + z) = \cos z\\
\sin(2\pi - z) &= \sin(-z) = -\sin z\\
\cos(2\pi - z) &= \cos(-z) = \cos z
\end{aligned}$$

Théorème 12.6.25 (Irrationnalité de π)
π est irrationnel.

Preuve : Fait en DM. □

On s'intéresse maintenant à la périodicité de ces fonctions. On aura besoin d'un

Lemme 12.6.26
Soit $f \in \mathscr{C}(\mathbb{R})$, périodique, non constante. Alors il existe $\mathrm{T} \in \mathbb{R}_+^\star$ tel que l'ensemble des périodes de f soit $\mathrm{T}\mathbb{Z}$.

Preuve : Notons $\mathscr{P}$ l'ensemble des périodes de f. Si p et q sont des périodes de f,
$$\forall x \in \mathbb{R} \qquad f(x+p) = f(x) \qquad \text{et} \qquad f(x+q) = f(x)$$
et
$$\forall x \in \mathbb{R} \qquad f(x+p+q) = f(x+p) = f(x)$$
Donc $p+q$ est une période. En outre,
$$\forall x \in \mathbb{R} \qquad f(x-p) = f(x-p+p) = f(x)$$
et $-p$ est une période. $\mathscr{P}$ est donc un sous-groupe de $\mathbb{R}$.

Supposons que $\mathscr{P}$ est dense dans $\mathbb{R}$, c'est-à-dire que
$$\forall x \in \mathbb{R} \quad \forall \eta > 0 \quad \exists p \in \mathscr{P} \qquad |x - p| \leqslant \eta$$
On fixe un $\varepsilon > 0$. La fonction f est continue en 0 donc il existe $\eta > 0$ tel que
$$\forall x \in [-\eta;\eta] \qquad |f(x) - f(0)| \leqslant \varepsilon$$
Soit $x \in \mathbb{R}$; par densité de $\mathscr{P}$, il existe une période p de f, telle que $|x-p| \leqslant \eta$. Donc
$$|f(x) - f(0)| = |f(x-p) - f(0)| \leqslant \varepsilon$$
Ceci est vrai pour tout $\varepsilon > 0$ donc $f(x) = f(0)$ et f est constante : c'est une contradiction. On a alors vu en DM qu'il existe $\mathrm{T} > 0$, tel que $\mathscr{P} = \mathrm{T}\mathbb{Z}$. □

Théorème 12.6.27 (Périodicité et variations)

1. *Pour tout $k \in \mathbb{Z}$, le cosinus est une bijection de $[k\pi\,;(k+1)\pi]$ sur $[-1\,;1]$. Elle est strictement croissante sur cet intervalle si, et seulement si, k est pair.*
2. *Pour tout $k \in \mathbb{Z}$, le sinus est une bijection de $\left[-\frac{\pi}{2}+k\pi\,;\frac{\pi}{2}+k\pi\right]$ sur $[-1\,;1]$. Elle est strictement croissante sur cet intervalle si, et seulement si, k est pair.*
3. *Soient a et b dans $\mathbb{R}$. On a*

$$\cos a = \cos b \iff (a = b\ [2\pi] \quad ou \quad a = -b\ [2\pi])$$

et

$$\sin a = \sin b \iff (a = b\ [2\pi] \quad ou \quad a = \pi - b\ [2\pi])$$

4. *Les fonctions sinus et cosinus sont 2π-périodiques.Toute période de sinus ou cosinus est un multiple entier relatif de 2π.*

Preuve : La 2π-périodicité vient d'une des formules prouvées précédemment.

On sait que sin est strictement positive sur $]0\,;\frac{\pi}{2}[$ d'après le **lemme 6.22** et parce que $0 \leqslant \frac{\pi}{2} \leqslant 2$. De plus,

$$\forall x \in \left[\frac{\pi}{2}\,;\pi\right[\qquad \sin x = \sin(\pi - x) > 0 \qquad \text{car} \qquad \pi - x \in \left]0\,;\frac{\pi}{2}\right]$$

Par suite, cos est strictement décroissante sur $[0\,;\pi]$. Comme elle est continue, le **corollaire 4.9** dit

$$\cos([0\,;\pi]) = [\cos\pi\,;\cos 0] = [-1\,;1]$$

cos est donc une bijection strictement décroissante de $[0\,;\pi]$ sur $[-1\,;1]$. Alors si $k \in \mathbb{Z}$, la formule

$$\forall x \in [k\pi\,;(k+1)\pi] \qquad \cos x = \cos(x - k\pi + k\pi) = (-1)^k \cos(x - k\pi)$$

montre que cos est une bijection de $[k\pi\,;(k+1)\pi]$ sur $[-1\,;1]$, décroissante si et seulement si k est pair.

On sait alors que cos est strictement croissante sur $[-\pi\,;0]$. Donc

$$\forall x \in \left]-\frac{\pi}{2}\,;0\right] \qquad \cos x > \cos\frac{\pi}{2} = 0$$

Et on sait déjà que cos est strictement positive sur $[0\,;\frac{\pi}{2}[$, par définition de π. Ainsi, cos est strictement positive sur $]-\frac{\pi}{2}\,;\frac{\pi}{2}[$ et sin est strictement croissante sur cet intervalle. Puisqu'elle est continue, le **corollaire 4.9** donne

$$\sin\left(\left[-\frac{\pi}{2}\,;\frac{\pi}{2}\right]\right) = \left[\sin\frac{-\pi}{2}\,;\sin\frac{\pi}{2}\right] = [-1\,;1]$$

Par suite, sin est une bijection strictement croissante de $[-\frac{\pi}{2}\,;\frac{\pi}{2}]$ sur $[-1\,;1]$. Si $k \in \mathbb{Z}$ est donné, la formule

$$\forall x \in \left[-\frac{\pi}{2}+k\pi\,;-\frac{\pi}{2}+(k+1)\pi\right] \qquad \sin x = \sin(x - k\pi + k\pi) = (-1)^k \sin(x - k\pi)$$

prouve que sin est une bijection de $[-\frac{\pi}{2}+k\pi\,;\frac{\pi}{2}+k\pi]$ sur $[-1\,;1]$, strictement croissante si et seulement si k est pair.

Donnons-nous deux réels a et b, tels que $\cos a = \cos b$, avec par exemple $a \leqslant b$. On note k la partie entière de $\frac{a}{2\pi}$, de sorte que

$$k \leqslant \frac{a}{2\pi} < k+1 \qquad \text{ou encore} \qquad a \in [2k\pi\,;2(k+1)\pi[$$

On pose aussi $\ell = \left\lfloor \frac{b}{2\pi} \right\rfloor$ et l'on a $b \in [2\ell\pi\,;2(\ell+1)\pi[$

Supposons d'abord que $k = \ell = 0$. Si a et b sont dans $[0;\pi[$, par injectivité de cos sur cet intervalle, on a $a = b$. S'ils sont dans $[\pi;2\pi[$, c'est la même chose. Et si $a \in [0;\pi[$ et $b \in [\pi;2\pi[$, on obtient $2\pi - b \in [0;\pi[$ donc $a = 2\pi - b$.

Si k ou ℓ n'est pas nul, on a

$$\cos(a - 2k\pi) = \cos a = \cos b = \cos(b - 2\ell\pi)$$

donc $$a - 2k\pi = b - 2\ell\pi \qquad \text{ou} \qquad a - 2k\pi = 2\pi - b + 2\ell\pi$$

Dans tous les cas, $$a = b\ [2\pi] \qquad \text{ou} \qquad a = -b\ [2\pi]$$

Supposons maintenant que $\sin a = \sin b$. Alors

$$\cos\left(\frac{\pi}{2} - a\right) = \sin a = \sin b = \cos\left(\frac{\pi}{2} - b\right)$$

et $$\frac{\pi}{2} - a = \frac{\pi}{2} - b\ [2\pi] \qquad \text{ou} \qquad \frac{\pi}{2} - a = b - \frac{\pi}{2}\ [2\pi]$$

Finalement, $$a = b\ [2\pi] \qquad \text{ou} \qquad a = \pi - b\ [2\pi]$$

On termine en étudiant les périodes de ces fonctions. On commence par remarquer qu'un réel $T > 0$ est une période du cosinus si, et seulement si, il est une période du sinus. En effet, d'après les formules de dérivation, si T est une période du cosinus, alors

$$\forall x \in \mathbb{R} \qquad \cos'(x + T) = \cos'(x)$$

donc $$\forall x \in \mathbb{R} \qquad -\sin(x + T) = -\sin x$$

et T est une période du sinus. La réciproque fonctionne de la même manière. Il suffit donc de trouver les périodes de cos.

Comme cos n'est pas nulle, le **lemme 6.26** montre qu'il existe $T > 0$ et $n \in \mathbb{N}$ tel que $2\pi = nT$. Remarquons que $\cos T = 1$; mais les seules solutions de cette équation dans $[0;2\pi]$ sont 0 et 2π, d'après ce qui précède. Donc $T = 2\pi$. □

Corollaire 12.6.28
Soient a et b deux nombres réels tels que $a^2 + b^2 = 1$. *Il existe un unique* $\theta_0 \in [0;2\pi[$ *tel que* $a = \cos\theta_0$ *et* $b = \sin\theta_0$.

Preuve : On suppose, par exemple, que $a, b \geqslant 0$. On sait que $a^2 + b^2 = 1$ donc $a, b \in [-1;1]$. Il existe $\theta_0 \in [0;\frac{\pi}{2}]$ tel que $b = \sin\theta_0$. On a alors

$$a^2 = 1 - b^2 = 1 - \sin^2\theta_0 = \cos^2\theta_0$$

donc $$\cos\theta_0 = \pm a$$

Comme $\theta_0 \in [0;\frac{\pi}{2}]$, on sait que $\cos\theta_0 \geqslant 0$ donc $\cos\theta_0 = a$.

Montrons l'unicité. Soit $\theta \in [0;2\pi]$ tel que $\cos\theta = a$ et $\sin\theta = b$. Puisque $b = \sin\theta \geqslant 0$, on doit avoir $\theta \in [0;\pi]$. De ce fait, $\theta = \theta_0$ ou $\theta = \pi - \theta_0$. Mais dans le deuxième cas, on a $\cos\theta = -\cos\theta_0 = -a$, ce qui est absurde.

Dans le cas où $a \geqslant 0$ et $b \leqslant 0$. Alors $-b \geqslant 0$ donc il existe un unique $\theta \in [0;2\pi[$ tel que

$$a = \cos\theta \qquad \text{et} \qquad -b = \sin\theta$$

d'où $a = \cos(2\pi - \theta)$ et $b = -\sin\theta = \sin(2\pi - \theta)$

En prenant $\theta_0 = 2\pi - \theta$, on a montré l'existence. Pour l'unicité, on voit que si θ_1 est tel que $\cos\theta_1 = a$ et $\sin\theta_1 = b$, alors

$$a = \cos\theta_1 = \cos(2\pi - \theta_1) \qquad \text{et} \qquad -b = -\sin\theta_1 = \sin(2\pi - \theta_1)$$

Mais θ est l'unique élément de $[0\,;2\pi[$ avec cette propriété donc

$$2\pi - \theta_1 = \theta \qquad \text{et} \qquad \theta_1 = 2\pi - \theta = \theta_0$$

Les deux autres cas se traitent de la même manière. □

On termine en calculant les dernières valeurs remarquables de cos et sin, pour pouvoir tracer leurs graphes. On sait que $\cos\frac{\pi}{4} \geqslant 0$ car cos est positive sur $[0\,;\frac{\pi}{2}]$; et l'on a

$$0 = \cos\frac{\pi}{2} = 2\cos^2\frac{\pi}{4} - 1 \qquad \text{d'où} \qquad \cos\frac{\pi}{4} = \frac{\sqrt{2}}{2}$$

Ensuite, $$\sin\frac{\pi}{4} = \cos\left(\frac{\pi}{2} - \frac{\pi}{4}\right) = \cos\frac{\pi}{4} = \frac{\sqrt{2}}{2}$$

Puis $$0 = \cos\frac{\pi}{2} = \cos\left(\frac{\pi}{3} + \frac{\pi}{6}\right) = \cos\frac{\pi}{3}\cos\frac{\pi}{6} - \sin\frac{\pi}{3}\sin\frac{\pi}{6}$$

et $$\cos\frac{\pi}{6} = \cos\left(\frac{\pi}{3} - \frac{\pi}{6}\right) = \cos\frac{\pi}{3}\cos\frac{\pi}{6} + \sin\frac{\pi}{3}\sin\frac{\pi}{6}$$

d'où $$\cos\frac{\pi}{6} = 2\cos\frac{\pi}{3}\cos\frac{\pi}{6}$$

Mais $\frac{\pi}{6} \in]0\,;\frac{\pi}{2}[$ et cos ne s'annule pas dans cet intervalle. D'où

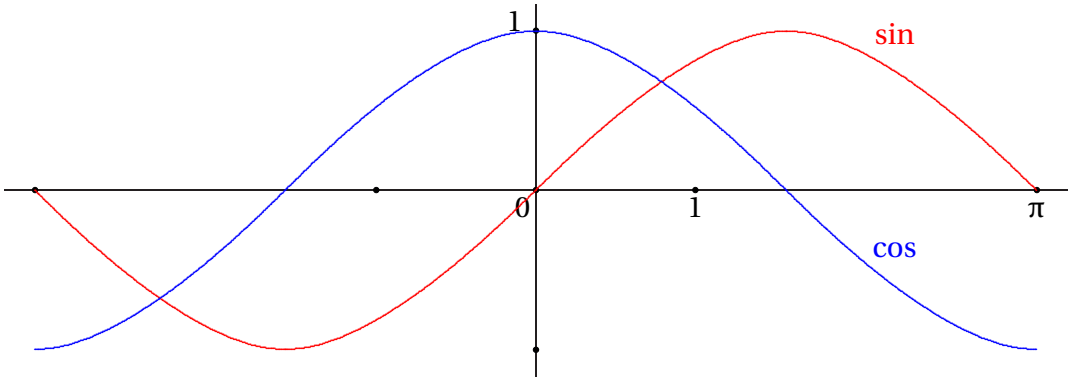
$$\cos\frac{\pi}{3} = \frac{1}{2}$$

Ensuite, $$\sin^2\frac{\pi}{3} = 1 - \cos^2\frac{\pi}{3} = \frac{3}{4} \qquad \text{donc} \qquad \sin\frac{\pi}{3} = \frac{\sqrt{3}}{2}$$

car le sinus est positif sur $[0\,;\frac{\pi}{2}]$. Enfin,

$$\cos\frac{\pi}{6} = \sin\left(\frac{\pi}{2} - \frac{\pi}{6}\right) = \sin\frac{\pi}{3} = \frac{\sqrt{3}}{2}$$

et $$\sin\frac{\pi}{6} = \cos\left(\frac{\pi}{2} - \frac{\pi}{6}\right) = \cos\frac{\pi}{3} = \frac{1}{2}$$



12.6.8 Fonctions circulaires réciproques

La Fonction Arcsinus

La fonction sinus n'est clairement pas une bijection sur $[-1\,;1]$: en effet, elle est 2π-périodique donc toute valeur entre -1 et 1 a une infinité d'antécédents par la fonction sinus.

Mais on peut essayer de se restreindre à un intervalle le plus gros et le plus simple possible, sur lequel le sinus est bijectif. Ainsi, on constate que sin est strictement croissante sur $[-\frac{\pi}{2}\,;\frac{\pi}{2}]$, donc bijective sur $[-1\,;1]$. Au-delà de $\frac{\pi}{2}$, certaines valeurs sont atteintes une deuxième fois. De même avant $-\frac{\pi}{2}$. On définit donc :

Définition 12.6.29
La fonction Arcsinus, notée arcsin, est la bijection réciproque de la fonction sin restreinte à $[-\frac{\pi}{2}\,;\frac{\pi}{2}]$.

Théorème 12.6.30
arcsin *est une fonction impaire, définie sur* $[-1\,;1]$ *à valeurs dans* $[-\frac{\pi}{2}\,;\frac{\pi}{2}]$. *Elle est caractérisée par la propriété fondamentale*

$$\forall x \in [-1\,;1] \qquad \sin\arcsin x = x$$

De plus
$$\forall x \in \left[-\frac{\pi}{2}\,;\frac{\pi}{2}\right] \qquad \arcsin\sin x = x$$

Preuve : Seul le fait que arcsin est impaire est à établir : les autres propriétés découlent de la définition d'une bijection. Soit $x \in [-1\,;1]$; $\arcsin(-x)$ est l'unique solution dans $[-\frac{\pi}{2}\,;\frac{\pi}{2}]$ de l'équation d'inconnue y :

$$\sin y = -x \qquad (\mathbf{E})$$

Or
$$\sin(-\arcsin x) = -\sin\arcsin x = -x$$

car la fonction sinus est impaire. Donc $-\arcsin x$ est solution de l'équation (**E**) et est compris entre $-\frac{\pi}{2}$ et $\frac{\pi}{2}$. Il vient $-\arcsin x = \arcsin(-x)$. □

Intéressons-nous maintenant aux propriétés de dérivabilité de cette nouvelle fonction.

Théorème 12.6.31
1. $\forall x \in \left[-\frac{\pi}{2}\,;\frac{\pi}{2}\right] \qquad \cos\arcsin x = \sqrt{1-x^2}$
2. *La fonction* arcsin *est dérivable sur* $]-1\,;1[$ *et*
$$\forall x \in]-1\,;1[\qquad \arcsin' x = \frac{1}{\sqrt{1-x^2}}$$
3. *La fonction* arcsin *est strictement croissante sur* $[-1\,;1]$.

Preuve :

1. Soit $x \in [-\frac{\pi}{2}\,;\frac{\pi}{2}]$. On sait que
$$\cos^2\arcsin x + \underbrace{\sin^2\arcsin x}_{=x^2} = 1$$
d'où
$$\cos\arcsin x = \sqrt{1-x^2} \qquad \text{ou} \qquad -\sqrt{1-x^2}$$

Pour déterminer s'il s'agit de $\sqrt{1-x^2}$ ou $-\sqrt{1-x^2}$, on réfléchit une minute : $\arcsin x$ est compris entre $-\frac{\pi}{2}$ et $\frac{\pi}{2}$. Par conséquent, $\cos\arcsin x$ est positif. D'où

$$\forall x \in [-1\,;1] \qquad \cos\arcsin x = \sqrt{1-x^2}$$

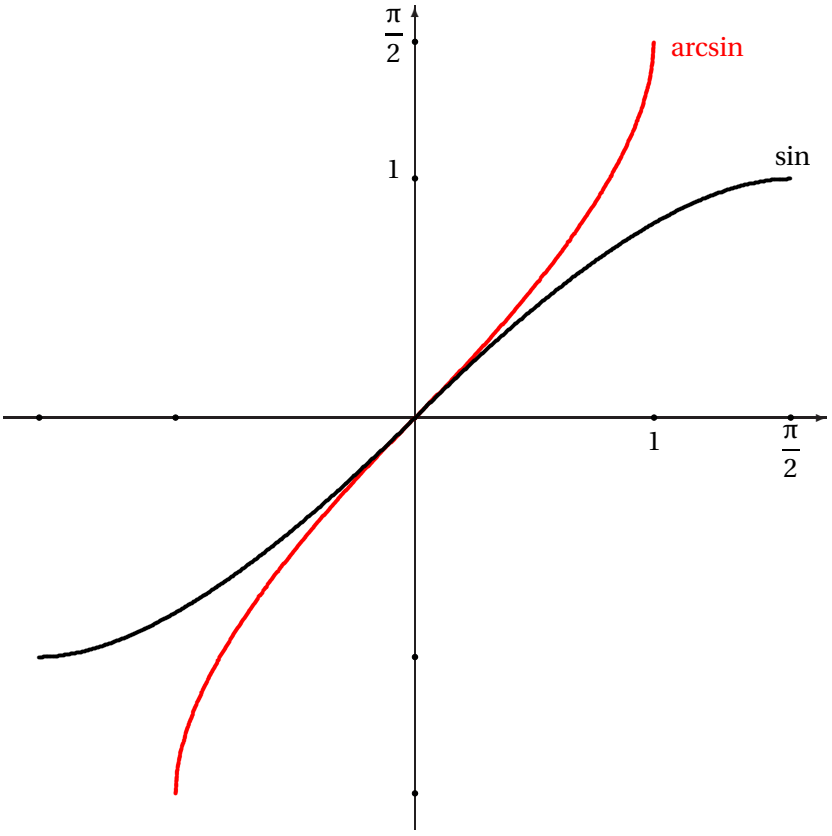
2. D'après le théorème de dérivabilité d'une réciproque, comme la dérivée de sin est cos, qui ne s'annule pas sur $]-\frac{\pi}{2}\,;\frac{\pi}{2}[$ et comme sin est bijective de cet intervalle sur $]-1\,;1[$, sa reciproque arcsin est dérivable sur $]-1\,;1[$. La valeur de sa dérivée est donnée par ce même théorème :

$$\forall x \in]-1\,;1[\qquad \arcsin' x = \frac{1}{\sin'\arcsin x} = \frac{1}{\cos\arcsin x} = \frac{1}{\sqrt{1-x^2}}$$

3. Ce point est clair puisque $\arcsin'$ est strictement positive sur $]-1\,;1[$. □

On termine en donnant quelques valeurs de arcsin et en traçant son graphe :

x	-1	$-\frac{\sqrt{3}}{2}$	$-\frac{\sqrt{2}}{2}$	$-\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1
$\arcsin x$	$-\frac{\pi}{2}$	$-\frac{\pi}{3}$	$-\frac{\pi}{4}$	$-\frac{\pi}{6}$	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$



Il est important de se rappeler l'énoncé exact de la propriété

$$\forall x \in \left[-\frac{\pi}{2}\,;\frac{\pi}{2}\right] \qquad \arcsin\sin x = x$$

établie au **Théorème 3.2**. Elle dit bien que x doit se trouver compris entre $-\frac{\pi}{2}$ et $\frac{\pi}{2}$ pour que

la formule $\arcsin\sin x = x$ soit valable. Et pas autre part !!!

Par exemple, $\arcsin\sin\frac{\pi}{3} = \frac{\pi}{3}$ mais $\arcsin\sin\frac{2\pi}{3} = \arcsin\frac{\sqrt{3}}{2} = \frac{\pi}{3}$

La Fonction Arccosinus

On se permet d'aller beaucoup plus vite dans cette section, dans la mesure où le travail est très similaire à celui effectué dans la précédente.

Définition 12.6.32
La fonction Arccosinus, notée arccos, est la bijection réciproque de la fonction cos restreinte à $[0\,;\pi]$.

Théorème 12.6.33
arccos *est une fonction définie sur* $[-1\,;1]$ *à valeurs dans* $[0\,;\pi]$. *Elle est caractérisée par la propriété fondamentale*

$$\forall x \in [-1\,;1] \qquad \cos\arccos x = x$$

En outre $$\forall x \in [0\,;\pi] \qquad \arccos\cos x = x$$

Enfin, $$\forall x \in [-1\,;1] \qquad \arccos(-x) = \pi - \arccos x$$

Preuve : Seule la dernière assertion n'est pas une conséquence directe des **Définition 1.3** et **Théorème 1.4**. On rappelle que $\arccos(-x)$ est l'unique solution $y \in [0\,;\pi]$ de l'équation

$$\cos y = -x$$

Or, $$\pi - x \in [0\,;\pi] \qquad \text{et} \qquad \cos(\pi - x) = -x$$

Par conséquent, $$\arccos(-x) = \pi - x$$ □

Remarquons que cette dernière propriété nous assure que le graphe de la fonction arccos est symétrique par rapport au point $A = (0, \frac{\pi}{2})$.

En effet, notons $M = (x, \arccos x)$ et $N = (-x, \arccos(-x))$ pour un $x \in [-1\,;1]$. D'après le **Théorème 3.5**, on a en fait $N = (-x, \pi - \arccos x)$. On constate alors que

$$\overrightarrow{AM} = (x, \arccos x) - \left(0, \frac{\pi}{2}\right) = \left(x, \arccos x - \frac{\pi}{2}\right)$$

et $$\overrightarrow{NA} = \left(0, \frac{\pi}{2}\right) - (-x, \pi - \arccos x) = \left(x, \arccos x - \frac{\pi}{2}\right)$$

d'où $$\overrightarrow{AM} = \overrightarrow{NA}$$

Cette relation vectorielle exprime bien que les points M et N sont symétriques par rapport à A. On constatera cette symétrie lorsqu'on donnera le graphe de arccos.

Comme pour la fonction arcsin, on s'intéresse à la dérivabilité de arccos.

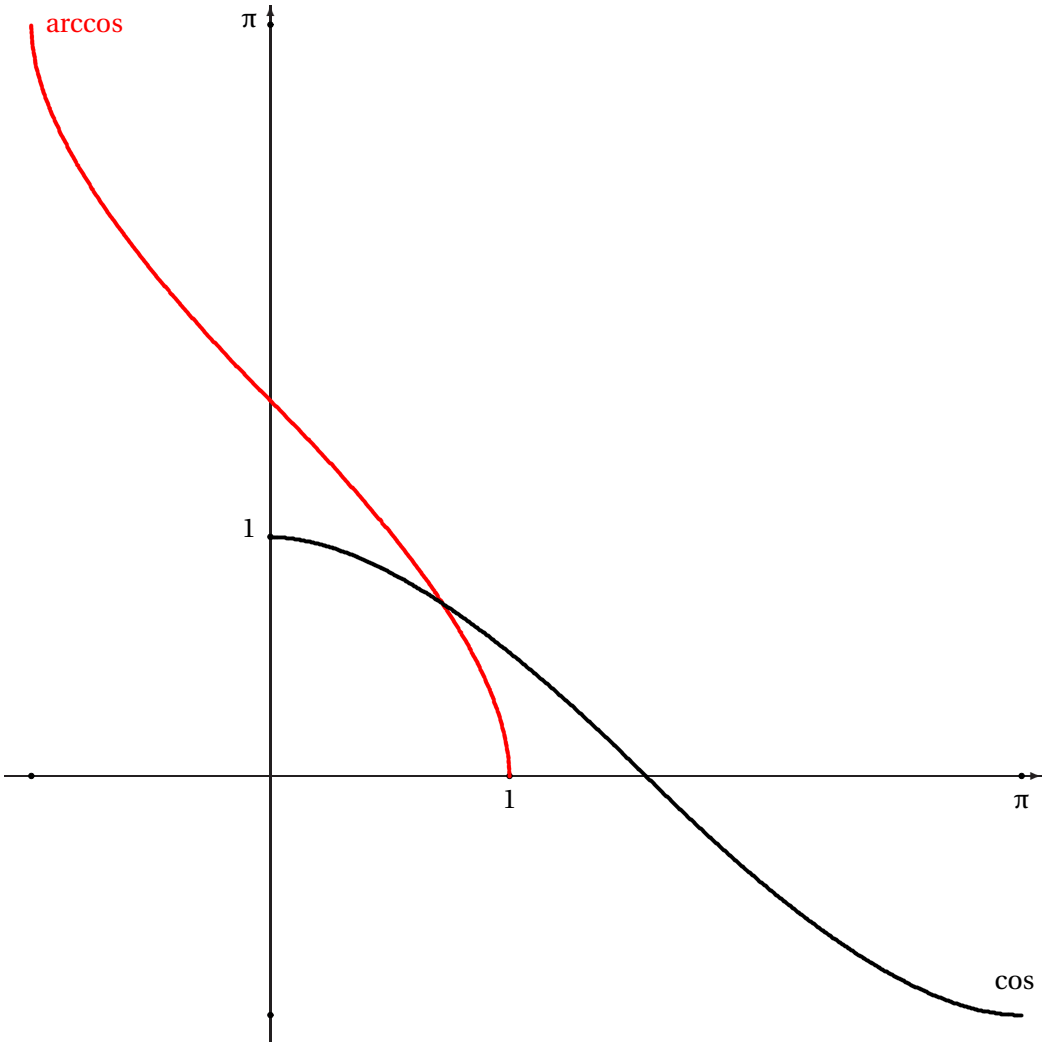
Théorème 12.6.34

1. $\forall x \in [-1\,;1] \qquad \sin\arccos x = \sqrt{1-x^2}$
2. *La fonction* arccos *est dérivable sur* $]-1\,;1[$ *et*
$$\forall x \in]-1\,;1[\qquad \arccos' x = -\frac{1}{\sqrt{1-x^2}}$$
3. *La fonction* arccos *est strictement décroissante sur* $[-1\,;1]$.
4. $\forall x \in [-1,1] \qquad \arccos x + \arcsin x = \dfrac{\pi}{2}$

Preuve :

1. On fixe x dans $[-1\,;1]$. On sait que
$$\underbrace{\cos^2\arccos x}_{=x^2} + \sin^2\arccos x = 1$$
d'où $\qquad \sin\arccos x = \sqrt{1-x^2} \qquad$ ou $\qquad -\sqrt{1-x^2}$
Or, $\arccos x$ est compris entre 0 et π donc $\sin\arccos x$ est positif et la conclusion s'ensuit.
2. La fonction cos est dérivable sur $]0\,;\pi[$, réalise une bijection de cet intervalle sur $]-1\,;1[$ et sa dérivée $-\sin$ ne s'y annule pas. D'après le **Théorème 1.5**, arccos est dérivable sur $]-1\,;1[$ et
$$\forall x \in]-1\,;1[\qquad \arccos' x = \frac{1}{\cos'\arccos x} = \frac{1}{-\sin\arccos x} = -\frac{1}{\sqrt{1-x^2}}$$
3. La décroissance de arccos est immédiate, compte tenu du fait que la dérivée est strictement négative sur $]-1\,;1[$.
4. On constate, à la lumière des calculs de $\arccos'$ et $\arcsin'$, que
$$\forall x \in]-1\,;1[\qquad \arccos' x = -\arcsin' x$$
Autrement dit $\qquad \forall x \in]-1\,;1[\qquad (\arccos + \arcsin)'(x) = 0$
Et la fonction $\arccos + \arcsin$ est constante sur $]-1\,;1[$. Cette constante peut être obtenue en évaluant en n'importe quel point de l'intervalle $]-1\,;1[$. Par exemple :
$$\arccos 0 + \arcsin 0 = \frac{\pi}{2} + 0 = \frac{\pi}{2}$$
donc $\qquad \forall x \in]-1\,;1[\qquad \arccos x + \arcsin x = \dfrac{\pi}{2}$
On vérifie enfin que
$$\arccos(-1) + \arcsin(-1) = \pi - \frac{\pi}{2} = \frac{\pi}{2} \qquad \text{et} \qquad \arccos 1 + \arcsin 1 = 0 + \frac{\pi}{2} = \frac{\pi}{2}$$
ce qui achève la demonstration. □

D'après le théorème précédent, la courbe de la fonction arccos peut être aisément déduite de celle de arcsin : il suffit de retourner cette dernière autour de l'axe des abscisses, puis de la remonter de $\frac{\pi}{2}$:



La Fonction Arctangente

Il s'agit de la dernière fonction circulaire réciproque, qui inverse la fonction tangente.

Définition 12.6.35
La fonction Arctangente, notée arctan, est la bijection réciproque de la fonction tan restreinte à $]-\frac{\pi}{2};\frac{\pi}{2}[$.

