

2021-2022



Mathématiques
MP2I



Hugo SALOU

TABLE DES MATIÈRES

Table des matières	i
0 Logique (rudiments)	1
1 Algèbre de Boole	1
2 Déduction naturelle	4
3 Raisonnement par l'absurde	4
4 Prédicat	5
1 Calculs algébriques	6
1 Sommes	6
2 Formules à connaître	11
3 Sommes doubles	14
4 Sommes sur un ensemble fini	15
5 Produits	16
6 Rappels sur \ln et \exp	16
2 Nombres complexes	18
1 Trigonométrie	18
2 Nombres complexes de module 1	22
3 Géométrie des nombres complexes	24
4 Exponentielle complexe	32
5 Fonctions de \mathbb{R} dans \mathbb{C}	33
3 Étude de fonctions	38
1 Calculs de limites	39
2 Asymptotes, branches paraboliques et prolongement par continuité	41
4 Fonctions usuelles	44
1 Logarithme népérien	44
2 Exponentielle	48
3 Fonctions puissances	50
4 Exponentielle et logarithme de base a	53
5 Fonctions trigonométriques	55
6 Fonctions trigonométriques réciproques	58
7 Trigonométrie hyperbolique	64

5	Calcul intégral	69
1	Généralités	69
6	Équations différentielles linéaires	72
1	74
2	Annexe	75
7	Développements limités	76
8	Ensembles, applications, relations et lois de composition	80
1	Théorie naïve des ensembles	80
2	Applications	84
3	Relations binaires	90
4	Lois de composition	97
5	Divers	101
9	Inégalités dans \mathbb{R}	105
1	105
2	105
3	105
4	Bornes supérieures	105
5	Partie entière	108
6	Densité	108
7	109
8	109
9	Propriétés de (\mathbb{R}, \leq)	111
10	Inégalités Classiques	113
11	Valeur Absolue	116
12	Bornes Inférieure / Supérieure	117
13	Partie Entière	120
14	Densité	121
15	Intervalles	122
16	Fonction Convexes	125
10	Nombres entiers - \mathbb{N}	132
1	Axiomatique de \mathbb{N}	132
2	Récurrence	133
3	Divisibilité	135
4	Arithmétique modulaire	138
5	Axiomatique de \mathbb{N}	141
6	Réurrences	142
7	Divisibilité	143
8	Division Euclidienne	144
9	Arithmétique Modulaire	146
10	PGCD et PPCM	148
11	Décomposition en Facteurs Premiers	154
11	Suites numériques	157
1	Modes de définition	157
2	Limites	157
3	Limites et inégalités	165
4	Suites extraites	171
5	Suites récurrentes	175
6	Comparaison de suites	177
7	Suites complexes	180
8	Annexe	183
12	Structures algébriques usuelles	186
1	Groupes	186
2	Anneaux	198
3	Corps	204
4	Actions de groupes	206
5	Bilan	207

13 Systèmes linéaires et calculs matriciels	208
14 Continuité	217
1 Définition d'une limite de fonctions	217
2 Continuité uniforme	227
3 Fonctions à valeurs dans \mathbb{C}	231
4 Annexe	231
15 Espaces vectoriels	233
1 Définition et premières propriétés	233
2 Sous-espaces vectoriels	235
3 Familles de vecteurs	243
16 Dérivation	252
1 Définition et premières propriétés	252
2 Théorème de Rolle et accroissements finis	254
3 Dérivées n -ièmes	258
4 Fonctions à valeurs complexes	262
17 Dimension finie	264
18 Polynômes formels	272
1 Définition	272
2 Évaluation	278
3 Arithmétique dans $\mathbb{K}[X]$	282
4 L'espace vectoriel $\mathbb{K}[X]$	294
19 Applications linéaires	301
1 Premières propriétés	301
2 Noyau et image	304
3 Théorème du rang	306
4 Formes linéaires	309
5 Projections et symétries	315
20 Fractions rationnelles	320
1 Construction de $\mathbb{K}(X)$	320
2 Décomposition en éléments simples	325
21 Matrices et applications linéaires	336
1 Matrices d'un vecteur	336
2 Matrice d'une famille de vecteurs	337
3 Matrices d'une application linéaire	340
4 Formules de changement de bases	345
5 Conséquences	352
6 Matrices par blocs	356
22 Fonctions de deux variables	360
1 Quelques généralités	360
2 Topologie de \mathbb{R}^2	361
3 Dérivation	369
23 Dénombrement	380
1 Cardinal d'un ensemble	380
2 Dénombrement	387
3 Preuves combinatoires	392
4 Bilan	394
24 Groupe symétrique	395
1 Mise en situation	395
2 Cycles	397
3 Transpositions	402
4 Signature d'une permutation	403
5 Bilan	405

25 Séries numériques	407
1 Définitions et premières propriétés	407
2 Séries à termes positifs	409
3 Comparaison avec une intégrale	410
4 Opérations sur les séries	413
5 Séries absolument convergente	414
6 Séries alternées	415
7 Résumé et exemples	416
8 Applications	419
8.1 Formule de Stirling	419
8.2 Développement décimal	422
8.3 Exponentielle	425
26 Déterminant	427
1 Motivation	427
2 Définitions	428
3 Déterminant d'un endomorphisme	432
4 Déterminant d'une matrice carrée	434
5 Développement suivant une ligne ou une colonne	437
27 Espace probabilisé fini	442
1 Définitions	442
2 Probabilité conditionnelle	444
3 Événements indépendants	451
4 Bilan	453
28 Sous-espaces affines d'un espace vectoriel	455
1 Espace affine (HORS PROGRAMME)	455
2 Sous-espaces affines	458
3 Parallélisme et hyperplans	460
4 Repère affine	460
29 Produit scalaire	462
1 Définitions	462
2 Quelques formules	464
3 Familles orthogonales	466
4 Projection orthogonale	471
5 Annexe	477
5.1 Produit vectoriel	477
5.2 Calcul différentiel	479
5.3 Séries de Fourier	480
5.4 Espace-temps de Minkowsky	481
30 Intégrale de Riemann	483
1 Intégrale d'une fonction en escaliers	483
2 Sommes de Darboux	485
3 Propriétés de l'intégrale	488
4 Théorème fondamental de l'Analyse	492
5 Fonctions continues par morceaux	494
6 Sommes de Riemann	495
7 Retour sur les formules de Taylor	497
8 Fonctions réglées	499
31 Variables aléatoires	500
1 Définitions	500
2 Exemples de lois	501
3 Couples de variables aléatoires	502
4 Familles de variables aléatoires	503
5 Espérance d'une variable aléatoire	504
6 Variance	507
7 Covariance (HORS-PROGRAMME)	511
8 Loi des grands nombres	512

32 Familles sommables	516
1 Motivation	516
2 Familles sommables positives	516
3 Familles sommables réelles	520
4 Familles sommables de nombres complexes	524
5 Produit de Cauchy de deux séries	525
33 Annexe	527
1 Algorithme de Metropolis-Hastings	527
2 Gradient automatique	528
Index	531

CHAPITRE

0

LOGIQUE (RUDIMENTS)

Définition: Un proposition est un énoncé qui est soit vrai, soit faux.

EXEMPLE:

$A : "B \text{ est vraie } "$ $B : "A \text{ est fausse } "$ $\left. \begin{array}{l} A \\ B \end{array} \right\}$ Le système $\{A, B\}$ est une auto-contradiction

Définition: Démontrer une proposition revient à prouver qu'elle est vraie.

1 Algèbre de Boole

Définition: Soient A et B deux propositions. La proposition A et B est définie par la table de vérité suivante :

A	B	A et B
V	V	V
V	F	F
F	V	F
F	F	F

Définition: Soient A et B deux propositions. La proposition A ou B est définie par la table de vérité suivante :

A	B	$A \text{ ou } B$
V	V	V
V	F	V
F	V	V
F	F	F

Définition: Soit A une proposition. La négation de A , notée $\text{non}(A)$ est définie par :

A	$\text{non}(A)$
V	F
F	V

Définition: Deux propositions A et B sont équivalentes si elles ont la même table de vérité. Dans ce cas, on note $A \iff B$.

Proposition: Soient A , B et C trois propositions.

1. $(A \text{ et } B) \text{ et } C \iff A \text{ et } (B \text{ et } C)$
2. $A \text{ et } A \iff A$
3. $A \text{ et } B \iff B \text{ et } A$
4. $(A \text{ ou } B) \text{ ou } C \iff A \text{ ou } (B \text{ ou } C)$
5. $A \text{ ou } A \iff A$
6. $A \text{ ou } B \iff B \text{ ou } A$
7. $\text{non}(\text{non}(A)) \iff A$
8. $A \text{ et } (B \text{ ou } C) \iff A \text{ et } B \text{ ou } A \text{ et } C$
9. $A \text{ ou } (B \text{ et } C) \iff (A \text{ ou } B) \text{ et } (A \text{ et } C)$
10. $\text{non}(A \text{ et } B) \iff \text{non}(A) \text{ ou } \text{non}(B)$
11. $\text{non}(A \text{ ou } B) \iff \text{non}(A) \text{ et } \text{non}(B)$

Preuve:

8.

A	B	C	$B \text{ ou } C$	$A \text{ et } (B \text{ ou } C)$	$A \text{ et } B$	$A \text{ et } C$	$(A \text{ et } B) \text{ ou } (A \text{ et } C)$
V	V	V	V	V	V	V	V
V	V	F	V	V	F	F	V
V	F	V	V	V	F	V	V
V	F	F	F	F	F	F	F
F	V	V	V	F	F	F	F
F	V	F	V	F	F	F	F
F	F	V	V	F	F	F	F
F	F	F	F	F	F	F	F

10.

A	B	A et B	non (A et B)	non (A)	non (B)	non (A) ou non (B)
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

□

Définition: Soient A et B deux propositions. La proposition $A \implies B$ (A implique B) est définie par :

A	B	$A \implies B$
V	V	V
V	F	F
F	V	V
F	F	V

Définition: Soient A et B deux propositions telles que $A \implies B$ est vraie. On dit que A est une condition suffisante pour que B soit vraie. On dit que B est une condition nécessaire pour que A soit vraie.

Proposition (Contraposée): Soient A et B deux propositions.

$$(A \implies B) \iff (\text{non } B \implies \text{non } A)$$

A	B	non A	non B	non $B \implies \text{non } A$	$A \implies B$
V	V	F	F	V	V
V	F	F	V	F	F
F	V	V	F	V	V
F	F	V	V	V	V

□

Proposition: Soient A et B deux propositions.

$$(A \implies B) \iff ((A \implies B) \text{ et } (B \implies A))$$

Preuve:

A	B	$A \iff B$	$A \implies B$	$B \implies A$	$(A \implies B) \text{ et } (B \implies A)$
V	V	V	V	V	V
V	F	F	F	V	F
F	V	F	V	F	F
F	F	V	V	V	V

□

Proposition: Soient A et B deux propositions.

$$(A \implies B) \iff (B \text{ ou non } (A))$$

Preuve:

On obtient par contraposée

$$\text{non } (A \implies B) \iff (A \text{ et non } (B))$$

donc

$$\begin{aligned} (A \implies B) &\iff \text{non } (A \text{ et non } (B)) \\ &\iff \text{non } (A) \text{ ou } \text{non } (\text{non } (B)) \\ &\iff \text{non } (A) \text{ ou } B \\ &\iff B \text{ ou non } (A) \end{aligned}$$

□

2 Déduction naturelle

Dans ce paragraphe, A et B sont deux propositions.