Théorème 12.6.36
arctan *est la fonction définie sur* $\mathbb{R}$ *à valeurs dans* $]-\frac{\pi}{2};\frac{\pi}{2}[$ *caractérisée par*

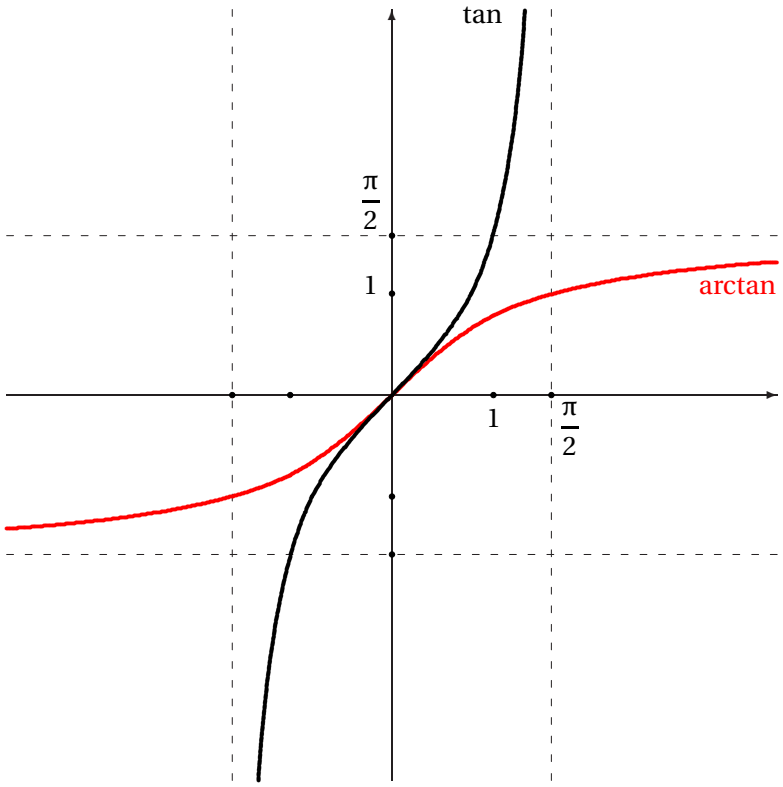
$$\forall x \in \mathbb{R} \qquad \tan\arctan x = x$$

De plus,
$$\forall x \in \left]-\frac{\pi}{2};\frac{\pi}{2}\right[\qquad \arctan\tan x = x$$

Enfin,
$$\forall x \in \left]-\frac{\pi}{2};\frac{\pi}{2}\right[\qquad \arctan(-x) = -\arctan x$$

Preuve : Tout marche comme avec l'arcsinus. La seule différence se trouve être les intervalles considérés : cela est dû au fait que tan est une bijection de $]-\frac{\pi}{2};\frac{\pi}{2}[$ sur $\mathbb{R}$. Sa bijection réciproque est donc une fonction de $\mathbb{R}$ sur $]-\frac{\pi}{2};\frac{\pi}{2}[$. □

Le graphe d'arctan ressemble à :



Parlons maintenant des propriétés de dérivabilité et des limites de arctan.

Théorème 12.6.37

1. *La fonction* arctan *est dérivable sur* $\mathbb{R}$ *et*
$$\forall x \in \mathbb{R} \qquad \arctan' x = \frac{1}{1+x^2}$$
2. *La fonction* arctan *est strictement croissante sur* $\mathbb{R}$.
3. $\forall x > 0 \qquad \arctan x + \arctan \dfrac{1}{x} = \dfrac{\pi}{2}$
4. $\lim\limits_{x\to-\infty} \arctan x = -\dfrac{\pi}{2}$ *et* $\lim\limits_{x\to+\infty} \arctan x = \dfrac{\pi}{2}$
5. arctan *est de classe* $\mathscr{C}^\infty$ *sur* $\mathbb{R}$. *De plus,*
$$\forall n \in \mathbb{N} \qquad \arctan x = \sum_{k=0}^{n} (-1)^k \frac{x^{2k+1}}{2k+1} + o(x^{2n+2})$$
et
$$\forall x \in [-1;1] \qquad \arctan x = \lim_{n\to\infty} \sum_{k=0}^{n} (-1)^k \frac{x^{2k+1}}{2k+1}$$

Preuve :

1. Encore et toujours le théorème de dérivabilité d'une réciproque : la dérivée de la fonction tan vaut $1+\tan^2$ et ne s'annule donc jamais sur $]-\frac{\pi}{2};\frac{\pi}{2}[$. Sa réciproque est donc dérivable sur $\mathbb{R}$ et
$$\forall x\in\mathbb{R}\qquad \arctan' x=\frac{1}{\tan'(\arctan x)}=\frac{1}{1+\tan^2\arctan x}=\frac{1}{1+x^2}$$
2. Il en découle que la fonction tan est strictement croissante : sa dérivée est en effet strictement positive.
3. On définit $$\forall x>0\qquad g(x)=\arctan x+\arctan\frac{1}{x}$$
g est dérivable d'après le théorème de dérivation des fonctions composées, et
$$\forall x>0\qquad g'(x)=\arctan' x-\frac{1}{x^2}\arctan'\frac{1}{x}=\frac{1}{1+x^2}-\frac{1}{x^2(1+1/x^2)}=0$$
La fonction g est donc constante. La valeur de cette constante peut être lue en tout point. En particulier :
$$g(1)=\arctan 1+\arctan 1=\frac{\pi}{4}+\frac{\pi}{4}=\frac{\pi}{2}$$
Conclusion : $$\forall x>0\qquad \arctan x+\arctan\frac{1}{x}=\frac{\pi}{2}$$
4. D'après le théorème de la limite monotone, arctan admet une limite ℓ en $+\infty$. Aussi, comme arctan est dérivable en 0, on sait que
$$\lim_{x\to 0}\arctan x=\arctan 0=0$$
On peut donc appliquer le théorème de composition des limites et la relation montrée au point 3 pour obtenir :
$$\frac{\pi}{2}=\lim_{x\to 0^+}\arctan x+\lim_{x\to 0^+}\arctan\frac{1}{x}=0+\ell$$
d'où $$\lim_{x\to+\infty}\arctan x=\frac{\pi}{2}$$
Comme arctan est impaire, $$\lim_{x\to-\infty}\arctan x=-\frac{\pi}{2}$$ □
5. La dérivée d'arctan est de classe $\mathscr{C}^\infty$ donc arctan est infiniment dérivable. On a
$$\forall x\in\mathbb{R}\qquad \arctan'(x)=\frac{1}{1+x^2}=\frac{1}{2}\left(\frac{1}{1-\mathrm{i}x}+\frac{1}{1+\mathrm{i}x}\right)$$
donc $$\forall x\in\mathbb{R}\quad\forall n\in\mathbb{N}^\star\qquad \arctan^{(n)}(x)=\frac{(n-1)!\mathrm{i}^{n-1}}{2}\left(\frac{(-1)^{n-1}}{(1-\mathrm{i}x)^n}+\frac{1}{(1+\mathrm{i}x)^n}\right)$$
donc $$\forall n\in\mathbb{N}^\star\qquad \arctan^{(n)}(0)=\frac{(n-1)!\mathrm{i}^{n-1}}{2}((-1)^{n-1}+1)$$
$$=\begin{cases}0 & \text{si } n \text{ est pair}\\ (n-1)!(-1)^{(n-1)/2} & \text{si } n \text{ est impair}\end{cases}$$

D'après le théorème de Taylor-Young,

$$\forall n \in \mathbb{N} \qquad \arctan x \underset{x\to 0}{=} \sum_{k=0}^{n} (-1)^k \frac{x^{2k+1}}{(2k+1)} + o(x^{2k+2})$$

À présent, soient $x \in [0\,;1]$ et $n \in \mathbb{N}$. On commence par estimer $\arctan^{(2n+2)}$:

$$\forall y \in [-x\,;x] \qquad \arctan^{(2n+2)}(y) = \frac{(2n+1)!(-1)^n \mathrm{i}}{2}\Big(\frac{-1}{(1-\mathrm{i}y)^{2n+2}} + \frac{1}{(1+\mathrm{i}y)^{2n+2}}\Big)$$

$$\begin{aligned}\text{donc} \qquad \forall y \in [-x\,;x] \qquad |\arctan^{(2n+2)}(y)| &\leqslant \frac{(2n+1)!}{2}\Big(\frac{1}{|1-\mathrm{i}y|^{2n+2}} + \frac{1}{|1+\mathrm{i}y|^{2n+2}}\Big)\\ &\leqslant \frac{(2n+1)!}{(1+y^2)^n} \leqslant (2n+1)!\end{aligned}$$

Comme arctan est de classe $\mathscr{C}^{2n+1}$ et $2n+2$ fois dérivable sur $[-x\,;x]$, l'inégalité de Taylor-Lagrange fournit

$$\Big|\arctan x - \sum_{k=0}^{n} (-1)^k \frac{x^{2k+1}}{2k+1}\Big| \leqslant \frac{(2n+1)!}{(2n+2)!}\, x \leqslant \frac{1}{2n+2}$$

$$\text{d'où} \qquad \forall x \in [0\,;1] \qquad \arctan x = \lim_{n\to\infty} \sum_{k=0}^{n} (-1)^k \frac{x^{2k+1}}{2k+1}$$

Comme arctan est impaire, cette formule est aussi vraie pour $x \in [-1\,;0]$. □

12.6.9 Fonctions Hyperboliques

Fonctions Hyperboliques Directes

Définition 12.6.38
Les fonctions cosinus et sinus hyperboliques, notées ch et sh, sont définies sur $\mathbb{C}$ par les relations

$$\forall z \in \mathbb{C} \qquad \operatorname{ch} z = \frac{\mathrm{e}^z + \mathrm{e}^{-z}}{2} = \cos(\mathrm{i}z) \qquad \text{et} \qquad \operatorname{sh} z = \frac{\mathrm{e}^z - \mathrm{e}^{-z}}{2} = -\mathrm{i}\sin(\mathrm{i}z)$$

La fonction ch s'annule sur $\{\mathrm{i}\frac{\pi}{2} + k\pi \mid k \in \mathbb{Z}\}$ et l'on peut définir la fonction tangente hyperbolique, notée th par la relation

$$\forall z \in \mathbb{C} \setminus \Big\{\mathrm{i}\frac{\pi}{2} + k\pi \mid k \in \mathbb{Z}\Big\} \qquad \operatorname{th} z = \frac{\operatorname{sh} z}{\operatorname{ch} z} = \frac{\mathrm{e}^z - \mathrm{e}^{-z}}{\mathrm{e}^z + \mathrm{e}^{-z}}$$

Les propriétés suivantes ne demandent rien d'autre qu'un petit calcul.

Théorème 12.6.39

1. $\forall z \in \mathbb{C} \qquad \operatorname{ch} z = \cos(iz) = \lim_{n\to\infty} \sum_{k=0}^{n} \frac{z^{2k}}{(2k)!} \qquad \operatorname{sh} z = -i\sin(iz) = \lim_{n\to\infty} \sum_{k=0}^{n} \frac{z^{2k+1}}{(2k+1)!}$
2. $\forall z \in \mathbb{C} \qquad \operatorname{ch}^2 z - \operatorname{sh}^2 z = 1$
3. ch, sh *et* th *sont infiniment dérivables sur* $\mathbb{R}$ *et l'on a*

$$\forall x \in \mathbb{R} \qquad \operatorname{ch}' x = \operatorname{sh} x \qquad \operatorname{sh}' x = \operatorname{ch} x \qquad \textit{et} \qquad \operatorname{th}' x = \frac{1}{\operatorname{ch}^2 x} = 1 - \operatorname{th}^2 x$$

4. ch *est paire ;* sh *et* th *sont impaires.*

5. *Ces fonctions, restreintes à* $\mathbb{R}$*, admettent les limite suivantes :*

$$\lim_{x\to+\infty} \operatorname{ch} x = \lim_{x\to-\infty} \operatorname{ch} x = +\infty$$

$$\lim_{x\to-\infty} \operatorname{sh} x = -\infty \qquad et \qquad \lim_{x\to+\infty} \operatorname{sh} x = +\infty$$

$$\lim_{x\to-\infty} \operatorname{th} x = -1 \qquad et \qquad \lim_{x\to+\infty} \operatorname{th} x = 1$$

6. th *et* sh *sont strictement croissantes sur* $\mathbb{R}$.
   ch *est strictement décroissante (resp. croissante) sur* $\mathbb{R}_-$ *(resp.* $\mathbb{R}_+$*).*

> Ces fonctions sont surtout étudiées du fait de leur analogie avec les fonctions de trigonométrie circulaire, comme nous allons le voir. Mais aussi parce que leurs réciproques ont des derivées intéressantes.
>
> Il est également notable que la fonction ch a une interprétation physique simple. Si l'on prend une chaîne et qu'on la pend par ses deux bouts, la courbe qu'elle forme est de la forme $x \longmapsto A\operatorname{ch}(\alpha x+\beta)$. Cette courbe est appelée « chaînette ».

Théorème 12.6.40
Les fonctions ch*, sh et* th *satisfont les formules d'addition suivantes :*

$$\begin{aligned}
\forall \alpha,\beta\in\mathbb{C} \qquad \operatorname{ch}(\alpha+\beta) &= \operatorname{ch}\alpha\operatorname{ch}\beta+\operatorname{sh}\alpha\operatorname{sh}\beta\\
\operatorname{sh}(\alpha+\beta) &= \operatorname{sh}\alpha\operatorname{ch}\beta+\operatorname{sh}\beta\operatorname{ch}\alpha\\
\operatorname{th}(\alpha+\beta) &= \frac{\operatorname{th}\alpha+\operatorname{th}\beta}{1+\operatorname{th}\alpha\operatorname{th}\beta}\\
\operatorname{ch}\alpha+\operatorname{ch}\beta &= 2\operatorname{ch}\frac{\alpha+\beta}{2}\operatorname{sh}\frac{\alpha-\beta}{2}\\
\operatorname{sh}\alpha+\operatorname{sh}\beta &= 2\operatorname{sh}\frac{\alpha+\beta}{2}\operatorname{ch}\frac{\alpha-\beta}{2}
\end{aligned}$$

12.7 Développements limités

12.7.1 Définitions et premières propriétés

Définition 12.7.1
Soit f une fonction définie dans un voisinage de $a\in\mathbb{R}$. Soit $n\in\mathbb{N}$. On dit que f *admet un développement limité en* a *à l'ordre* n si, et seulement si, il existe $(a_0,\dots,a_n)\in\mathbb{R}^n$ tel que

$$f(x) \underset{x\to a}{=} a_0+a_1(x-a)+\cdots+a_n(x-a)^n+o((x-a)^n)$$

$\sum_{k=0}^{n} a_k(X-a)^k$ est appelée *une partie régulière d'un développement limité de* f *à l'ordre* n.

Commençons par une observation qui nous simplifiera la vie : dans la mesure où l'on peut composer à droite dans les expressions faisant intervenir les « petits o », une fonction f admet un développement limité à l'ordre n en $a \in \mathbb{R}$ si et seulement si

$$f(x) \underset{x\to a}{=} \sum_{k=0}^{n} a_k (x-a)^k + o((x-a)^n) \iff f(a+h) \underset{h\to 0}{=} \sum_{k=0}^{n} a_k h^k + o(h^n)$$

Cette équivalence est obtenue en composant à droite par $h \longmapsto a+h$ l'expression de gauche et par $x \longmapsto x-a$ l'expression de droite. Ainsi, f admet un développement limité à l'ordre n en a si et seulement si $h \longmapsto f(a+h)$ en admet un à l'ordre n en 0. Conclusion : il suffit d'étudier les développements limités en 0, tous les autres peuvent s'y ramener. Nous ferons donc cela.

Remarquons aussi que si f admet un développement limité à l'ordre n en 0, alors il en admet un à tout ordre $m \leqslant n$. En effet, si l'on a

$$f(x) \underset{x\to 0}{=} \sum_{k=0}^{n} a_k x^k + o(x^n)$$

il est également vrai que

$$f(x) \underset{x\to 0}{=} \sum_{k=0}^{m} a_k x^k + o(x^m)$$

dans la mesure où toute puissance de x supérieure à $m+1$ est négligeable devant x^m.

Enfin, si on note p l'indice (s'il existe) du premier coefficient non nul dans un développement limité de f à l'ordre n en 0, on a alors

$$f(x) \underset{x\to 0}{=} a_p x^p + o(x^p)$$

Autrement dit,

$$f(x) \underset{x\to 0}{\sim} a_p x^p$$

Donc les développements limités ont comme application immédiate la recherche d'équivalents, et donc de limites.

Théorème 12.7.2 (Unicité des coefficients d'un DL)
Soit f une fonction admettant au voisinage de 0 un développement limité à l'ordre n. Alors ce dernier est unique.

Preuve : Supposons que f admette en 0 les deux développements limités suivants à l'ordre n :

$$f(x) \underset{x\to 0}{=} \sum_{k=0}^{n} a_k x^k + o(x^n)$$

et

$$f(x) \underset{x\to 0}{=} \sum_{k=0}^{n} b_k x^k + o(x^n)$$

Notons

$$A = \{k \in [\![0\,;n]\!] \mid a_k \neq b_k\}$$

et supposons A non vide. Il admet donc un plus petit élément, noté p. Ce qui signifie que

$$\forall k < p \qquad a_k = b_k$$

D'après la dernière remarque formulée plus haut,

$$f(x) \underset{x\to 0}{=} a_p x^p + o(x^p) \qquad \text{et} \qquad f(x) \underset{x\to 0}{=} b_p x^p + o(x^p)$$

Par suite,

$$a_p - b_p \underset{x\to 0}{=} o(1)$$

ce qui implique que $a_p - b_p = 0$. C'est une contradiction. Donc A est vide et

$$\forall k \in [\![0\,;n]\!] \qquad a_k = b_k$$ □

Théorème 12.7.3 (Développements limités et régularité)

- *Une fonction admet un développement limité à l'ordre 0 en* 0 *si, et seulement si, elle est continue en 0.*
- *Une fonction admet un développement limité à l'ordre 1 en 0 si, et seulement si, elle est dérivable en 0.*
- *Toute fonction de classe $\mathscr{C}^n$ au voisinage de 0 admet un développement limité à l'ordre n en 0.*

Preuve : Tout a déjà été fait dans les paragraphes sur la continuité et la dérivabilité. Le dernier point, en particulier, résulte du théorème de Taylor-Young. □

> Notons que l'existence d'un développement limité à l'ordre n et d'une dérivée n-ème sont des notions équivalentes **uniquement pour $n = 0$ ou $n = 1$!**
>
> Il existe ainsi des fonctions admettant un développement limité à l'ordre 2 en 0, mais qui ne sont pas 2 fois dérivables. Prenons par exemple
>
> $$\forall x \in \mathbb{R} \qquad f(x) = \begin{cases} x^3 \sin\dfrac{1}{x^2} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases}$$
>
> Alors $$f(x) = x^2 \times x \sin\frac{1}{x^2} = o(x^2)$$
> et f admet bien un développement limité à l'ordre 2 en 0. On a
>
> $$\forall x \in \mathbb{R}^\star \qquad f'(x) = 3x^2 \sin\frac{1}{x^2} - 2\cos\frac{1}{x^2}$$
>
> qui n'admet pas de limite en 0. Donc f' n'a aucune chance d'être continue en 0 ; elle en a encore moins d'être dérivable deux fois en 0.
>
> On peut faire encore mieux (ou pire, suivant les points de vue) : il existe des fonctions qui admettent des développements limités à tout ordre en 0, sans pour autant être ne serait-ce que $\mathscr{C}^1$ au voisinage de 0. Vérifiez qu'une telle fonction est $x \longmapsto \mathrm{e}^{-1/x^2} \sin \mathrm{e}^{1/x^2}$.

12.7.2 Opérations sur les développements limités

On pourrait se dire que grâce à la formule de Taylor, on est capable de trouver tous les développements limités qu'on souhaite pourvu que la fonction considérée soit suffisamment régulière. Théoriquement, c'est vrai. Pratiquement, les calculs de dérivées n-èmes sont inhumains pour la plupart des fonctions. Heureusement, il y a plus simple.

Théorème 12.7.4 (Addition des développements limités)
Soient f et g deux fonctions qui ont, au voisinage de 0*, un développement limité à l'ordre n. Alors $f + g$ admet un développement limité à l'ordre n en 0, dont la partie régulière est la somme des parties régulières de f et g.*

Preuve : Il s'agit simplement des règles d'addition entre relations avec « petits o ». Si on sait que

$$f(x) \underset{x\to 0}{=} \sum_{k=0}^{n} a_k x^k + \mathrm{o}(x^n)$$

et
$$g(x) \underset{x\to 0}{=} \sum_{k=0}^{n} b_k x^k + \mathrm{o}(x^n)$$

alors
$$(f+g)(x) = f(x) + g(x) \underset{x\to 0}{=} \sum_{k=0}^{n} (a_k + b_k) x^k + \mathrm{o}(x^n)$$ □

Théorème 12.7.5 (Multiplication des développements limités)
Soient f et g deux fonctions qui ont, au voisinage de 0, un développement limité à l'ordre n. Alors fg admet un développement limité à l'ordre n en 0, dont la partie régulière est le produit des parties régulières de f et g, tronqué à l'ordre n (c'est-à-dire qu'on se débarasse des termes d'ordre $n+1$ ou supérieur).

Preuve : Notons
$$f(x) \underset{x\to 0}{=} \underbrace{\sum_{k=0}^{n} a_k x^k}_{=\mathrm{A}(x)} + \mathrm{o}(x^n)$$

et
$$g(x) \underset{x\to 0}{=} \underbrace{\sum_{k=0}^{n} b_k x^k}_{=\mathrm{B}(x)} + \mathrm{o}(x^n)$$

Alors
$$f(x)g(x) \underset{x\to 0}{=} \mathrm{A}(x)\mathrm{B}(x) + (\mathrm{A}(x) + \mathrm{B}(x))\mathrm{o}(x^n) + \mathrm{o}(x^{2n})$$

Or,
$$(\mathrm{A}(x) + \mathrm{B}(x))\,\mathrm{o}(x^n) = \mathrm{o}(x^n) \qquad \text{et} \qquad \mathrm{o}(x^{2n}) = \mathrm{o}(x^n)$$

donc
$$f(x)g(x) \underset{x\to 0}{=} \mathrm{A}(x)\mathrm{B}(x) + \mathrm{o}(x^n)$$

Et tous les termes du polynôme AB dont le degré est supérieur à $n+1$ sont négligeables devant x^n et on peut les intégrer dans le $\mathrm{o}(x^n)$. On obtient alors le produit AB, tronqué à l'ordre n. □

Théorème 12.7.6 (Composition des développements limités, admis)
Soient f et g deux fonctions qui ont, au voisinage de 0, un développement limité à l'ordre n. On suppose de plus que $g(0) = 0$. Posons

$$f(x) \underset{x\to 0}{=} \mathrm{A}(x) + o(x^n) \qquad g(x) \underset{x\to 0}{=} \mathrm{B}(x) + o(x^n) \qquad \textit{avec} \qquad \mathrm{A}, \mathrm{B} \in \mathbb{R}_n[\mathrm{X}]$$

Alors $f \circ g$ admet un développement limité à l'ordre n en 0, dont la partie régulière est le polynôme composé $\mathrm{A} \circ \mathrm{B}$, tronqué à l'ordre n.

Preuve : Dans la mesure où $g(0) = \mathrm{B}(0) = 0$, 0 est racine de B. Notons p son ordre ; il existe $\mathrm{B}_1 \in \mathbb{R}_{n-p}[\mathrm{X}]$ tel que $\mathrm{B} = \mathrm{X}^p \mathrm{B}_1$ et $\mathrm{B}_1(0) \neq 0$. On sait qu'on peut composer à droite dans une relation faisant intervenir un « petit o » donc

$$f(g(x)) \underset{x\to 0}{=} \mathrm{A}(g(x)) + \mathrm{o}(g(x)^n)$$

Or,
$$g(x)^n = x^n \mathrm{B}_1(x)^n \qquad \text{donc} \qquad \mathrm{o}(g(x)^n) \underset{x\to 0}{=} \mathrm{o}(x^n)$$

d'où $$f(g(x)) \underset{x\to 0}{=} \mathrm{A}(\mathrm{B}(x)+\mathrm{o}(x^n))+\mathrm{o}(x^n)$$

Posons $$\mathrm{A}=\sum_{k=0}^{n}\mathrm{A}_k\mathrm{X}^k$$

de sorte que $$\mathrm{A}(\mathrm{B}(x)+\mathrm{o}(x^n)) \underset{x\to 0}{=} \sum_{k=0}^{n}\mathrm{A}_k(\mathrm{B}(x)+\mathrm{o}(x^n))^k$$

Ensuite, $$(\mathrm{B}(x)+\mathrm{o}(x^n))^k \underset{x\to 0}{=} \mathrm{B}(x)^k+\sum_{j=1}^{k}\binom{k}{j}\mathrm{B}(x)^{k-j}\mathrm{o}(x^{nj})=\mathrm{B}(x)^k+\mathrm{o}(x^n)$$

d'où $$f(g(x)) \underset{x\to 0}{=} \sum_{k=0}^{n}\mathrm{A}_k\mathrm{B}(x)^k+\mathrm{o}(x^n)=\mathrm{A}(\mathrm{B}(x))+\mathrm{o}(x^n)$$

Mais dans le polynôme $\mathrm{A}\circ\mathrm{B}$, les termes de degré supérieur à $n+1$ peuvent être négligés devant x^n. Donc on obtient bien que $f\circ g$ admet un développement limité à l'ordre n en 0, dont la partie régulière est $\mathrm{A}\circ\mathrm{B}$ tronqué à l'ordre n. □

Exemple 12.7.7
Imaginons qu'on ait à développer $\cos(\sin x)$ à l'ordre 3 en 0. Le théorème de composition des développements limités nous dit qu'on aura besoin du développement à l'ordre 3 du sinus et du cosinus. On commence par les écrire :

$$\cos x=1-\frac{x^2}{2}+\mathrm{o}(x^3) \qquad \text{et} \qquad \sin x=x-\frac{x^3}{6}+\mathrm{o}(x^3)$$

Les parties régulières sont, en respectant les notations de l'énoncé :

$$\mathrm{A}=1-\frac{\mathrm{X}^2}{2} \qquad \text{et} \qquad \mathrm{B}=\mathrm{X}-\frac{\mathrm{X}^3}{6}$$

On calcule le polynôme $\mathrm{A}\circ\mathrm{B}$, en prenant bien soin de ne pas calculer les termes de degré 4 ou plus, car on va de toute manière les négliger. On voit qu'on aura juste besoin du calcul de B^2, qu'on fait immédiatement :

$$\mathrm{B}^2=\left(\mathrm{X}-\frac{\mathrm{X}^3}{6}\right)^2=\mathrm{X}^2+\text{termes de degré 4 ou plus}$$

d'où $$\mathrm{A}\circ\mathrm{B}=1-\frac{\mathrm{X}^2}{2}+\text{termes de degré 4 ou plus}$$

et $$\cos\sin x \underset{x\to 0}{=} 1-\frac{x^2}{2}+\mathrm{o}(x^3)$$

Une remarque au passage : le $x^3/6$ du sinus n'a servi à rien. Pouvait-on le prévoir ? Oui, avec de l'habitude et en connaissant nos développements de fonctions usuelles sur le bout des doigts. En effet, on pouvait se dire que le cosinus n'a pas de terme d'ordre 1 donc ferait immédiatement intervenir le carré du développement du sinus ; et ce dernier (toujours dans notre tête) n'a clairement pas de terme d'ordre 3. Faire cette gymnastique avant de se lancer dans le calcul d'un développement limité est fondamental pour éviter de longs calculs et diminuer les risques d'erreurs.

Exemple 12.7.8
On peut désormais calculer les développements limités d'inverses, à l'aide de la formule

$$\frac{1}{1+x}=\sum_{k=0}^{n}(-1)^k x^k+\mathrm{o}(x^n)$$

En effet, si f est une fonction telle que $f(0) = a \neq 0$, on a

$$\frac{1}{f(x)} = \frac{1}{a + (f(x) - a)} = \frac{1}{a} \frac{1}{1 + \frac{f(x)-a}{a}}$$

La fonction $h : x \longmapsto \dfrac{f(x) - a}{a}$ s'annule en 0 donc si f admet un développement limité en 0, le théorème de composition nous dit comment obtenir celui de $1/f$.

Exemple 12.7.9
Mettons cela en œuvre pour calculer le développement à l'ordre 4 de $1/\cos x$ en 0. On a

$$\frac{1}{\cos x} = \frac{1}{1 + (\cos x - 1)}$$

On aura besoin du développement à l'ordre 4 de $1/(1+x)$ et de $\cos x - 1$ en 0. On les écrit :

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 + x^4 + o(x^4)$$

et

$$\cos x - 1 = -\frac{x^2}{2} + \frac{x^4}{24} + o(x^4)$$

Pour conserver les notations du théorème de composition, on prend

$$A = 1 - X + X^2 - X^3 + X^4 \qquad \text{et} \qquad B = -\frac{X^2}{2} + \frac{X^4}{24}$$

et on doit calculer $A \circ B = 1 - B + B^2 - B^3 + B^4$. Il nous faut donc les puissances de B ; on n'oublie pas que seuls les termes de degré inférieur à 4 nous intéressent, donc on ne perd pas de temps à calculer les autres. On a

$$B = -\frac{X^2}{2} + \frac{X^4}{24}$$

$$B^2 = \frac{X^4}{4} + \text{termes de degré 5 ou plus}$$

$$B^3 = \text{termes de degré 6 ou plus}$$

$$B^4 = \text{termes de degré 8 ou plus}$$

donc

$$\begin{aligned} A \circ B &= 1 + \frac{X^2}{2} - \frac{X^4}{24} + \frac{X^4}{4} + \text{termes de degré 5 ou plus} \\ &= 1 + \frac{X^2}{2} + \frac{5X^4}{24} + \text{termes de degré 5 ou plus} \end{aligned}$$

et

$$\frac{1}{\cos x} \underset{x \to 0}{=} 1 + \frac{x^2}{2} + \frac{5x^4}{24} + o(x^4)$$

En fait, on peut même pousser ce développement plus loin d'un ordre, sans travail supplémentaire : le cosinus est une fonction paire, donc il n'y aura pas de termes de degré impair. D'où

$$\frac{1}{\cos x} \underset{x \to 0}{=} 1 + \frac{x^2}{2} + \frac{5x^4}{24} + o(x^5)$$

Profitons-en pour illustrer le théorème de multiplication des développements limités, dans le but d'obtenir tan à l'ordre 5 en 0. On a

$$\tan x = \frac{\sin x}{\cos x} = \sin x \times \frac{1}{\cos x}$$

et $$\sin x \underset{x\to 0}{=} x - \frac{x^3}{6} + \frac{x^5}{120} + o(x^5)$$

Il suffit de multiplier ce développement avec celui qu'on vient d'obtenir, en négligeant les termes de degré 6 ou plus. On trouve :

$$\tan x \underset{x\to 0}{=} \left(x + \frac{x^3}{2} + \frac{5x^5}{24}\right) - \frac{1}{6}\left(x^3 + \frac{x^5}{2}\right) + \frac{x^5}{120} + o(x^5)$$

Tous calculs faits, $$\tan x \underset{x\to 0}{=} x + \frac{x^3}{3} + \frac{2x^5}{15} + o(x^5)$$

La dernière opération qui nous intéresse est la dérivation. Avant d'aborder un théorème de dérivation des développements limités, nous aurons besoin d'un lemme :

Lemme 12.7.10
Soit f une fonction dérivable au voisinage de 0, telle que

$$f'(x) \underset{x\to 0}{=} o(x^n)$$

Alors $$f(x) \underset{x\to 0}{=} f(0) + o(x^{n+1})$$

Preuve : C'est une conséquence de la règle de l'Hospital. On a

$$\lim_{x\to 0} \frac{f(x) - f(0)}{x^{n+1}} = \lim_{x\to 0} \frac{f'(x)}{x^n} = 0$$ □

Théorème 12.7.11 (Dérivation des développements limités)
Soit f une fonction derivable, telle que f' admet un développement limité à l'ordre n en 0. Alors f admet un développement limité à l'ordre $n+1$ en 0, dont la dérivée est le développement de f'.

Preuve : On sait que f' admet un développement limité à l'ordre n en 0, qu'on écrit sous la forme :

$$f'(x) \underset{x\to 0}{=} \sum_{k=0}^{n} a_k x^k + o(x^n)$$

On considère la fonction auxiliaire définie par l'expression

$$g(x) = f(x) - \sum_{k=0}^{n} \frac{a_k}{k+1} x^{k+1}$$

Alors g est dérivable au voisinage de 0 et

$$g'(x) = f'(x) - \sum_{k=0}^{n} a_k x^k = o(x^n)$$

D'après le **Lemme 6.10**,

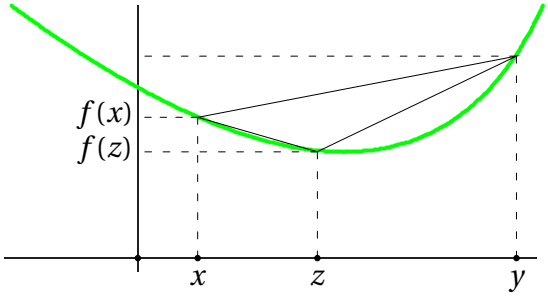
$$g(x) = g(0) + o(x^{n+1}) = f(0) + o(x^{n+1})$$

d'où $$f(x) = f(0) + \sum_{k=0}^{n} \frac{a_k}{k+1} x^{k+1} + o(x^{n+1})$$ □

12.8 Convexité

Ce dernier paragraphe est consacré à l'étude d'une propriété particulière à certaines fonctions : la convexité. C'est un outil très utile pour obtenir des inégalités intéressantes, très difficiles (voire impossible) à avoir autrement.

Une fonction convexe f est une fonction, définie sur un intervalle, dont le graphe se trouve au-dessous de toutes ses cordes : si x et y sont dans le domaine de définition de f, on demande que pour tout $z \in [x\,;\,y]$, le point $(z, f(z))$ se trouve au-dessous de la droite qui relie les points $(x, f(x))$ et $(y, f(y))$:



La droite qui relie les points $(x, f(x))$ et $(y, f(y))$ est dirigée par le vecteur

$$u = \begin{bmatrix} y-x \\ f(y)-f(x) \end{bmatrix}$$

et l'on a $\qquad (x, f(x)) = (x, f(x)) + 0 \times u \qquad (y, f(y)) = (x, f(x)) + 1 \times u$

Le segment qui relie $(x, f(x))$ à $(y, f(y))$ est donc l'ensemble des points

$$\{(x, f(x)) + \theta\, u \mid \theta \in [0\,;\,1]\} = \{(\theta x + (1-\theta)\, y, \theta f(x) + (1-\theta) f(y)) \mid \theta \in [0\,;\,1]\}$$

Tout ceci motive la définition suivante :

Définition 12.8.1 (Fonctions convexes et concaves)
Soit f une fonction définie sur un intervalle I. On dit que f est *convexe* si, et seulement si,

$$\forall x, y \in \mathrm{I} \quad \forall \theta \in [0\,;\,1] \qquad f(\theta x + (1-\theta)\, y) \leqslant \theta f(x) + (1-\theta) f(y)$$

On dit qu'elle est *strictement convexe* si l'inégalité est stricte pour $\theta \in]0\,;\,1[$.

Enfin, on dit qu'elle est *(strictement) concave* si, et seulement si, $-f$ est (strictement) convexe.

Montrer qu'une fonction est convexe est, à partir de la seule définition, une chose assez difficile. Le but de cette section est de trouver des conditions simples qui impliquent la convexité, de manière à pouvoir exploiter ces inégalités. Commençons par observer que :

Proposition 12.8.2
Soit f une fonction définie sur un intervalle I. *Elle est convexe si, et seulement si,*

$$\forall x, z, y \in \mathrm{I} \qquad x < z < y \implies \frac{f(z)-f(x)}{z-x} \leqslant \frac{f(y)-f(x)}{y-x} \tag{1}$$

Dans ce cas, on peut ajouter que

$$\forall x, y, z \in \mathrm{I} \qquad x < z < y \implies \frac{f(z)-f(x)}{z-x} \leqslant \frac{f(y)-f(x)}{y-x} \leqslant \frac{f(y)-f(z)}{y-z} \tag{2}$$

f est strictement convexe si, et seulement si, on a la proposition (**1**) *avec des inégalités sont strictes. Dans ce cas, la proposition* (**2**) *est vraie, avec des inégalités strictes.*

Preuve : Montrons la partie sur la convexité stricte ; la preuve pour la convexité large est identique, à ceci près qu'on a des inégalités larges tout du long. Donnons-nous $x < y < z$ dans I ; on a alors

$$z = \theta x + (1-\theta) y \qquad \text{avec} \qquad \theta = \frac{y-z}{y-x} \qquad 1-\theta = \frac{z-x}{y-x}$$

Supposons que f est strictement convexe. Alors

$$f(z) < \theta f(x) + (1-\theta) f(y) = (1-\theta)(f(y) - f(x)) + f(x)$$

d'où
$$f(z) - f(x) < (1-\theta)(f(y) - f(x))$$

et
$$\frac{f(z)-f(x)}{z-x} < \frac{f(y)-f(z)}{y-x}$$

Mais on peut aussi écrire que

$$\theta f(x) + (1-\theta) f(y) = \theta(f(x) - f(y)) + f(y)$$

donc
$$f(z) - f(y) < \theta(f(x) - f(y))$$

et
$$\frac{f(z)-f(y)}{y-z} < \frac{f(x)-f(y)}{y-x}$$

ou encore
$$\frac{f(y)-f(x)}{y-x} < \frac{f(y)-f(z)}{y-z}$$

On a bien $\forall x, y, z \in \mathrm{I} \qquad x < y < z \implies \dfrac{f(z)-f(x)}{z-x} < \dfrac{f(y)-f(x)}{y-x} < \dfrac{f(y)-f(z)}{y-z}$

Réciproquement, supposons la condition (**1**), avec des inégalités strictes. On se donne $x, y \in \mathrm{I}$ et $\theta \in]0\,;1[$ et on pose $z = \theta x + (1-\theta) y$. On a alors

$$\theta = \frac{y-z}{y-x} \qquad (1-\theta) = \frac{z-x}{y-x}$$

et notre inégalité s'écrit, en fonction de θ :

$$\frac{f(z)-f(x)}{1-\theta} < f(y) - f(x) < \frac{f(y)-f(z)}{\theta}$$

En utilisant l'inégalité de gauche, il vient

$$f(z) - f(x) < (1-\theta)(f(y) - f(x))$$

d'où
$$f(\theta x + (1-\theta y) = f(z) < \theta f(x) + (1-\theta) f(y)$$ □

Corollaire 12.8.3
Soit f une fonction convexe sur un intervalle I. *Alors elle est dérivable à gauche et à droite en tout point intérieur à* I. *De plus,*

$$\forall x \in \overset{\circ}{\mathrm{I}} \qquad f'_d(z) \leqslant f'_g(z)$$

et
$$\forall x, y \in \overset{\circ}{\mathrm{I}} \qquad x < y \implies f'_d(x) \leqslant f'_g(y)$$

Si f est strictement convexe, cette inégalité est stricte.

Preuve : On suppose f convexe et on pose, pour tout $z \in \overset{\circ}{\mathrm{I}}$,

$$\mathrm{I}_z^- = \mathrm{I} \cap]-\infty ; z[\qquad \mathrm{I}_z^+ = \mathrm{I} \cap]z ; +\infty[$$

Le fait que z est intérieur à I assure que ces intervalles ne sont pas vides et cela rend possible toute la suite de la démonstration. On définit aussi deux fonctions g_- et g_+ :

$$\forall x \in \mathrm{I}_z^- \qquad g_-(x) = \frac{f(z)-f(x)}{z-x}$$

et

$$\forall y \in \mathrm{I}_z^+ \qquad g_+(x) = \frac{f(y)-f(z)}{y-z}$$

La **proposition 8.2** montre que g_- est majorée et g_+ est minorée puisque

$$\forall x \in \mathrm{I}_z^- \quad \forall y \in \mathrm{I}_z^+ \qquad g_-(x) \leqslant g_+(y)$$

Ceci montre aussi que

$$\operatorname*{Sup}_{x \in \mathrm{I}_z^-} g_-(x) \leqslant \operatorname*{Inf}_{y \in \mathrm{I}_z^+} g_+(y)$$

De plus, si $x < x'$ sont dans I_-, on a $x < x' < z$ donc

$$g_-(x) = \frac{f(z)-f(x)}{z-x} \leqslant \frac{f(z)-f(x')}{z-x'} = g_-(x')$$

g_- est croissante, majorée. D'après le théorème de la limite monotone, $\lim\limits_{x \to z^-} g_-(x)$ existe et est finie : f est dérivable à gauche en z et

$$f'_g(z) = \operatorname*{Sup}_{x \in \mathrm{I}_z^-} g_-(x)$$

De la même manière, on montre que g_+ est croissante, minorée, donc $\lim\limits_{y \to z^+} g_+(y)$ existe et est finie : f est dérivable à droite en z. Ceci montre que f est dérivable à gauche et à droite en tout point et

$$f'_d(z) = \operatorname*{Inf}_{y \in \mathrm{I}_z^+} g_+(y)$$

On a donc

$$f'_g(z) \leqslant f'_d(z)$$

On fixe maintenant x et y dans I. On sait que

$$\forall z \in]x ; y[\qquad \frac{f(z)-f(x)}{z-x} \leqslant \frac{f(y)-f(x)}{y-x}$$

donc

$$f'_d(x) \leqslant \frac{f(y)-f(x)}{y-x}$$

De même,

$$\forall z \in]x ; y[\qquad \frac{f(y)-f(x)}{y-x} \leqslant \frac{f(y)-f(z)}{y-z}$$

donc

$$\frac{f(y)-f(x)}{y-x} \leqslant f'_g(y)$$

ce qui fournit

$$f'_d(x) \leqslant f'_g(y)$$

Enfin, on suppose que f est strictement convexe et on se donne $x < y$ dans I. Pour avoir l'inégalité stricte, on va avoir besoin de deux points intermédiaire $z_0 < z_1$ dans $]x\,;\,y[$. D'après ce qu'on a vu plus haut,

$$f'_d(x) \leqslant \frac{f(z_0)-f(x)}{z_0-x} \qquad (\text{car } x < z_0)$$

et
$$\frac{f(y)-f(z_1)}{y-z_1} \leqslant f'_g(y) \qquad (\text{car } z_1 < y)$$

De plus,
$$\frac{f(z_0)-f(x)}{z_0-x} < \frac{f(z_1)-f(z_0)}{z_1-z_0} \qquad (\text{car } x < z_0 < z_1)$$

et enfin
$$\frac{f(z_1)-f(z_0)}{z_1-z_0} < \frac{f(y)-f(z_1)}{y-z_1} \qquad (\text{car } z_0 < z_1 < y)$$

Par suite,
$$f'_d(x) \leqslant \frac{f(z_0)-f(x)}{z_0-x} < \frac{f(z_1)-f(z_0)}{z_1-z_0} < \frac{f(y)-f(z_1)}{y-z_1} \leqslant f'_g(y) \qquad \square$$

Corollaire 12.8.4
Toute fonction convexe sur un intervalle ouvert est continue.

Corollaire 12.8.5
Soit f une fonction dérivable sur I. *Les propositions suivantes sont équivalentes :*

1. *f est convexe (resp. strictement convexe) ;*
2. *f' est croissante (resp. strictement croissante) ;*
3. *le graphe de f est au-dessus de toutes ses tangentes (resp. strictement), c'est-à-dire*

$$\forall x_0 \in \mathrm{I} \quad \forall x \in \mathrm{I}\setminus\{x_0\} \qquad f'(x_0)(x-x_0)+f(x_0) \leqslant f(x) \qquad \textit{(resp. <)}$$

Preuve : Supposons que f est convexe (resp. strictement). Comme elle est dérivable sur I, le **corollaire 8.3** montre que f' est croissante (resp. strictement).

Supposons f' croissante (resp. strictement). Soient $x_0 \in \mathrm{I}$ et $x \neq x_0$; par exemple, supposons $x < x_0$. D'après le théorème des accroissements finis, il existe $c \in]x\,;\,x_0[$ tel que

$$\frac{f(x)-f(x_0)}{x-x_0} = f'(c)$$

Mais $c < x_0$ et f' est croissante (resp. strictement) donc $f'(c) \leqslant f'(x_0)$ (resp. $f'(c) < f'(x_0)$). Par suite,

$$\frac{f(x_0)-f(x)}{x_0-x} \leqslant f'(x_0) \qquad (\text{resp. } <)$$

On ferait de même si $x_0 < x$.

Enfin, supposons que le graphe de f est au-dessus (resp. strictement) de toutes ses tangentes. On se donne $x < y$ dans I et $\lambda \in]0\,;\,1[$. On note $z = \lambda x + (1-\lambda)y$; comme le graphe de f est au-dessus de sa tangente en z, on a

$$\lambda f(x) + (1-\lambda) f(y) \geqslant \lambda(f(z)+f'(z)(x-z)) + (1-\lambda)(f(z)+f'(z)(y-z)) \qquad (\text{resp. } >)$$

Mais un calcul montre que le membre de droite se simplifie en $f(z)$: f est convexe (resp. strictement). □

Ce théorème est très utile, puisqu'on a des outils pour étudier la croissance d'une fonction ; et il fournit alors des conséquences géométriques intéressantes.

Par exemple, l'exponentielle est strictement convexe d'après ce théorème. Si $c \in \mathbb{R}$, on peut dire que

$$\forall x \in \mathbb{R} \setminus \{c\} \qquad \mathrm{e}^x > \mathrm{e}^c(x-c) + \mathrm{e}^c = \mathrm{e}^c(x+1-c)$$

On retrouve en particulier, sans le moindre calcul, l'inégalité classique

$$\forall x \in \mathbb{R} \setminus \{0\} \qquad \mathrm{e}^x > 1 + x$$

De la même manière, le logarithme est immédiatement concave et l'on en déduit

$$\forall x \in \mathbb{R}_+ \setminus \{1\} \qquad \ln x < x - 1$$

Les deux corollaires suivants sont triviaux d'après ce qui précède :

Corollaire 12.8.6
Soit f une fonction deux fois dérivable sur I. *Elle est convexe si, et seulement si, f'' est positive sur* I.

Définition 12.8.7 (Point d'inflexion)
Soit f une fonction définie sur I. Soit a un point intérieur à I. On dit que *a est un point d'inflexion de f* si, et seulement si f est convexe dans un voisinage à gauche de a, et concave dans un voisinage à droite de a. Ou le contraire.

Corollaire 12.8.8
Soit f une fonction de classe $\mathscr{C}^2$ sur I. *Soit a un point intérieur à* I. *C'est un point d'inflexion de f si, et seulement si, $f''(a) = 0$ et f'' change de signe en a.*

Enfin, l'inégalité de convexité peut être généralisée à plusieurs points intermédiaires :

Théorème 12.8.9 (Convexité généralisée)
Soit f une fonction convexe sur un intervalle I. *Pour tout entier $n \geqslant 2$, pour tous $x_1, \dots, x_n \in$ I et pour tous $\lambda_1, \dots, \lambda_n \in]0\,;1[$, tels que $\sum_{k=1}^{n} \lambda_k = 1$, on a*

$$f\Big(\sum_{k=1}^{n} \lambda_k x_k\Big) \leqslant \sum_{k=1}^{n} \lambda_k f(x_k)$$

Si f est strictement convexe, l'inégalité est stricte.

Preuve : On procède par récurrence. Le cas $n = 2$ est simplement la définition d'une fonction convexe.

Soit $n \geqslant 2$ un entier ; on suppose savoir que pour tous $x_1, \dots, x_n \in$ I et pour tous $\lambda_1, \dots, \lambda_n \in]0\,;1[$ tels que $\sum_{k=1}^{n} \lambda_k = 1$, on a

$$f\Big(\sum_{k=1}^{n} \lambda_k x_k\Big) \leqslant \sum_{k=1}^{n} \lambda_k f(x_k)$$

Soient $x_1,\dots,x_{n+1}\in \mathrm{I}$ et $\lambda_1,\dots,\lambda_{n+1}\in]0\,;1[$, tels que $\sum_{k=1}^{n+1}\lambda_k = 1$. On pose

$$\lambda = 1-\lambda_{n+1} > 0 \qquad x = \sum_{k=1}^{n}\frac{\lambda_k}{\lambda}$$

de sorte que $\displaystyle\sum_{k=1}^{n}\frac{\lambda_k}{\lambda} = \frac{1-\lambda_{n+1}}{\lambda} = 1$ et $\lambda x + (1-\lambda)x_{n+1} = \sum_{k=1}^{n+1}\frac{\lambda_k}{\lambda}x_k$

On sait que $$f(x) = f\Big(\sum_{k=1}^{n}\frac{\lambda_k}{\lambda}x_k\Big) \leqslant \sum_{k=1}^{n}\frac{\lambda_k}{\lambda}f(x_k)$$

donc
$$\begin{aligned} f\Big(\sum_{k=1}^{n+1}\lambda_k x_k\Big) = f(\lambda x + (1-\lambda)x_{n+1}) &\leqslant \lambda f(x) + (1-\lambda)f(x_{n+1}) \\ &\leqslant \sum_{k=1}^{n}\lambda_k f(x_k) + \lambda_{n+1}f(x_{n+1}) \end{aligned}$$

Ceci démontre la propriété au rang $n+1$. On a gagné. □

Chapitre 13

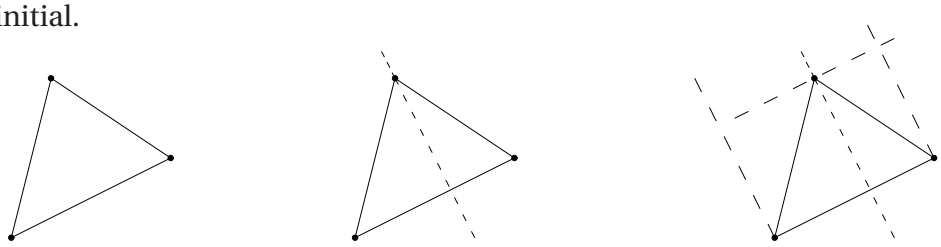
Intégration

Dans ce chapitre, nous souhaitons construire un outil, l'intégrale, dont l'application première sera la mesure de l'aire algébrique se trouvant entre la courbe représentative d'une fonction et l'axe des abscisses.

Pour comprendre la démarche qui va suivre, il convient de s'interroger sur ce que signifie « l'aire » d'une partie du plan. Il est clair pour tous que l'aire d'un rectangle doit être le produit de sa longueur et de sa largeur. Mais au-delà de ça, on bidouille pour calculer d'autres aires.

Ainsi, on se dit qu'une partie sans épaisseur doit avoir une aire nulle et que la réunion de deux parties du plan séparées uniquement par une frontière sans épaisseur doit être la somme des aires de chacun des parties.

C'est ainsi qu'on est capable d'accéder à l'aire d'un triangle : on le sépare en deux triangles rectangles à l'aide d'une hauteur. Et on observe que chacun de ces triangles est un demi-rectangle ; ce qui permet de calculer l'aire de chacun de ces triangles ; et en ajoutant les deux, d'obtenir l'aire du triangle initial.



Et de manière plus générale, on imagine bien qu'on serait capable de calculer l'aire de n'importe quel polygône, en le découpant en suffisamment de triangles et de rectangles. On obtient ainsi une valeur exacte de l'aire.

En revanche, comment calculer l'aire de parties du plan délimitées par des courbes non rectilignes ? On essaie simplement de se ramener aux aires qu'on s'ait déjà calculer : celles de rectangles. Si la courbe est suffisamment régulière (notion à définir proprement), elle devrait localement, en zoomant très fort, paraître rectiligne. Notre premier problème à considérer est donc le suivant : dans quelle mesure peut-on approcher une courbe par une réunion de segments de droites ?

13.1 Intégrale des fonctions en escalier

13.1.1 Fonctions en escalier

Définition 13.1.1 (Subdivision d'un intervalle)
Soit $A \subset [a\,;b]$. On dit qu'il s'agit d'une *subdivision de* $[a\,;b]$ si et seulement si A est fini et contient les extrémités a et b.

Étant donnée une subdivision A de $[a\,;b]$, on sait, puisqu'il s'agit d'un ensemble fini, que ses éléments peuvent être ordonnés de manière strictement croissante. De plus, le plus petit élément de A est a et le plus grand élément de A est b. On notera :

$$A = \{a = a_0 < a_1 < \cdots < a_{n-1} < a_n = b\}$$

Une subdivision a essentiellement une utilité : fournir un découpage de $[a\,;b]$ en intervalles ouverts disjoints, à un nombre fini de points près.

$$[a\,;b] = A \cup]a_0\,;a_1[\cup]a_1\,;a_2[\cup \cdots \cup]a_{n-1}\,;a_n[$$

Si on a deux subdivision A et B de $[a\,;b]$ telles que $A \subset B$, cela signifie que B découpe $[a\,;b]$ en plus de sous-intervalles que A. On pose donc

Définition 13.1.2 (Finesse d'une subdivision)
Soient A et B deux subdivisions de $[a\,;b]$. On dit que B est plus fine que A si et seulement si $A \subset B$.

Définition 13.1.3 (Fonctions en escalier)
Soit f une fonction définie sur $[a\,;b]$. On dit que f *est en escalier* si, et seulement si, il existe une subdivision $A = \{a_0 = a < a_1 < \cdots < a_n = b\}$ de $[a\,;b]$ telle que f est constante sur chacun des intervalles $]a_i\,;a_{i+1}[$ pour tout $i \in [\![0\,;n-1]\!]$. Une telle subdivision sera dite *adaptée à* f.

L'ensemble des fonctions en escalier sur $[a\,;b]$ est noté $\mathscr{E}([a\,;b])$.

Lemme 13.1.4
Soient f une fonction en escalier sur $[a\,;b]$ et A *une subdivision adaptée à f. Toute subdivision plus fine que* A *est également adaptée à f.*

Preuve : On montre d'abord qu'en ajoutant un point à A, on obtient aussi une subdivision adaptée à f. Notons

$$A = \{a_0 = a < a_1 < \cdots < a_n = b\}$$

notre subdivision de $[a\,;b]$ adaptée à f. Donc il existe des réels $y_0, \ldots, y_{n-1}$ tels que

$$\forall i \in [\![0\,;n-1]\!] \quad \forall x \in]a_i\,;a_{i+1}[\qquad f(x) = y_i$$

Donnons-nous un point $c \in [a\,;b]$. Rappelons-nous que

$$[a\,;b] = A \cup]a_0\,;a_1[\cup \cdots \cup]a_{n-1}\,;a_n[$$

et ces ensembles sont deux-à-deux disjoints. Donc on est dans l'un des deux cas suivants :

- Soit $c \in A$, auquel cas $A \cup \{c\} = A$ est une subdivision adaptée à f.
- Soit $c \notin A$, auquel cas existe un unique $i_0 \in [\![0\,;n-1]\!]$ tel que $c \in]a_{i_0}\,;a_{i_0+1}[$. Notons $B = A \cup \{c\}$ la subdivision de $[a\,;b]$ ainsi obtenue :

$$B = \{a_0 = a < \cdots < a_{i_0} < c < a_{i_0+1} < \cdots < a_n = b\}$$

et montrons qu'elle est adaptée à f. Pour tout $i \in [\![0\,;n-1]\!] \setminus \{i_0\}$, on sait que f est constante égale à y_i sur $]a_i\,;a_{i+1}[$.
Sur $]a_{i_0}\,;c[$ et $]c\,;a_{i_0+1}[$, qui sont inclus dans $]a_{i_0}\,;a_{i_0+1}[$, f est constante égale à y_{i_0}.
Donc B est bien adaptée à f.

Le lemme n'est alors que le résultat d'une récurrence immédiate. Soit B une subdivision plus fine que A ; par définition, $A \subset B$. Comme A et B sont finis, $B \setminus A$ est fini et on peut l'énumérer :

$$B \setminus A = \{c_1, \dots, c_m\}$$

de sorte que $$B = A \cup (B \setminus A) = A \cup \{c_1\} \cup \cdots \cup \{c_m\}$$

D'après notre résultat préliminaire, $A \cup \{c_1\}$ est adaptée à f. Donc $A \cup \{c_1\} \cup \{c_2\}$ aussi. Donc $A \cup \{c_1\} \cup \{c_2\} \cup \{c_3\}$ aussi. Et de proche-en-proche, B est adaptée à f. □

Théorème 13.1.5
$\mathscr{E}([a\,;b])$ est un $\mathbb{R}$-espace vectoriel.

Preuve : Soient λ et μ deux nombres réels. Soient f et g deux fonctions en escalier sur $[a\,;b]$. Soient A et B des subdivisions adaptées à f et g respectivement. Alors $A \cup B$ est une subdivision de $[a\,;b]$: en effet, $A \cup B$ est fini car A et B le sont, et contient a et b puisque A et B contiennent ces points.

$A \cup B$ est donc une subdivision de $[a\,;b]$, plus fine que A et plus fine que B. Elle est, d'après le **lemme 1.4**, adaptée à f et g à la fois. Énumérons ses éléments :

$$A \cup B = \{a_0 = a < a_1 < \cdots < a_{n-1} < a_n = b\}$$

On sait que f et g sont constantes sur chacun des intervalles $]a_i\,;a_{i+1}[$. Donc $\lambda f + \mu g$ est aussi constante sur chacun de ces intervalles. Ce qui montre que $\lambda f + \mu g$ est en escalier et que $A \cup B$ est une subdivision adaptée à cette fonction. □

13.1.2 Intégrale des fonctions en escalier

Définition 13.1.6
Soit f une fonction en escalier sur $[a\,;b]$. Soit A une subdivision de $[a\,;b]$ adaptée à f, qu'on énumère :

$$A = \{a_0 = a < a_1 < \cdots < a_{n-1} < a_n = b\}$$

Pour tout $i \in [\![0\,;n-1]\!]$, on note y_i la valeur constante prise par f sur $]a_i\,;a_{i+1}[$. On appelle *intégrale de f sur $[a\,;b]$ adaptée à la subdivision* A le nombre réel

$$\int_{[a\,;b]}^{A} f = \sum_{i=0}^{n-1} y_i(a_{i+1} - a_i)$$

Il suffit de faire un dessin pour voir que $\displaystyle\int_{[a\,;b]}^{A} f$ n'est autre que la somme algébrique des aires comprises entre les « marches d'escalier » constituant f et l'axe des abscisses. Tout simplement car l'aire d'un rectangle, c'est le produit de sa longueur par sa largeur.

Notre définition semble faire intervenir la subdivision de $[a\,;b]$ adaptée à f choisie. Montrons qu'il n'en est rien.

Lemme 13.1.7
Soit f une fonction en escalier sur $[a\,;b]$. Si A *et* B *sont deux subdivisions de $[a\,;b]$ adaptées à f,*

$$\int_{[a\,;b]}^{\mathrm{A}} f = \int_{[a\,;b]}^{\mathrm{B}} f$$

L'intégrale d'une fonction en escalier sur $[a\,;b]$ ne dépend donc pas de la subdivision adaptée à f choisie. Cette valeur commune à toutes les subdivisions sera appelée intégrale de f sur $[a\,;b]$.

Preuve : Le principe est le même que pour le **lemme 1.4** : on montre d'abord que l'intégrale de f par rapport à une subdivision ne change pas si on ajoute un point à celle-ci.

Soit A une subdivision adaptée à f, qu'on énumère

$$\mathrm{A} = \{a_0 = a < a_1 < \cdots < a_{n-1} < a_n = b\}$$

On note y_i la valeur prise par f sur l'intervalle $]a_i\,;a_{i+1}[$, pour tout $i \in [\![0\,;n-1]\!]$. Soit $c \in [a\,;b]$. Comme tout à l'heure, il y a deux possibilités :

- Soit $c \in \mathrm{A}$, auquel cas $\mathrm{A}\cup\{c\} = \mathrm{A}$ et on a immédiatement
$$\int_{[a\,;b]}^{\mathrm{A}} f = \int_{[a\,;b]}^{\mathrm{A}\cup\{c\}} f$$
- Soit $c \notin \mathrm{A}$, auquel cas il existe un unique $i_0 \in [\![0\,;n-1]\!]$ tel que $c \in]a_{i_0}\,;a_{i_0+1}[$. Et f prend la valeur y_{i_0} sur $]a_{i_0}\,;c[$ et $]c\,;a_{i_0+1}[$. Donc
$$\begin{aligned}\int_{[a\,;b]}^{\mathrm{A}\cup\{c\}} f &= \sum_{i=0}^{i_0-1} y_i(a_{i+1}-a_i) + \underbrace{y_{i_0}(c-a_{i_0}) + y_{i_0}(a_{i_0+1}-c)}_{=y_{i_0}(a_{i_0+1}-a_{i_0})} + \sum_{i=i_0+1}^{n-1} y_i(a_{i+1}-a_i)\\ &= \sum_{i=0}^{n-1} y_i(a_{i+1}-a_i) = \int_{[a\,;b]}^{\mathrm{A}} f\end{aligned}$$

Ainsi, quel que soit le cas de figure,

$$\int_{[a\,;b]}^{\mathrm{A}} f = \int_{[a\,;b]}^{\mathrm{A}\cup\{c\}} f$$

Nous pouvons achever de démontrer le lemme. Une récurrence immédiate montre que

$$\int_{[a\,;b]}^{\mathrm{A}} f = \int_{[a\,;b]}^{\mathrm{B}} f$$

si B est une subdivision plus fine que A (on rappelle que B est automatiquement adaptée à f d'après le **lemme 1.4**), puisque B est obtenue en ajoutant à A un nombre fini de points.

Enfin, si B est n'importe quelle subdivision adaptée à f (pas forcément plus fine que A), alors $\mathrm{A}\cup\mathrm{B}$ est une subdivision de $[a\,;b]$, plus fine que A ou B, donc adaptée à f. Et d'après ce qu'on vient de voir :

$$\int_{[a\,;b]}^{\mathrm{A}} f = \int_{[a\,;b]}^{\mathrm{A}\cup\mathrm{B}} f \qquad \text{et} \qquad \int_{[a\,;b]}^{\mathrm{B}} f = \int_{[a\,;b]}^{\mathrm{A}\cup\mathrm{B}} f$$

Par suite,
$$\int_{[a\,;b]}^{\mathrm{A}} f = \int_{[a\,;b]}^{\mathrm{B}} f$$
□

13.1.3 Propriétés

Théorème 13.1.8 (Propriétés de l'intégrale des fonctions en escalier)

- ***Relation de Chasles :*** *Soit f une fonction en escalier sur $[a\,;b]$. Pour tout c dans $]a\,;b[$, f est en escalier sur $[a\,;c]$ et $[c\,;b]$ et*
$$\int_{[a\,;b]} f = \int_{[a\,;c]} f + \int_{[c\,;b]} f$$
- ***Linéarité :*** *l'application* $\mathscr{E}([a\,;b]) \longrightarrow \mathbb{R}$, $f \longmapsto \int_{[a\,;b]} f$ *est linéaire.*
- ***Positivité :*** *si $f \in \mathscr{E}([a\,;b])$ est positive, sauf en un nombre fini de points, alors $\int_{[a\,;b]} f \geqslant 0$.*

Preuve : Commençons par la relation de Chasles. Soient f en escalier sur $[a\,;b]$ et $c \in]a\,;b[$.

Soit A une subdvision de $[a\,;b]$ adaptée à f. Alors $\mathrm{A}\cup\{c\}$ est une subdivision de $[a\,;b]$, plus fine que A, donc adaptée à f. Du coup, $(\mathrm{A}\cup\{c\})\cap[a\,;c]$ est une subdivision de $[a\,;c]$, adaptée à f ce qui montre que f est en escalier sur $[a\,;c]$. De même, f est en escalier sur $[c\,;b]$.