A et B

Comment démontrer A et B ?

- On démontre A
- On démontre B

Comment utiliser l'hypothèse A et B ?

On utilise A ou on utilise B .

A ou B

Comment démontrer A ou B ?

On essaie de démontrer A . Si on y arrive, alors on a prouvé A ou B sinon on démontre B .

Variante

On suppose A faux. On démontre B .

Comment utiliser l'hypothèse A ou B ?

On fait une disjonction des cas :

- Cas 1 : On suppose A
- Cas 2 : On suppose B

$A \implies B$

Comment démontrer $A \implies B$?

On suppose A . On démontre B .

Comment utiliser l'hypothèse $A \implies B$?

On démontre A . On utilise B .

3 Raisonnement par l'absurde

Situation :

Soient A et B deux propositions.
On veut montrer $A \implies B$.

On suppose A. On suppose aussi B faux.
On cherche à faire apparaître une contradiction (\neg)

4 Prédicat

Définition: Un prédicat $P(x)$ est un énoncé dont la valeur de vérité dépend de l'objet x , élément d'un ensemble E .

Le domaine de validité de P est l'ensemble des valeurs x de E pour lesquelles $P(x)$ est vraie :

$$\{x \in E \mid P(x)\}$$

REMARQUE (Notation):

On écrit

$$\forall x \in E, P(x)$$

pour dire que $P(x)$ est vraie pour tous les x de E .

On écrit

$$\exists x \in E, P(x)$$

pour dire qu'il existe (au moins) un élément $x \in E$ pour lequel $P(x)$ est vraie.

On écrit

$$\exists! x \in E, P(x)$$

pour dire qu'il existe un unique élément $x \in E$ tel que $P(x)$ est vraie.

$$\boxed{\forall x \in E, P(x)}$$

Comment démontrer $\forall x \in E, P(x)$?

Soit $x \in E$ (fixé quelconque). Montrons $P(x)$.

Comment utiliser $\forall x \in E, P(x)$?

On choisit (spécialise) une ou plusieurs (voir toutes) valeurs de x et on exploite $P(x)$.

EXEMPLE:

Soient $a, b, c \in \mathbb{R}$. On suppose que

$$\forall n \in \mathbb{N}, a + b \times 2^n + c \times 3^n$$

Montrons que $a = b = c = 0$.

$$\text{On sait que } (S) : \begin{cases} a + b + c = 0 & (n = 0) \\ a + 2b + 3c = 0 & (n = 1) \\ a + 4b + 9c = 0 & (n = 2) \end{cases}$$

$$(S) \iff \begin{cases} a + b + c = 0 \\ b + 2c = 0 \\ 3b + 8c = 0 \end{cases} \iff \begin{cases} a + b + c = 0 \\ b + 2c = 0 \\ 2c = 0 \end{cases} \iff \begin{cases} c = 0 \\ b = 0 \\ a = 0 \end{cases}$$

CHAPITRE

1

CALCULS ALGÉBRIQUES

1 Sommes

REMARQUE (Notation):

Soit $(u_n)_{n \in \mathbb{N}}$ une suite de nombres complexes. Pour $p \leq q \in \mathbb{N}$, on note

$$\sum_{k=p}^q u_k$$

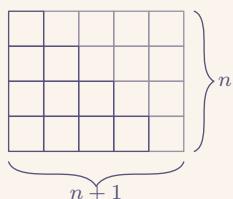
le nombre $u_p + u_{p+1} + \dots + u_q$.

Par convention,

$$\sum_{k=p}^q u_k = 0 \quad \text{si } q < p.$$

EXEMPLE:

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



Proposition: Soit $(u_n)_{n \in \mathbb{N}}$ une suite de nombres complexes.

$$\forall n \in \mathbb{N}, \sum_{k=0}^n u_k = \sum_{k=0}^n u_{n-k}$$

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

$$\begin{aligned} \sum_{k=0}^n u_{n-k} &= u_n + u_{n-1} + u_{n-2} + \cdots + u_0 \\ &= u_0 + u_1 + u_2 + \cdots + u_n \\ &= \sum_{k=0}^n u_k \end{aligned}$$

□

Proposition: Soient $(u_n)_{n \in \mathbb{N}}$ une suite de nombres complexes, $(p, q, r, s) \in \mathbb{N}^4$ et $\varphi : \llbracket p, q \rrbracket \rightarrow \llbracket r, s \rrbracket$ une bijection (i.e. $\forall y \in \llbracket r, s \rrbracket, \exists! x \in \llbracket p, q \rrbracket, \varphi(x) = y$).

Alors,

$$\sum_{k=r}^s u_k = \sum_{k=p}^q u_{\varphi(k)}.$$

Preuve:

$$\begin{aligned} \sum_{k=p}^q u_{\varphi(k)} &= u_{\varphi(p)} + u_{\varphi(p+1)} + \cdots + u_{\varphi(q)} \\ \sum_{k=r}^s u_k &= u_r + u_{r+1} + \cdots + u_s \end{aligned}$$

Comme φ est bijective, chaque terme u_k avec $k \in \llbracket r, s \rrbracket$ apparaît une fois et une seule fois dans la somme

$$u_{\varphi(p)} + u_{\varphi(p+1)} + \cdots + u_{\varphi(q)}.$$

Ainsi, les deux sommes sont identiques. □

EXEMPLE:

On pose

$$\forall k \in \mathbb{N}, u_k = \frac{1}{k-4}.$$

On pose également $\varphi : \llbracket 1, 5 \rrbracket \rightarrow \llbracket -1, 3 \rrbracket$: une bijection.

Alors,

$$\sum_{k=-1}^3 \frac{1}{k-4} = -\frac{1}{5} - \frac{1}{4} - \frac{1}{3} - \frac{1}{2} - 1$$

et

$$\begin{aligned} \sum_{k=1}^5 u_{\varphi(k)} &= \frac{1}{\varphi(1)-4} + \frac{1}{\varphi(2)-4} + \frac{1}{\varphi(3)-4} + \frac{1}{\varphi(4)-4} + \frac{1}{\varphi(5)-4} \\ &= -\frac{1}{5} - \frac{1}{3} - \frac{1}{3} - \frac{1}{2} - 1. \end{aligned}$$

EXEMPLE:

Soit φ la bijection définie par

$$\varphi : \llbracket 1, 5 \rrbracket \longrightarrow \llbracket 1, 5 \rrbracket$$

$$k \longmapsto \begin{cases} 2 & \text{si } k = 1 \\ 3 & \text{si } k = 2 \\ 1 & \text{si } k = 3 \\ 4 & \text{si } k = 4 \\ 5 & \text{si } k = 5 \end{cases}$$

$$\begin{aligned} \sum_{k=1}^5 u_k &= u_1 + u_2 + u_3 + u_4 + u_5 \\ \sum_{k=1}^5 u_{\varphi(k)} &= u_2 + u_3 + u_1 + u_4 + u_5 \end{aligned}$$

Proposition (télescopage): Soit $(u_k)_{k \in \mathbb{N}}$ une suite de nombres complexes.

$$\forall p \leq q \in \mathbb{N}, \sum_{k=p}^q (u_{k+1} - u_k) = u_{q+1} - u_p.$$

Preuve: MÉTHODE1 Soient $p \leq q$.

$$\begin{aligned} \sum_{k=p}^q (u_{k+1} - u_k) &= \cancel{u_{p+1}} - u_p + \cancel{u_{p+2}} - \cancel{u_{p+1}} \cdots + u_{q+1} - \cancel{u_q} \\ &= u_{q+1} - u_p \end{aligned}$$

MÉTHODE2 Soient $p \leq q$.

$$\sum_{k=p}^q (u_{k+1} - u_k) = \sum_{k=p}^q u_{k+1} - \sum_{k=p}^q u_k$$

Soit $\varphi : \frac{\llbracket p, q \rrbracket}{k} \longrightarrow \frac{\llbracket p+1, q+1 \rrbracket}{k+1}$. φ est bijective donc

$$\sum_{k=p}^q u_{k+1} = \sum_{k=p}^q u_{\varphi(k)} = \sum_{k=p+1}^{q+1} u_k.$$

D'où,

$$\begin{aligned} \sum_{k=p}^q (u_{k+1} - u_k) &= \sum_{k=p+1}^{q+1} u_k - \sum_{k=p}^q u_k \\ &= \left(u_{q+1} + \sum_{k=p+1}^q u_k \right) - \left(u_p + \sum_{k=p+1}^q u_k \right) \\ &= u_{q+1} - u_p \end{aligned}$$

□

REMARQUE (Analogie avec le calcul intégral):

$$\int_a^b f'(x) \, dx = f(b) - f(a).$$

EXEMPLE:

Calculer $\sum_{k=1}^n \frac{1}{k(k+1)}$ pour $n \in \mathbb{N}^*$.

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

$$\begin{aligned} \forall k \in \llbracket 1, n \rrbracket, \frac{1}{k(k+1)} &= \frac{(1+k)-k}{k(k+1)} \\ &= \frac{k+1}{k(k+1)} - \frac{k}{k(k+1)} \\ &= \frac{1}{k} - \frac{1}{k+1} \end{aligned}$$

et, par télescopage, on obtient donc

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

Par contre, on n'a pas de formule simple pour $\sum_{k=1}^n \frac{1}{k^2}$ (mais on sait que $\sum_{k=1}^n \xrightarrow{n \rightarrow +\infty} \frac{\pi^2}{6}$).

EXEMPLE (à connaître):

Calculer $\sum_{k=1}^n k^2$ et $\sum_{k=1}^n k^3$ pour $n \in \mathbb{N}^*$.

On cherche $(u_n)_{n \in \mathbb{N}}$ telle que

$$\forall k \in \mathbb{N}^*, u_{k+1} - u_k = k^2.$$

On cherche donc (u_k) sous la forme

$$\forall k \in \mathbb{N}^*, u_k = ak^3 + bk^2 + ck + d$$

avec $(a, b, c, d) \in \mathbb{R}^4$.

Soit $k \in \mathbb{N}^*$.

$$\begin{aligned} u_{k+1} - u_k &= a(k+1)^3 + b(k+1)^2 + c(k+1) + d - ak^3 - bk^2 - ck - d \\ &= a(k^3 + 3k^2 + 3k + 1) + b(k^2 + 2k + 1) + c(k + 1) - ak^3 - bk^2 - ck \\ &= k^2 \times a + k(3a + 2b) + (a + b + c) \end{aligned}$$

On résout le système

$$(S) : \begin{cases} 3a = 1, \\ 3a + 2b = 0, \\ a + b + c. \end{cases} \iff \begin{cases} a = \frac{1}{3}, \\ b = -\frac{1}{2}, \\ c = \frac{1}{2} - \frac{1}{3} = \frac{1}{6}. \end{cases}$$

On vient de montrer que,

$$\forall k \in \mathbb{N}^*, k^2 = u_{k+1} - u_k \quad \text{avec } u_k = \frac{1}{3}k^3 - \frac{1}{2}k^2 + \frac{1}{6}k.$$

Donc, par télescopage,

$$\begin{aligned} \forall n \in \mathbb{N}^*, \sum_{k=1}^n k^2 &= u_{n+1} - u_1 \\ &= \frac{1}{3}(n+1)^3 - \frac{1}{2}(n+1)^2 + \frac{1}{6}(n+1) - \frac{1}{3} + \frac{1}{2} - \frac{1}{6} \\ &= \frac{n+1}{6} (2(n+1)^2 - 3(n+1) + 1) \\ &= \frac{n+1}{6} (2n^2 + 4n + 2 - 3n - 3 + 1) \\ &= \frac{n(n-1)(2n+1)}{6} \end{aligned}$$

Proposition: Soit $n \in \mathbb{N}$ et $q \in \mathbb{C}$,

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

Preuve:

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

1.

$$\begin{aligned} (1-q) \sum_{k=0}^n q^k &= \sum_{k=0}^n q^k - q \sum_{k=0}^n q^k \\ &= \sum_{k=0}^n q^k - \sum_{k=0}^n q^{k+1} \\ &= \sum_{k=0}^n (q^k - q^{k+1}) \\ &= 1 - q^{n+1} \end{aligned}$$

Si $q \neq 1$,

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

Si $q = 1$,

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

2. On pose, pour $n \in \mathbb{N}$, $S_n = \sum_{k=0}^n q^k$.

On a, d'une part :

$$\forall n \in \mathbb{N}, S_{n+1} = \sum_{k=0}^{n+1} q^k = S_n + q^{n+1}$$

et d'autre part

$$\forall n \in \mathbb{N}, S_{n+1} = 1 + \sum_{k=1}^{n+1} q^k = 1 + qS_n.$$

Et donc,

$$\begin{aligned} \forall n \in \mathbb{N}, 1 + qS_n &= S_n + q^{n+1} \iff 1 + (q-1)S_n = q^{n+1} \\ &\iff S_n(q-1) = q^{n+1} - 1 \\ &\iff S_n = \frac{q^{n+1} - 1}{q-1} \text{ pour } q \neq 1. \end{aligned}$$

□

2 Formules à connaître

Définition: Soient $k, n \in \mathbb{N}$. On définit “ k parmi n ” par

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

Proposition: Avec les notations précédentes,

- 1. $\binom{n}{k} = \binom{n}{n-k}$
- 2. $\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}$

Preuve: 1. $\binom{n}{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$

2.

$$\begin{aligned} \binom{n}{k+1} + \binom{n}{k} &= \frac{n!(n-k)}{(k+1)!(n-k-1)!(n-k)} + \frac{n!(k+1)}{k!(n-k)!(k+1)} \\ &= \frac{n!(n-k+k+1)}{(k+1)!(n-k)!} \\ &= \frac{(n+1)!}{(k+1)!(n-k)!} \\ &= \binom{n+1}{k+1} \end{aligned}$$

□

Proposition (binôme de Newton): Soient $(a, b) \in \mathbb{C}^2$ et $n \in \mathbb{N}$. Alors

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

sauf si $\begin{cases} a + b = 0, \\ n = 0. \end{cases}$

REMARQUE (triangle de Pascal):

$n = 0$					1			
$n = 1$				1		1		
$n = 2$			1		2		1	
$n = 3$		1		3		3		1
$n = 4$	1		4		6		4	
$n = 5$	1	5		10		10	5	1
$n = 6$	1	6	15		20		15	6
								1

EXEMPLE:

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

Preuve:

Soient $(a, b) \in \mathbb{C}^2$.

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

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

avec la convention $\forall z \in \mathbb{C}, z^0 = 1$.

— Soit $n \in \mathbb{N}$. On suppose $P(n)$ vraie. Montrons $P(n+1)$.

$$\begin{aligned} (a + b)^{n+1} &= (a + b)(a + b)^n \\ &= (a + b) \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} \\ &= a \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} + b \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} \\ &= \sum_{k=0}^n \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^n a^k b^{n+1-k} \end{aligned}$$

On pose $\varphi : \begin{matrix} \llbracket 0, n \rrbracket \\ k \end{matrix} \longrightarrow \begin{matrix} \llbracket 1, n+1 \rrbracket \\ k+1 \end{matrix}$ bijective.

Donc,

$$\begin{aligned} \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} &= \sum_{k=0}^n u_{\varphi(k)} \\ &= \sum_{k=1}^{n+1} u_k \text{ où } \forall n \in \llbracket 1, n+1 \rrbracket, u_k = \binom{n}{k-1} a^k b^{n-k+1}. \end{aligned}$$

D'où

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

— Montrons $P(0)$ $(a+b)^0 = 1$.

$$\sum_{k=0}^0 \binom{0}{k} a^k b^{0-k} = \binom{0}{0} a^0 b^0 = 1 \times 1 \times 1$$

Donc,

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

□

EXEMPLE:

Calculer, pour tout $n \in \mathbb{N}$, $\sum_{k=0}^n (-1)^k \binom{n}{k}$. On applique la formule du binôme de Newton avec $a = -1$ et $b = 1$:

$$\forall n \in \mathbb{N}, \sum_{k=0}^n (-1)^k \binom{n}{k} = (-1+1)^n = \begin{cases} 0 & \text{si } n > 0, \\ 1 & \text{si } n = 0. \end{cases}$$

Proposition: Soient $(a, b) \in \mathbb{C}^2$ et $n \in \mathbb{N}$. Alors,

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

Preuve:

$$\begin{aligned}
(a - b) \sum_{k=0}^{n-1} a^k &= \sum_{k=0}^{n-1} a^{k+1} b^{n-1-k} + \sum_{k=0}^{n-1} a^k b^{n-k} \\
&= \sum_{k=0}^{n-1} (\underbrace{a^{k+1} b^{n-(k+1)}}_{u_{k+1}} - \underbrace{a^k b^{n-k}}_{u_k}) \\
&= u_n - u_0 \\
&= a^n - b^n
\end{aligned}$$

□

3 Sommes doubles

EXEMPLE:

$$\begin{aligned}
S &= \sum_{i=1}^n \sum_{j=1}^i a_{i,j} \\
S &= \sum_{j=1}^1 a_{1,j} + \sum_{j=1}^2 a_{2,j} + \sum_{j=3}^3 a_{3,j} + \cdots + \sum_{j=1}^n a_{n,j} \\
&= a_{11} \\
&\quad + a_{21} + a_{22} \\
&\quad + a_{31} + a_{32} + a_{33} \\
&\quad \vdots \\
&\quad + a_{n,1} + \cdots + a_{n,n}
\end{aligned}$$

EXEMPLE:

$$\begin{aligned}
\sum_{i=1}^n \sum_{j=1}^i &= \sum_{i=1}^n (2^i - 1) \\
&= \sum_{i=1}^n 2^i - n \\
&= 2 \times \frac{1 - 2^n}{1 - 2} - n \\
&= 2(2^n - 1) - n
\end{aligned}$$

EXEMPLE:

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

$$S = \sum_{j=1}^i \sum_{i=1}^n \binom{i}{j}$$

Aucun sens !

EXEMPLE:

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

$$S = \sum_{i=1}^n \sum_{j=i}^n \binom{i}{j}$$

On pose

$$a_{j,i} = \binom{i}{j}.$$

Alors,

$$\begin{aligned} S &= a_{11} + a_{12} + \cdots + \boxed{a_{1n}} \\ &\quad + a_{22} + \cdots + a_{2n} \\ &\quad \ddots \quad \vdots \\ &\quad + a_{nn} \end{aligned}$$

$$\begin{aligned} \sum_{j=1}^i a_{j,i} &= \sum_{j=1}^i \binom{i}{j} & \square &= \sum_{j=1}^n a_{j,n} = \sum_{j=1}^n \binom{n}{j} \\ &= 2^i - 1 & &= 2^n - 1 \end{aligned}$$

Donc,

$$\sum_{i=1}^n \sum_{j=1}^i \binom{i}{j} = 2(2^n - 1) - n.$$

4 Sommes sur un ensemble fini

Définition: Soit I un ensemble fini. Soit $(a_i)_{i \in I}$ une famille de nombres complexes.

On note $\sum_{i \in I} a_i$ la somme des éléments de cette famille.

EXEMPLE:

Soit $I = \{\clubsuit, \heartsuit, \spadesuit, \diamondsuit\}$. On pose

$$\begin{cases} a_{\heartsuit} = 0 \\ a_{\clubsuit} = -1 \\ a_{\spadesuit} = i \\ a_{\diamondsuit} = 1 + i. \end{cases}$$

Alors

$$\sum_{j \in I} a_j = 0 - 1 + i + 1 + i = 2i.$$

EXEMPLE:

Avec $I = \{x \mapsto x^2, x \mapsto x^3, x \mapsto x^4\}$, on pose $\forall i \in I, a_i = i(2)$.

Alors,

$$\sum_{i \in I} a_i = 2^2 + 2^3 + 2^4.$$

EXEMPLE:

$$\begin{aligned} - \sum_{k \in \llbracket 1, n \rrbracket} 2^k &= \sum_{k=1}^n 2^k = 2(2^n - 1). \\ - \sum_{\substack{k \in \llbracket 1, n \rrbracket \\ k \text{ pair}}} 2^k &= \sum_{\substack{1 \leq j \leq \frac{n}{2} \\ j \text{ entier}}} 2^{2j}. \end{aligned}$$

Proposition: Soit $\varphi : I \rightarrow J$ une bijection et $(a_j)_{j \in J}$ une famille de nombres com-

plexes. Alors

$$\sum_{j \in J} a_j = \sum_{i \in I} a_{\varphi(i)}.$$

□

EXEMPLE:

$$\sum_{i \in \{2, 4, 6, 8\}} a_i = \sum_{j=1}^4 a_{2j}.$$

EXEMPLE:

$$\begin{aligned} S &= \sum_{i=1}^n \sum_{j=i}^n a_{ij} = \sum_{(i,j) \in \{(1,1), \dots, (1,n), (2,2), \dots, (2,n), \dots, (n,n)\}} a_{ij} \\ &= \sum_{1 \leq i \leq j \leq n} a_{ij} \\ &= \sum_{j=1}^n \sum_{i=1}^j a_{ij}. \end{aligned}$$

5 Produits

Définition: Soit $(a_i)_{i \in I}$ une famille de nombres complexes.