Posons $\mathrm{A}_- = (\mathrm{A}\cup\{c\})\cap[a\,;c] = \{a_0 = a < \cdots < a_n = c\}$

et $\mathrm{A}_+ = (\mathrm{A}\cup\{c\})\cup[c\,;b] = \{a_n = c < \cdots < a_m = b\}$

Remarquons que $\mathrm{A}_-\cup\mathrm{A}_+ = \mathrm{A}\cup\{c\}$

Pour $i \in [\![0\,;m-1]\!]$, notons y_i la valeur prise par f sur $]a_i\,;a_{i+1}[$. D'après le **lemme 1.7**

$$\int_{[a\,;c]} f = \int_{[a\,;c]}^{\mathrm{A}_-} f = \sum_{i=0}^{n-1} y_i(a_{i+1}-a_i)$$

et
$$\int_{[c\,;b]} f = \int_{[c\,;b]}^{\mathrm{A}_+} f = \sum_{i=n}^{m-1} y_i(a_{i+1}-a_i)$$

Par suite,
$$\int_{[a\,;c]} f + \int_{[c\,;b]} f = \sum_{i=0}^{m-1} y_i(a_{i+1}-a_i) = \int_{[a\,;b]}^{\mathrm{A}\cup\{c\}} f = \int_{[a\,;b]} f$$

Passons à la linéarité. Soient f et g en escalier sur $[a\,;b]$, soient λ et μ des nombres réels. On se donner A et B des subdivisions de $[a\,;b]$ adaptées respectivement à f et g. De sorte que $\mathrm{A}\cup\mathrm{B}$ est une subdivision adaptée à la fois à f, g et $\lambda f+\mu g$. On énumère cette subdivision

$$\mathrm{A}\cup\mathrm{B} = \{a_0 = a < \cdots < a_n = b\}$$

et on note y_i (resp. z_i) la valeur prise par f sur l'intervalle $]a_i\,;a_{i+1}[$ pour chaque $i \in [\![0\,;n-1]\!]$. D'après le **lemme 1.7**,

$$\begin{aligned}\int_{[a\,;b]}(\lambda f+\mu g) &= \int_{[a\,;b]}^{\mathrm{A}\cup\mathrm{B}} f = \sum_{i=0}^{n-1}(\lambda y_i+\mu z_i)(a_{i+1}-a_i)\\ &= \lambda\sum_{i=0}^{n-1} y_i(a_{i+1}-a_i) + \mu\sum_{i=0}^{n-1} z_i(a_{i+1}-a_i) = \lambda\int_{[a\,;b]}^{\mathrm{A}\cup\mathrm{B}} f + \mu\int_{[a\,;b]}^{\mathrm{A}\cup\mathrm{B}} g\end{aligned}$$

$$\int_{[a\,;b]}(\lambda f+\mu g) = \lambda\int_{[a\,;b]} f + \mu\int_{[a\,;b]} g$$

Enfin, la positivité est vraiment triviale. □

13.2 Fonctions continues par morceaux

13.2.1 Définition

Définition 13.2.1 (Fonctions continues par morceaux)
Soit f une fonction définie sur $[a;b]$. On dit qu'elle est *continue par morceaux sur* $[a;b]$ si, et seulement si, il existe une subdivision $\mathrm{A} = \{a_0 = a < \cdots < a_n = b\}$ de $[a;b]$ telle que, pour tout $i \in [\![0; n-1]\!]$,

- f est continue sur $]a_i ; a_{i+1}[$;
- f est prolongeable par continuité à $[a_i ; a_{i+1}]$.

Une subdivision pour laquelle f vérifie ces propriétés est dite *adaptée à* f.

L'ensemble des fonctions continues par morceaux sur $[a;b]$ est noté $\mathscr{C}_{\mathsf{pm}}([a;b])$.

Autrement, une fonction continue par morceaux sur $[a;b]$ est une fonction telle qu'on puisse partitionner $[a;b]$ en sous-intervalles, à l'intérieur desquels f est continue et aux bornes desquels f admet une limite à gauche et à droite. Bref, elle peut être découpée en morceaux continus. D'où le nom.

Lemme 13.2.2
Soit f continue par morceaux sur $[a;b]$. Soit A *une subdivision adaptée à f. Toute subdivision plus fine que* A *est adaptée à f.*

Preuve : Adapter la preuve pour les fonctions en escalier. □

Théorème 13.2.3
L'ensemble $\mathscr{C}_{pm}([a;b])$ est un $\mathbb{R}$-espace vectoriel qui contient $\mathscr{E}([a;b])$.

Preuve : Adapter la preuve pour les fonctions en escalier. □

13.2.2 Approximation par des fonctions en escalier

Nous allons montrer un résultat d'approximation fondamental : toute fonction f, continue par morceaux sur $[a;b]$, peut être approchée *uniformément*, à la précision souhaitée, par des fonctions en escalier. Le mot important ici est *uniformément* : cela signifie qu'étant donnée une précision $\varepsilon > 0$ donnée, il existe une fonction en escalier φ telle que l'erreur $|f(x) - \varphi(x)|$ n'est nulle part supérieure à ε.

Nous aurons d'abord besoin d'un lemme technique :

Lemme 13.2.4 (Lemme de Heine)
Soit f une fonction continue sur $[a;b]$. Pour tout $\varepsilon > 0$, il existe $\eta > 0$ tel que

$$\forall (x,y) \in [a;b]^2 \qquad (|x-y| \leqslant \eta \implies |f(x) - f(y)| \leqslant \varepsilon)$$

Preuve : Supposons la conclusion fausse : il existe $\varepsilon > 0$ tel que,

$$\forall \eta > 0 \quad \exists (x,y) \in [a;b]^2 \qquad |x-y| \leqslant \eta \qquad \text{et} \qquad |f(x) - f(y)| \geqslant \varepsilon$$

Prenons pour η des valeurs particulières : pour tout entier n, il existe x_n et y_n dans $[a;b]$, tels que

$$|x_n - y_n| \leqslant \frac{1}{n} \qquad \text{et} \qquad |f(x_n) - f(y_n)| \geqslant \varepsilon$$

D'après le théorème de Bolzano-Weierstrass, $(x_n)_{n\in\mathbb{N}}$ admet une sous-suite convergente qu'on note $(x_{\varphi(n)})_{n\in\mathbb{N}}$ de limite x. Et la suite $(y_{\varphi(n)})_{n\in\mathbb{N}}$ admet à son tour une sous-suite convergente $(y_{\varphi(\psi(n))})_{n\in\mathbb{N}}$, de limite y.

Or, $(x_{\varphi(\psi(n))})_{n\in\mathbb{N}}$ est une suite extraite de $(x_{\varphi(n)})_{n\in\mathbb{N}}$, donc converge également vers x. De plus,

$$\forall n\in\mathbb{N} \qquad |x_{\varphi(\psi(n))}-y_{\varphi(\psi(n))}|\leqslant\frac{1}{\varphi(\psi(n))} \qquad \text{et} \qquad |f(x_{\varphi(\psi(n))})-f(y_{\varphi(\psi(n))})|\geqslant\varepsilon$$

En passant à la limite, il vient

$$|x-y|\leqslant 0 \qquad \text{et} \qquad |f(x)-f(y)|\geqslant\varepsilon$$

Ces deux résultat se contredisent puisqu'ils impliquent respectivement que $x=y$ et $f(x)\neq f(y)$.□

Théorème 13.2.5 (Approximation des fonctions continues)
Soit f une fonction continue sur $[a;b]$. Soit $\varepsilon>0$ fixé. Il existe des fonctions en escalier φ_1 et φ_2 telles que

$$\forall x\in[a;b] \qquad \varphi_1(x)\leqslant f(x)\leqslant\varphi_2(x) \qquad et \qquad \varphi_2(x)-\varphi_1(x)\leqslant\varepsilon$$

Preuve : On se donne $\varepsilon>0$. D'après le lemme de Heine, il existe $\eta>0$ tel que

$$\forall x,y\in[a;b] \qquad |x-y|\leqslant\eta \implies |f(x)-f(y)|\leqslant\varepsilon$$

On se donne alors une subdivision A de $[a;b]$, de pas η. Par exemple, en posant $n=\left[\frac{b-a}{\eta}\right]$, on prend

$$\forall k\in[\![0;n-1]\!] \qquad a_k=a+k\eta \qquad \text{et} \qquad a_n=b$$

La fonction f est continue sur chacun des intervalles $[a_k;a_{k+1}]$ et atteint donc sur celui-ci son minimum et son maximum : il existe $c_k,d_k\in[a_k;a_{k+1}]$, tels que

$$\forall x\in[a_k;a_{k+1}] \qquad f(c_k)\leqslant f(x)\leqslant f(d_k)$$

De plus, dans la mesure où deux éléments de cet intervalle sont distants de moins de η, on a

$$forall x\in[a_k;a_{k+1}] \qquad 0\leqslant f(x)-f(c_k)\leqslant\varepsilon \qquad \text{et} \qquad 0\leqslant f(d_k)-f(x)$$

On définit alors deux fonctions en escalier φ_1 et φ_2 de la manière suivante : sur chaque intervalle $[a_k;a_{k+1}[$, φ_1 est constante égale à $f(c_k)$ et φ_2 est constante égale à $f(d_k)$. En b, elles valent toutes deux $f(b)$. On a alors

$$\forall x\in[a;b] \qquad \varphi_1(x)\leqslant f(x)\leqslant\varphi_2(x)$$

et $$\forall x\in[a;b] \qquad 0\leqslant f(x)-\varphi_1(x)\leqslant\varepsilon \qquad \text{et} \qquad 0\leqslant\varphi_2(x)-f(x)\leqslant\varepsilon$$

d'où $$\forall x\in[a;b] \qquad \varphi_2(x)-\varphi_1(x)\leqslant 2\varepsilon$$

Ce qui achève la démonstration. □

Corollaire 13.2.6 (Approximation des fonctions continues par morceaux)
Soit f une fonction continue par morceaux sur $[a;b]$. Soit $\varepsilon>0$ fixé. Il existe des fonctions en escalier φ_1 et φ_2 telles que

$$\forall x\in[a;b] \quad \varphi_1(x)\leqslant f(x)\leqslant\varphi_2(x) \qquad et \qquad \varphi_2(x)-\varphi_1(x)\leqslant\varepsilon$$

Preuve : Immédiat, il suffit d'utiliser le théorème sur chacun des intervalles déterminés par une subdivision adaptée à f. □

13.3 Fonction intégrables

13.3.1 Définition

Définition 13.3.1
Soit f une fonction définie sur $[a;b]$. On appelle intégrale supérieure de f le nombre

$$\int_{[a;b]}^{\star} f = \mathrm{Inf}\left\{\int_{[a;b]} \varphi \mid \varphi \in \mathscr{E}([a;b]) \quad \varphi \geqslant f\right\}$$

On appelle intégrale inférieure de f sur $[a;b]$ le nombre

$$\int_{\star}^{[a;b]} f = \mathrm{Sup}\left\{\int_{[a;b]} \varphi \mid \varphi \in \mathscr{E}([a;b]) \quad \varphi \leqslant f\right\}$$

Intuitivement, l'intégrale supérieure de f est la meilleure approximation de l'aire algébrique se trouvant entre la courbe représentative de f et l'axe des abscisses, à l'aide de fonctions en escalier qui majorent f.

Tandis que l'intégrale inférieure de f est la meilleure approximation de l'aire algébrique se trouvant entre la courbe représentative de f et l'axe des abscisses, à l'aide de fonctions en escalier qui minorent f.

Naturellement, on dira que cette aire existe si l'intégrale supérieure et l'intégrale inférieure coïncident.

Définition 13.3.2 (Fonctions intégrables)
Soit f une fonction définie sur $[a;b]$. Elle sera dite intégrable sur $[a;b]$ si, et seulement si,

$$\int_{[a;b]}^{\star} f = \int_{\star}^{[a;b]} f$$

Cette valeur commune sera alors appelée *intégrale de f sur $[a;b]$* et notée $\displaystyle\int_{[a;b]} f$ ou $\displaystyle\int_a^b f(t)\,\mathrm{d}t$.

Évidemment, une première chose à vérifier est la cohérence de nos définitions : une fonction en escalier est-elle intégrable ? Et si oui, son intégrale au sens de la **définition 3.2** correspond-elle bien à celle au sens du **lemme 1.7** ?

Proposition 13.3.3
Toute fonction f en escalier sur $[a;b]$ est intégrable et les deux définitions de $\displaystyle\int_{[a;b]} f$ coïncident.

Preuve : Si φ est une fonction en escalier qui majore f, on a, d'après le **théorème 1.8**,

$$\int_{[a;b]} f \leqslant \int_{[a;b]} \varphi$$

donc

$$\int_{[a;b]} f \leqslant \int_{[a;b]}^{\star} f$$

De plus, f est une fonction en escalier qui majore f donc on a en fait

$$\int_{[a;b]} f \geqslant \int_{[a;b]}^{\star} f$$

De la même manière, on montre que

$$\int_{[a;b]} f = \int_{\star}^{[a;b]} f$$

f est bien intégrable ; ses intégrales supérieure et inférieure coïncident en outre avec son intégrale au sens de la définition **1.8**, ce qui achève la démonstration. □

13.3.2 Propriétés élémentaires

On commence par établir les propriétés usuelles de linéarité de l'intégrale. Mais il faut faire les choses petit à petit pour rendre la démonstration plus digeste.

Lemme 13.3.4
Soient f et g deux fonctions intégrables sur $[a;b]$. Soient λ et μ deux nombres réels positifs. Alors $\lambda f + \mu g$ est intégrable sur $[a;b]$ et

$$\int_{[a;b]} (\lambda f + \mu g) = \lambda \int_{[a;b]} f + \mu \int_{[a;b]} g$$

Preuve : Soient φ et ψ des fonctions en escalier, majorant respectivement f et g :

$$\forall x \in [a;b] \qquad f(x) \leqslant \varphi(x) \qquad \text{et} \qquad g(x) \leqslant \psi(x)$$

Puisque λ et μ sont positifs, on a

$$\forall x \in [a;b] \qquad \lambda f(x) + \mu g(x) \leqslant \lambda\varphi(x) + \mu\psi(x)$$

donc
$$\int_{[a;b]}^{\star} (\lambda f + \mu g) \leqslant \int_{[a;b]} (\lambda\varphi + \mu\psi) = \lambda \int_{[a;b]} \varphi + \mu \int_{[a;b]} \psi$$

La dernière égalité provient du fait que φ et ψ sont en escalier, et on sait que la linéarité de l'intégrale est valable pour ces fonctions d'après le **théorème 1.8**.

Cette inégalité est valable pour toutes fonctions φ et ψ majorant f et g respectivement. Par définition de l'infimum, on en déduit que

$$\int_{[a;b]}^{\star} (\lambda f + \mu g) \leqslant \lambda \int_{[a;b]}^{\star} f + \mu \int_{[a;b]}^{\star} g = \lambda \int_{[a;b]} f + \mu \int_{[a;b]} f$$

La dernière égalité provient du fait que f et g sont intégrables.

De la même manière, on établit que

$$\lambda \int_{[a;b]} f + \mu \int_{[a;b]} g \leqslant \int_{\star}^{[a;b]} (\lambda f + \mu g)$$

De sorte que
$$\int_{\star}^{[a;b]} (\lambda f + \mu g) = \int_{[a;b]}^{\star} (\lambda f + \mu g) = \lambda \int_{[a;b]} f + \mu \int_{[a;b]} g$$

Ainsi, $\lambda f + \mu g$ est intégrable et son intégrale vaut $\lambda \int_{[a;b]} f + \mu \int_{[a;b]} g$. □

Lemme 13.3.5
Soit f une fonction intégrable sur $[a;b]$. Alors $-f$ est intégrable sur $[a;b]$ et

$$\int_{[a;b]} (-f) = -\int_{[a;b]} f$$

Preuve : On se rappelle des relations

$$\mathrm{Sup}\,(-\mathrm{A}) = -\mathrm{Inf}\,\mathrm{A} \qquad \text{et} \qquad \mathrm{Inf}\,(-\mathrm{A}) = -\mathrm{Sup}\,\mathrm{A}$$

si A est un ensemble borné, non vide. On constate que

$$\begin{aligned}
\int_{[a;b]}^{\star}(-f) &= \mathrm{Inf}\Big\{\int_{[a;b]}\varphi \mid \varphi\in\mathscr{E}([a;b]) \quad -f\leqslant\varphi\Big\}\\
&= \mathrm{Inf}\Big\{-\int_{[a;b]}(-\varphi) \mid \varphi\in\mathscr{E}([a;b]) \quad f\geqslant-\varphi\Big\}\\
&= \mathrm{Inf}\Big\{-\int_{[a;b]}\varphi \mid \varphi\in\mathscr{E}([a;b]) \quad f\geqslant\varphi\Big\}\\
&= -\mathrm{Sup}\Big\{\int_{[a;b]}\varphi \mid \varphi\in\mathscr{E}([a;b]) \quad f\geqslant\varphi\Big\}
\end{aligned}$$

$$\int_{[a;b]}^{\star}(-f) = -\int_{\star}^{[a;b]} f = -\int_{[a;b]} f$$

De même, $$\int_{\star}^{[a;b]}(-f) = -\int_{[a;b]} f$$

Les intégrales inférieure et supérieure de $-f$ sont bien égales : $-f$ est intégrable. Et son intégrale n'est autre que $-\int_{[a;b]} f$. □

Théorème 13.3.6 (Linéarité de l'intégrale)
L'ensemble $\mathscr{I}([a;b])$ est un $\mathbb{R}$-espace vectoriel et l'intégrale en est une forme linéaire.

Preuve : Soient f et g intégrables, soient λ et μ des réels.

- S'ils sont tous deux positifs, le **lemme 3.4** montre que $\lambda f+\mu g$ est intégrable et que
$$\int_{[a;b]}(\lambda f+\mu g) = \lambda\int_{[a;b]} f+\mu\int_{[a;b]} g$$
- S'ils sont tous deux négatifs, alors $-\lambda$ et $-\mu$ sont positifs donc (**lemme 3.4**) $-\lambda f-\mu g$ est intégrable et
$$\int_{[a;b]}(-\lambda f-\mu g) = -\lambda\int_{[a;b]} f-\mu\int_{[a;b]} g$$
Le **lemme 3.5** établit alors que $\lambda f+\mu g$ est intégrable et que
$$\int_{[a;b]}(\lambda f+\mu f) = -\int_{[a;b]}(-\lambda f-\mu g) = \lambda\int_{[a;b]} f+\mu\int_{[a;b]} g$$
- Si $\lambda\geqslant 0$ et $\mu\leqslant 0$: le **lemme 3.5** montre que $-g$ est intégrable et que
$$\int_{[a;b]}(-g) = -\int_{[a;b]} g$$
Le lemme **3.4** montre, quant à lui, que $\lambda f+\mu g = \lambda f-\mu(-g)$ est intégrable et que
$$\int_{[a;b]}\lambda f+\mu g = \lambda\int_{[a;b]} f-\mu\int_{[a;b]}(-g) = \lambda\int_{[a;b]} f+\mu\int_{[a;b]} g$$
- Si $\lambda\leqslant 0$ et $\mu\geqslant 0$, on échange les rôles de f et g et on utilise le resultat précédent. □

Théorème 13.3.7 (Relation de Chasles)
Soit f une fonction définie sur $[a;b]$, bornée. Soit $c \in]a;b[$. Alors f est intégrable sur $[a;b]$ si, et seulement si, elle est intégrable sur $[a;c]$ et $[c;b]$, auquel cas

$$\int_{[a;b]} f = \int_{[a;c]} f + \int_{[c;b]} f$$

Preuve : On suppose simplement f bornée pour l'instant. On se donne $\varphi \in \mathscr{E}([a;b])$ qui majore f et on note φ_1 et φ_2 les restrictions de φ à $[a;c]$ et $[c;b]$ respectivement. Alors

$$\forall x \in [a;c] \qquad f(x) \leqslant \varphi_1(x) \qquad \text{et} \qquad \forall x \in [c;b] \qquad f(x) \leqslant \varphi_2(x)$$

Du coup
$$\int_{[a;c]}^{\star} f \leqslant \int_{[a;c]} \varphi_1 \qquad \text{et} \qquad \int_{[c;b]}^{\star} f \leqslant \int_{[c;b]} \varphi_2$$

Par suite,
$$\begin{aligned}\int_{[a;c]}^{\star} f + \int_{[c;b]}^{\star} f &\leqslant \int_{[a;c]} \varphi_1 + \int_{[c;b]} \varphi_2 \\ &\leqslant \int_{[a;c]} \varphi + \int_{[c;b]} \varphi = \int_{[a;b]} \varphi\end{aligned}$$

On a utilisé à la fin la relation de Chasles dont on sait qu'elle est valable pour les fonctions en escalier. Ce qui précède est valable, rappelons-le, pour toute fonction en escalier φ majorant f. Donc

$$\int_{[a;c]}^{\star} f + \int_{[c;b]}^{\star} f \leqslant \int_{[a;b]}^{\star} f$$

Montrons qu'il y a en fait égalité. Pour ce faire, on se donne deux fonctions en escalier φ_1 et φ_2, majorant f respectivement sur $[a;c]$ et sur $[c;b]$. On définit alors

$$\forall x \in [a;b] \qquad \varphi(x) = \begin{cases} \varphi_1(x) & \text{si } x \in [a;c] \\ \varphi_2(x) & \text{si } x \in]c;b] \end{cases}$$

De sorte que φ majore f sur $[a;b]$. On a

$$\int_{[a;b]}^{\star} f \leqslant \int_{[a;b]} \varphi = \int_{[a;c]} \varphi_1 + \int_{[a;b]} \varphi_2$$

Et, ceci étant valable pour tout choix de φ_1 et φ_2, on en déduit que

$$\int_{[a;b]}^{\star} f \leqslant \int_{[a;c]}^{\star} f + \int_{[c;b]}^{\star} f$$

Comme annoncé,
$$\int_{[a;b]}^{\star} f = \int_{[a;c]}^{\star} f + \int_{[c;b]}^{\star} f$$

De la même manière,
$$\int_{\star}^{[a;b]} f = \int_{\star}^{[a;c]} f + \int_{\star}^{[c;b]} f$$

Maintenant, supposons f intégrable à la fois sur $[a;c]$ et $[c;b]$. Par définition, cela signifie que

$$\int_{[a;c]}^{\star} f = \int_{\star}^{[c;b]} f \qquad \text{et} \qquad \int_{[c;b]}^{\star} f = \int_{\star}^{[c;b]} f$$

Du coup,
$$\int_{[a;b]}^{\star} f = \int_{\star}^{[a;b]} f$$

et f est bien intégrable. En outre, on voit que la relation de Chasles est bien satisfaite.

Réciproquement, supposons f intégrable sur $[a;b]$. Ses intégrales supérieure et inférieure sur cet intervalle coïncident donc

$$\int_{[a;c]}^{\star} f + \int_{[c;b]}^{\star} f = \int_{\star}^{[a;c]} f + \int_{\star}^{[c;b]} f \tag{1}$$

Mais $$\int_{\star}^{[a;c]} f \leqslant \int_{[a;c]}^{\star} f \qquad \text{et} \qquad \int_{\star}^{[c;b]} f \leqslant \int_{\star}^{[c;b]}$$

Si l'une de ces inégalités est stricte, la relation (**1**) ne peut se produire. Donc ces deux inégalités sont, en fait, des égalités. f est bien intégrable à la fois sur $[a;c]$ et $[c;b]$. □

Théorème 13.3.8 (Positivité de l'intégrale)
Soit f une fonction intégrable sur $[a;b]$, positive sauf peut-être en un nombre fini de points. Alors $\int_{[a;b]} f \geqslant 0$.

Preuve : L'intégrale de f est égale à son intégrale supérieure, qui est clairement positive par définition et d'après la positivité de l'intégrale des fonctions en escalier (**Théorème 1.8**). □

Corollaire 13.3.9 (Croissance de l'intégrale)
Soient f et g deux fonctions intégrables sur $[a;b]$ telles que $f \leqslant g$. Alors $\int_{[a;b]} f \leqslant \int_{[a;b]} g$.

Preuve : Trivial : on utilise le théorème précédent avec $g - f$. □

Définition 13.3.10 (Parties positive et négative d'une fonction)
Soit f une fonction définie sur un ensemble A. On pose

$$\forall x \in \mathrm{A} \qquad f_+(x) = \mathrm{Max}(f(x),0) = \begin{cases} f(x) & \text{si } f(x) \geqslant 0 \\ 0 & \text{si } f(x) < 0 \end{cases}$$

et $$f_-(x) = -\mathrm{Min}(f(x),0) = \begin{cases} -f(x) & \text{si } f(x) \leqslant 0 \\ 0 & \text{si } f(x) > 0 \end{cases}$$

Ces fonctions sont appelées respectivement *partie positive* et *partie négative* de f.

Proposition 13.3.11
Soit f une fonction. On a $f = f_+ - f_-$ et $|f| = f_+ + f_-$.

Preuve : C'est une simple vérification. □

Proposition 13.3.12
Si f est en escalier, f_+, f_- et $|f|$ sont en escalier.

Preuve : Simple vérification également. □

Théorème 13.3.13 (Inégalité triangulaire généralisée)
Soit f intégrable sur $[a;b]$. Les fonctions f_+, f_- et $|f|$ sont aussi intégrables sur $[a;b]$. De plus,

$$\left|\int_{[a;b]} f\right| \leqslant \int_{[a;b]} |f|$$

Preuve : Soit $\varepsilon > 0$. Il existe des fonctions en escalier φ et ψ telles que

$$\varphi \leqslant f \leqslant \psi \qquad \text{et} \qquad \begin{cases} \varepsilon + \displaystyle\int_{[a;b]} f \leqslant \int_{[a;b]} \varphi \leqslant \int_{[a;b]} f \\ \displaystyle\int_{[a;b]} f \leqslant \int_{[a;b]} \psi \leqslant \varepsilon + \int_{[a;b]} f \end{cases}$$

En particulier, $$0 \leqslant \int_{[a;b]} (\psi - \varphi) \leqslant 2\varepsilon$$

Les fonctions φ_+ et ψ_+ sont en escalier d'après la **proposition 3.11**. On commence par les comparer à f_+. Soit $x \in [a;b]$.

– Si $f(x) \leqslant 0$: par définition, $f_+(x) = 0$. En outre, puisque $\varphi \leqslant f$, on a aussi $\varphi(x) \leqslant 0$ donc $\varphi_+(x) = 0$. D'où

$$\varphi_+(x) \leqslant f(x) \leqslant \psi_+(x)$$

– Si $f(x) \geqslant 0$: par définition, $f_+(x) = f(x)$. En outre, puisque $f \leqslant \psi$, on a aussi $\psi(x) \geqslant 0$. Donc

$$\varphi_+(x) \leqslant \varphi(x) \leqslant f(x) = f_+(x) \leqslant \psi(x) = \psi_+(x)$$

En résumé, $$\varphi_+ \leqslant f_+ \leqslant \psi_+$$

Par suite, $$\int_{[a;b]} \varphi_+ \leqslant \int_{\star}^{[a;b]} f_+ \leqslant \int_{[a;b]}^{\star} f_+ \leqslant \int_{[a;b]} \psi_+$$

D'où $$0 \leqslant \int_{[a;b]}^{\star} f_+ - \int_{\star}^{[a;b]} f_+ \leqslant \int_{[a;b]} (\psi_+ - \varphi_+)$$

Mais $\psi_+ - \varphi_+ \leqslant \psi - \varphi$ donc $\displaystyle\int_{[a;b]} (\psi_+ - \varphi_+) \leqslant \int_{[a;b]} (\psi - \varphi) \leqslant 2\varepsilon$

Ainsi, $$\forall \varepsilon > 0 \qquad 0 \leqslant \int_{[a;b]}^{\star} f_+ - \int_{\star}^{[a;b]} f_+ \leqslant 2\varepsilon$$

Ce qui établit que $$\int_{[a;b]}^{\star} f_+ = \int_{\star}^{[a;b]} f_+$$

et f_+ est intégrable. Dans la mesure où $f_- = f_+ - f$, il s'ensuit que f_- est également intégrable. Enfin, $|f| = f_+ + f_-$ l'est aussi. On termine par l'inégalité proposée :

$$\left|\int_{[a;b]} f\right| = \left|\int_{[a;b]} (f_+ - f_-)\right| \leqslant \underbrace{\left|\int_{[a;b]} f_+\right|}_{\geqslant 0} + \underbrace{\left|\int_{[a;b]} f_-\right|}_{\geqslant 0} = \int_{[a;b]} \underbrace{(f_+ + f_-)}_{=|f|} \qquad \square$$

13.4 Intégrale des fonctions continues par morceaux

On démontre dans ce paragraphe que les fonctions continues par morceaux sont intégrables. Cela permettra de leur appliquer tout ce qui a été fait dans la partie précédente. Ensuite, on démontre le théorème fondamental du chapitre, qui relie intégration et dérivation. Finalement, on présente les deux principales techniques de calcul intégral : l'intégration par parties et le changement de variable.

13.4.1 Intégrabilité des fonctions continues par morceaux

Théorème 13.4.1
Toute fonction continue par morceaux sur $[a\,;b]$ *est intégrable.*

Preuve : On sort le **théorème 2.5** de derrière les fagots. Soit f continue par morceaux sur $[a\,;b]$. On sait, évidemment, que

$$\int_{\star}^{[a;b]} f \leqslant \int_{[a;b]}^{\star} f$$

C'est l'inégalité reciproque qu'il nous reste à établir. Si $\varepsilon > 0$ est donné, on sait qu'il existe deux fonctions en escalier φ_1 et φ_2 telles que

$$\varphi_1 \leqslant f \leqslant \varphi_2 \qquad \text{et} \qquad \varphi_2 - \varphi_1 \leqslant \varepsilon$$

Puisque $\varphi_1 \leqslant f$, on sait que

$$\int_{[a;b]} \varphi_1 \leqslant \int_{[a;b]}^{\star} f$$

De même,
$$\int_{[a;b]}^{\star} f \leqslant \int_{[a;b]} \varphi_2$$

Par suite,
$$0 \leqslant \int_{[a;b]}^{\star} f - \int_{\star}^{[a;b]} f \leqslant \int_{[a;b]} (\varphi_2 - \varphi_1) \leqslant \varepsilon(b-a)$$

Ceci étant vrai pour tout $\varepsilon > 0$, il s'ensuit que

$$\int_{[a;b]}^{\star} f = \int_{\star}^{[a;b]} f$$

f est bien intégrable. □

Théorème 13.4.2 (Inégalité de la moyenne généralisée)
Soient f et g deux fonctions continues par morceaux sur $[a\,;b]$. *Alors*

$$\left|\int_{[a;b]} fg\right| \leqslant \operatorname*{Sup}_{x\in[a;b]} |f(x)| \int_{[a;b]} |g|$$

En particulier,
$$\left|\int_{[a;b]} f\right| \leqslant (b-a) \operatorname*{Sup}_{x\in[a;b]} |f(x)|$$

Preuve : Les fonctions f et g étant continues par morceaux, il en est de même de fg. Celle-ci est donc intégrable et le **Théorème 3.13** assure que

$$\left|\int_{[a;b]} fg\right| \leqslant \int_{[a;b]} |fg|$$

Or, $$\forall y \in [a;b] \qquad |f(y)| \leqslant \sup_{x\in[a;b]} |f(x)|$$

donc $$\left|\int_{[a;b]} fg\right| \leqslant \sup_{x\in[a;b]} |f(x)| \int_{[a;b]} |g|$$

Pour obtenir la deuxième inégalité, il suffit de prendre $g = 1$. □

13.4.2 Sommes de Riemann

Définition 13.4.3

Soient f une fonction définie sur $[a;b]$ et $\mathrm{A} = \{a_0 = a < a_1 < \cdots < a_n = b\}$ une subdivision de $[a;b]$. On appelle *somme de Riemann de f associée à* A le réel

$$\mathrm{S_A}(f) = \sum_{k=0}^{n-1} f(a_k)(a_{k+1} - a_k)$$

Théorème 13.4.4

Soient f une fonction continue sur $[a;b]$ et $(\mathrm{A}_n)_{n\in\mathbb{N}}$ une suite de subdivisions, telle que

$$\lim_{n\to\infty} p(\mathrm{A}_n) = 0$$

Alors la suite des sommes de Riemann $(\mathrm{S}_{\mathrm{A}_n}(f))_{n\in\mathbb{N}}$ est convergente et sa limite est $\displaystyle\int_{[a;b]} f$.

Preuve : C'est à nouveau une conséquence presqu'immédiate du **lemme de Heine**. On fixe $\varepsilon > 0$ et on utilise ce lemme pour obtenir un $\eta > 0$ tel que

$$\forall x, y \in [a;b] \qquad |x-y| \leqslant \eta \implies |f(x) - f(y)| \leqslant \varepsilon$$

Comme le pas des subdivisions $(\mathrm{A}_n)_{n\in\mathbb{N}}$ tend vers 0, il existe un entier N tel que

$$\forall n \geqslant \mathrm{N} \qquad p(\mathrm{A}_n) \leqslant \eta$$

On fixe $n \geqslant \mathrm{N}$ et on considère la partition A_n, qu'on note

$$\mathrm{A}_n = \{a_0 = a < a_1 < \cdots < a_p = b\}$$

On définit alors une fonction en escalier φ de la manière suivante : si $x \in [a;b[$, il existe un unique $k \in [\![0; p-1]\!]$ tel que $x \in [a_k; a_{k+1}[$; on pose alors $\varphi(x) = f(a_k)$. Et si $x = b$, on pose $\varphi(x) = f(x)$. De cette manière, A_n est une subdivision adaptée à φ et l'on a

$$\int_{[a;b]} \varphi = \sum_{k=0}^{p-1} f(a_k)(a_{k+1} - a_k) = \mathrm{S}_{\mathrm{A}_n}(f)$$

De plus, si $k \in [\![0; p-1]\!]$ et si $x \in [a_k; a_{k+1}[$, on a $|x - a_k| \leqslant p(\mathrm{A}_n) \leqslant \eta$ donc

$$|f(x) - \varphi(x)| = |f(x) - f(a_k)| \leqslant \varepsilon$$

Autrement dit, $$\forall x \in [a;b] \qquad |f(x) - \varphi(x)| \leqslant \varepsilon$$

D'après l'inégalité de la moyenne et parce que f et φ sont intégrables,

$$\left|\int_{[a;b]} f - \mathrm{S}_{\mathrm{A}_n}(f)\right| = \left|\int_{[a;b]} (f-\varphi)\right| \leqslant \int_{[a;b]} |f-\varphi| \leqslant \varepsilon(b-a) \qquad \square$$

Corollaire 13.4.5 (Théorème de Riemann)
Soit $f \in \mathscr{C}([a;b])$. Alors $\lim_{n\to\infty} \frac{1}{n} \sum_{k=0}^{n-1} f\left(a + k\frac{b-a}{n}\right)$ existe et vaut $\int_{[a;b]} f$.