On note $\prod_{i \in I} a_i$ le produit de ces éléments.

Proposition: Soit $(u_n)_{n \in \mathbb{N}}$ une suite de nombres complexes non nuls. Alors

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

□

REMARQUE (Δ Attention):

$$\prod_{i \in I} (\lambda a_i) = \lambda^{\#I} \times \prod_{i \in I} a_i$$

où $\#I$ est le nombre d'éléments de I .

6 Rappels sur \ln et \exp

Proposition:

— Soit $(a_i)_{i \in I}$ une famille finie de réels strictement positifs. Alors,

$$\ln \left(\prod_{i \in I} a_i \right) = \sum_{i \in I} \ln a_i.$$

— Soit $(b_i)_{i \in I}$ une famille de réels. Alors

$$\exp\left(\sum_{i \in I} b_i\right) = \prod_{i \in I} \exp(b_i).$$

REMARQUE:

Soit $f : I \rightarrow \mathbb{R}^*$ dérivable. On pose $g : x \mapsto \ln |f(x)|$.

Alors g est dérivable sur I et

$$\forall x \in I, g'(x) = \frac{f'(x)}{f(x)}$$

On dit que $\frac{f'}{f}$ est la dérivée logarithmique de f .

Soient $f_1, f_2 : I \rightarrow \mathbb{R}^*$ dérivables. Alors

$$\frac{(f_1 f_2)'}{f_1 f_2} = \frac{f'_1}{f_1} + \frac{f'_2}{f_2}.$$

REMARQUE:

Soit $a \in \mathbb{R}$.

- Soit $n \in \mathbb{N}^*$. Alors, $a^n = \overbrace{a \times a \times a \times \cdots \times a}^{n \text{ fois}}$.
- Soit $n \in \mathbb{Z}_*^-$. Si $a \neq 0$, alors $a^n = \frac{1}{a^{-n}}$.
- Si $a \neq 0$, $a^0 = 1$ et $\forall p, q \in \mathbb{Z}, a^p \times a^q = a^{p+q}$.
- Soit $p \in \mathbb{Z}$ et $a > 0$.

$$a^p = \exp(\ln a^p) = \exp(p \ln a) = e^{p \ln a}.$$

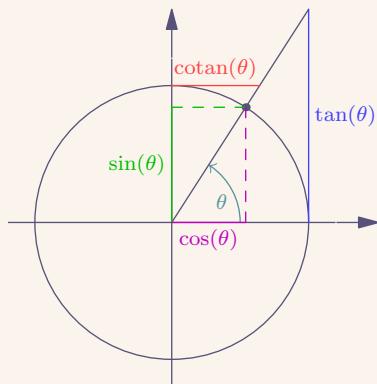
Définition: Soit $a \in \mathbb{R}_*^+$ et $p \in \mathbb{R}$. On pose $a^p = e^{p \ln a}$.

CHAPITRE

2

NOMBRES COMPLEXES

1 Trigonométrie



Définition: On définit, pour

$$\begin{aligned}\theta &\in \bigcup_{k \in \mathbb{Z}} \left[-\frac{\pi}{2} + k\pi, \frac{\pi}{2} + k\pi \right] \\ \iff \theta &\in \mathbb{R} \setminus \left\{ \frac{\pi}{2} + 2\pi k \mid k \in \mathbb{Z} \right\}\end{aligned}$$

la tangente de θ par

$$\tan \theta = \frac{\sin \theta}{\cos \theta}$$

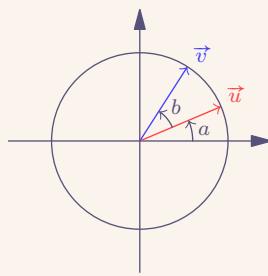
Définition: Pour $\theta \in \bigcup_{k \in \mathbb{Z}}] - k\pi, (k+1)\pi[$, on définit la contangente de θ par

$$\cotan \theta = \frac{\cos \theta}{\sin \theta}$$

Proposition: Soient $(a, b) \in \mathbb{R}^2$.

1. $\cos(-a) = \cos(a)$
2. $\cos(a + 2\pi) = \cos(a)$
3. $\cos(a + \pi) = -\cos(a)$
4. $\cos(\pi - a) = -\cos(a)$
5. $\sin(-a) = -\sin(a)$
6. $\sin(a + 2\pi) = \sin(a)$
7. $\sin(a + \pi) = -\sin(a)$
8. $\sin(\pi - a) = \sin(a)$
9. $\cos(a + b) = \cos(a) \cos(b) - \sin(a) \sin(b)$
10. $\sin(a + b) = \cos(a) \sin(b) + \sin(a) \cos(b)$
11. $\cos\left(\frac{\pi}{2} - a\right) = \sin(a)$
12. $\sin\left(\frac{\pi}{2} - a\right) = \cos(a)$

Preuve: 8. Soient $\vec{u} = (\cos(a), \sin(a))$ et $\vec{v} = (\cos(b), \sin(b))$



D'une part, $\vec{u} \cdot \vec{v} = \cos(a) \cos(b) + \sin(a) \sin(b)$

D'autre part, $\vec{u} \cdot \vec{v} = \|\vec{u}\| \times \|\vec{v}\| \times \cos(\widehat{\vec{u}, \vec{v}}) = \cos(a - b)$

On a montré que

$$\forall (a, b) \in \mathbb{R}^2, \cos(a - b) = \cos(a) \cos(b) + \sin(a) \sin(b)$$

$$\text{d'où } \forall (a, b) \in \mathbb{R}^2, \cos(a + b) = \cos(a) \cos(b) - \sin(a) \sin(b)$$

11. $\forall a \in \mathbb{R}, \cos\left(\frac{\pi}{2} - a\right) = \underbrace{\cos\left(\frac{\pi}{2}\right)}_{=0} \cos(a) + \underbrace{\sin\left(\frac{\pi}{2}\right)}_{=1} \sin(a) = \sin(a)$
12. $\forall a \in \mathbb{R}, \cos(a) = \cos\left(-a + \frac{\pi}{2} + \frac{\pi}{2}\right) = \sin\left(\frac{\pi}{2} - a\right)$
- 10.

$$\begin{aligned} \forall (a, b) \in \mathbb{R}^2, \sin(a + b) &= \cos\left(\left(\frac{\pi}{2} - a\right) - b\right) \\ &= \cos\left(\frac{\pi}{2} - a\right) \cos(b) + \sin\left(\frac{\pi}{2} - a\right) \sin(b) \\ &= \sin(a) \cos(b) + \cos(a) \sin(b) \end{aligned}$$

□

Proposition: Soient a et b deux réels tels que $a \not\equiv \frac{\pi}{2} [\pi]$ et $b \not\equiv \frac{\pi}{2} [\pi]$.

1. $\tan(a + \pi) = \tan(a)$
2. $\tan(-a) = -\tan(a)$
3. Si $a + b \not\equiv \frac{\pi}{2} [\pi]$, alors, $\tan(a + b) = \frac{\tan(a) + \tan(b)}{1 - \tan(a) \tan(b)}$

Preuve: 3. On suppose $a + b \not\equiv \frac{\pi}{2} [\pi]$

$$\begin{aligned}
\tan(a+b) &= \frac{\sin(a+b)}{\cos(a+b)} \\
&= \frac{\sin(a)\cos(b)+\sin(b)\cos(a)}{\cos(a)\cos(b)-\sin(a)\sin(b)} \\
&= \frac{\frac{\sin(a)\cos(b)}{\cos(a)\cos(b)} + \frac{\sin(b)\cos(a)}{\cos(a)\cos(b)}}{\frac{\cos(a)\cos(b)-\sin(a)\sin(b)}{\cos(a)\cos(b)}} \\
&= \frac{\tan(a)+\tan(b)}{1-\tan(a)\tan(b)}
\end{aligned}$$

□

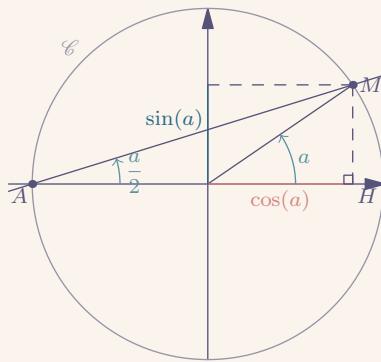
Proposition: Soit $a \in \mathbb{R}$.

1. Si $a \notin \frac{\pi}{2} [\pi]$, alors, $1 + \tan^2(a) = \frac{1}{\cos^2(a)}$
2. Si $a \notin \pi [2\pi]$
 - $\cos(a) = \frac{1 - \tan^2(\frac{a}{2})}{1 + \tan(\frac{a}{2})}$
 - $\sin(a) = \frac{2 \tan(\frac{a}{2})}{1 + \tan^2(\frac{a}{2})}$
 - Si $a \notin \frac{\pi}{2} [\pi]$, $\tan(a) = \frac{2 \tan(\frac{a}{2})}{1 + \tan^2(\frac{a}{2})}$

Preuve: 1. On suppose que $a \notin \frac{\pi}{2} [\pi]$

$$1 + \tan^2(a) = 1 + \frac{\sin^2(a)}{\cos^2(a)} = \frac{\cos^2(a) + \sin^2(a)}{\cos^2(a)} = \frac{1}{\cos^2(a)}$$

2. On peut le prouver par le calcul avec les formules de la tangente mais on peut également le prouver géométriquement.



Soit $M(x_0, y_0) \neq A$ sur le cercle trigonométrique \mathcal{C} . On note t la pente de la demi-droite $[AM)$.

On en déduit que l'équation de la droite (AM) est

$$y = tx + t = t(x + 1)$$

On sait que $M \in (AM)$ donc

$$y_0 = t(x_0 + 1)$$

On sait aussi que $x_0^2 + y_0^2 = 1$

Donc,

$$x_0 + t^2(x_0 + 1)^2 = 1$$

et donc

$$x_0^2 \underbrace{(1 + t^2)}_{\neq 0} + 2t^2x_0 + t^2 - 1 = 0$$

On résout cette équation du second degré et on trouve deux racines : $x_0 = -1$ et

$$x_0 = \frac{1 - t^2}{1 + t^2}.$$

Comme $M \neq A$, $x_0 = \frac{1 - t^2}{1 + t^2}$ et $y_0 = t \left(\frac{1 - t^2}{1 + t^2} + 1 \right) = \frac{2t}{1 + t^2}$

Enfin,

$$t = \frac{|HM|}{|AH|} = \tan\left(\frac{a}{2}\right)$$

car AHM est rectangle en H (d'après le théorème de Thalès)

Donc,

$$\begin{cases} \cos(a) = \frac{1 - \tan^2\left(\frac{a}{2}\right)}{1 + \tan^2\left(\frac{a}{2}\right)} \\ \sin(a) = \frac{2 \tan\left(\frac{a}{2}\right)}{1 + \tan^2\left(\frac{a}{2}\right)} \end{cases}$$

□

2 Nombres complexes de module 1

Proposition: Soient $(a, b) \in \mathbb{R}^2$.

$$(\cos(a) + i \sin(a)) \times (\cos(b) + i \sin(b)) = \cos(a + b) + i \sin(a + b)$$

Preuve:

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

□

Définition: Pour $a \in \mathbb{R}$, on pose $e^{ia} = \cos(a) + i \sin(a)$
Ainsi, $\forall (a, b) \in \mathbb{R}^2, e^{ia} \times e^{ib} = e^{i(a+b)}$

Proposition: Soient a, b, c trois nombres complexes avec $a \neq 0$ et z_1, z_2 les racines de $P : z \mapsto az^2 + bz + c$

$$\text{Alors, } z_1 \times z_2 = \frac{c}{a} \text{ et } z_1 + z_2 = -\frac{b}{a}$$

EXEMPLE:

$$(E) : z^2 - 3z + 2 = 0$$

On remarque que $2 \times 1 = 2$ et $2 + 1 = 3$ donc 2 et 1 sont deux solutions de (E) .

Preuve: MÉTHODE 1 Soit $\Delta = b^2 - 4ac$ et δ une racine carrée de Δ

$$z_1 = \frac{-b - \delta}{2a} \text{ et } z_2 = \frac{-b + \delta}{2a}$$

Donc,

$$z_1 \times z_2 = \frac{b^2 - \delta^2}{4a^2} = \frac{b^2 - \Delta}{4a^2} = \frac{4ac}{4a^2} = \frac{c}{a} z_1 + z_2 = \frac{-b - b - \delta + \delta}{2a} = -\frac{2b}{2a} = -\frac{b}{a}$$

MÉTHODE 2

$$\forall z \in \mathbb{C}, az^2 + bz + c = a(z - z_1)(z - z_2) = a(z^2 - (z_1 + z_2)z + z_1 z_2)$$

En particulier,

$$\begin{cases} \text{avec } z = 0, & c = az_1 z_2 \\ \text{avec } z = 0, & \cancel{d} + b + \cancel{c} = a(\cancel{1} - (z_1 + z_2) + \cancel{z_1 z_2}) \end{cases}$$

donc

$$b = -a(z_1 + z_2)$$

et donc

$$\begin{cases} z_1 z_2 = \frac{c}{a} \\ z_1 + z_2 = -\frac{b}{a} \end{cases}$$

□

Proposition: Soient $(a, b, c) \in \mathbb{C}^3$ et z_1, z_2, z_3 les solutions de

$$z^3 + az^2 + bz + c = 0$$

Alors,

$$\begin{cases} z_1 z_2 z_3 = -c \\ z_1 z_2 + z_2 z_3 + z_1 z_3 = b \\ z_1 + z_2 + z_3 = -a \end{cases}$$

□

Proposition: Soient a_1, a_2, \dots, a_n des nombres complexes et z_1, z_2, \dots, z_n les solutions de

$$z^n + a_{n-1} z^{n-1} + \dots + a_0 = 1$$

Alors,

$$\forall k \in [\![1, n]\!], \sum_{1 \leq i_1 \leq i_2 \leq \dots \leq i_k \leq n} z_{i_1} \times z_{i_2} \times \dots \times z_{i_k} = (-1)^k a_{n-k}$$

$$\left| \begin{array}{l} \sum_{k=1}^n z_k = -a_{n-1} \\ \prod_{k=1}^n z_k = (-1)^k a_0 \end{array} \right.$$

Preuve (incomplète pour $n = 3$):

$$\begin{aligned} \forall z \in \mathbb{C}, z^3 + az^2 + bz + c &= (z - z_1)(z - z_2)(z - z_3) = z^3 + z^2(-z_1 - z_2 - z_3) \\ &\quad + z(z_2 z_3 + z_1 z_2 + z_1 z_3) \\ &\quad - z_1 z_2 z_3 \end{aligned}$$

On identifie $\begin{cases} a = -z_1 - z_2 - z_3 \\ b = z_1 z_2 + z_2 z_3 + z_1 z_3 \\ c = -z_1 z_2 z_3 \end{cases}$

□

EXEMPLE:

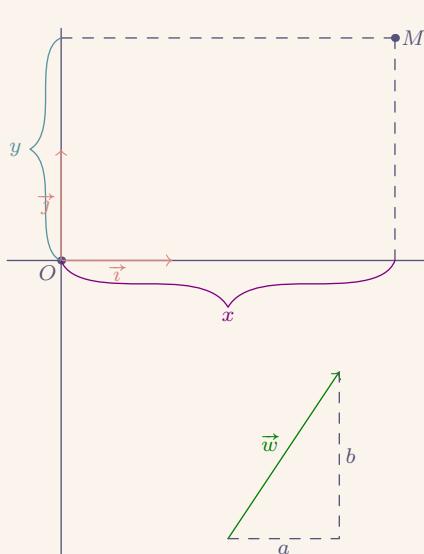
On pose

$$\begin{cases} s = z_1 + z_2 + z_3 \\ q = z_1 z_2 + z_2 z_3 + z_1 z_3 \\ p = z_1 z_2 z_3 \end{cases}$$

et $P = z_1^3 + z_2^3 + z_3^3$

3 Géométrie des nombres complexes

Dans ce paragraphe, \mathcal{P} désigne un plan euclidien muni d'un repère orthonormé (O, \vec{i}, \vec{j})



Définition: Soit $M \in \mathcal{P}$. On note (x, y) les coordonnées du point M par rapport au

repère (O, \vec{v}, \vec{j})

L'affixe de M est le nombre

$$z_M = x + iy \in \mathbb{C}$$

Soit $\vec{w} \in \mathcal{P}$ (le plan des vecteurs) et (a, b) les coordonnées de \vec{w} .

L'affixe de \vec{w} est

$$z_{\vec{w}} = a + ib \in \mathbb{C}$$

Proposition: Soit $(A, B) \in \mathcal{P}^2$ et $(\vec{w}_1, \vec{w}_2) \in \mathcal{P}^2$

1. $z_{\vec{AB}} = z_B - z_A$
2. $z_{\vec{w}_1 + \vec{w}_2} = z_{\vec{w}_1} + z_{\vec{w}_2}$

□

Proposition: Soit $(\vec{w}_1, \vec{w}_2) \in \mathcal{P}^2$ avec $\vec{w}_1 \neq \vec{0}$ et $\vec{w}_2 \neq \vec{0}$

Alors, $\left| \frac{z_{\vec{w}_1}}{z_{\vec{w}_2}} \right| = \frac{\|\vec{w}_1\|}{\|\vec{w}_2\|}$ et $\arg \left(\frac{z_{\vec{w}_1}}{z_{\vec{w}_2}} \right) = \underbrace{(\vec{w}_1, \vec{w}_2)}_{\text{l'angle entre } \vec{w}_1 \text{ et } \vec{w}_2}$

Preuve:

Soient $(r_1, r_2) \in (\mathbb{R}^+)^2$ et $(\theta_1, \theta_2) \in [0, 2\pi]^2$ tels que

$$z_{\vec{w}_1} = r_1 e^{i\theta_1} \text{ et } z_{\vec{w}_2} = r_2 e^{i\theta_2}$$

Alors,

$$\frac{z_{\vec{w}_1}}{z_{\vec{w}_2}} = \frac{r_1}{r_2} e^{i(\theta_1 - \theta_2)}$$

donc

$$\begin{cases} \left| \frac{z_{\vec{w}_1}}{z_{\vec{w}_2}} \right| = \frac{r_1}{r_2} = \frac{\|\vec{w}_1\|}{\|\vec{w}_2\|} \\ \arg \left(\frac{z_{\vec{w}_1}}{z_{\vec{w}_2}} \right) \equiv \theta_1 - \theta_2 \ [2\pi] \end{cases}$$

car $\theta_1 - \theta_2$ est l'angle entre \vec{w}_1 et \vec{w}_2

□

Corollaire: Avec les hypothèses et notations précédentes,

1. \vec{w}_1 et \vec{w}_2 sont collinéaires $\iff \frac{z_{\vec{w}_1}}{z_{\vec{w}_2}} \in \mathbb{R}$
2. \vec{w}_1 et \vec{w}_2 sont orthogonaux $\iff \frac{z_{\vec{w}_1}}{z_{\vec{w}_2}} \in i\mathbb{R}$

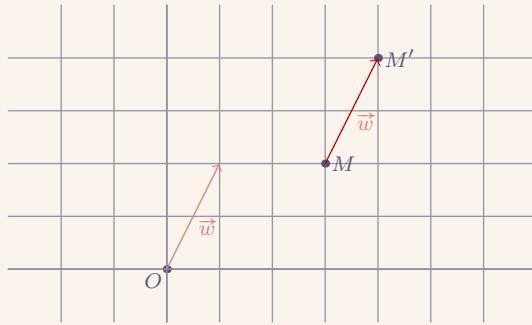
Preuve: 1.

$$\begin{aligned} \vec{w_1} \text{ et } \vec{w_2} \text{ sont colinéaires} &\iff (\widehat{\vec{w_1}}, \widehat{\vec{w_2}}) \equiv 0 \ [\pi] \\ &\iff \arg\left(\frac{z_{\vec{w_1}}}{z_{\vec{w_2}}}\right) \equiv 0 \ [\pi] \\ &\iff \frac{z_{\vec{w_1}}}{z_{\vec{w_2}}} \in \mathbb{R} \end{aligned}$$

2.

$$\begin{aligned} \vec{w_1} \text{ et } \vec{w_2} \text{ sont orthogonaux} &\iff (\widehat{\vec{w_1}}, \widehat{\vec{w_2}}) \equiv \frac{\pi}{2} \ [\pi] \\ &\iff \arg\left(\frac{z_{\vec{w_1}}}{z_{\vec{w_2}}}\right) \equiv \frac{\pi}{2} \ [\pi] \\ &\iff \frac{z_{\vec{w_1}}}{z_{\vec{w_2}}} \in i\mathbb{R} \end{aligned}$$

□



Définition: Soit $\vec{w} \in \mathcal{P}$. La translation de vecteur \vec{w} est l'application

$$\begin{aligned} t_{\vec{w}} : \mathcal{P} &\longrightarrow \mathcal{P} \\ M &\longmapsto M' \end{aligned}$$

où M' vérifie $\overrightarrow{MM'} = \vec{w}$

Proposition: Soit $\vec{w} \in \mathcal{P}$ et $(M, M') \in \mathcal{P}^2$

$$M' = t_{\vec{w}}(M) \iff z_{M'} = z_M + z_{\vec{w}}$$

Preuve:

$$\begin{aligned} M' = t_{\vec{w}}(M) &\iff \overrightarrow{MM'} = \vec{w} \\ &\iff z_M - z_{M'} = z_{\vec{w}} \\ &\iff z_{M'} = z_M + z_{\vec{w}} \end{aligned}$$

□

EXEMPLE (Décrire l'ensemble $E = \{M \in \mathcal{P} \mid \exists t \in \mathbb{R}, z_M = 1 + e^{it}\}$):

L'ensemble $\mathcal{C} = \{M \in \mathcal{P} \mid \exists t \in \mathbb{R}, z_M = e^{it}\}$ est le cercle trigonométrique. La translation $t_{\vec{u}}$ a pour expression complexe $z \mapsto z + 1$. Donc, $E = t_{\vec{u}}(\mathcal{C})$ est le cercle de rayon 1 et de centre le point d'affixe 1.