13.5 Intégration et dérivation

C'est bien beau d'avoir défini l'intégrale... Mais encore faut-il savoir calculer l'intégrale d'une fonction.

Définition 13.5.1
Soit f une fonction intégrable sur $[a;b]$. Si $x, y \in [a;b]$, on pose

$$\int_x^y f(t)\,\mathrm{d}t = \begin{cases} \displaystyle\int_{[x;y]} f & \text{si } x \leqslant y \\ \displaystyle -\int_{[y;x]} f & \text{si } x > y \end{cases}$$

Ainsi, par définition, $\int_x^y f(t)\,\mathrm{d}t = -\int_y^x f(t)\,\mathrm{d}t$ si x et y sont quelconques. L'inégalité de la moyenne devient donc

$$\left|\int_x^y f(t)\,\mathrm{d}t\right| \leqslant |x-y| \sup_{t\in[a;b]} |f(t)|$$

On va déduire de ceci le théorème fondamental du calcul intégral :

Théorème 13.5.2 (Théorème fondamental du calcul intégral)
Soit f une fonction continue par morceaux sur $[a;b]$. On pose

$$\forall x \in [a;b] \qquad \mathrm{F}(x) = \int_a^x f(t)\,dt$$

Alors F *est dérivable à gauche et à droite en tout point de $]a;b[$. De plus,*

$$\forall x \in [a;b] \qquad \mathrm{F}'_g(x) = \lim_{y\to x^-} f(y) \qquad \text{et} \qquad \mathrm{F}'_d(x) = \lim_{y\to x^+} f(y)$$

Elle est aussi dérivable en a et b et

$$\mathrm{F}'(a) = \lim_{y\to a} f(y) \qquad \mathrm{F}'(b) = \lim_{y\to b} f(y)$$

En particulier, F *est continue.*

Preuve : Soit $x \in]a;b[$. Notons $\ell = \lim_{y\to x^+} f(y)$. On se donne $\varepsilon > 0$; il existe donc $\eta > 0$ tel que

$$\forall y \in]x;\, x+\eta[\qquad |f(x) - \ell| \leqslant \varepsilon$$

Soit $h \in]0;\eta[$. On cherche à évaluer $\frac{\mathrm{F}(x+h)-\mathrm{F}(x)-\ell h}{h}$. Pour cela, l'astuce réside dans le fait que

$$\int_x^{x+h} \ell\,\mathrm{d}t = \ell \int_x^{x+h} \mathrm{d}t = \ell h$$

et $$\mathrm{F}(x+h)=\int_a^{x+h} f(t)\,\mathrm{d}t=\int_a^x f(t)\,\mathrm{d}t+\int_x^{x+h} f(t)\,\mathrm{d}t=\mathrm{F}(x)+\int_x^{x+h} f(t)\,\mathrm{d}t$$

Du coup, $$\mathrm{F}(x+h)-\mathrm{F}(x)-\ell h=\int_x^{x+h} f(t)\,\mathrm{d}t-\int_x^{x+h}\ell\,\mathrm{d}t=\int_x^{x+h}(f(t)-\ell)\,\mathrm{d}t$$

et $$\left|\mathrm{F}(x+h)-\mathrm{F}(x)-\ell h\right|\leqslant\int_x^{x+h}|f(t)-\ell|$$

Or, la fonction $|f-\ell|$ est majorée par ε sur $[x\,;x+h]$ puisque $[x\,;x+h]\subset[x\,;x+\eta[$. D'après l'inégalité de la moyenne,

$$\left|\mathrm{F}(x+h)-\mathrm{F}(x)-\ell h\right|\leqslant\varepsilon h$$

et $$\frac{\left|\mathrm{F}(x+h)-\mathrm{F}(x)-\ell h\right|}{h}\leqslant\varepsilon$$

Ceci étant valable pour tout $h\in]0\,;\eta[$, on a bien

$$\lim_{h\to0^+}\frac{\mathrm{F}(x+h)-\mathrm{F}(x)}{h}=\ell$$

F est dérivable à droite en x et $\mathrm{F}'_d(x)=\ell$.

On procèderait de même pour la dérivabilité à gauche, ou pour la derivabilité en a et b. □

Définition 13.5.3 (Primitives d'une fonction)
Soit f une fonction définie sur $[a\,;b]$. On appelle primitive de f toute fonction F, dérivable, telle que $\mathrm{F}'=f$.

On observe que deux primitives F_1 et F_2 d'une même fonction f, si elles existent évidemment, diffèrent d'une constante : en effet,

$$\forall x\in[a\,;b]\qquad(\mathrm{F}_1-\mathrm{F}_2)'(x)=\mathrm{F}'_1(x)-\mathrm{F}'_2(x)=f(x)-f(x)=0$$

donc $\mathrm{F}_1-\mathrm{F}_2$ est constante, comme démontré dans le cours sur la dérivation.

Corollaire 13.5.4
Toute fonction continue sur un intervalle I *admet des primitives. Si* $a\in\mathrm{I}$, *la fonction* $x\longmapsto\displaystyle\int_a^x f(t)\,dt$ *est l'unique primitive de* f *sur* I *qui s'annule en* a.

Preuve : Soit f continue sur I. Soit $a\in\mathrm{I}$. La fonction $\mathrm{F}:x\longmapsto\displaystyle\int_a^x f(t)\,\mathrm{d}t$ est une primitive de f, d'après le **théorème 5.2**, puisque tout point de I est un point de continuité de f.

Évidemment, $\mathrm{F}(a)=0$. Si G est une autre primitive de f, elle diffère de F par une constante : $\mathrm{G}=\mathrm{F}+\mathrm{K}$ avec $\mathrm{K}\in\mathbb{R}$. Du coup, si $\mathrm{G}(a)=0$, c'est que $\mathrm{K}=0$. Par suite $\mathrm{G}=\mathrm{F}$: F est l'unique primitive de f qui s'annule en a. □

Corollaire 13.5.5
Soit f *une fonction continue sur un intervalle* I. *Soit* F *une primitive de* f. *Alors*

$$\forall x,y\in\mathrm{I}\qquad\int_x^y f(t)\,dt=\mathrm{F}(y)-\mathrm{F}(x)$$

On notera alors $$\int_x^y f(t)\,dt=\left[\mathrm{F}(t)\right]_x^y$$

Preuve : On fixe $x \in \mathrm{I}$ et on considère la fonction $\mathrm{G} : y \longmapsto \mathrm{F}(y) - \mathrm{F}(x)$. Alors G est une primitive de f, qui s'annule en y. Par suite,

$$\forall x \in \mathrm{I} \qquad \mathrm{F}(x) - \mathrm{F}(y) = \int_y^x f(t)\,\mathrm{d}t \qquad \square$$

13.5.1 Intégrales usuelles

Savoir exprimer une primitive d'une fonction à l'aide de fonctions usuelles n'est pas une tâche facile. Elle est même parfois impossible. Il y a néanmoins des fonctions qui sont faciles à primitiver. En voici une liste.

- $$\forall a, x > 0 \qquad \int_a^x \frac{\mathrm{d}t}{t} = \ln t - \ln a$$

  Il s'agit en fait de la définition du logarithme népérien, qui est l'unique primitive de $t \longmapsto 1/t$ sur $\mathbb{R}_+^\star$ s'annulant en 1.
- Soit $\alpha \geqslant 0$. Alors
$$\forall a, x \in \mathbb{R} \qquad \int_a^x t^\alpha\,\mathrm{d}t = \frac{x^{1+\alpha} - a^{1+\alpha}}{1+\alpha}$$
- Soit $\alpha < 0$, différent de -1. On a
$$\forall a, x \in \mathbb{R}_+^\star \qquad \int_a^x t^\alpha\,\mathrm{d}t = \frac{x^{1+\alpha} - a^{1+\alpha}}{1+\alpha}$$
et
$$\forall a, x \in \mathbb{R}_-^\star \qquad \int_a^x t^\alpha\,\mathrm{d}t = \frac{x^{1+\alpha} - a^{1+\alpha}}{1+\alpha}$$
On est, évidemment, obligé de donner les deux cas, puisque la fonction $t \longmapsto t^\alpha$ n'est pas définie (et encore moins continue) en 0. On ne peut primitiver que des fonctions continues.
- $$\forall a, x \in \mathbb{R} \qquad \int_a^x \mathrm{e}^t\,\mathrm{d}t = \mathrm{e}^x - \mathrm{e}^a$$
- $$\forall a, x \in \mathbb{R} \qquad \int_a^x \cos t\,\mathrm{d}t = \sin x - \sin a$$
- $$\forall a, x \in \mathbb{R} \qquad \int_a^x \sin t\,\mathrm{d}t = \cos a - \cos x$$
- $$\forall a, x \in \mathbb{R} \qquad \int_a^x \frac{\mathrm{d}t}{1+t^2} = \arctan x - \arctan a$$
- $$\forall a, x \in]-1\,;1[\qquad \int_a^x \frac{\mathrm{d}t}{\sqrt{1-t^2}} = \arcsin x - \arcsin a = \arccos a - \arccos x$$
- $$\forall a, x \in \mathbb{R} \qquad \int_a^x \mathrm{ch}\, t\,\mathrm{d}t = \mathrm{sh}\, x - \mathrm{sh}\, a$$
- $$\forall a, x \in \mathbb{R} \qquad \int_a^x \mathrm{sh}\, t\,\mathrm{d}t = \mathrm{ch}\, x - \mathrm{ch}\, a$$

- $\forall a, x > 1 \qquad \displaystyle\int_a^x \frac{\mathrm{d}t}{\sqrt{t^2-1}} = \operatorname{argch} x - \operatorname{argch} a$
- $\forall a, x \in \mathbb{R} \qquad \displaystyle\int_a^x \frac{\mathrm{d}t}{\sqrt{1+t^2}} = \operatorname{argsh} x - \operatorname{argsh} a$
- $\forall a, x \in]-1\,;1[\qquad \displaystyle\int_a^x \frac{\mathrm{d}t}{1-t^2} = \operatorname{argth} x - \operatorname{argth} a$

On n'est évidemment pas limité à ces calculs simples. Il est tout-à-fait possible qu'une primitive ne saute pas aux yeux, mais qu'elle soit malgré tout calculable. Il faut pour cela bidouiller un peu, plus ou moins au hasard, en utilisant les propriétés connues des fonctions usuelles. Par exemple :

$$\forall a, x \in \mathbb{R} \qquad \int_a^x \sin^2 t \,\mathrm{d}t = \frac{1}{2}(x-a) - \frac{1}{4}(\sin 2x - \sin 2a)$$

Pour voir cela, on doit utiliser la formule de trigonométrie

$$\cos(2\alpha) = 1 - 2\sin^2\alpha \qquad \text{d'où} \qquad \sin^2\alpha = \frac{1-\cos 2\alpha}{2}$$

qui se primitive aisément.

En revanche, il est plus difficile de voir que

$$\forall a, x > 0 \qquad \int_a^x \ln t \,\mathrm{d}t = x\ln x - x - a\ln a + a$$

ou encore que $\forall a, x \in \left]-\dfrac{\pi}{2}\,;\dfrac{\pi}{2}\right[\qquad \displaystyle\int_a^x \frac{\mathrm{d}t}{\cos t} = \ln\tan\left(\frac{2x+\pi}{4}\right) - \ln\tan\left(\frac{2a+\pi}{4}\right)$

Il faut pour cela des techniques plus élaborées. Les plus simples à utiliser sont l'intégration par parties et le changement de variable.

13.5.2 Intégration par parties

Théorème 13.5.6 (Intégration par parties)
Soient f et g deux fonctions de classe $\mathscr{C}^1$ sur un intervalle I. *Pour tous* α *et* β *dans* I,

$$\int_\alpha^\beta f'(t)g(t)\,dt = \big[f(t)g(t)\big]_\alpha^\beta - \int_\alpha^\beta f(t)g'(t)\,dt$$

Preuve : Les fonctions f et g étant de classe $\mathscr{C}^1$, il en est de même de fg et l'on a

$$\big[f(t)g(t)\big]_\alpha^\beta = \int_\alpha^\beta (fg)'(t)\,\mathrm{d}t = \int_\alpha^\beta f'(t)g(t)\,\mathrm{d}t + \int_\alpha^\beta f(t)g'(t)\,\mathrm{d}t$$

Remarquons qu'on a pu séparer les intégrales parce que $f'g$ et $g'f$ sont continues donc intégrables. La formule d'intégration par parties s'ensuit immédiatement. □

Exemple 13.5.7
Aussi bizarre que cela puisse paraître, cette formule évidente permet de calculer de nombreuses primitives. L'idée étant qu'une fonction h, dont on ne voit pas de primitive *a priori* fait peut-être partie du développement de $(fg)'$.

Encore faut-il trouver f et g judicieusement, de manière à ce que $h = f'g$, et qu'une primitive de fg' soit facile à calculer. Ces choses-là viennent avec l'habitude. Par exemple,

$$\int_1^x \ln t\,\mathrm{d}t = \int_1^x \underbrace{1}_{=f'} \times \underbrace{\ln t}\,\mathrm{d}t = \big[t\ln t\big]_1^x - \int_1^x t\times\frac{1}{t}\,\mathrm{d}t$$
$$= x\ln x - (x-1)$$

On peut aussi calculer une intégrale en utilisant plusieurs intégrations par parties successives. Posons

$$\mathrm{I}_n = \int_0^1 t^n\,\mathrm{e}^{-t}\,\mathrm{d}t$$

On voit bien que si on intégre par parties en dérivant de t^n, on fait baisser la puissance de t, de manière à trouver une relation de récurrence entre I_n et I_{n-1} :

$$\mathrm{I}_n = \big[-t^n\,\mathrm{e}^{-t}\big]_0^1 + n\int_0^1 t^{n-1}\,\mathrm{e}^{-t}\,\mathrm{d}t = -\mathrm{e}^{-1} + n\mathrm{I}_{n-1}$$

soit $$\forall n \geqslant 1 \qquad \mathrm{I}_n - n\mathrm{I}_{n-1} = -\mathrm{e}^{-1}$$

On peut alors trouver I_n par des méthodes d'algèbre linéaire par exemple.

13.5.3 Changement de variable

Théorème 13.5.8 (Changement de variable)
Soient $f \in \mathscr{C}(\mathrm{I})$, $\varphi \in \mathscr{C}^1(\mathrm{J})$, telles que $\varphi(\mathrm{J}) \subset \mathrm{I}$. Alors pour tous $\alpha, \beta \in \mathrm{J}$,

$$\int_\alpha^\beta f(\varphi(t))\,\varphi'(t)\,dt = \int_{\varphi(a)}^{\varphi(b)} f(u)\,du$$

Preuve : Soit F une primitive de f sur I. On sait qu'il en existe, puisque f est continue sur I. Puisque F est dérivable sur I et φ est dérivable sur J, on a

$$\forall t \in \mathrm{J} \qquad (\mathrm{F}\circ\varphi)'(t) = \mathrm{F}'(\varphi(t))\varphi'(t) = f(\varphi(t))\varphi'(t)$$

Donc $\mathrm{F}\circ\varphi$ est une primitive sur I de $(f\circ\varphi)\,\varphi'$. Mais cette fonction est continue donc

$$\int_\alpha^\beta f(\varphi(t))\,\varphi'(t)\,\mathrm{d}t = \big[\mathrm{F}(\varphi(t))\big]_{t=a}^{t=b} = \mathrm{F}(\varphi(b)) - \mathrm{F}(\varphi(a))$$

Mais f est continue sur $[\varphi(a)\,;\varphi(b)] \subset \mathrm{I}$ et F en est une primitive donc

$$\int_{\varphi(a)}^{\varphi(b)} f(u)\,\mathrm{d}u = \big[\mathrm{F}(u)\big]_{u=\varphi(a)}^{u=\varphi(b)} = \mathrm{F}(\varphi(b)) - \mathrm{F}(\varphi(a))$$

On a bien $$\int_a^b f(\varphi(t))\,\varphi'(t)\,\mathrm{d}t = \int_{\varphi(a)}^{\varphi(b)} f(u)\,\mathrm{d}u$$ □

Exemple 13.5.9

1. Ce théorème permet de calculer beaucoup d'intégrales de fonctions continues dont une primitive n'apparaît pas naturellement. En pratique, on est confronté à une intégrale

$$\int_a^b f(u)\,\mathrm{d}u$$

Tout se passe comme si l'on « pose » $u = \varphi(t)$, qu'on « remplace » le $\mathrm{d}u$ par $\varphi'(t)\,\mathrm{d}t$, et qu'on cherche α et β tels que $a = \varphi(\alpha)$ et $b = \varphi(\beta)$.

Ce raisonnement est faux si l'on ne prend pas de précautions avec les ensembles de définition de nos fonctions. Mais il peut être fait au brouillon, lorsqu'on souhaite arriver rapidement à une idée de réponse ; au moment de rédiger un calcul rigoureux, il faudra être sûr que chaque étape du calcul peut être justifiée.

2. Par exemple, soit $x \in [-1\,;1]$; la fonction $t \longmapsto \sqrt{1-t^2}$ est continue sur $[-1\,;1]$ et on peut considérer

$$\mathrm{I}(x) = \int_0^x \sqrt{1-t^2}\,\mathrm{d}t$$

On définit
$$\varphi : \left[-\frac{\pi}{2}\,;\frac{\pi}{2}\right] \longrightarrow [-1\,;1], \quad t \longmapsto \sin t$$

Cette fonction est de classe $\mathscr{C}^1$ sur $[-\frac{\pi}{2}\,;\frac{\pi}{2}]$ et son image est $[-1\,;1]$. De plus,

$$\varphi(0) = 0 \qquad \text{et} \qquad \varphi(\arcsin x) = x$$

d'où $$\mathrm{I}(x) = \int_{\varphi(0)}^{\varphi(\arcsin x)} \sqrt{1-t^2}\,\mathrm{d}t = \int_0^{\arcsin x} \sqrt{1-\sin^2 t}\cos t\,\mathrm{d}t = \int_0^{\arcsin x} |\cos t|\cos t\,\mathrm{d}t$$

Mais $[0\,;\arcsin x] \subset [-\frac{\pi}{2}\,;\frac{\pi}{2}]$ et

$$\forall\, t \in \left[-\frac{\pi}{2}\,;\frac{\pi}{2}\right] \qquad |\cos t| = \cos t$$

donc
$$\begin{aligned}\mathrm{I}(x) &= \int_0^{\arcsin x} \cos^2 t\,\mathrm{d}t = \frac{1}{2}\int_0^{\arcsin x} (1+\cos 2t)\,\mathrm{d}t = \frac{1}{2}\Big[t + \frac{\sin 2t}{2}\Big]_0^{\arcsin x} \\ &= \frac{1}{2}\Big(\arcsin x + \frac{\sin 2\arcsin x}{2}\Big) = \frac{1}{2}\big(\arcsin x + x\sqrt{1-x^2}\big)\end{aligned}$$

3. Il ne faut, cependant, pas utiliser ce théorème n'importe comment. Par exemple, soit $x > 0$ et supposons qu'on ait à calculer

$$\mathrm{I}(x) = \int_{-1}^x \frac{t^2}{1+t^2}\,\mathrm{d}t$$

Cette intégrale est facile à calculer directement en décomposant la fraction rationnelle :

$$\mathrm{I}(x) = \int_{-1}^x \Big(1 - \frac{1}{1+t^2}\Big)\,\mathrm{d}t = \big[t - \arctan t\big]_{-1}^x = x - \arctan x + 1 - \frac{\pi}{4}$$

Supposons qu'on a décidé plutôt de (mal) utiliser le théorème de changement de variable. Lorsqu'on ne prend pas de précautions, on dit « Je pose $u = t^2$ donc $t = \sqrt{|u|}$ et $\mathrm{d}t = \frac{\mathrm{d}u}{2\sqrt{|u|}}$ » pour obtenir

$$\mathrm{I}(x) = \int_1^{x^2} \frac{u}{1+u}\,\frac{\mathrm{d}u}{2\sqrt{|u|}} = \frac{1}{2}\int_1^{x^2} \frac{\sqrt{u}}{1+u}\,\mathrm{d}u$$

Il est facile de vérifier qu'une primitive de l'intégrande est $u \longmapsto \sqrt{u} - \arctan\sqrt{u}$ donc

$$\mathrm{I}(x) = \big[\sqrt{u} - \arctan\sqrt{u}\big]_1^{x^2} = |x| - \arctan|x| - 1 + \frac{\pi}{4} = x - \arctan x - 1 + \frac{\pi}{4}$$

L'expression obtenue est fausse. Tout simplement parce que le changement de variables à été fait n'importe comment : en particulier, la fonction $t \longmapsto \sqrt{|t|}$ n'est pas $\mathscr{C}^1$ sur $[-1\,;+\infty[$.

13.5.4 La formule de Taylor

L'intégrale permet de donner une nouvelle formule de Taylor, qui a l'avantage d'être une égalité (et non pas une égalité au voisinage d'un point). C'est la formule de Taylor la plus précise et son utilisation est à privilégier lorsqu'on souhaite étudier la convergence d'une série de Taylor, par exemple.

Théorème 13.5.10 (Formule de Taylor avec reste intégral)
Soient n un entier, f une fonction de classe $\mathscr{C}^{n+1}$ sur un intervalle I. *Soient a et b dans* I. *Alors*

$$f(b) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(b-a)^k + \int_a^b \frac{(b-t)^n}{n!} f^{(n+1)}(t)\,dt$$

Preuve : Il s'agit d'une simple récurrence, à l'aide d'intégrations par parties successives. On commence avec

$$f(b) = f(a) + \int_a^b f'(t)\,\mathrm{d}t$$

qui est valable parce que f est une primitive de f', qui est continue. On suppose alors le théorème vrai pour un certain $n \in \mathbb{N}$ et on se donne f de classe $\mathscr{C}^{n+2}$ sur I. On a

$$f(b) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(b-a)^k + \int_a^b \frac{(b-t)^n}{n!} f^{(n+1)}(t)\,\mathrm{d}t$$

Les fonctions $t \longmapsto -\frac{(b-t)^{n+1}}{(n+1)!}$ et $f^{(n+1)}$ sont toutes deux de classe $\mathscr{C}^1$; d'après le théorème d'intégration par parties,

$$\int_a^b \frac{(b-t)^n}{n!} f^{(n+1)}(t)\,\mathrm{d}t = \Big[\frac{-(b-t)^{n+1}}{(n+1)!}\Big]_a^b + \int_a^b \frac{(b-t)^{n+1}}{(n+1)!} f^{(n+2)}(t)\,\mathrm{d}t$$

ce qui achève la démonstration. □

13.6 Fonctions à valeurs complexes

13.6.1 Intégrabilité

La théorie de l'intégration peut se généraliser assez facilement aux fonctions à valeurs complexes, avec une définition naturelle en séparant parties réelle et imaginaire.

Définition 13.6.1 (Intégrabilité des fonctions à valeurs complexes)
Soit f définie sur I, à valeurs complexes. On dit que f est intégrable si, et seulement si, $\mathrm{Re}\, f$ et $\mathrm{Im}\, f$ sont intégrables. Dans ce cas, on définit

$$\int_{[a;b]} f = \int_{[a;b]} \mathrm{Re}\, f + \mathrm{i} \int_{[a;b]} \mathrm{Im}\, f$$

De fait, on voit que, par définition, si f est à valeurs complexes, intégrable, alors

$$\mathrm{Re} \int_{[a;b]} f = \int_{[a;b]} \mathrm{Re}\, f \qquad \mathrm{Im} \int_{[a;b]} f = \int_{[a;b]} \mathrm{Im}\, f$$

Il est alors clair que

$$\overline{\int_{[a;b]} f} = \int_{[a;b]} \overline{f}$$

Tous les résultats qui relient intégration et dérivation se prolongent naturellement des fonctions à valeurs réelles aux fonctions à valeurs complexes : on dit merci à la linéarité des opérations sur les limites (continuité, dérivabilité). Plus précisément, les **théorèmes 4.1**, **4.4**, **4.5**, **5.2**, **5.4**, **5.5**, **5.6**, **5.8** et **5.10** restent vrais avec les fonctions à valeurs complexes.

Il reste une inégalité, vraie pour les fonctions à valeurs réelles ou complexes, mais qui a une démonstration non triviale dans le cas complexe. Il s'agit de l'inégalité triangulaire :

$$\left|\int_{[a;b]} f\right| \leqslant \int_{[a;b]} |f|$$

Nous aurons d'abord besoin d'un lemme :

Lemme 13.6.2
Soient f et g deux fonctions à valeurs complexes, définies sur I, *intégrables. Alors fg est intégrable.*

Preuve : Commençons par le cas où f et g sont à valeurs réelles positives. Si elles sont toutes les deux nulles, le résultat est trivial donc on suppose f ou g non nulle. Notons

$$M_f = \operatorname{Sup} f \qquad \text{et} \qquad M_g = \operatorname{Sup} g$$

Soit $\varepsilon > 0$; on sait qu'il existe des fonctions φ_1, φ_2, ψ_1 et ψ_2, en escalier, telles que

$$\varphi_1 \leqslant f \leqslant \psi_1 \qquad \varphi_2 \leqslant g \leqslant \psi_2$$

et

$$\int_{[a;b]} (\psi_1 - \varphi_1) \leqslant \varepsilon \qquad \int_{[a;b]} (\psi_2 - \varphi_2) \leqslant \varepsilon$$

On peut supposer que φ_1 est à valeurs positives ; sinon on la remplace par sa partie positive, qui approche encore mieux l'intégrale (inférieure) de f. De même, on modifie φ_2, si nécessaire, pour la rendre positive.

$$\varphi_1\varphi_2 \leqslant fg \leqslant \psi_1\psi_2$$

de sorte que

$$\int_{[a;b]} \varphi_1\varphi_2 \leqslant \int_{\star}^{[a;b]} fg \leqslant \int_{[a;b]}^{\star} fg \leqslant \int_{[a;b]} \psi_1\psi_2$$

et

$$\int_{[a;b]}^{\star} fg - \int_{\star}^{[a;b]} fg \leqslant \int_{[a;b]} (\psi_1\psi_2 - \varphi_1\varphi_2)$$

On peut également supposer que $\psi_1 \leqslant M_f$; en effet, si ce n'est pas le cas, on remplace ψ_1 par $\operatorname{Min}(\psi_1, M_f)$, qui approche encore mieux l'intégrale supérieure de f. On a alors

$$\begin{aligned}\int_{[a;b]} (\psi_1\psi_2 - \varphi_1\varphi_2) &= \int_{[a;b]} \big(\psi_1(\psi_2 - \varphi_2) + \varphi_2(\psi_1 - \varphi_1)\big) \\ &\leqslant M_f \int_{[a;b]} (\psi_2 - \varphi_2) + M_g \int_{[a;b]} (\psi_1 - \varphi_1)\end{aligned}$$

$$\int_{[a;b]} (\psi_1\psi_2 - \varphi_1\varphi_2) \leqslant (M_f + M_g)\varepsilon$$

Ou encore

$$\int_{[a;b]} \psi_1\psi_2 \leqslant \varepsilon + \int_{[a;b]}^{\varphi} {}_2\varphi_1$$

Finalement,

$$\int_{[a;b]}^{\star} fg - \int_{\star}^{[a;b]} fg \leqslant \varepsilon$$

Mais ε était quelconque donc fg est bien intégrable.

On a donc montré que le produit de deux fonctions intégrables, à valeurs réelles, positives, est intégrable. Supposons maintenant que f et g sont à valeurs réelles, intégrables. On sait que f_+, f_-, g_+ et g_- sont intégrables ; mais

$$fg = f_+g_+ - f_+g_- - f_-g_+ + f_-g_-$$

Chacun de ces produits est intégrable donc fg est intégrable.

Enfin, supposons que f et g sont à valeurs complexes. Alors les parties réelles et imaginaires de ces fonctions sont intégrables. Mais

$$fg = \operatorname{Re} f \operatorname{Re} g - \operatorname{Im} f \operatorname{Im} g + \mathrm{i}(\operatorname{Re} f \operatorname{Im} g + \operatorname{Im} f \operatorname{Re} g)$$

D'après ce qui précède, fg est intégrable. □

Lemme 13.6.3
Soit f intégrable sur $[a;b]$, à valeurs positives. Alors $\sqrt{f}$ est intégrable.

Preuve : On fixe un $\varepsilon > 0$. Il existe des fonctions en escalier φ et ψ, telles que

$$0 \leqslant \varphi \leqslant f \leqslant \psi \qquad \text{et} \qquad \int_{[a;b]} (\psi - \varphi) \leqslant \varepsilon$$

La fonction racine carrée est croissante donc

$$\sqrt{\varphi} \leqslant \sqrt{f} \leqslant \sqrt{\psi}$$

Par suite,
$$\int_{[a;b]} \sqrt{\varphi} \leqslant \int_\star \sqrt{f} \leqslant \int_{[a;b]}^\star \sqrt{f} \leqslant \int_{[a;b]} \sqrt{\psi}$$

d'où
$$\int_{[a;b]}^\star \sqrt{f} - \int_\star^{[a;b]} f \leqslant \int_{[a;b]} (\sqrt{\psi} - \sqrt{\varphi})$$

On se donne une subdivision $a_0 = a < a_1 < \cdots < a_n = b$ de $[a;b]$, adaptée à ψ et φ. Si on fixe $k \in [\![0; n-1]\!]$, φ et ψ sont constantes sur $]a_k; a_{k+1}[$. On note ces constantes φ_k et ψ_k :

$$\int_{[a;b]} (\sqrt{\psi} - \sqrt{\varphi}) = \sum_{k=0}^{n-1} (a_{k+1} - a_k)(\sqrt{\psi_k} - \sqrt{\varphi_k})$$

Mais il est facile de vérifier que $\forall 0 < x < y \qquad \sqrt{y} - \sqrt{x} \leqslant \sqrt{y - x}$

d'où
$$\int_{[a;b]} (\sqrt{\psi} - \sqrt{\varphi}) \leqslant \sum_{k=0}^{n-1} (a_{k+1} - a_k)\sqrt{\psi_k - \varphi_k} = (b-a) \sum_{k=0}^{n-1} \frac{a_{k+1} - a_k}{b-a} \sqrt{\psi_k - \varphi_k}$$

La fonction racine carrée est concave sur $\mathbb{R}_+$ donc l'inégalité de Jensen fournit

$$\begin{aligned} \int_{[a;b]} (\sqrt{\psi} - \sqrt{\varphi}) &\leqslant (b-a)\sqrt{\sum_{k=0}^{n-1} \frac{a_{k+1} - a_k}{b-a} (\psi_k - \varphi_k)} \\ &\leqslant \sqrt{b-a}\sqrt{\int_{[a;b]} (\psi - \varphi)} \leqslant \sqrt{\varepsilon(b-a)} \end{aligned}$$

Finalement,
$$\int_{[a;b]}^\star \sqrt{f} - \int_\star^{[a;b]} \sqrt{f} \leqslant \sqrt{\varepsilon(b-a)}$$

Comme ε était quelconque, on a bien l'intégrabilité de $\sqrt{f}$. □

Corollaire 13.6.4
Soit f une fonction à valeurs complexes, intégrable sur $[a;b]$. Alors $|f|$ est intégrable et

$$\left|\int_{[a;b]} f\right| \leqslant \int_{[a;b]} |f|$$

Preuve : Puisque f est intégrable, ses parties réelle et imaginaire sont intégrables. Donc

$$|f|^2 = (\mathrm{Re}\, f)^2 + (\mathrm{Im}\, f)^2$$

est aussi intégrable. Et enfin, il en est de même de $|f| = \sqrt{|f|^2}$.

Notons $\mathrm{I} = \displaystyle\int_{[a;b]} f$; on sait qu'il existe $\theta \in [0;2\pi[$ tel que $|\mathrm{I}| = \mathrm{I}\,\mathrm{e}^{\mathrm{i}\theta}$. On définit alors

$$g = \mathrm{Re}\,(f\,\mathrm{e}^{\mathrm{i}\theta})$$

Comme f est intégrable, $f\,\mathrm{e}^{\mathrm{i}\theta}$ est intégrable ; donc sa partie réelle, g, l'est aussi. De plus,

$$\int_{[a;b]} g = \int_{[a;b]} \mathrm{Re}\,(f\,\mathrm{e}^{\mathrm{i}\theta}) = \mathrm{Re}\Big(\int_{[a;b]} f\,\mathrm{e}^{\mathrm{i}\theta}\Big) = \mathrm{Re}\,(\mathrm{I}\,\mathrm{e}^{\mathrm{i}\theta}) = |\mathrm{I}|$$

et

$$|g| = |\mathrm{Re}\,(f\,\mathrm{e}^{\mathrm{i}\theta})| \leqslant |f|$$

Comme $|g|$ et $|f|$ sont intégrable et à valeurs réelles, on peut utiliser l'inégalité triangulaire généralisée (**théorème 3.13**) et la croissance de l'intégrale :

$$|\mathrm{I}| = \int_{[a;b]} g \leqslant \int_{[a;b]} |g| \leqslant \int_{[a;b]} |f|$$

Ceci achève la démonstration. □

Corollaire 13.6.5 (Inégalité de la moyenne généralisée)
Soient f et g deux fonctions intégrables sur $[a;b]$, à valeurs complexes. Alors

$$\left|\int_{[a;b]} fg\right| \leqslant \underset{[a;b]}{Sup}|f| \int_{[a;b]} |g|$$

13.6.2 Le théorème de relêvement

Si f est une fonction, à valeurs complexes, définie sur un intervalle I, pour tout $t \in \mathrm{I}$, il existe des réels $r(t) \geqslant 0$ et $\theta(t)$ tels que $f(t) = r(t)\,\mathrm{e}^{\mathrm{i}\theta(t)}$.

L'étude de la régularité de la fonction r peut être faite à partir de la connaissance de f, puisque $r = |f|$. En revanche, si l'on ne prend pas de précaution sur le choix de l'argument θ, on est loin de pouvoir garantir sa régularité : en effet, il existe pour chaque t une infinité de choix possibles pour $\theta(t)$ et cette fonction θ peut être très discontinue.

Par exemple, prenons la fonction toute simple $f : t \longmapsto \mathrm{e}^{\mathrm{i}t}$. On peut tout-à-fait poser

$$\forall\, t \in [0;2\pi] \qquad \theta(t) = \begin{cases} t & \text{si } t \in [0;\pi] \\ t + 2\pi & \text{si } t \in]\pi;2\pi] \end{cases}$$

On a bien

$$\forall\, t \in [0;2\pi] \qquad f(t) = \mathrm{e}^{\mathrm{i}\theta(t)}$$

Mais la fonction θ choisie n'est pas continue en π. Il est même possible de choisir θ de manière à ce qu'elle soit discontinue en tout point.

Tout théorème qui affirme qu'il est possible de choisir θ de manière à ce que cette fonction soit régulière, est appelé *théorème de relêvement*. Suivant les hypothèses de régularité sur f, il est plus ou moins facile de construire un θ bien régulier. Voici un exemple d'un tel théorème :

Théorème 13.6.6 (Théorème du relèvement au moins $\mathscr{C}^1$)
Soit f une fonction à valeurs complexes, de classe $\mathscr{C}^n$ sur I *avec $n \geqslant 1$ et telle que*

$$\forall t \in \mathrm{I} \qquad |f(t)| = 1$$

Il existe une fonction θ *à valeurs réelles, de classe $\mathscr{C}^n$ sur* I*, telle que*

$$\forall t \in \mathrm{I} \qquad f(t) = exp(i\theta(t))$$

Preuve : On sait que $|f|^2 = f\overline{f} = 1$ sur I donc

$$f'\overline{f} + f\overline{f}' = 0 \qquad \text{ou encore} \qquad f'\overline{f} = -f\overline{f}'$$

Comme f ne s'annule pas, il vient

$$\frac{f'}{f} = -\overline{\left(\frac{f'}{f}\right)}$$

donc $\frac{f'}{f}$ est à valeurs imaginaires pures. Ou encore $\frac{1}{\mathrm{i}}\frac{f'}{f}$ est à valeurs réelles. On fixe $a \in \mathrm{I}$; la fonction $\frac{f'}{f}$ est continue donc intégrable et l'on peut définir

$$\forall t \in \mathrm{I} \qquad \varphi(t) = \frac{1}{\mathrm{i}}\int_a^t \frac{f'(u)}{f(u)}\,\mathrm{d}u$$

Alors φ est à valeurs réelles, dérivable et

$$\forall t \in \mathrm{I} \qquad \varphi'(t) = \frac{1}{i}\frac{f'(t)}{f(t)}$$

Comme f est de classe $\mathscr{C}^n$, on voit que φ' est de classe $\mathscr{C}^{n-1}$ donc φ est de classe $\mathscr{C}^n$. On pose ensuite

$$\forall t \in \mathrm{I} \qquad g(t) = f(t)\overline{f(a)}\exp(-\mathrm{i}\varphi(t))$$

Alors g est dérivable sur I d'après les théorèmes généraux et

$$\begin{aligned}\forall t \in \mathrm{I} \qquad g'(t) &= -\mathrm{i}\varphi'(t)f(t)\exp(-\mathrm{i}\varphi(t)) + f'(t)\exp(-\mathrm{i}\varphi(t)) \\ &= \exp(-\mathrm{i}\varphi(t))\big(f'(t) - \mathrm{i}f(t)\varphi'(t)\big) = 0\end{aligned}$$

g est donc constante sur I. Mais $g(a) = |f(a)|^2 = 1$ donc

$$\forall t \in \mathrm{I} \qquad f(t)\overline{f(a)}\exp(-\mathrm{i}\varphi(t)) = 1$$

$$\forall t \in \mathrm{I} \qquad f(t) = f(a)\exp(\mathrm{i}\varphi(t))$$

Il suffit de poser $\theta = \varphi + \alpha$, où α est un argument de $f(a)$. □

Chapitre 14

Espaces Préhilbertiens réels

Ce chapitre généralise aux espaces vectoriels réels les notions de produit scalaire et d'orthogonalité bien connues en dimensions 2 et 3. Dans tout le chapitre, E est un $\mathbb{R}$-espace vectoriel.

14.1 Premières définitions

14.1.1 Produits scalaires

Définition 14.1.1 (Produit scalaire)
Soit $f : \mathrm{E}^2 \longrightarrow \mathbb{R}$ une application. On dit qu'elle est :

- *bilinéaire* si, et seulement si,

$$\forall x, y, z \in \mathrm{E} \quad \forall \lambda \in \mathbb{K} \qquad f(\lambda x + y, z) = \lambda f(x, z) + f(y, z)$$

  et $$\forall x, y, z \in \mathrm{E} \quad \forall \lambda \in \mathbb{K} \qquad f(z, \lambda x + y) = \lambda f(z, x) + f(z, y)$$

- *symétrique* si, et seulement si,

$$\forall x, y \in \mathrm{E} \qquad f(x, y) = f(y, x)$$

- *définie* si, et seulement si,

$$\forall x \in \mathrm{E} \qquad f(x, x) = 0 \implies x = 0$$

- *positive* si, et seulement si,

$$\forall x \in \mathrm{E} \qquad f(x, x) \geqslant 0$$

- *non dégénérée* si, et seulement si,

$$\forall x \in \mathrm{E} \qquad (\forall y \in \mathrm{E} \quad f(x, y) = 0) \implies x = 0$$

Enfin, on appelle *produit scalaire sur* E toute application bilinéaire, symétrique, définie, positive. Un *espace préhilbertien réel* est un couple $(\mathrm{E}, \langle \ | \ \rangle)$ où E est un $\mathbb{R}$-espace vectoriel et $\langle \ | \ \rangle$ est un produit scalaire. Si E est de dimension finie, on dit qu'il est *euclidien*.

Observons que, pour montrer qu'une application est un produit scalaire, il est plus rapide d'établir d'abord la symétrie : en effet, suffit alors de montrer la linéarité par rapport à la première variable pour avoir la bilinéarité.

Exemple 14.1.2

1. Soit n un entier non nul. Si x est un vecteur dans $\mathbb{R}^n$, on notera $x_1,\dots,x_n$ ses coordonnées dans la base canonique. On pose

$$\forall x,y\in\mathbb{R}^n \qquad \langle x\mid y\rangle=\sum_{k=1}^{n}x_k y_k={}^t x\,y$$

Il est évident que $\langle\ |\ \rangle$ est un produit scalaire. En particulier, on utilise le fait qu'un carré est toujours positif dans $\mathbb{R}$ et qu'une somme de réels positifs est nulle si, et seulement si, chaque réel est nul.

Ce produit scalaire fait de $\mathbb{R}^n$ un espace préhilbertien réel. On l'appelle le produit scalaire canonique sur $\mathbb{R}^n$.

Dans le cas où $n=2$ ou $n=3$, on retrouve les produits scalaires usuels dans $\mathbb{R}^2$ et $\mathbb{R}^3$.

2. n est toujours un entier non nul. On se donne un $\mathbb{R}$-espace vectoriel de dimension finie E, avec une base $\mathscr{B}$ quelconque. Si $x\in\mathrm{E}$, on notera $x_1,\dots,x_n$ ses coordonnées dans la base $\mathscr{B}$. Si l'on pose

$$\forall x,y\in\mathrm{E} \qquad \langle x\mid y\rangle=\sum_{k=1}^{n}x_k y_k$$

on définit un produit scalaire sur E.

Observons que ce produit scalaire dépend évidemment de la base choisie ; en général, si l'on change de base, on n'obtient pas le même produit scalaire. Également, si $\mathrm{E}=\mathbb{R}^n$ et $\mathscr{B}$ est la base canonique, alors on a simplement le produit scalaire canonique défini juste au-dessus.

3. Prenons par exemple $\mathrm{E}=\mathbb{R}^3$ et la base $\mathscr{B}$ formée par les vecteurs

$$e_1=\begin{bmatrix}1\\0\\-1\end{bmatrix} \qquad e_2=\begin{bmatrix}1\\1\\0\end{bmatrix} \qquad e_3=\begin{bmatrix}0\\1\\2\end{bmatrix}$$

Il s'agit bien d'une base puisque

$$\det(e_1,e_2,e_3)=\begin{vmatrix}1&1&0\\0&1&1\\-1&0&2\end{vmatrix}=1\neq 0$$

et un petit calcul montre que si $x\in\mathbb{R}^n$, alors ses coordonnées dans la base $\mathscr{B}$ sont

$$[x]_{\mathscr{B}}=\begin{bmatrix}2x_1-2x_2+x_3\\-x_1+2x_2-x_3\\x_1-x_2+x_3\end{bmatrix}$$

Si on note $\langle\ |\ \rangle_c$ le produit scalaire canonique et $\langle\ |\ \rangle_{\mathscr{B}}$ le produit scalaire dans la base $\mathscr{B}$, on a pour tous x et y dans $\mathbb{R}^n$:

$$\langle x\mid y\rangle_c=x_1y_1+x_2y_2+x_3y_3$$

et $$\langle x\mid y\rangle_{\mathscr{B}}=6x_1y_1-7x_1y_2+4x_1y_3-7x_2y_1+9x_2y_2-5x_2y_3+4x_3y_1-5x_3y_2+3x_3y_3$$

Ceci montre clairement que $\langle\ |\ \rangle_c$ et $\langle\ |\ \rangle_{\mathscr{B}}$ n'ont aucune raison d'être identiques.

4. On note $\mathrm{E}=\mathscr{C}([0\,;1])$, le $\mathbb{R}$-espace vectoriel des fonctions continues sur $[0\,;1]$ et on pose

$$\forall f,g\in\mathrm{E} \qquad \langle f\mid g\rangle=\int_{[0\,;1]}fg$$

D'après les propriétés de l'intégrale, $\langle\ |\ \rangle$ est bien un produit scalaire sur E. En particulier, pour montrer qu'il est défini, on utilise le fait qu'une fonction *continue* sur $[0\,;1]$, qui a une intégrale nulle, est nulle. La continuité est essentielle ici.

Théorème 14.1.3 (Inégalité de Cauchy-Schwarz)
Soit f une forme bilinéaire symétrique positive sur E. *Alors*

$$\forall x, y \in \mathrm{E} \qquad f(x,y)^2 \leqslant f(x,x)\, f(y,y)$$

Si, de plus, f est un produit scalaire, et si $x, y \in \mathrm{E}$, l'inégalité de Cauchy-Schwarz est une égalité si, et seulement si, (x, y) est liée.

Preuve : Soient x et y dans E. Comme f est positive, $f(x+\lambda y, x+\lambda y)$ est positif pour tout λ réel. Mais par bilinérité et symétrie, on a

$$f(x+\lambda y, x+\lambda y) = f(x,y) + 2\lambda f(x,y) + \lambda^2 f(y,y)$$

Cette quantité est positive pour tout λ donc le trinôme $\mathrm{X}^2 f(y,y) + 2f(x,y)\mathrm{X} + f(x,x)$ a un discriminant négatif :

$$4f(x,y)^2 - 4f(x,x)\, f(y,y) \leqslant 0$$

Supposons maintenant que f est un produit scalaire. Soient x et y dans E et on suppose que $f(x,y)^2 = f(x,x)\, f(y,y)$. Alors le trinôme $\mathrm{X}^2 f(y,y) + 2f(x,y)\mathrm{X} + f(x,x)$ a une racine (double) donc il existe $\lambda \in \mathbb{R}$ tel que $f(x+\lambda y, x+\lambda y) = 0$. Comme f est définie, on sait que $x + \lambda y = 0$ donc (x, y) est liée. La réciproque est triviale, par simple calcul. □

Proposition 14.1.4
Soit $f : \mathrm{E}^2 \longrightarrow \mathbb{R}$ une application. Si elle est définie, alors elle est non dégénérée.

Si f est bilinéaire, symétrique, positive, non dégénérée, alors elle est définie (et c'est donc un produit scalaire).

Preuve : Supposons f définie. Soit $x \in \mathrm{E}$ tel que

$$\forall y \in \mathrm{E} \qquad f(x,y) = 0$$

Alors en particulier $f(x,x) = 0$ donc $x = 0$.

Supposons maintenant que f est bilinéaire, symétrique, positive, non dégénérée. On se donne un $x \in \mathrm{E}$ tel que $f(x,x) = 0$. D'après l'inégalité de Cauchy-Schwarz, pour tout $y \in \mathrm{E}$,

$$f(x,y)^2 \leqslant f(x,x)\, f(y,y) = 0$$

Comme $f(x,y)$ est réel, il est nul. Mais y était quelconque ; comme f est non dégénérée, $x = 0$: f est définie. □

14.1.2 Normes

Définition 14.1.5
Soit E un $\mathbb{R}$-espace vectoriel. Soit $\| \ \| : \mathrm{E} \longrightarrow \mathbb{R}_+$ une application. On dit que $\| \ \|$ est une *norme* si, et seulement si,

$$\forall x \in \mathrm{E} \qquad \|x\| = 0 \implies x = 0$$

$$\forall x \in \mathrm{E} \quad \forall \lambda \in \mathbb{R} \qquad \|\lambda x\| = |\lambda|\, \|x\|$$

et

$$\forall x, y \in \mathrm{E} \qquad \|x+y\| \leqslant \|x\| + \|y\|$$

Définition 14.1.6 (Norme euclidienne)
Soit $(E, \langle\ |\ \rangle)$ un espace préhilbertien réel. On appelle *norme euclidienne* sur E, associée au produit scalaire $\langle\ |\ \rangle$, l'application $\|\ \|$ définie par

$$\forall x \in E \qquad \|x\| = \sqrt{\langle x \mid x \rangle}$$

Proposition 14.1.7 (Propriétés des normes euclidiennes)
Soit $(E, \langle\ |\ \rangle)$ *un espace préhilbertien réel.*

1. ***Positivité stricte*** $\forall x \in E \setminus \{0\} \qquad \|x\| > 0$
2. ***Homogénéité*** $\forall x \in E \quad \forall \lambda \in \mathbb{R} \qquad \|\lambda x\| = |\lambda| \, \|x\|$
3. ***Inégalité de Cauchy-Schwarz*** $\forall x, y \in E \qquad |\langle x \mid y \rangle| \leqslant \|x\| \, \|y\|$
   avec égalité si, et seulement si, (x, y) *est liée.*
4. ***Relation du parallélogramme*** $\forall x, y \in E \qquad \|x+y\|^2 + \|x-y\|^2 = 2(\|x\|^2 + \|y\|^2)$
5. ***Identités de polarisation*** $\forall x, y \in E$
$$\langle x \mid y \rangle = \frac{1}{2}(\|x+y\|^2 - \|x\|^2 - \|y\|^2)$$
$$= \frac{1}{4}(\|x+y\|^2 - \|x-y\|^2)$$
6. ***Inégalité de Minkowski*** $\forall x, y \in E \qquad \big|\|x\| - \|y\|\big| \leqslant \|x \pm y\| \leqslant \|x\| + \|y\|$

En particulier, la norme euclidienne est une norme.

Preuve : La première propriété est une conséquence du fait que le produit scalaire est positif, défini. La deuxième est une récriture de l'inégalité de Cauchy-Schwarz.

Donnons-nous x et y dans E. En utilisant la bilinéarité et la symétrie du produit scalaire, on a

$$\|x+y\|^2 = \langle x+y \mid x+y \rangle = \langle x \mid x \rangle + 2\langle x \mid y \rangle + \langle y \mid y \rangle = \|x\|^2 + \|y\|^2 + 2\langle x \mid y \rangle$$

ce qui fournit la première identité de polarisation. On a également

$$\|x-y\|^2 = \|x\|^2 + \|y\|^2 - 2\langle x \mid y \rangle$$

et l'on en déduit la deuxième identité de polarisation et la relation du parallélogramme. Ensuite, d'après Cauchy-Schwarz, on sait que

$$\big|\langle x \mid y \rangle\big| \leqslant \|x\| \, \|y\|$$

d'où $$\|x \pm y\|^2 \leqslant \|x\|^2 + \|y\|^2 + 2\|x\| \, \|y\| = (\|x\| + \|y\|)^2$$

et $$\|x \pm y\| \leqslant \|x\| + \|y\|$$

Enfin, cette relation étant vraie pour tous x et y, on a

$$\|x\| = \|x \pm y \mp y\| \leqslant \|x \pm y\| + \|y\|$$

donc $$\|x\| - \|y\| \leqslant \|x \pm y\|$$

et de même, $$\|y\| - \|x\| \leqslant \|x \pm y\|$$ □

14.2 Orthogonalité

14.2.1 Définitions et premières propriétés

Définition 14.2.1 (Orthogonalité)
Soit $(E, \langle\ |\ \rangle)$ un espace préhilbertien réel. Soient x et y deux vecteurs de E. On dit qu'ils sont *orthogonaux* si, et seulement si, $\langle x \mid y\rangle = 0$. On notera alors $x \perp y$.

Soit $A \subset E$ une partie formée d'au moins deux éléments. On dit que c'est une *famille orthogonale* si, et seulement si,

$$\forall x, y \in A \qquad x \neq y \implies x \perp y$$

Enfin, on dira que A est *orthonormée* si, et seulement si, elle est orthogonale et tous ses éléments ont pour norme 1.

Il est évident, parce qu'un produit scalaire est symétrique, que $x \perp y$ équivaut à $y \perp x$. Également, le seul vecteur orthogonal à lui-même est 0 car le produit scalaire est défini ; enfin, le seul vecteur orthogonal à tous les vecteurs de E est aussi le vecteur nul car le produit scalaire est non dégénéré.

Proposition 14.2.2 (Théorème de Pythagore)
Soient $(E, \langle\ |\ \rangle)$ *un espace préhilbertien réel,* n *un entier non nul et* $(x_1, \dots, x_n)$ *une famille orthogonale. Alors pour tous réels* $\lambda_1, \dots, \lambda_n$*,*

$$\left\| \sum_{k=1}^{n} \lambda_k x_k \right\|^2 = \sum_{k=1}^{n} \lambda_k^2 \|x_k\|^2$$

Preuve : C'est une conséquence immédiate de la bilinéarité du produit scalaire. Si $\lambda_1, \dots, \lambda_n$ sont dans $\mathbb{R}$, on a

$$\left\| \sum_{k=1}^{n} \lambda_k x_k \right\|^2 = \left\langle \sum_{k=1}^{n} \lambda_k x_k \,\middle|\, \sum_{\ell=1}^{n} \lambda_\ell x_\ell \right\rangle = \sum_{k=1}^{n} \sum_{\ell=1}^{n} \lambda_k \lambda_\ell \underbrace{\langle x_k \mid x_\ell \rangle}_{=0 \text{ si } k \neq \ell} = \sum_{k=1}^{n} \lambda_k^2 \|x_k\|^2 \qquad \square$$

Définition 14.2.3
Soient $(E, \langle\ |\ \rangle)$ un espace préhilbertien réel et $A \subset E$. On appelle *orthogonal de* A, noté A°, l'ensemble des vecteurs orthogonaux à tous les vecteurs de A :

$$A^\circ = \{x \in E \mid \forall a \in A \quad x \perp a\}$$

Proposition 14.2.4
Soient $(E, \langle\ |\ \rangle)$ *un espace préhilbertien réel. On se donne* A *et* B *des sous-ensembles de* E *non vides.*

1. $\{0\}^\circ = E$ *et* $E^\circ = \{0\}$.
2. *Soient* $e_1, \dots, e_n$ *dans* E*, non nuls. Si la famille* $(e_1, \dots, e_n)$ *est orthogonale, alors elle est libre.*
3. $A^\circ = (\mathit{Vect} A)^\circ$ *; de plus,* A° *est un sous-espace vectoriel de* E *et* $A \subset A^{\circ\circ}$.
4. $(A \cup B)^\circ = (\mathit{Vect} A + \mathit{Vect} B)^\circ = A^\circ \cap B^\circ$.
5. $A^\circ + B^\circ \subset (\mathit{Vect} A \cap \mathit{Vect} B)^\circ$.
6. *Si* $A \subset B$*, alors* $B^\circ \subset A^\circ$.
7. *Si* F *est un sous-espace vectoriel de* E*, alors* F *et* F° *sont en somme directe.*

Preuve : Tout vecteur x de E est orthogonal au vecteur nul, puisque

$$2\langle x \mid 0\rangle = \langle x \mid 2\times 0\rangle = \langle x \mid 0\rangle$$

Par suite, $\{0\}^\circ = \mathrm{E}$. Le fait que $\mathrm{E}^\circ = \{0\}$ a déjà été observé plus haut.

Soient $e_1, \dots, e_n$ dans E, non nuls, tels que $(e_1, \dots, e_n)$ est une famille orthogonale. On suppose la famille liée ; alors l'un de ces vecteurs, par exemple e_n, est combinaison linéaire des autres. Il existe $\lambda_1, \dots, \lambda_{n-1} \in \mathbb{R}$ tels que

$$e_n = \sum_{k=1}^{n-1} \lambda_k e_k$$

Alors
$$\|e_n\|^2 = \langle e_n \mid e_n\rangle = \left\langle \sum_{k=1}^{n-1} \lambda_k e_k \;\middle|\; e_n \right\rangle = \sum_{k=1}^{n-1} \lambda \langle e_k \mid e_n\rangle = 0$$

Mais e_n n'est pas nul donc $\|e_n\| \neq 0$ et on a une contradiction.

Pour tout élément x de E, on note φ_x l'application

$$\begin{aligned} \varphi_x : \ & \mathrm{E} \longrightarrow \mathbb{R} \\ & y \longmapsto \langle x \mid y\rangle \end{aligned}$$

Le produit scalaire est linéaire par rapport à la seconde variable donc φ_x est une forme linéaire. Si A est une partie de E, on a

$$\mathrm{A}^\circ = \{y \in \mathrm{E} \mid \forall x \in \mathrm{A} \quad \langle x \mid y\rangle = 0\} = \bigcap_{x\in \mathrm{A}} \mathrm{Ker}\,\varphi_x$$

donc A° est un sous-espace vectoriel de E, car c'est une intersection de sous-espaces.

Si $x \in \mathrm{A}$, il est, par définition, orthogonal à tous les éléments de A° donc $x \in \mathrm{A}^{\circ\circ}$.

Si B est une autre partie de E avec $\mathrm{A} \subset \mathrm{B}$, on a

$$\mathrm{B}^\circ = \bigcap_{x\in \mathrm{B}} \mathrm{Ker}\,\varphi_x \subset \bigcap_{x\in \mathrm{A}} \mathrm{Ker}\,\varphi_x = \mathrm{A}^\circ$$

En particulier, comme $\mathrm{A} \subset \mathrm{Vect\,A}$, on a $(\mathrm{Vect\,A})^\circ \subset \mathrm{A}^\circ$. Réciproquement, si $x \in \mathrm{A}^\circ$, il est orthogonal à tout élément de A ; donc orthogonal à toute combinaison linéaire finie d'éléments de A, par bilinéarité du produit scalaire. Donc $\mathrm{A}^\circ = (\mathrm{Vect\,A})^\circ$.

Il s'ensuit que, pour toutes parties non vides A et B,

$$(\mathrm{A}\cup\mathrm{B})^\circ = (\mathrm{Vect}\,(\mathrm{A}\cup\mathrm{B}))^\circ = (\mathrm{Vect\,A} + \mathrm{Vect\,B})^\circ$$

puisque $\mathrm{Vect\,A} + \mathrm{Vect\,B} = \mathrm{Vect}\,(\mathrm{A}\cup\mathrm{B})$. Si $x \in \mathrm{A}^\circ \cap \mathrm{B}^\circ$, il est orthogonal à tout élément de A et à tout élément de B : il est donc orthogonal à tout élément de $\mathrm{A}\cup\mathrm{B}$. On a bien $\mathrm{A}^\circ \cap \mathrm{B}^\circ \subset (\mathrm{A}\cup\mathrm{B})^\circ$. La réciproque est tout aussi évidente.

Enfin, on a $(\mathrm{Vect\,A} \cap \mathrm{Vect\,B})$ inclus dans $\mathrm{Vect\,A}$ et dans $\mathrm{Vect\,B}$ donc

$$\mathrm{A}^\circ = (\mathrm{Vect\,A})^\circ \subset (\mathrm{Vect\,A} \cap \mathrm{Vect\,B})^\circ \qquad \text{et} \qquad \mathrm{B}^\circ = (\mathrm{Vect\,B})^\circ \subset (\mathrm{Vect\,A} \cap \mathrm{Vect\,B})\circ$$

d'où
$$(\mathrm{A}^\circ \cup \mathrm{B}^\circ) \subset (\mathrm{Vect\,A} \cap \mathrm{Vect\,B})\circ$$

Mais $\mathrm{A}^\circ + \mathrm{B}^\circ$ est le plus petit sous-espace de E qui contient $\mathrm{A}^\circ \cup \mathrm{B}^\circ$. En particulier, il est inclus dans $(\mathrm{Vect\,A} \cap \mathrm{Vect\,B})\circ$. □

14.2.2 L'algorithme de Schmidt

L'algorithme de Schmidt est un outil fondamental pour construire une famille orthonormée à partir d'une famille libre finie.

Théorème 14.2.5 (Théorème de Schmidt)
Soient $(E, \langle \mid \rangle)$ *un espace préhilbertien réel,* n *un entier non nul et* $(e_1, \dots, e_n)$ *une famille libre de* E. *Alors il existe une famille orthonormée* $(v_1, \dots, v_n)$ *telle que*

$$\forall k \in [\![1\,;n]\!] \qquad Vect(e_1, \dots, e_k) = Vect(v_1, \dots, v_k)$$

Preuve : On démontre ceci par récurrence. On définit pour tout entier n non nul la proposition $\mathscr{P}(n)$: « si E est un espace préhilbertien réel et $(e_1, \dots, e_n)$ est une famille libre, il existe $(v_1, \dots, v_n)$ orthonormée telle que

$$\forall k \in [\![1\,;n]\!] \qquad \text{Vect}(e_1, \dots, e_k) = \text{Vect}(v_1, \dots, v_k) \qquad \text{»}$$

- $\mathscr{P}(1)$ **est vraie** : Soit (e_1) une famille libre dans un espace préhilbertien réel. Alors e_1 n'est pas nul, et $\|e_1\| \neq 0$. On pose $v_1 = \frac{e_1}{\|e_1\|}$ et on a gagné.
- $\mathscr{P}(n) \Longrightarrow \mathscr{P}(n+1)$: Soit n un entier non nul tel que $\mathscr{P}(n)$ est vraie. On se donne un espace préhilbertien réel E et une famille libre $(e_1, \dots, e_{n+1})$ dans E. Alors $(e_1, \dots, e_n)$ est libre : d'après $\mathscr{P}(n)$, on peut trouver $(v_1, \dots, v_n)$ orthonormée telle que

  $$\forall k \in [\![1\,;n]\!] \qquad \text{Vect}(e_1, \dots, e_k) = \text{Vect}(v_1, \dots, v_k)$$

  Il reste donc seulement à trouver v_{n+1}. On se donne des réels $\lambda_1, \dots, \lambda_n$ et on pose

  $$u = e_{n+1} + \sum_{k=1}^{n} \lambda_k v_k$$

  On cherche les bonnes valeurs pour $\lambda_1, \dots, \lambda_n$, de manière à ce que u soit orthogonal à $v_1, \dots, v_n$. Si $i \in [\![1\,;n]\!]$, on a par bilinéarité du produit scalaire

  $$\langle u \mid v_i \rangle = \langle e_{n+1} \mid v_i \rangle + \sum_{k=1}^{n} \lambda_k \underbrace{\langle v_k \mid v_i \rangle}_{=\delta_{i,j}} = \langle e_{n+1} \mid v_i \rangle + \lambda_i$$

  On voit donc que $u \perp v_i$ si, et seulement si, $\lambda_i = -\langle e_{n+1} \mid v_i \rangle$. On pose donc

  $$\forall i \in [\![1\,;n]\!] \qquad \lambda_i = -\langle e_{n+1} \mid v_i \rangle$$

  De cette manière, $(v_1, \dots, v_n, u)$ est orthogonale. Elle est donc libre et en particulier $u \neq 0$. Il suffit donc de poser $v_{n+1} = \frac{u}{\|u\|}$ pour avoir $(v_1, \dots, v_{n+1})$ orthonormée.
  De plus, on sait déjà que

  $$\forall k \in [\![1\,;n]\!] \qquad \text{Vect}(e_1, \dots, e_k) = \text{Vect}(v_1, \dots, v_k)$$

  En outre, par construction, $v_{n+1} \in \text{Vect}(v_1, \dots, v_n, e_{n+1}) = \text{Vect}(e_1, \dots, e_n, e_{n+1})$ donc

  $$\text{Vect}(v_1, \dots, v_{n+1}) \subset \text{Vect}(e_1, \dots, e_{n+1})$$

  Mais ces espaces sont de même dimension, égale à $n+1$, car les familles $(e_1, \dots, e_{n+1})$ et $(v_1, \dots, v_{n+1})$ sont libres. Donc ils sont égaux, ce qui démontre $\mathscr{P}(n+1)$.
- **Conclusion** : $\mathscr{P}(n)$ est vraie pour tout entier n non nul. □

Exemple 14.2.6
La preuve du théorème de Schmidt a pour avantage de montrer précisément comment construire une base orthonormée à partir d'une famille libre.

Prenons par exemple comme espace $E = \mathbb{R}[X]$, avec le produit scalaire

$$\forall P, Q \in E \qquad \langle P \mid Q \rangle = \int_{-1}^{1} P(x)Q(x)\,dx$$

Observons déjà que c'est bien un produit scalaire ; toutes les propriétés de la définition sont triviales, sauf peut-être le fait que $\langle \ | \ \rangle$ est définie. Si P est tel que $\langle P \mid P \rangle = 0$, alors P est la fonction nulle sur $[-1\,;1]$. Mais un polynôme qui a une infinité de racines est nul, donc $P = 0$.