Proposition: Soient $\vec{w}_1, \vec{w}_2 \in \mathcal{P}$.

$$t_{\vec{w}_2} \circ t_{\vec{w}_1} = t_{\vec{w}_1 + \vec{w}_2}$$

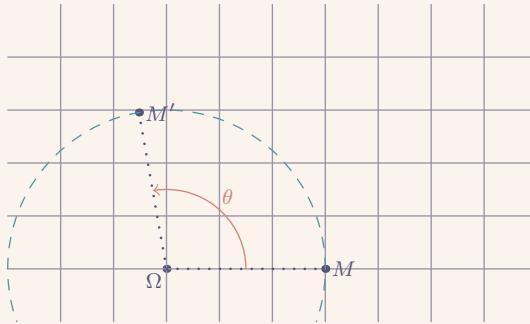
Preuve:

Soit $M \in \mathcal{P}$ d'affixe z . On pose $M_1 = t_{\vec{w}_1}(M)$ et $M' = t_{\vec{w}_1}(M_1)$ et on note également $M'' = t_{\vec{w}_1 + \vec{w}_2}(M)$

$$\begin{aligned} z_{M'} &= z_{M_1} + z_{\vec{w}_2} \\ &= (z + z_{\vec{w}_1}) + z_{\vec{w}_2} \\ &= z + z_{\vec{w}_1 + \vec{w}_2} \end{aligned}$$

Donc, $M' = M''$

□



Définition: Soit $\Omega \in \mathcal{P}$ et $\theta \in \mathbb{R}$.

La rotation de centre Ω et d'angle θ est l'application

$$\begin{aligned} \rho_{\Omega, \theta} : \mathcal{P} &\longrightarrow \mathcal{P} \\ M &\longmapsto M' \end{aligned}$$

où M' vérifie

$$\begin{cases} \|\overrightarrow{\Omega M}\| = \|\overrightarrow{\Omega M'}\| \\ (\widehat{\overrightarrow{\Omega M}}, \widehat{\overrightarrow{\Omega M'}}) = \theta \end{cases}$$

Proposition: Soit $\Omega \in \mathcal{P}$ d'affixe ω , $\theta \in \mathbb{R}$ et $(M, M') \in \mathcal{P}^2$

$$(*) : \quad M' = \rho_{\Omega, \theta}(M) \iff z_{M'} = \omega + e^{i\theta}(z_M - \omega)$$

Preuve: CAS 1 On suppose $M \neq \Omega$.

$$\begin{aligned} M' = \rho_{\Omega, \theta}(M) &\iff \begin{cases} \|\overrightarrow{\Omega M}\| = \|\overrightarrow{\Omega M'}\| \\ (\widehat{\overrightarrow{\Omega M}}, \widehat{\overrightarrow{\Omega M'}}) = \theta \end{cases} \\ &\iff \begin{cases} |z_{\overrightarrow{\Omega M}}| = |z_{\overrightarrow{\Omega M'}}| \\ \arg\left(\frac{z_{\overrightarrow{\Omega M}}}{z_{\overrightarrow{\Omega M'}}}\right) = \theta \end{cases} \\ &\iff e^{i\theta} = \frac{z_{\overrightarrow{\Omega M}}}{z_{\overrightarrow{\Omega M'}}} \\ &\iff z_{\overrightarrow{\Omega M'}} = e^{i\theta} z_{\overrightarrow{\Omega M}} \\ &\iff z_{M'} - \omega = e^{i\theta} (z_M - \omega) \\ &\iff z_{M'} = \omega + e^{i\theta} (z_M - \omega) \end{aligned}$$

CAS 2 On suppose $M = \Omega$.

Alors,

$$\begin{aligned} M' = \rho_{\Omega, \theta}(M) &\iff M' = M \\ &\iff z_{M'} = z_M \\ &\iff z_{M'} = z_M + e^{i\theta} (z_M - z_M) \\ &\iff z_{M'} = \omega + e^{i\theta} (z_M - \omega) \end{aligned}$$

□

REMARQUE (Cas particulier):

Si $\Omega = O$ alors

$$(*) \iff z_{M'} = e^{i\theta} z_M$$

Corollaire: Soit $\Omega \in \mathcal{P}$ d'affixe ω et $\theta \in \mathbb{R}$.

$$\begin{aligned} \rho_{\Omega, \theta} &= t_{\overrightarrow{O\Omega}} \circ \rho_{O, \theta} \circ t_{\overrightarrow{\Omega O}} \\ &= t_{\overrightarrow{O\Omega}} \circ \rho_{O, \theta} \circ (t_{\overrightarrow{O\Omega}})^{-1} \end{aligned}$$

Proposition: Soient $(\Omega_1, \Omega_2) \in \mathcal{P}^2$ et $(\theta_1, \theta_2) \in \mathbb{R}^2$

$$\rho_{\Omega_1, \theta_1} \circ \rho_{\Omega_1, \theta_2} = \rho_{\Omega_1, \theta_1 + \theta_2} = \rho_{\Omega_1, \theta_2} \circ \rho_{\Omega_1, \theta_1}$$

Si $\begin{cases} \Omega_1 \neq \Omega_2 \\ \theta_1 + \theta_2 \not\equiv 0 \ [2\pi] \end{cases}$ alors $\rho_{\Omega_1, \theta_1} \circ \rho_{\Omega_2, \theta_2}$ est une rotation d'angle $\theta_1 + \theta_2$

Si $\begin{cases} \Omega_1 \neq \Omega_2 \\ \theta_1 + \theta_2 \equiv 0 \ [2\pi] \end{cases}$ alors $\rho_{\Omega_1, \theta_1} \circ \rho_{\Omega_2, \theta_2}$ est une translation

Preuve:

On note ω_1 l'affixe de Ω_1 et ω_2 l'affixe de Ω_2 . On pose $\rho_1 = \rho_{\Omega_1, \theta_1}$ et $\rho_2 = \rho_{\Omega_2, \theta_2}$

Soit $M \in \mathcal{P}$ d'affixe z . On pose

$$\begin{aligned} M_2 &= \rho_2(M) \\ M' &= \rho_1 \circ \rho_2(M) = \rho_1(M_2) \end{aligned}$$

et on note z_2 et z' les affixes de M_2 et M'
On a

$$\begin{aligned} z' &= \omega_1 + e^{i\theta_1}(z_2 - \omega_1) \\ &= \omega_1 + e^{i\theta_1}(\omega_2 + e^{i\theta_2}(z - \omega_2) - \omega_1) \\ &= \omega_1 + \omega_2 e^{i\theta_1} - \omega_1 e^{i\theta_1} + e^{i(\theta_1+\theta_2)}(z - \omega_2) \end{aligned}$$

1. On suppose $\Omega_1 = \Omega_2$ donc $\omega_1 = \omega_2$. On a donc

$$z' = \omega_1 + e^{i(\theta_1+\theta_2)}(z - \omega_1)$$

On reconnaît l'expression d'une rotation de centre Ω_1 et d'angle $\theta_1 + \theta_2$

2. On suppose $\Omega_1 \neq \Omega_2$ et $\theta_1 + \theta_2 \equiv 0 \ [2\pi]$. On a donc

$$\begin{aligned} z' &= \underbrace{\omega_1 + \omega_2 e^{i\theta_1} - \omega_1 e^{i\theta_1}}_{= z + \omega} - \omega_2 + z \\ &= z + \omega \end{aligned}$$

On reconnaît l'expression d'une translation de vecteur ω .

3. On suppose $\Omega_1 \neq \Omega_2$ et $\theta_1 + \theta_2 \not\equiv 0 \ [2\pi]$
On cherche $\omega \in \mathbb{C}$ tel que

$$\begin{aligned} \forall z \in \mathbb{C}, \omega + e^{i(\theta_1+\theta_2)}(z - \omega) &= \omega_1 + \omega_2 e^{i\theta_1} - \omega_1 e^{i\theta_1} + e^{i(\theta_1+\theta_2)}(z - \omega_2) \\ \iff \omega - e^{i(\theta_1+\theta_2)}\omega &= \omega_1 + \omega_2 e^{i\theta_1} - \omega_1 e^{i\theta_1} - \omega_2 e^{i(\theta_1+\theta_2)} \\ \iff \omega &= \frac{\omega_1 + \omega_2 e^{i\theta_1} - \omega_1 e^{i\theta_1} - \omega_2 e^{i(\theta_1+\theta_2)}}{1 - e^{i(\theta_1+\theta_2)}} \end{aligned}$$

On reconnaît l'expression complexe d'une rotation d'angle $\theta_1 + \theta_2$ de centre Ω
d'affixe ω

□

Proposition: Soit $\Omega \in \mathcal{P}$ d'affixe ω , $\vec{w} \in \overrightarrow{\mathcal{P}}$ d'affixe u . Soit $\theta \in \mathbb{R}$ avec $\theta \not\equiv 0 \ [2\pi]$.

- $t_{\vec{w}} \circ \rho_{\Omega, \theta}$ est une rotation d'angle θ
- $\rho_{\Omega, \theta} \circ t_{\vec{w}}$ est aussi une rotation d'angle θ

Preuve:

Soit $M \in \mathcal{P}$ d'affixe z et $M' = t_{\vec{w}} \circ \rho_{\Omega, \theta}(M)$ d'affixe z'

On a alors :

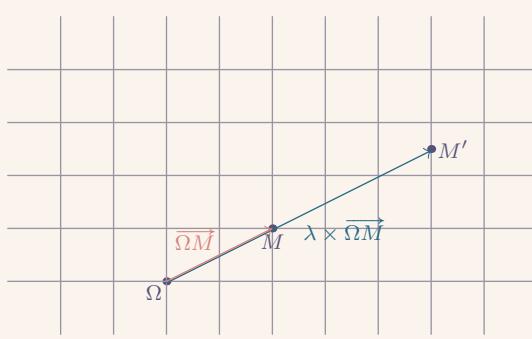
$$z' = (\omega + e^{i\theta}(z - \omega)) + u$$

On cherche $\omega' \in \mathbb{C}$ tel que

$$\begin{aligned} \forall z \in \mathbb{C}, \omega + u + e^{i\theta}(z - \omega) &= \omega' + e^{i\theta}(z - \omega') \\ \iff \omega + u - e^{i\theta}\omega &= \omega' - e^{i\theta}\omega' \\ \iff \omega' &= \frac{\omega + u - e^{i\theta}\omega}{1 - e^{i\theta}} \end{aligned}$$

On reconnaît l'expression complexe d'une rotation d'angle θ

□



Définition: Soit $\Omega \in \mathcal{P}$ et $\lambda \in \mathbb{R}$.