On considère la famille $(1, X, X^2)$, qui est libre dans E et on lui applique le procédé de Schmidt pour l'orthonormaliser. On a

$$\|1\|^2 = \int_{-1}^{1} dx = 2$$

et on pose $$v_1 = \frac{1}{\|1\|} = \frac{\sqrt{2}}{2}$$

On a calcule alors

$$\langle v_1 \mid X \rangle = \frac{\sqrt{2}}{2} \int_{-1}^{1} x\,dx = 0$$

et on pose $$u_2 = X - \langle v_1 \mid X \rangle v_1 = X$$

qui est orthogonal à v_1. Il reste à le rendre normé donc calcule

$$\|u_2\|^2 = \int_{-1}^{1} x^2\,dx = \frac{2}{3}$$

et on pose $$v_2 = \frac{u_2}{\|u_2\|} = \frac{\sqrt{3}}{\sqrt{2}} X$$

À ce stade, on a une famille orthonormée (v_1, v_2). Pour calculer le troisième vecteur, on commence par déterminer

$$\langle v_1 \mid X^2 \rangle = \frac{\sqrt{2}}{2} \int_{-1}^{1} x^2\,dx = \frac{\sqrt{2}}{3} \qquad \langle v_2 \mid X^2 \rangle = \frac{\sqrt{3}}{\sqrt{2}} \int_{-1}^{1} x^3\,dx = 0$$

On définit $$u_3 = X^2 - \langle v_2 \mid X^2 \rangle v_2 - \langle v_1 \mid X^2 \rangle v_1 = X^2 - \frac{1}{3}$$

Par construction, (v_1, v_2, u_3) est orthogonale. Il reste à normer u_3 :

$$\|u_3\|^2 = \int_{-1}^{1} \left(x^2 - \frac{\sqrt{1}}{3}\right)^2 dx = \frac{8}{45}$$

En posant $$v_3 = \frac{3\sqrt{5}}{2\sqrt{2}}\left(X^2 - \frac{1}{3}\right)$$

on a construit une base orthonormée (v_1, v_2, v_3), à partir de (e_1, e_2, e_3), qui conserve les sous-espaces intermédiaires. La famille

$$\left(\frac{\sqrt{2}}{2}, \frac{\sqrt{3}}{\sqrt{2}} X, \frac{3\sqrt{5}}{2\sqrt{2}}\left(X^2 - \frac{1}{3}\right)\right)$$

est une base orthonormée de $\mathbb{R}_2[X]$ pour le produit scalaire $\langle \ | \ \rangle$.

Corollaire 14.2.7
Soient $(\mathrm{E}, \langle\ |\ \rangle)$ *un espace préhilbertien réel et* F *un sous-espace de dimension finie, non nulle, de* E. *Alors* F *admet des bases orthonormées.*

De plus, si $n = \dim \mathrm{F}$ *et* $(e_1, \dots, e_n)$ *est une base orthonormée de* F, *on a*

$$\forall x \in \mathrm{F} \qquad x = \sum_{k=1}^{n} \langle x \mid e_k \rangle e_k$$

Preuve : Le théorème de Schmidt assure l'existence de bases orthonormées pour F. On en construit une, notée $(e_1, \dots, e_n)$. On se donne $x \in \mathrm{F}$ et on considère

$$y = \sum_{k=1}^{n} \langle x \mid e_k \rangle e_k$$

Comme les vecteurs $(e_1, \dots, e_n)$ sont orthogonaux deux-à-deux, on voit que

$$\forall k \in [\![1\,;\, n]\!] \qquad \langle y \mid e_k \rangle = \langle x \mid e_k \rangle$$

ou encore

$$\forall k \in [\![1\,;\, n]\!] \qquad \langle y - x \mid e_k \rangle = 0$$

Alors par linéarité du produit scalaire par rapport à la deuxième variable, et parce que la famille $(e_1, \dots, e_n)$ engendre F, on a

$$\forall z \in \mathrm{F} \qquad \langle y - x \mid z \rangle = 0$$

En particulier, $y - x \in \mathrm{F}$ puisque y et x sont dans F d'où $\|y - x\|^2 = 0$ et $y = x$. □

14.2.3 Projection orthogonale sur un sous-espace

Il s'agit maintenant de généraliser la notion de projection orthogonale dont on a l'habitude dans le plan ou dans l'espace. Intuitivement, le projeté orthogonal d'un vecteur $\|x\|$ sur un sous-espace F doit être un élément de F qui minimise la distance entre x et les vecteurs de F.

Proposition 14.2.8
Soient $(\mathrm{E}, \langle\ |\ \rangle)$ *un espace préhilbertien réel et* F *un sous-espace de dimension finie. Si* $x \in \mathrm{E}$, *il existe un unique élément* $p_{\mathrm{F}} x$ *de* F, *tel que*

$$\|x - p_{\mathrm{F}} x\| = Inf\{\|x - z\| \mid z \in \mathrm{F}\}$$

De plus, $x - p_{\mathrm{F}} x$ *est orthogonal à* F *et*

$$\|p_{\mathrm{F}} x\| \leqslant \|x\|$$

avec égalité si, et seulement si, $x \in \mathrm{F}$.
Enfin, si F *est de dimension finie n non nulle et rapporté à une base orthonormée* $(e_1, \dots, e_n)$, *on a*

$$p_{\mathrm{F}} x = \sum_{k=1}^{n} \langle x \mid e_k \rangle e_k$$

$p_{\mathrm{F}} x$ *est appelé la projection orthogonale de* x *sur* F.

Preuve : Notons n la dimension de F. Le théorème est trivial si $n = 0$ donc on suppose n non nul. Comme F est de dimension finie, on peut y trouver une base orthonormée $(e_1, \dots, e_n)$. Si x est donné dans E, on définit

$$p_{\mathrm{F}} x = \sum_{k=1}^{n} \langle x \mid e_k \rangle e_k$$

Par définition, $p_F x$ est dans F et parce que $(e_1,\dots,e_n)$ est orthonormée, on a

$$\forall k \in [\![1\,;n]\!] \qquad \langle p_F x \mid e_k\rangle = \langle x \mid e_k\rangle$$

On se donne maintenant un $z \in F$, quelconque. Toujours du fait que $(e_1,\dots,e_n)$ est orthonormée, on sait que

$$z = \sum_{k=1}^{n} \langle z \mid e_k\rangle e_k$$

et $$\langle p_F x \mid z\rangle = \sum_{k=1}^{n} \langle x \mid e_k\rangle \langle z \mid e_k\rangle = \left\langle x \,\middle|\, \sum_{k=1}^{n} \langle z \mid e_k\rangle e_k \right\rangle = \langle x \mid z\rangle$$

D'où $$\forall z \in F \qquad \langle x - p_F x \mid z\rangle = 0$$

Ceci démontre que $x - p_F x$ est orthogonal à F. Par conséquent, d'après le théorème de Pythagore,

$$\forall z \in F \qquad \|x-z\|^2 = \|\underbrace{x-p_F x}_{\in F^\circ} + \underbrace{p_F x - z}_{\in F}\|^2 = \|x-p_F x\|^2 + \|p_F x - z\|^2 \geqslant \|x-p_F x\|^2 \qquad (\star)$$

et l'on a bien $$\|x-p_F x\| = \operatorname{Min}\{\|x-z\| \mid z \in F\}$$

Mais la relation $(\star)$ montre aussi que si $z \in F$ est tel que $\|x-z\| = \|x-p_F x\|$, alors $\|p_F x - z\| = 0$ donc $z = p_F x$. Par suite, $p_F x$ est bien l'unique vecteur de F qui réalise ce minimum.

Enfin, comme $x - p_F x$ est orthogonal à $p_F x$, on a

$$\|p_F x\|^2 = \|x\|^2 - \|x-p_F x\|^2 \leqslant \|x\|^2$$

ce qui fournit l'inégalité de Bessel. Et on voit qu'on a une égalité si, et seulement si, $\|x-p_F x\|^2 = 0$, c'est-à-dire $x = p_F x$, ou encore $x \in F$. □

Exemple 14.2.9
Supposons qu'on cherche à calculer

$$m = \operatorname{Inf}\left\{ \int_{-1}^{1} \left(e^x + a + bx + cx^2\right)^2 dx \;\middle|\; a,b,c \in \mathbb{R}\right\}$$

Une manière consiste à étudier la fonction définie par

$$\forall a,b,c \in \mathbb{R}^3 \qquad f(a,b,c) = \int_{-1}^{1} \left(e^x + a + bx + cx^2\right)^2 dx$$

en étudiant ses dérivées partielles et en cherchant où celles-ci s'annulent. Ce n'est pas très drôle.

On peut aussi donner une structure euclidienne à l'espace $E = \mathscr{C}([-1\,;1])$ en posant

$$\forall f,g \in E \qquad \langle f \mid g\rangle = \int_{[-1;1]} fg$$

Si on note

$$e_1 : x \longmapsto 1 \qquad e_2 : x \longmapsto x \qquad e_3 : x \longmapsto x^2$$

et $F = \operatorname{Vect}(e_1,e_2,e_3)$, alors on a simplement

$$m = \operatorname{Inf}\{\|\exp - f\|^2 \mid f \in F\}$$

Le théorème de projection répond exactement à cette question puisque $m = \|\exp - p_F \exp\|^2$. Il suffit donc de trouver une base orthonormée (v_1,v_2,v_3) de F (déjà calculée dans l'exemple précédent), calculer

$$\langle \exp \mid v_1\rangle = \frac{\sqrt{2}}{2}\left(e - \frac{1}{e}\right) \qquad \langle \exp \mid v_2\rangle = \frac{\sqrt{6}}{e} \qquad \langle \exp \mid v_3\rangle = \frac{\sqrt{5}}{\sqrt{2}}\left(e - \frac{7}{e}\right)$$

$$\|\exp\|^2 = \frac{1}{2}\left(e^2 - \frac{1}{e^2}\right) \qquad \|p_F \exp\|^2 = \langle \exp \mid v_1\rangle^2 + \langle \exp \mid v_2\rangle^2 + \langle \exp \mid v_3\rangle^2 = 3\left(e^2 - 12 + \frac{43}{e^2}\right)$$

d'où $$m = \|\exp - p_F \exp\|^2 = \|\exp\|^2 - \|p_F \exp\|^2 = \frac{1}{2}\left(5e^2 + 259 - \frac{72}{e^2}\right)$$

Proposition 14.2.10
Soient $(E, \langle \mid \rangle)$ *un espace préhilbertien réel et* F *un sous-espace de dimension finie. On note* p_F *l'application de projection orthogonale de* E *sur* F. p_F *est la projection sur* F, *parallèlement à* F°. *De plus,*

$$\forall x, y \in E \qquad \langle p_F x \mid y\rangle = \langle x \mid p_F y\rangle$$

Preuve : Soit n la dimension de F. Si $n = 0$, le théorème est trivial donc on suppose n non nul. Si on note $(e_1, \dots, e_n)$ une base orthonormée de F, on a

$$\forall x \in E \qquad p_F x = \sum_{k=1}^{n} \langle x \mid e_k\rangle e_k$$

La linéarité du produit scalaire par rapport à la première variable assure la linéarité de p_F.

Si $x \in F$, on a $\|x - x\| = 0 = \text{Inf}\{\|x - z\| \mid z \in F\}$ donc $p_F x = x$. Ceci montre à la fois que $F = \text{Im}\, p_F$ et que

$$\forall x \in E \qquad p_F(\underbrace{p_F x}_{\in F}) = p_F x$$

donc p_F est une projection, d'image F. Enfin, si $x \in E$, on a

$$\begin{aligned} x \in \text{Ker}\, p_F &\iff \sum_{k=1}^{n} \langle x \mid e_k\rangle e_k = 0 \\ &\iff \forall k \in [\![1\,;n]\!] \qquad \langle x \mid e_k = 0\rangle \\ &\iff x \in \{e_1, \dots, e_n\}^\circ = (\text{Vect}\,(e_1, \dots, e_n))^\circ = F^\circ \end{aligned}$$

d'où $$\text{Ker}\, p_F = F^\circ$$

Enfin, donnons-nous x et y dans E. On a

$$p_F x = \sum_{k=1}^{n} \langle x \mid e_k\rangle e_k \qquad \text{donc} \qquad \langle p_F x \mid y\rangle = \sum_{k=1}^{n} \langle x \mid e_k\rangle \langle e_k \mid y\rangle$$

et de même $$\langle x \mid p_F y\rangle = \sum_{k=1}^{n} \langle y \mid e_k\rangle \langle x \mid e_k\rangle$$

Comme le produit scalaire est symétrique, et la multiplication dans $\mathbb{R}$ est commutative, il vient $\langle p_F x \mid y\rangle = \langle x \mid p_F y\rangle$. □

Corollaire 14.2.11
Soient $(E, \langle \mid \rangle)$ *préhilbertien réel et* F *un sous-espace de* E, *de dimension finie. Alors*

$$F^{\circ\circ} = F \qquad \textit{et} \qquad F^{\circ\circ\circ} = F^\circ$$

Preuve : On sait déjà que $F \subset (F^\circ)^\circ$. Réciproquement, soit $x \in F^{\circ\circ}$. On a

$$x = p_F x + (x - p_F x)$$

On sait que $x - p_F x \in F^\circ$ donc $x \perp (x - p_F x)$; et $p_F x \in F$ donc $p_F x \perp (x - p_F x)$. Par suite,

$$\langle x \mid x - p_{\mathrm{F}} x\rangle = 0 = \underbrace{\langle p_{\mathrm{F}} x \mid x - p_{\mathrm{F}} x\rangle}_{=0} + \langle x - p_{\mathrm{F}} x \mid x - p_{\mathrm{F}} x\rangle$$

et $$\|x - p_{\mathrm{F}} x\|^2 = 0 \qquad \text{d'où} \qquad x - p_{\mathrm{F}} x = 0$$

Ceci montre que $p_{\mathrm{F}} x = x$ donc $x \in \mathrm{F}$: on a bien $\mathrm{F}^{\circ\circ} = \mathrm{F}$. Et du coup, $\mathrm{F}^{\circ\circ\circ} = \mathrm{F}^{\circ}$. □

14.3 Espaces euclidiens

14.3.1 Résumé

Un espace euclidien est, par définition, un espace préhilbertien réel $(\mathrm{E}, \langle\ |\ \rangle)$ qui est de dimension finie. Comme tous les sous-espaces de E sont, eux-mêmes, de dimension finie, les résultats obtenus précédemment ont une formulation qui peut être simplifiée. La proposition suivante est une conséquence triviale de ce qui a été fait plus haut.

Proposition 14.3.1
Soit $(\mathrm{E}, \langle\ |\ \rangle)$ *un espace euclidien de dimension n non nulle.*

- E *admet des bases orthonormées.*
- *Si* $(e_1, \ldots, e_n)$ *est une base orthonormée, alors*

$$\forall x \in \mathrm{E} \qquad x = \sum_{k=1}^{n} \langle x \mid e_k\rangle\, e_k$$

- *Si* F *est un sous-espace non nul de* E*, alors* $\mathrm{F}^{\circ\circ} = \mathrm{F}$ *et* F° *est un supplémentaire de* F*, appelé le supplémentaire orthogonal de* F *dans* E*. La projection orthogonale* p_{F} *sur* F *existe et il s'agit de la projection sur* F *parallèlement à* F°*. Enfin, si* $(u_1, \ldots, u_k)$ *est une base de* F*, on a*

$$\forall x \in \mathrm{E} \qquad p_{\mathrm{F}} x = \sum_{i=1}^{k} \langle x \mid u_i\rangle\, u_i$$

14.3.2 Automorphismes orthogonaux

Définition 14.3.2
Soit $(\mathrm{E}, \langle\ |\ \rangle$ un espace euclidien. Soit $f : \mathrm{E} \longrightarrow \mathrm{E}$ une application. On dira que

- f *préserve les distances* si, et seulement si,

$$\forall x, y \in \mathrm{E} \qquad \|f(x) - f(y)\| = \|x - y\|$$

- f *préserve le produit scalaire* si, et seulement si,

$$\forall x, y \in \mathrm{E} \qquad \langle f(x) \mid f(y)\rangle = \langle x \mid y\rangle$$

- f *préserve la norme* si, et seulement si,

$$\forall x \in \mathrm{E} \qquad \|f(x)\| = \|x\|$$

Le très joli résultat qui suit dit que, essentiellement, ces trois propriétés sont équivalentes.

Lemme 14.3.3
Soit $(\mathrm{E}, \langle\ |\ \rangle)$ *un espace euclidien de dimension n non nulle. Soit* f *une application de* E *dans* E*. Les assertions suivantes sont équivalentes :*

1. *f préserve les distances et $f(0)=0$;*
2. *f préserve le produit scalaire ;*
3. *f est linéaire et il existe une base orthonormée $(e_1,\dots,e_n)$ de* E *telle que $(f(e_1),\dots,f(e_n))$ soit une base orthonormée ;*
4. *f est linéaire et préserve la norme.*

De plus, si f satisfait une de ces propriétés, c'est un automorphisme de E.

Ce théorème est particulièrement joli et puissant ; en particulier parce que le seul fait de préserver les distances et le vecteur nul (assertion 1) ou le produit scalaire (assertion 2) suffit à assurer la linéarité (assertions 3 et 4).

Preuve : Supposons que f préserve la distance. Comme $f(0)=0$, on a immédiatement que

$$\forall x\in \mathrm{E} \qquad \|f(x)\| = \|f(x)-f(0)\| = \|x-0\| = \|x\|$$

Par suite, si x et y sont dans E, on a

$$\begin{aligned}\|x-y\|^2 = \|f(x)-f(y)\|^2 &= \|f(x)\|^2+\|f(y)\|^2-2\langle f(x)\mid f(y)\rangle\\ &= \|x\|^2+\|y\|^2-2\langle f(x)\mid f(y)\rangle\\ \|x-y\|^2 &= \|x-y\|^2+2\langle x\mid y\rangle-2\langle f(x)\mid f(y)\rangle\end{aligned}$$

d'où $$\forall x,y\in \mathrm{E} \qquad \langle f(x)\mid f(y)\rangle = \langle x\mid y\rangle$$

La deuxième assertion est vraie.

Supposons maintenant que f préserve le produit scalaire. Soit $(e_1,\dots,e_n)$ une base orthonormée de E. On a

$$\forall i,j\in[\![1\,;n]\!] \qquad \langle f(e_i)\mid f(e_j)\rangle = \langle e_i\mid e_j\rangle$$

Ainsi, $(f(e_1),\dots,f(e_n))$ est une famille orthonormée de E. Elle est donc libre ; mais comme E est de dimension n, c'est une base orthonormée de E.

Reste à montrer que f est linéaire. C'est assez simple : prenons x et y dans E et λ dans $\mathbb{R}$. Alors

$$\begin{aligned}\|f(\lambda x+y)-\lambda f(x)-f(y)\|^2 = \|f(\lambda x+y)\|^2+\|f(x)\|^2+\|f(y)\|^2&\\ -2\lambda\langle f(\lambda x+y)\mid f(x)\rangle-2\langle f(\lambda x+y)\mid f(y)\rangle-2\langle f(x)\mid f(y)\rangle&\end{aligned}$$

Comme f préserve le produit scalaire, il vient

$$\begin{aligned}\|f(\lambda x+y)-\lambda f(x)-f(y)\|^2 &= \|\lambda x+y\|^2+\|x\|^2+\|y\|^2-2\lambda\langle\lambda x+y\mid x\rangle-2\langle\lambda x+y\mid y\rangle-2\langle x\mid y\rangle\\ &= \|(\lambda x+y)-\lambda x-y\|^2=0\end{aligned}$$

Par suite, $f(\lambda x+y)-\lambda f(x)-f(y)=0$: f est bien linéaire. La proposition 3 est vraie. En outre, elle transforme une base en une base, donc c'est un automorphisme de E.

Supposons que f est linéaire et qu'il existe une base orthonormée $(e_1,\dots,e_n)$ de E telle que $(f(e_1),\dots,f(e_n))$ soit orthonormée. Soit x un vecteur dans E. Comme $(e_1,\dots,e_n)$ est orthonormée, on a

$$x=\sum_{k=1}^{n}\langle x\mid e_k\rangle\, e_k$$

donc $$\|x\|^2=\sum_{k=1}^{n}|\langle x\mid e_k\rangle|^2 \qquad \text{et} \qquad f(x)=\sum_{k=1}^{n}\langle x\mid e_k\rangle\, f(e_k)$$

Mais $(f(e_1),\dots,f(e_n))$ est aussi une base orthonormée d'où

$$\|f(x)\|^2 = \sum_{k=1}^{n} |\langle x \mid e_k\rangle|^2 = \|x\|^2$$

Ainsi, f préserve la norme et 4 est vraie.

Enfin, supposons que f est linéaire et préserve la norme. Immédiatement, $\|f(0)\| = \|0\|$ donc $f(0) = 0$. Et comme f est linéaire,

$$\forall x, y \in \mathrm{E} \qquad \|f(x) - f(y)\| = \|f(x-y)\| = \|x-y\|$$

La proposition 1 est vraie. □

Définition 14.3.4 (Automorphismes orthogonaux)
Soit $(\mathrm{E}, \langle\ |\ \rangle$ un espace euclidien. Toute application de E dans E, qui vérifie une des propriétés équivalentes du **lemme 3.3**, est appelée *automorphisme orthogonal de* E.

L'ensemble des automorphismes orthogonaux de E est noté $\mathscr{O}(\mathrm{E})$.

Définition 14.3.5 (Matrices orthogonales)
Soient $n \in \mathbb{N}^\star$ et $\mathrm{M} \in \mathrm{M}_n(\mathbb{R})$. On dit que M est une matrice orthogonale si, et seulement si, ${}^t\mathrm{M}\,\mathrm{M} = \mathrm{I}_n$.

L'ensemble des matrices $n \times n$ orthogonales est noté $\mathrm{O}_n(\mathbb{R})$.

Proposition 14.3.6
Soit n un entier non nul. $\mathrm{O}_n(\mathbb{R})$ *est un sous-groupe de* $\mathrm{GL}_n(\mathbb{R})$. *Toute matrice orthogonale a pour déterminant 1 ou* -1.

Si $\mathrm{M} \in \mathrm{M}_n(\mathbb{R})$, *on note* $\mathrm{C}_1,\dots,\mathrm{C}_n$ *ses colonnes et* $\mathrm{L}_1,\dots,\mathrm{L}_n$ *ses lignes. Les assertions suivantes sont équivalentes :*

1. $\mathrm{M} \in \mathrm{O}_n(\mathbb{R})$;
2. ${}^t\mathrm{M} \in \mathrm{O}_n(\mathbb{R})$;
3. $\mathrm{C}_1,\dots,\mathrm{C}_n$ *est une base orthonormée de* $\mathbb{R}^n$ *pour le produit scalaire canonique ;*
4. ${}^t\mathrm{L}_1,\dots,{}^t\mathrm{L}_n$ *est une base orthonormée de* $\mathbb{R}^n$ *pour le produit scalaire canonique.*

Preuve : Si $\mathrm{M} \in \mathrm{O}_n(\mathbb{R})$, alors ${}^t\mathrm{M}\mathrm{M} = \mathrm{I}_n$ donc M est inversible à gauche et son inverse à gauche est ${}^t\mathrm{M}$. Mais on sait qu'inversibilité à gauche équivaut à inversibilité à droite donc $\mathrm{M} \in \mathrm{GL}_n(\mathbb{R})$ et $\mathrm{M}\,{}^t\mathrm{M} = \mathrm{I}_n$. Ceci démontre en même temps que les assertions *1* et *2* sont équivalentes, et que $\mathrm{O}_n(\mathbb{R}) \subset \mathrm{GL}_n(\mathbb{R})$. En outre, on a

$$\det({}^t\mathrm{M}\mathrm{M}) = (\det {}^t\mathrm{M})(\det \mathrm{M}) = (\det \mathrm{M})^2$$

donc si M est orthogonale, son déterminant vaut 1 ou -1.

Montrons que $\mathrm{O}_n(\mathbb{R})$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$. Soient M et N deux matrices orthogonales. Par définition,

$${}^t\mathrm{M}\,\mathrm{M} = \mathrm{I}_n \qquad \text{et} \qquad {}^t\mathrm{N}\mathrm{N} = \mathrm{I}_n$$

Alors $${}^t(\mathrm{MN})\mathrm{MN} = ({}^t\mathrm{N}\,{}^t\mathrm{M})\mathrm{MN} = {}^t\mathrm{N}({}^t\mathrm{M}\mathrm{M})\mathrm{N} = {}^t\mathrm{N}\mathrm{N} = \mathrm{I}_n$$

donc $\mathrm{O}_n(\mathbb{R})$ est stable par produit. Enfin, si M est orthogonale, on a vu que $\mathrm{M}^{-1} = {}^t\mathrm{M}$ est aussi orthogonale. Ainsi, $\mathrm{O}_n(\mathbb{R})$ est bien un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.

On note $\langle\ |\ \rangle_c$ le produit scalaire canonique dans $\mathbb{R}^n$. On se donne $\mathrm{M} \in \mathrm{O}_n(\mathbb{R})$; ses colonnes sont netées $(\mathrm{C}_1,\dots,\mathrm{C}_n)$:

$$\forall i \in [\![1\,;n]\!] \qquad \mathrm{C}_i = \begin{bmatrix} m_{1,i} \\ \vdots \\ m_{n,i} \end{bmatrix}$$

Si i et j sont dans $[\![1\,;n]\!]$, on remarque que

$$\langle \mathrm{C}_i \mid \mathrm{C}_j \rangle_c = \sum_{k=1}^{n} m_{k,i}\, m_{k,j} = \sum_{k=1}^{n} ({}^t\mathrm{M})_{j,k} \mathrm{M}_{k,i} = ({}^t\mathrm{M}\mathrm{M})_{j,i}$$

Compte-tenu de ce calcul, on voit facilement que

$$\begin{aligned} \mathrm{M} \in \mathrm{O}_n(\mathbb{R}) &\iff {}^t\mathrm{M}\mathrm{M} = \mathrm{I}_n \\ &\iff \forall i,j \in [\![1\,;n]\!] \quad ({}^t\mathrm{M}\mathrm{M})_{j,i} = \delta_{i,j} \\ &\iff \forall i,j \in [\![1\,;n]\!] \quad \langle \mathrm{C}_i \mid \mathrm{C}_j \rangle_c = \delta_{i,j} \\ \mathrm{M} \in \mathrm{O}_n(\mathbb{R}) &\iff (\mathrm{C}_1, \dots, \mathrm{C}_n) \text{ est une base orthonormée de } \mathbb{R}^n \end{aligned}$$

Ceci montre que *1* et *3* sont équivalentes. On procède de même pour *2* et *4*. □

Définition 14.3.7
Soit $n \in \mathbb{N}^\star$. L'ensemble des matrices orthogonales $n \times n$, dont le déterminant vaut 1, est appelé *groupe spécial orthogonal d'ordre* n et on le note $\mathrm{SO}_n(\mathbb{R})$. C'est un sous-groupe de $\mathrm{O}_n(\mathbb{R})$ et ses éléments sont appelés des *rotations*.

Théorème 14.3.8
Soient $(\mathrm{E}, \langle \mid \rangle)$ *euclidien,* $f \in \mathscr{L}(\mathrm{E})$ *et* $\mathscr{B}$ *une base orthonormée de* E. *Alors* f *est un automorphisme orthogonal si, et seulement si, sa matrice dans la base* $\mathscr{B}$ *est othogonale.*

> Ce théorème peut être reformulé d'une manière plus abstraite, mais aussi plus claire. Si l'on note $n \neq 0$ la dimension de E et $\mathscr{B}$ une base quelconque de E, on sait qu'on a un isomorphisme d'anneaux
>
> $$\begin{aligned} \mathrm{Mat}_{\mathscr{B}} : \ \mathscr{L}(\mathrm{E}) &\longrightarrow \mathrm{M}_n(\mathbb{R}) \\ f &\longmapsto \mathrm{Mat}_{\mathscr{B}} f \end{aligned}$$
>
> On sait déjà que $\mathrm{Mat}_{\mathscr{B}}$ réalise un isomorphisme de groupes entre $\mathscr{GL}(\mathrm{E})$ et $\mathrm{GL}_n(\mathbb{R})$. Le théorème précédent nous dit aussi que, si $\mathscr{B}$ est orthonormée, alors $\mathrm{Mat}_{\mathscr{B}}$ est aussi un isomorphisme de groupes entre $\mathscr{O}(\mathrm{E})$ et $\mathrm{O}_n(\mathbb{R})$.

Preuve : Notons $\mathscr{B} = (e_1, \dots, e_n)$ notre base orthonormée et $\mathrm{M} = \mathrm{Mat}_{\mathscr{B}} f$:

$$\mathrm{M} = \begin{bmatrix} m_{1,1} & \cdots & m_{1,n} \\ \vdots & & \vdots \\ m_{n,1} & \cdots & m_{n,n} \end{bmatrix}$$

Par définition, si $i \in [\![1\,;n]\!]$, la i-ème colonne de M donne les coordonnées de $f(e_i)$ dans la base $\mathscr{B}$:

$$\forall i \in [\![1\,;n]\!] \qquad f(e_i) = \sum_{k=1}^{n} m_{k,i}\, e_k$$

Comme la base $\mathscr{B}$ est orthonormée, si $i, j \in [\![1\,;n]\!]$, on a

$$\langle f(e_i) \mid f(e_j) \rangle = \sum_{k=1}^{n} m_{k,i} m_{k,j} = \langle \mathrm{C}_i \mid \mathrm{C}_j \rangle_c$$

On voit que $(f(e_1),\dots,f(e_n))$ est orthonormée si, et seulement si, $(C_1,\dots,C_n)$ est orthonormée dans $\mathbb{R}^n$, ce qui équivaut à dire (**proposition 3.6**) que M est une matrice orthogonale. □

Proposition 14.3.9
Soient $(E,\langle\,|\,\rangle)$ *un espace euclidien et* $\mathscr{B}$ *une base orthonormée. Soit* $\mathscr{B}'$ *une autre base de* E. *Alors* $\mathscr{B}'$ *est orthonormée si, et seulement si, la matrice de passage* $P_{\mathscr{B}}^{\mathscr{B}'}$ *est orthogonale. Dans ce cas,* $det_{\mathscr{B}}(\mathscr{B}')$ *vaut 1 ou* -1.

Preuve : Notons $\mathscr{B}=(e_1,\dots,e_n)$ et $\mathscr{B}'=(e'_1,\dots,e'_n)$. La matrice de passage $P_{\mathscr{B}}^{\mathscr{B}'}$ est aussi la matrice, par rapport à la base $\mathscr{B}$, de l'application linéaire f qui transforme chaque e_i en e'_i. En utilisant le **lemme 3.3** et le **théorème 3.7**, on a

$$\begin{aligned}(e'_1,\dots,e'_n)\text{ orthonormée} &\iff (f(e_1),\dots,f(e_n))\text{ orthonormée}\\ &\iff f\in\mathscr{O}(E)\\ &\iff P_{\mathscr{B}}^{\mathscr{B}'}=\mathrm{Mat}_{\mathscr{B}}f\in O_n(\mathbb{R})\end{aligned}$$

Si l'on suppose que $\mathscr{B}'$ est orthonormée, alors $\det_{\mathscr{B}}\mathscr{B}'$ est le déterminant de la matrice de passage $P_{\mathscr{B}}^{\mathscr{B}'}$, qui vaut 1 ou -1 puisqu'il s'agit d'une matrice orthogonale. □

On peut voir immédiatement un intérêt de travailler avec des bases orthonormées. En effet, lors d'un changement de base orthonormée, la matrice de passage P est orthogonale : son inverse est donc ${}^tP$, ce qui rend son calcul absolument trivial.

Ainsi, supposons que f est un endomorphisme d'un espace euclidien, $\mathscr{B}$ et $\mathscr{B}'$ sont deux bases orthonormées. On note

$$M=\mathrm{Mat}_{\mathscr{B}}f\qquad M'=\mathrm{Mat}_{\mathscr{B}'}f\qquad P=P_{\mathscr{B}}^{\mathscr{B}'}$$

On a tout simplement $M'={}^tPMP$ et $M=PM'{}^tP$.