L'homothétie de centre Ω et de rapport λ est l'application

$$\begin{aligned} h_{\Omega, \lambda} : \mathcal{P} &\longrightarrow \mathcal{P} \\ M &\longmapsto M' \end{aligned}$$

où M' vérifie $\overrightarrow{\Omega M'} = \lambda \overrightarrow{\Omega M}$

Proposition: Soit $\Omega \in \mathcal{P}$ d'affixe ω , $\lambda \in \mathbb{R}$. Soient $M \in \mathcal{P}$ d'affixe z et $M' \in \mathcal{P}$ d'affixe z' .

$$M' = h_{\Omega, \lambda}(M) \iff z' = \omega + \lambda(z - \omega)$$

Preuve:

$$\begin{aligned} M' = h_{\Omega, \lambda}(M) &\iff \overrightarrow{\Omega M'} = \lambda \overrightarrow{\Omega M} \\ &\iff z \overrightarrow{\Omega M'} = z \lambda \overrightarrow{\Omega M} \\ &\iff z' - \omega = \lambda(z - \omega) \\ &\iff z' = \omega + \lambda(z - \omega) \end{aligned}$$

□

Proposition: Soient $(\Omega_1, \Omega_2) \in \mathcal{P}^2$ et $(\lambda_1, \lambda_2) \in \mathcal{P}^2$

1. Si $\Omega_1 = \Omega_2$ alors, $h_{\Omega_1, \lambda_1} \circ h_{\Omega_2, \lambda_2} = h_{\Omega_1, \lambda_1 \lambda_2}$
2. Si $\Omega_1 \neq \Omega_2$ et $\lambda_1 \lambda_2 \neq 1$, alors, $h_{\Omega_1, \lambda_1} \circ h_{\Omega_2, \lambda_2}$ est une homothétie de rapport

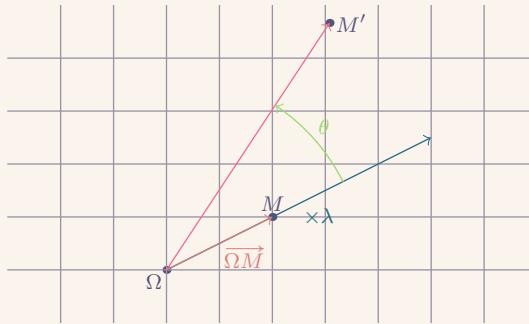
- $\lambda_1 \lambda_2$
3. Si $\Omega_1 \neq \Omega_2$ et $\lambda_1 \lambda_2 = 1$, alors, $h_{\Omega_1, \lambda_1} \circ h_{\Omega_2, \lambda_2}$ est une translation.

□

Proposition: Soit $\Omega \in \mathcal{P}$, $\lambda \in \mathbb{R} \setminus \{1\}$, $\vec{w} \in \overline{\mathcal{P}}$.
Alors, $t_{\vec{w}} \circ h_{\Omega, \lambda}$ et $h_{\Omega, \lambda} \circ t_{\vec{w}}$ sont homothéties de rapport λ .

□

REMARQUE (Cas particulier):
Soit $M \in \mathcal{P}$ d'affixe z , $\lambda \in \mathbb{R}$ et $M' = h_{O, \lambda}(M)$ d'affixe z'
On a $z' = \lambda z$



Définition: Soient $\Omega \in \mathcal{P}$, $(\theta, \lambda) \in \mathbb{R}^2$. La similitude (directe) de centre Ω , d'angle θ et de rapport λ est

$$S_{\Omega, \theta, \lambda} = h_{\Omega, \lambda} \circ \rho_{\Omega, \theta}$$

Proposition: Avec les notations précédentes,

$$S_{\Omega, \theta, \lambda} = \rho_{\Omega, \theta} \circ h_{\Omega, \lambda}$$

Preuve:

On note ω l'affixe de Ω . L'expression complexe de $S_{\Omega, \theta, \lambda}$ est

$$\begin{aligned} z' &= \omega + \lambda(\omega + e^{i\theta}(z - \omega) - \omega) \\ &= \omega + \lambda e^{i\theta}(z - \omega) \end{aligned}$$

L'expression complexe de $\rho_{\Omega, \theta} \circ h_{\Omega, \lambda}$ est

$$\begin{aligned} z' &= \omega + e^{i\theta}(\omega + \lambda(z - \omega) - \omega) \\ &= \omega + \lambda e^{i\theta}(z - \omega) \end{aligned}$$

Les deux expressions sont identiques. □

Proposition: L'expression complexe de $S_{\Omega, \theta, \lambda}$ est

$$z' = \omega + \lambda e^{i\theta}(z - \omega)$$

4 Exponentielle complexe

Définition: Pour $z \in \mathbb{C}$, on pose

$$\exp(z) = e^{\Re(z)} \times (\cos(\Im(z)) + i \sin(\Im(z)))$$

Ainsi, si $z = a + ib$ avec $(a, b) \in \mathbb{R}^2$,

$$\exp(z) = \exp(a + ib) = e^a \times (\cos(b) + i \sin(b)) = e^a e^{ib}$$

Proposition: Soient $z_1, z_2 \in \mathbb{C}$.

$$\exp(z_1 + z_2) = \exp(z_1) \times \exp(z_2)$$

Preuve:

On pose $\begin{cases} z_1 = a + ib \\ z_2 = c + id \end{cases}$ avec $(a, b, c, d) \in \mathbb{R}^4$

$$\begin{aligned} \exp(z_1) \times \exp(z_2) &= e^a \times e^{ib} \times e^c \times e^{id} \\ &= e^{a+c} e^{i(b+d)} \\ &= \exp(z_1 + z_2) \end{aligned}$$

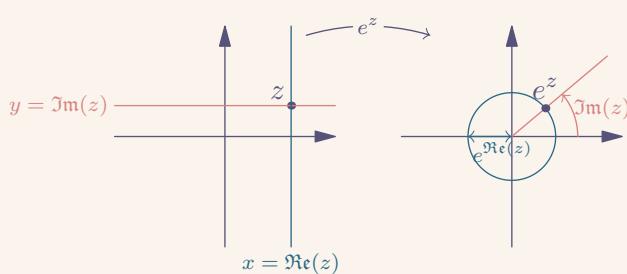
□

REMARQUE (Notation):

On écrit e^z à la place de $\exp(z)$ pour $z \in \mathbb{C}$.

Proposition:

$$\forall z \in \mathbb{C}, \begin{cases} |e^z| = e^{\Re(z)} \\ \arg(e^z) \equiv \Im(z) [2\pi] \end{cases}$$



REMARQUE:

$\exp : \mathbb{C} \rightarrow \mathbb{C}$ n'est pas bijective :

$$\begin{aligned} & \text{--- } \begin{cases} \exp(0) = \exp(2i\pi) = 1 \\ 0 \neq 2i\pi \end{cases} \\ & \text{--- } 0 \text{ n'a pas d'antécédant} \end{aligned}$$

Il n'y a donc pas de logarithme complexe.

5 Fonctions de \mathbb{R} dans \mathbb{C}

Définition: Soit f définie sur $D \subset \mathbb{R}$ à valeurs dans \mathbb{C} ($\forall x \in D, f(x) \in \mathbb{C}$)
On pose :

$$\begin{aligned} \Re(f) : D &\longrightarrow \mathbb{R} \\ x &\longmapsto \Re(f(x)) \end{aligned}$$

et

$$\begin{aligned} \Im(f) : D &\longrightarrow \mathbb{R} \\ x &\longmapsto \Im(f(x)) \end{aligned}$$

EXEMPLE:

$$\begin{aligned} f : [0, 2\pi[&\longrightarrow \mathbb{C} \\ x &\longmapsto e^{(1+i)x} \end{aligned}$$

On a :

$$\begin{aligned} \Re(f) : [0, 2\pi[&\longrightarrow \mathbb{R} \\ x &\longmapsto e^x \cos(x) \end{aligned}$$

et

$$\begin{aligned} \Im(f) : [0, 2\pi[&\longrightarrow \mathbb{R} \\ x &\longmapsto e^x \sin(x) \end{aligned}$$

Définition: Soit $f : D \rightarrow \mathbb{C}$. On dit que

- f est continue si $\Re(f)$ et $\Im(f)$ sont continues
 - f est dérivable si $\Re(f)$ et $\Im(f)$ sont dérivables.
- Dans ce cas, la dérivée de f est

$$\begin{aligned} f' : D &\longrightarrow \mathbb{C} \\ x &\longmapsto \Re(f)'(x) + i\Im(f)'(x) \end{aligned}$$

EXEMPLE:

$$\begin{aligned} f : [0, 2\pi[&\longrightarrow \mathbb{C} \\ x &\longmapsto e^{(1+i)x} \end{aligned}$$

$x \mapsto e^x$ et $x \mapsto \cos(x)$ sont dérivables sur $[0, 2\pi[$ donc $\Re(f)$ est dérivable.
 $x \mapsto e^x$ et $x \mapsto \sin(x)$ sont dérivables sur $[0, 2\pi[$ donc $\Im(f)$ est dérivable.
 Donc f est dérivable.

$$\forall x \in [0, 2\pi[, \begin{cases} \Re(f)'(x) = e^x \cos(x) - e^x \sin(x) \\ \Im(f)'(x) = e^x \cos(x) + e^x \sin(x) \end{cases}$$

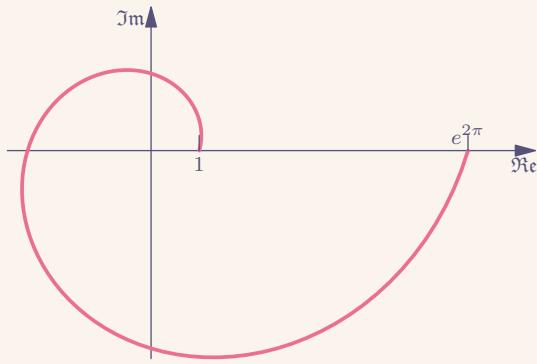
Donc,

$$\forall x \in [0, 2\pi[, f'(x) = e^x(\cos(x) - \sin(x)) + ie^x(\sin(x) + \cos(x))$$

REMARQUE:

On peut représenter f de la façon suivante.

$$\begin{aligned} f : [0, 2\pi[&\longrightarrow \mathbb{C} \\ t &\longmapsto e^{(1+i)t} \end{aligned}$$