Définition 14.3.10 (Orientation d'une base)
Soient $(E,\langle\,|\,\rangle)$ un espace euclidien et $\mathscr{B}$, $\mathscr{B}'$ deux bases de E. On dit qu'elles *ont la même orientation* si, et seulement si, $\det_{\mathscr{B}}\mathscr{B}'=1$.

Dans la mesure où $\det_{\mathscr{B}}\mathscr{B}'=(\det_{\mathscr{B}'}\mathscr{B})^{-1}$ (voir cours sur les déterminants), on voit que $\mathscr{B}$ et $\mathscr{B}'$ ont la même orientation si, et seulement si, $\mathscr{B}'$ et $\mathscr{B}$ ont la même orientation.

Et si l'on a trois bases orthonormées $\mathscr{B}$, $\mathscr{B}'$ et $\mathscr{B}''$, telles que $\mathscr{B}$ et $\mathscr{B}'$ ont la même orientation, et $\mathscr{B}'$ et $\mathscr{B}''$ aussi, alors (cours sur les déterminants) :

$$\det_{\mathscr{B}}\mathscr{B}''=(\det_{\mathscr{B}}\mathscr{B}')(\det_{\mathscr{B}'}\mathscr{B}'')=1$$

On a donc montré que

Proposition 14.3.11
« Avoir la même orientation » est une relation d'équivalence sur l'ensemble des bases orthonormées d'un espace euclidien E.

Définition 14.3.12 (Orientation de l'espace)
Soit $(E,\langle\,|\,\rangle)$ un espace euclidien. On dit qu'*on a orienté* E si on a choisi une classe d'équivalence C pour la relation « avoir la même orientation ». Dans ce cas, les bases de la classe C sont dites *directes* et celles qui ne sont pas dans C sont dites *indirectes*.

Exemple 14.3.13
Dans l'espace euclidien $\mathbb{R}^3$, on choisit l'orientation donnée par la base canonique (e_1, e_2, e_3). Considérons les vecteurs

$$v_1 = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\1\end{bmatrix} \qquad v_2 = \frac{1}{\sqrt{2}}\begin{bmatrix}-1\\0\\1\end{bmatrix}$$

On a déjà $v_1 \perp v_2$ et ces deux vecteurs sont orthogonaux à e_2. Donc on peut former les deux bases orthonormées (v_1, v_2, e_2) et $(v_1, v_2, -e_2)$. Il est certain qu'une des deux est directe, puisque

$$\det(v_1, v_2, -e_2) = -\det(v_1, v_2, e_2)$$

On calcule
$$\det(v_1, v_2, e_2) = \begin{vmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{vmatrix} = \frac{1}{2}\begin{vmatrix} 1 & -1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{vmatrix} = -1$$

Ainsi, pour notre choix d'orientation de l'espace, la base orthonormée (v_1, v_2, e_2) est indirecte, tandis que $(v_1, v_2, -e_2)$ est directe. Observons que d'après la propriété d'antisymétrie du déterminant, (v_1, e_2, v_2) est directe, par exemple.

14.3.3 Symétries orthogonales et réflexions

On a déjà vu dans le cours sur les espaces vectoriels que si $E = F \oplus G$ est une décomposition de E en deux sous-espaces supplémentaires, on peut définir la projection p_F sur F parallèlement à G, et la symétrie s_F par rapport à F, parallèlement à G.

Dans le cas où E est euclidien et F est un sous-espace vectoriel, on a une décomposition privilégiée $E = F \oplus F^\circ$, et donc une manière privilégiée de projeter sur F, ou de symétriser par rapport à F. On a d'ailleurs vu (**théorème 2.10**) que la projection orthogonale sur F est précisément la projection sur F parallèlement à F°.

On suppose dans ce paragraphe que $(E, \langle\,|\,\rangle)$ est euclidien de dimension $n \geqslant 2$.

Définition 14.3.14 (Symétrie orthogonale)
Soit F un sous-espace de E. On appelle *symétrie orthogonale* par rapport à F, notée s_F, la symétrie par rapport à F, parallèlement à F°.

Autrement dit, la symétrie orthogonale s_F, par rapport à F, est la symétrie associée à la somme directe orthogonale $E = F \oplus F^\circ$. Rappelons ce que cela signifie : si $x \in E$, il se décompose suivant cette somme directe

$$x = \underbrace{p_F(x)}_{\in F} + \underbrace{p_{F^\circ}(x)}_{\in F^\circ}$$

Par définition, $s_F(x)$ garde la composante de x suivant F, et change la composante suivant F° en son opposé :

$$s_F(x) = p_F(x) - p_{F^\circ}(x) = 2p_F(x) - \mathrm{id}(x)$$

Proposition 14.3.15
Toute symétrie orthogonale est un automorphisme orthogonal de E. *Réciproquement, toute symétrie de* E, *qui est un automorphisme orthogonal de* E, *est une symétrie orthogonale.*

Preuve : Soit F un sous-espace de E et s_F la symétrie orthogonale par rapport à F. Si $x \in E$, on a

$$x = p_F(x) + p_{F^\circ}(x) \qquad s_F(x) = p_F(x) - p_{F^\circ}(x) \qquad \text{avec} \qquad p_F(x) \perp p_{F^\circ}$$

donc $$\|s_F(x)\|^2 = \|p_F(x)\|^2 + \|p_{F^\circ}(x)\|^2 = \|x\|^2$$

d'après le théorème de Pythagore : s_F préserve la norme. Comme elle est aussi linéaire, c'est un automorphisme orthogonal de E.

Réciproquement, soit s une symétrie de E, qui soit aussi un automorphisme orthogonal de E. Alors il existe des sous-espaces supplémentaires F et G, tels que s soit la symétrie par rapport à F, parallèlement à G. Montrons que F et G sont orthogonaux : soient $x \in F$ et $y \in G$. Par définition de s,

$$s(x) = x \qquad s(y) = -y$$

donc $$x + y = s(x) - s(y) = s(x - y)$$

Mais s est un automorphisme orthogonal donc préserve la norme et

$$\|x + y\| = \|s(x - y)\| = \|x - y\|$$

Ainsi, $$4\langle x \mid y\rangle = \|x + y\|^2 - \|x - y\|^2 = 0$$

ce qui prouve bien que $x \perp y$. Par suite, s est une symétrie orthogonale. □

Définition 14.3.16 (Réflexion)
Soit $f \in \mathscr{L}(E)$. On dit que f est une *réflexion* si, et seulement si, f est la symétrie orthogonale par rapport à un hyperplan.

Proposition 14.3.17
Toute réflexion de E *est un automorphisme orthogonal de* E*, de déterminant* -1.

Preuve : Soit r une réflexion de E. Par définition, r est la symétrie orthogonale par rapport à un hyperplan H de E. D'après la **proposition 3.15**, c'est un automorphisme orthogonal de E.

Notons $n \geqslant 2$ la dimension de E. On sait que r est la symétrie orthogonale par rapport à un hyperplan H. Donc H est de dimension $n-1$ et H° est une droite, de dimension 1. On prend une base $(e_1, \ldots, e_{n-1})$ de H et une base (e_n) de H°. Alors $\mathscr{B} = (e_1, \ldots, e_{n-1}, e_n)$ est une base de E. De plus, par définition de r comme symétrie par rapport à H, parallèlement à H°, on sait que

$$\forall x \in H \qquad r(x) = x \qquad \forall x \in H^\circ \qquad r(x) = -x$$

Par suite, $$\mathrm{Mat}_{\mathscr{B}} r = \begin{bmatrix} I_{n-1} & 0 \\ 0 & -1 \end{bmatrix}$$

et le déterminant de r vaut bien -1. □

Théorème 14.3.18 (Décomposition en produit de réflexions)
Soit $(E, \langle\,|\,\rangle)$ *un espace euclidien de dimension* $n \geqslant 2$. *Tout automorphisme orthogonal de* E *peut être décomposé en produit d'au plus n réflexions.*

Preuve : On démontre ceci par récurrence sur la dimension de E. Le cas des espaces de dimension 2 sera traité dans le prochain paragraphe et on l'admet pour l'instant.

Soit $n \geqslant 2$ un entier. On suppose que tout automorphisme orthogonal d'un espace euclidien de dimension n peut être décomposé en produit d'au plus n réflexions. Soient E un espace euclidien de dimension $n+1$ et $f \in \mathscr{O}(\mathrm{E})$. On se donne une base orthonormée $\mathscr{B} = (e_1, \dots, e_n, e_{n+1})$ de E et on distingue deux cas :

- **Si $f(e_{n+1}) = e_{n+1}$** : Comme f est orthogonal et que $e_1, \dots, e_n$ sont orthogonaux à e_{n+1}, il vient que $f(e_1), \dots, f(e_{n+1})$ sont aussi orthogonaux à e_{n+1}. Donc

$$f\big(\mathrm{Vect}\,(e_1, \dots, e_n)\big) \subset \{e_{n+1}\}^\circ = \mathrm{Vect}\,(e_1, \dots, e_n)$$

Ainsi, f induit un endomorphisme de $\mathrm{F} = \mathrm{Vect}\,(e_1, \dots, e_n)$; plus précisément, si l'on définit

$$\forall x \in \mathrm{F} \qquad \tilde{f}(x) = f(x)$$

alors $\tilde{f}$ est un endomorphisme de F. En outre, $\tilde{f} \in \mathscr{O}(\mathrm{F})$ puisque

$$\forall x, y \in \mathrm{F} \qquad \langle \tilde{f}(x) \mid \tilde{f}(y) \rangle = \langle f(x) \mid f(y) \rangle = \langle x \mid y \rangle$$

D'après l'hypothèse de récurrence, il existe des réflexions $\tilde{r}_1, \dots, \tilde{r}_k$ de F, avec $k \leqslant n$, telles que $\tilde{f} = \tilde{r}_1 \cdots \tilde{r}_k$.
Pour chaque $j \in [\![1\,;k]\!]$, on note r_j l'endomorphisme de E qui vaut $\tilde{r}_j$ sur F et qui envoie e_{n+1} sur e_{n+1}. Alors r_j est une symétrie puisque $r_j^2 = \mathrm{id}$ sur F et sur $\mathrm{Vect}\, e_{n+1}$. De plus, si $x \in \mathrm{E}$, il se décompose de manière unique en $x = x_\mathrm{F} + y$ avec $y = \langle x \mid e_n \rangle\, e_n$ orthogonal à F ; donc

$$r_j(x) = r_j(x_\mathrm{F}) + r_j(y) = \underbrace{\tilde{r}_j(x_\mathrm{F})}_{\in \mathrm{F}} + y$$

et $$\|r_j(x)\|^2 = \|\tilde{r}_j(x_\mathrm{F})\|^2 + \|y\|^2 = \|x_\mathrm{F}\|^2 + \|y\|^2 = \|x\|^2$$

ce qui démontre que $r_j \in \mathscr{O}(\mathrm{E})$. D'après la proposition **3.15**, r_j est une symétrie orthogonale. Enfin, il est facile de voir que r_j est une réflexion puisque

$$\mathrm{Ker}\,(\tilde{r}_j - \mathrm{id}) \subset \mathrm{Ker}\,(r_j - \mathrm{id}) \qquad \text{et} \qquad e_{n+1} \in \mathrm{Ker}\,(r_j - \mathrm{id})$$

donc $$\mathrm{Ker}\,(\tilde{r}_j - \mathrm{id}) \oplus \mathrm{Vect}\,(e_{n+1}) \subset \mathrm{Ker}\,(r_j - \mathrm{id})$$

Mais $$\dim \mathrm{Ker}\,(\tilde{r}_j - \mathrm{id}) = n-1 \qquad \text{donc} \qquad \dim \mathrm{Ker}\,(r_j - \mathrm{id}) \geqslant n$$

et cette dimension n'est pas $n+1$, puisque r_j est une réflexion sur F, donc a au moins un vecteur qui n'est pas invariant. Ce qui démontre bien que r_j est une réflexion.
Mais on a $f = r_1 \cdots r_k$ puisque cette relation est vérifiée sur F et sur $\mathrm{Vect}\,(e_{n+1})$. Donc f peut être décomposé en produit d'au plus n réflexions.
- **Si $f(e_{n+1}) \neq e_{n+1}$** : Dans ce cas, on remarque que

$$e_{n+1} = \frac{1}{2}(e_{n+1} - f(e_{n+1})) + \frac{1}{2}(e_{n+1} + f(e_{n+1}))$$

et $$\langle e_{n+1} - f(e_{n+1}) \mid e_{n+1} + f(e_{n+1}) \rangle = \|e_{n+1}\|^2 - \|f(e_{n+1})\|^2 = 0$$

parce que $f \in \mathscr{O}(\mathrm{E})$ et préserve la norme. Si on note g la réflexion autour de l'hyperplan $(e_{n+1} - f(e_{n+1}))^\circ$, on a par définition

$$g(e_{n+1} - f(e_{n+1})) = -(e_{n+1} - f(e_{n+1})) = f(e_{n+1}) - e_{n+1}$$

et $g(e_{n+1} + f(e_{n+1})) = e_{n+1} + f(e_{n+1})$ car $(e_{n+1} + f(e_{n+1})) \perp (e_{n+1} - f(e_{n+1}))$

Ainsi, $$g(e_{n+1}) = f(e_{n+1})$$

et $$gf(e_{n+1}) = g^2(e_{n+1}) = e_{n+1}$$

car g est une symétrie. Donc $gf \in \mathscr{O}(\mathrm{E})$ et il fixe e_{n+1}. D'après le premier cas étudié, gf se décompose en produit d'au plus n réflexions. Mais $f = g(gf)$ se décompose alors en produit d'au plus $n+1$ réflexions. Ce qui achève la récurrence. □

La preuve de ce théorème explique comment faire, en pratique, pour décomposer un automorphisme orthogonal f en produit de réflexions. On commence par se donner une base orthonormée $(e_1, \dots, e_n)$ de l'espace. On note g_n la réflexion autour de l'hyperplan orthogonal à $e_n - f(e_n)$. Alors $g_n f$ est un automorphisme orthogonal qui fixe e_n et induit un automorphisme orthogonal de $\mathrm{Vect}(e_1, \dots, e_{n-1})$. On recommence alors la même procédure : on note g_{n-1} la réflexion autour de l'hyperplan $e_{n-1} - g_n f(e_{n-1})$. Alors $g_{n-1} g_n f$ est un automorphisme orthogonal qui fixe e_{n-1} et e_n. Et ainsi de suite.

Exemple 14.3.19
On considère la matrice

$$\mathrm{M} = \frac{1}{3}\begin{bmatrix} -2 & 2 & 1 \\ 2 & 1 & 2 \\ 1 & 2 & -2 \end{bmatrix} \in \mathrm{O}_3(\mathbb{R})$$

M représente un automorphisme orthogonal de $\mathbb{R}^3$ dans la base canonique ; on identifie l'automorphisme et sa matrice. Posons

$$u_3 = e_3 - \mathrm{M}e_3 = \frac{1}{3}\begin{bmatrix} -1 \\ -2 \\ 5 \end{bmatrix}$$

La projection orthogonale P_3 sur $\mathrm{Vect}\, u_3$ est donnée par

$$\forall x \in \mathbb{R}^3 \qquad \mathrm{P}_3(x) = \left\langle x \,\middle|\, \frac{u_3}{\|u_3\|} \right\rangle \frac{u_3}{\|u_3\|} = \frac{\langle x \mid u_3 \rangle}{\|u_3\|^2} u_3$$

et la réflexion autour de $(u_3)^\circ$ est donnée par

$$\forall x \in \mathbb{R}^3 \qquad \mathrm{S}_3 = \mathrm{I}_3 - 2\mathrm{P}_3$$

Après calculs, $$\mathrm{P}_3 = \frac{1}{30}\begin{bmatrix} 1 & 2 & -5 \\ 2 & 4 & -10 \\ -5 & -10 & 25 \end{bmatrix} \qquad \mathrm{S}_3 = \mathrm{I}_3 - 2\mathrm{P}_3 = \frac{1}{15}\begin{bmatrix} 14 & -2 & 5 \\ -2 & 11 & 10 \\ 5 & 10 & -10 \end{bmatrix}$$

Également, $$\mathrm{S}_3\mathrm{M} = \frac{1}{5}\begin{bmatrix} -4 & 4 & 0 \\ 4 & 3 & 0 \\ 0 & 0 & 5 \end{bmatrix}$$

On voit que, comme prévu, $\mathrm{S}_3\mathrm{M}$ induit un automorphisme orthogonal de $\mathrm{Vect}(e_1, e_2)$. On recommence, en travaillant cette fois avec e_2. Posons

$$u_2 = e_2 - \mathrm{S}_3\mathrm{M}e_2 = \frac{1}{5}\begin{bmatrix} -4 \\ 2 \\ 0 \end{bmatrix}$$

La projection orthogonale P_2 sur $\mathrm{Vect}\, u_2$ et la réflexion S_2 autour de $(u_2)^\perp$ sont données par

$$\forall x \in \mathbb{R}^3 \qquad \mathrm{P}_2(x) = \frac{\langle x \mid u_2 \rangle}{\|u_2\|^2} u_2 \qquad \mathrm{S}_2 = \mathrm{I}_3 - 2\mathrm{P}_2$$

Tous calculs faits, $$P_2 = \frac{1}{5}\begin{bmatrix} 4 & -2 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad S_2 = I_3 - 2P_2 = \frac{1}{5}\begin{bmatrix} -3 & 4 & 0 \\ 4 & 3 & 0 \\ 0 & 0 & 5 \end{bmatrix}$$

On remarque que $S_2 = S_3 M$, donc $S_3 M$ était déjà une réflexion. Du coup, une décomposition de M en produit de réflexions est

$$M = S_3 S_2 = \frac{1}{15}\begin{bmatrix} 14 & -2 & 5 \\ -2 & 11 & 10 \\ 5 & 10 & -10 \end{bmatrix} \times \frac{1}{5}\begin{bmatrix} -3 & 4 & 0 \\ 4 & 3 & 0 \\ 0 & 0 & 5 \end{bmatrix}$$

Cette procédure nous a même permis d'identifier géométriquement ces transformations : appliquer M, c'est la même chose que

- faire une réflexion autour du plan $(u_2)^\circ$, d'équation $-2x + y = 0$;
- suivie d'une réflexion autour du plan $(u_3)^\circ$, d'équation $x + 2y - 5z = 0$.

14.4 Automorphismes orthogonaux en dimension 2

L'étude du groupe orthogonal en dimension 2 est très simple. Étant donné un réel θ, on note

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \qquad S(\theta) = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}$$

On peut remarquer que ces matrices sont orthogonales, de déterminants respectifs 1 et -1. Par définition, $R(\theta)$ est une rotation de $\mathbb{R}^2$. Un simple dessin montre qu'il s'agit effectivement de la rotation d'angle θ.

Identifions la nature géométrique de $S(\theta)$. À tout hasard, on se demande s'il ne s'agit pas, peut-être, d'une réflexion. Auquel cas, il suffit de trouver $\mathrm{Ker}\,(S(\theta) - I_2)$ et $\mathrm{Ker}\,(S(\theta) + I_2)$. Un calcul facile prouve que

$$\mathrm{Ker}\,(S(\theta) - I_2) = \mathrm{Vect}\left(\begin{bmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{bmatrix}\right) \qquad \mathrm{Ker}\,(S(\theta) + I_2) = \mathrm{Vect}\left(\begin{bmatrix} -\sin\frac{\theta}{2} \\ \cos\frac{\theta}{2} \end{bmatrix}\right)$$

Géométriquement, $S(\theta)$ est donc la symétrie orthogonale autour de la droite qui fait un angle $\frac{\theta}{2}$ avec l'axe des abscisses.

On remarque aussi, par le calcul, que conformément à l'intuition,

$$\forall \theta, \varphi \in \mathbb{R} \qquad R(\theta)\,R(\varphi) = R(\theta + \varphi)$$

$$\forall \theta \in \mathbb{R} \qquad R(\theta)^{-1} = {}^t R(\theta) = R(-\theta)$$

et

$$\forall \theta \in \mathbb{R} \qquad R(\theta) = I_2 \iff \theta \in 2\pi\mathbb{Z}$$

De manière plus abstraite, mais aussi plus jolie, on vient de montrer que $R : \theta \longmapsto R(\theta)$ est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(SO_2(\mathbb{R}), \cdot)$, de noyau $2\pi\mathbb{Z}$.

Montrons qu'il est surjectif. Donnons-nous

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SO_2(\mathbb{R})$$

Ceci signifie que les colonnes de M forment une base orthonormée de $\mathbb{R}^2$ pour le produit scalaire canonique, et que $\det M = 1$. Ce qui fournit les relations :

$$\begin{cases} a^2+c^2=1 \\ b^2+d^2=1 \\ ab+cd=0 \\ ad-bc=1 \end{cases}$$

À l'aide des deux premières relations et de l'étude des fonctions sinus et cosinus, il existe des réels θ et φ dans $[0;2\pi[$, tels que

$$a=\cos\theta \qquad c=\sin\theta \qquad b=\sin\varphi \qquad d=-\cos\varphi$$

Ensuite, $$1=ad-bc=\cos\theta\cos\varphi+\sin\theta\sin\varphi=\cos(\theta-\varphi)$$

donc θ et φ sont égaux modulo 2π. Mais comme ils sont dans $[0;2\pi[$, ils sont égaux. Ainsi, $M=R(\theta)$ et on a montré que

Théorème 14.4.1 (Paramétrisation de $SO_2(\mathbb{R})$)
L'application R *est un morphisme surjectif de* $(\mathbb{R},+)$ *sur* $SO_2(\mathbb{R})$*, de noyau* $2\pi\mathbb{Z}$*. En particulier,* $SO_2(\mathbb{R})$ *est commutatif et*

$$SO_2(\mathbb{R})=\{R(\theta)\mid\theta\in\mathbb{R}\}$$

Le même raisonnement montre que tout automorphisme orthogonal de déterminant -1 est une réflexion de la forme $S(\theta)$. Comme toute matrice orthogonale est de déterminant 1 ou -1,

$$O_2(\mathbb{R})=\underbrace{\{R(\theta)\mid\theta\in\mathbb{R}\}}_{=SO_2(\mathbb{R})}\cup\{S(\theta)\mid\theta\in\mathbb{R}\}$$

Intéressons-nous maintenant à la structure multiplicative de ces réflexions. $S(\theta)$. Qu'obtient-on si on les compose ? Le calcul montre que

$$\forall\theta,\varphi\in\mathbb{R} \qquad S(\theta)S(\varphi)=R(\theta-\varphi)$$

Par conséquent, toute rotation peut s'écrire comme produit de deux réflexions : en effet, si $\theta\in\mathbb{R}$, on a $R(\theta)=S(\theta)S(0)$. Mais cette décomposition n'est pas unique, évidemment : il suffit de prendre deux réels quelconques φ et ψ, tels que $\varphi-\psi=\theta\ [2\pi]$, pour avoir $R(\theta)=S(\varphi)S(\psi)$.

Enfin, que donne le produit d'une rotation et d'une réflexion du type $S(\theta)$? Il suffit encore de faire le calcul

$$\forall\theta,\varphi\in\mathbb{R} \qquad S(\theta)R(\varphi)=S(\theta)S(\theta)S(\theta-\varphi)=S(\theta-\varphi)$$

et $$\forall\theta,\varphi\in\mathbb{R} \qquad R(\varphi)S(\theta)=S(\varphi+\theta)S(\theta)S(\theta)=S(\varphi+\theta)$$

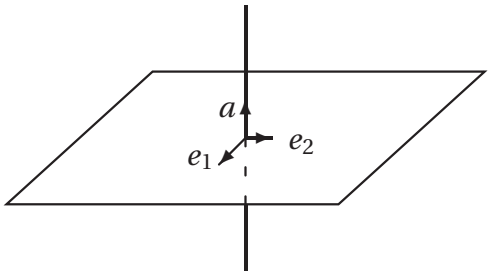
Il est intéressant de remarquer comme chacun de ces calculs est simple, et fournit immédiatement un résultat géométrique sans le moindre effort. Par exemple : si l'on fait une rotation d'angle φ, suivie d'une réflexion autour de la droite qui fait un angle $\theta/2$ avec l'horizontale, on obtient le même résultat que si l'on fait une réflexion autour de la droite qui fait un angle $\frac{\theta-\varphi}{2}$ avec l'horizontale. Ce n'est pas évident à voir géométriquement ; mais c'est trivial par le calcul matriciel.

14.5 Automorphismes orthogonaux en dimension 3

Commençons par expliquer comment il est possible d'orienter un plan, connaissant un vecteur normal à celui-ci.

Proposition 14.5.1 (Orientation d'un plan par un vecteur normal)
Soit E *un espace euclidien orienté de dimension 3. Soit* $a \in$ E *de norme 1. Il existe une unique orientation de* $P = (a)^\circ$ *telle que, pour toute base orthonormée directe* (e_1, e_2) *de* P*, la famille* (e_1, e_2, a) *est une base orthonormée directe de* E.

Cette proposition peut faire peur, mais ce qu'elle dit est intuitivement très simple : l'orientation d'une droite de E détermine de manière « naturelle » une orientation de son plan orthogonal.



Supposons avoir choisi l'orientation habituelle de $\mathbb{R}^3$, dans laquelle la base caonique est directe. On prend une base orthonormée (e_1, e_2) de $(a)^\circ$ comme sur le dessin, de manière à avoir (e_1, e_2, a) orthonormée directe. On souhaite choisir une orientation de $(a)^\circ$: naturellement, on décide de dire que (e_1, e_2) est directe.

Preuve : On sait que P a des bases orthonormées et on en prend une $(\varepsilon_1, \varepsilon_2)$. Alors $(\varepsilon_1, \varepsilon_2, a)$ est une base orthonormée de E. Si elle est directe, on pose

$$u_1 = \varepsilon_1 \qquad u_2 = \varepsilon_2$$

et si elle est indirecte, on pose

$$u_1 = \varepsilon_2 \qquad u_2 = \varepsilon_1$$

On a ainsi une base orthonormée directe (u_1, u_2, a) de E, telle que (u_1, u_2) est une base orthonormée de P.

On choisit alors comme orientation pour P celle donnée par (u_1, u_2). Par définition, ceci veut dire que, si (e_1, e_2) est une base orthonormée de P, elle est directe si, et seulement si,

$$\det_{(u_1,u_2)}(e_1, e_2) = 1$$

Maintenant, si (e_1, e_2) est une base orthonormée directe de P, la matrice de la famille (e_1, e_2) dans (u_1, u_2) est orthogonale, de déterminant 1. Donc il existe $\theta \in \mathbb{R}$ tel que la matrice de (e_1, e_2) dans la base (u_1, u_2) soit

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

Par suite, la matrice de (e_1, e_2, a) dans la base directe (u_1, u_2, a) est

$$\begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Son déterminant vaut 1, donc (u_1, u_2, a) est directe. Ceci démontre bien l'existence d'une orientation de P qui a la propriété demandée.

Pour l'unicité, c'est simple : supposons avoir choisi l'autre orientation de P. Ceci signifie que (u_1, u_2) est indirecte dans P, donc (le déterminant est alterné) que (u_2, u_1) est directe dans P. Alors la base (u_2, u_1, a) est indirecte dans E, toujours d'après les propriétés du déterminant. Et cette orientation ne satisfait pas la propriété voulue. □

Identifions maintenant les rotations d'un espace euclidien de dimension 3.

Proposition 14.5.2
Soient E *un espace euclidien de dimension 3 et* $f \in \mathscr{SO}(\mathrm{E})$. *Il existe une base orthonormée directe* $\mathscr{B} = (u, v, w)$ *de* E, *et* $\theta \in \mathbb{R}$, *tels que*

$$Mat_{\mathscr{B}}(f) = \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

On dit que f *est la rotation d'angle* θ *autour du vecteur* w.

Preuve : Si f est l'identité, la proposition est évidente puisque sa matrice est I_3 dans n'importe quelle base orthonormée ; il suffit alors de prendre $\theta = 0$.

Supposons alors que f n'est pas l'identité. Comme E est de dimension 3, f peut se décomposer comme produit d'une, deux ou trois réflexions. Mais f est dans $\mathscr{SO}(\mathrm{E})$ donc son déterminant vaut 1 ; par suite, f est le produit de deux réflexions distinctes r_1 et r_2. Par définition, $\mathrm{Ker}(r_1 - \mathrm{id})$ et $\mathrm{Ker}(r_2 - \mathrm{id})$ sont de dimension 2. D'après la relation de Grassmann, leur intersection est de dimension 1 : il existe w, de norme 1, tel que $r_1(w) = r_2(w) = w$. Par suite,

$$f(w) = r_1 r_2(w) = w$$

On note $\mathrm{P} = (w)^\circ$, qui est un plan. On l'oriente par son vecteur normal w, à l'aide de la **proposition 5.1**. Comme f préserve l'orthogonalité et que $f(w) = w$, P est stable par f : en effet,

$$\forall x \in \mathrm{P} \qquad \langle f(x) \mid w \rangle = \langle f(x) \mid f(w) \rangle = \langle x \mid w \rangle = 0$$

Donc f induit un automorphisme orthogonal de P. Et f ne fixe aucun vecteur de P, puisque $\mathrm{Ker}(f - \mathrm{id}) = \mathrm{Vect}\, w$. D'après l'étude des automorphismes orthogonaux en dimension 2, f est une rotation sur P. Alors si (u, v) est une base orthonormée directe de P, on trouve $\theta \in \mathbb{R}$ tels que la matrice de f dans la base (u, v) soit

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

Par suite, (u, v, w) est une base orthonormée directe de E, dans laquelle la matrice de f a la forme voulue. □

La preuve de ce théorème nous dit, à nouveau, comment faire pour identifier une rotation f. On commence par chercher $\mathrm{Ker}(f - \mathrm{id})$, qui est nécessairement de dimension 1 et on prend un vecteur w dedans, de norme 1.

Ensuite, on détermine le plan $\mathrm{P} = (w)^\circ$ et on en choisit une base orthonormée (u, v) telle que (u, v, w) soit orthonormée directe. La matrice de f dans cette base aura alors la bonne forme.

Exemple 14.5.3
On reprend la matrice de l'**exemple 3.19** :

$$M = \frac{1}{3}\begin{bmatrix} -2 & 2 & 1 \\ 2 & 1 & 2 \\ 1 & 2 & -2 \end{bmatrix}$$

Le calcul de son déterminant, ou bien sa décomposition comme produit de deux réflexions, prouvent qu'il s'agit d'une rotation. On recherche $\mathrm{Ker}(M - I_3)$ et le calcul donne

$$\mathrm{Ker}(M - I_3) = \mathrm{Vect}\begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}$$

et on pose $$w = \frac{1}{\sqrt{6}}\begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}$$

Pour trouver une base orthonormée de $(w)^\circ$, il y a plusieurs méthodes. On peut en chercher une base, et utiliser Schmidt pour l'orthonormer. Mais on peut aller plus vite, puisqu'on est dans $\mathbb{R}^3$: il est clair que

$$u = \frac{1}{\sqrt{5}}\begin{bmatrix} 0 \\ 1 \\ -2 \end{bmatrix}$$

est orthogonal à w et de norme 1. On pose alors

$$v = w \wedge u = \frac{1}{\sqrt{30}}\begin{bmatrix} 5 \\ -2 \\ -1 \end{bmatrix}$$

D'après les propriétés du produit vectoriel, (u, v, w) est une base orthonormée directe de $\mathbb{R}^3$. On peut alors trouver l'angle de la rotation M en décomposant Mu dans la base orthonormée (u, v) de $(w)^\circ$:

$$Mu = \frac{1}{\sqrt{5}}\begin{bmatrix} 0 \\ 1 \\ -2 \end{bmatrix} = -u$$

> Sur cet exemple, la décomposition de Mu s'obtient immédiatement. Mais en général, c'est à peine plus difficile puisque $Mu = \langle Mu \mid u\rangle\, u + \langle Mu \mid v\rangle\, v$.

Par suite, dans la base orthonormée directe (u, v, w), la matrice de M est

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

ou encore $$M = \frac{1}{30}\begin{bmatrix} 0 & 5 & \sqrt{5} \\ \sqrt{6} & -2 & 2\sqrt{5} \\ -2\sqrt{6} & -1 & \sqrt{5} \end{bmatrix}\begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & \sqrt{6} & -2\sqrt{6} \\ 5 & -2 & -1 \\ \sqrt{5} & 2\sqrt{5} & \sqrt{5} \end{bmatrix}$$

M est la rotation autour de w, d'angle π.