Proposition: Soient u et v deux fonctions dérivables sur $D \subset \mathbb{R}$ à valeurs dans \mathbb{C}

1. $u + v$ dérivable et $(u + v)' = u' + v'$
2. uv dérivable et $(uv)' = u'v + v'u$
3. Si $v \neq 0$, $\frac{u}{v}$ dérivable et $\left(\frac{u}{v}\right)' = \frac{u'v - v'u}{v^2}$

Preuve:

On pose $\begin{cases} a = \operatorname{Re}(u) \\ b = \operatorname{Im}(u) \end{cases}$ et $\begin{cases} c = \operatorname{Re}(v) \\ d = \operatorname{Im}(v) \end{cases}$

1. $\begin{cases} \operatorname{Re}(u + v) = a + c \\ \operatorname{Im}(u + v) = b + d \end{cases}$ donc $\begin{cases} \operatorname{Re}(u + v)' = a' + c' \\ \operatorname{Im}(u + v)' = b' + d' \end{cases}$ Donc,

$$\begin{aligned} (u + v)' &= a' + c' + i(b' + d') \\ &= (a' + ib') + (c' + id') \\ &= u' + v' \end{aligned}$$

2. $\begin{cases} \operatorname{Re}(uv) = ac - bd \\ \operatorname{Im}(uv) = ad + bc \end{cases}$ donc $\operatorname{Re}(uv)$ et $\operatorname{Im}(uv)$ sont dérivables et

$$\begin{cases} \operatorname{Re}(uv)' = a'c + c'a - b'd - d'b \\ \operatorname{Im}(uv)' = a'd + d'a + b'c + c'b \end{cases}$$

Donc,

$$(uv)' = a'c + c'a - b'd - d'b + i(a'd + d'a + b'c + c'b)$$

Or,

$$\begin{cases} u'v = (a' + ib')(c + id) = a'c - b'd + i(b'c + a'd) \\ v'u = (a + ib)(c' + id') = ac' - bd' + i(bc' + ad') \end{cases}$$

Donc,

$$(uv)' = u'v + v'u$$

3. On suppose que

$$\forall x \in D, v(x) \neq 0$$

On a donc

$$\forall x \in D, \frac{u}{v} = \frac{a + ib}{c + id} = \frac{(a + ib)(c - id)}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + i \frac{bc - ad}{c^2 + d^2}$$

C'est plus simple de voir $\frac{u}{v}$ comme le produit de u et de $\frac{1}{v}$

$$\frac{1}{v} = \frac{1}{c + id} = \frac{c - id}{c^2 + d^2}$$

$\underbrace{\frac{c}{c^2 + d^2}}_{=\Re(\frac{1}{v})}$ et $\underbrace{-\frac{d}{c^2 + d^2}}_{=\Im(\frac{1}{v})}$ sont dérivables donc $\frac{1}{v}$ aussi

$$\begin{aligned} \left(\Re \left(\frac{1}{v} \right) \right)' &= \left(\frac{c}{c^2 + d^2} \right)' = \frac{c'(c^2 + d^2) - c(2cc' + 2dd')}{(c^2 + d^2)^2} \\ \left(\Im \left(\frac{1}{v} \right) \right)' &= \left(-\frac{d}{c^2 + d^2} \right)' = \frac{-d'(c^2 + d^2) + d(2cc' + 2dd')}{(c^2 + d^2)^2} \end{aligned}$$

Donc, d'une part,

$$\begin{aligned} \left(\frac{1}{v} \right)' &= \frac{c'(c^2 + d^2) - c(2cc' - 2dd') - id'(c^2 + d^2) + d(2cc' + 2dd')}{(c^2 + d^2)^2} \\ &= \frac{(c^2 + d^2)(c' - id') + (2cc' + 2dd')(-c + id)}{(c^2 + d^2)^2} \\ &= \frac{-c'c^2 + c'd^2 - 2cdd' + i(2cc'd - d'c^2 + d^2d')}{(c^2 + d^2)^2} \end{aligned}$$

D'autre part,

$$\begin{aligned} \frac{-v'}{v^2} &= \frac{-c' - d'i}{(c + di)^2} \\ &= \frac{-(c' + id')(c - id)}{(c^2 + d^2)^2} \\ &= -\frac{(c' + id')(c^2 - 2icd - d^2)}{(c^2 + d^2)^2} \\ &= \frac{-c'c^2 + c'd^2 - 2cdd' + i(2cc'd - d'c^2 + d^2d')}{(c^2 + d^2)^2} \\ &= \left(\frac{1}{v} \right)' \end{aligned}$$

Donc, $\frac{u}{v}$ dérivable et

$$\left(\frac{u}{v} \right)' = u' \left(\frac{1}{v} \right) + u \left(\frac{1}{v} \right)' = \frac{u'}{v} - \frac{uv'}{v^2} = \frac{u'v - uv'}{v^2}$$

□

Proposition: Soit $v : D \rightarrow \mathbb{R}$ et $u : \mathbb{R} \rightarrow \mathbb{C}$ deux fonctions dérivables (avec $D \subset \mathbb{R}$). Alors, $u \circ v$ est dérivable et

$$(u \circ v)' = (u' \circ v) \times v'$$

Preuve:

On pose $u = a + ib$ avec $\begin{cases} a = \Re(u) \\ b = \Im(u) \end{cases}$ donc,

$$\forall x \in \mathbb{R}, u(x) = a(x) + ib(x)$$

Donc,

$$\forall x \in D, (u \circ v)(x) = a(v(x)) + ib(v(x))$$

Donc,

$$\Re(u \circ v) = a \circ v$$

$$\Im(u \circ v) = b \circ v$$

Or,

$$\begin{aligned} \Re(u \circ v)' &= (a \circ v)' = (a' \circ v) \times v' \\ \Im(u \circ v)' &= (b \circ v)' = (b' \circ v) \times v' \end{aligned}$$

D'où

$$\begin{aligned} (u \circ v)' &= (a' \circ v) \times v' + i(b' \circ v) \times v' \\ &= (a' \circ v + ib' \circ v) \times v' \\ &= ((a' + ib') \circ v) \times v' \\ &= (u' \circ v) \times v' \end{aligned}$$

□

Proposition: Soit $u : D \rightarrow \mathbb{C}$ et $f : \begin{array}{ccc} D & \longrightarrow & \mathbb{C} \\ x & \longmapsto & e^{u(x)} \end{array}$

Alors, f est dérivable sur D et

$$\forall x \in D, f'(x) = u'(x)e^{u(x)}$$

Preuve:

On pose $\begin{cases} a = \Re(u) \\ b = \Im(u) \end{cases}$ donc

$$\begin{aligned} \forall x \in D, f(x) &= e^{u(x)} \\ &= e^{a(x)+ib(x)} \\ &= e^{a(x)}(\cos(b(x)) + i \sin(b(x))) \end{aligned}$$

Donc, $\begin{cases} \Re(f) : x \mapsto e^{a(x)} \cos(b(x)) \\ \Im(f) : x \mapsto e^{a(x)} \sin(b(x)) \end{cases}$
 a, b, \cos, \sin, \exp sont dérivables donc $\Re(f)$ et $\Im(f)$ aussi donc f est dérivable.

□

CHAPITRE

3

ÉTUDE DE FONCTIONS

Étudier une fonction c'est déterminer tous les éléments (tangentes, asymptotes) qui permettent d'obtenir l'allure de la courbe représentative de la fonction.

EXEMPLE:

$$f : x \mapsto \frac{x^2 - 2x + 3}{x^2 + 2x - 3}$$

1. On détermine le domaine de définition de la fonction f .
Soit $x \in \mathbb{R}$.

$$x^2 + 2x - 3 = 0 \iff x \in \{-3, 1\} \quad \text{car} \quad \begin{cases} -3 + 1 = -2 = -\frac{b}{a} \\ -3 \times 1 = -3 = \frac{c}{a} \end{cases}$$

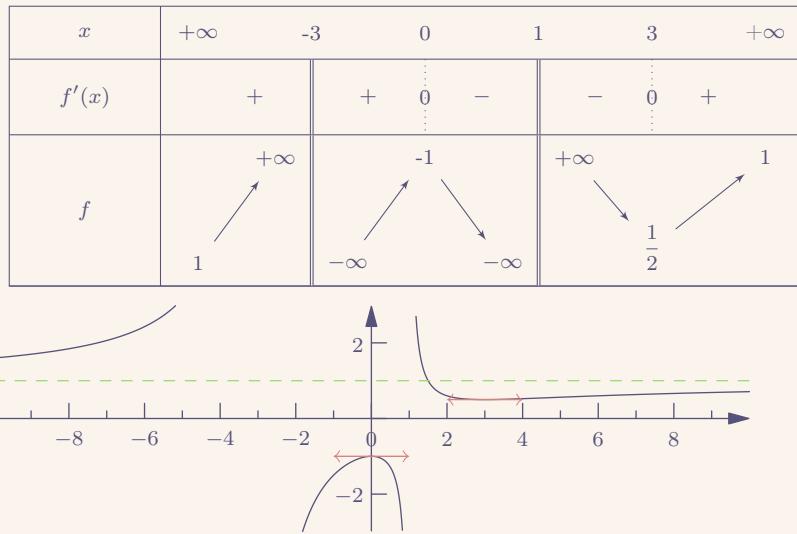
Donc f est définie sur $\mathcal{D} =]-\infty, -3[\cup]-3, -1[\cup]-1, +\infty[$

2. Asymptotes et limites
Soit $x \in \mathcal{D}$

$$\begin{aligned} f(x) &= \frac{\cancel{x^2} \left(1 - \frac{2}{x} + \frac{3}{x^2}\right)}{\cancel{x^2} \left(1 + \frac{2}{x} - \frac{3}{x^2}\right)} \xrightarrow[x \rightarrow \pm\infty]{} 1 \\ &\left. \begin{aligned} x^2 - 2x + 3 &\xrightarrow[x \rightarrow -3]{} 9 + 6 + 3 = 18 \\ x^2 + 2x - 3 &\xrightarrow[x \rightarrow -3]{} 0 \end{aligned} \right\} \text{ donc } \begin{cases} f(x) \xrightarrow[x \rightarrow -3]{} +\infty \\ f(x) \xrightarrow[x \rightarrow -3]{} -\infty \end{cases} \\ &\left. \begin{aligned} x^2 - 2x + 3 &\xrightarrow[x \rightarrow 1]{} 2 \\ x^2 + 2x - 3 &\xrightarrow[x \rightarrow 1]{} 0 \end{aligned} \right\} \text{ donc } \begin{cases} f(x) \xrightarrow[x \rightarrow 1]{} -\infty \\ f(x) \xrightarrow[x \rightarrow 1]{} +\infty \end{cases} \end{aligned}$$

3. f est dérivable sur \mathcal{D} et

$$\begin{aligned}\forall x \in \mathcal{D}, f'(x) &= \frac{2(x-1)(x^2+2x-3)-2(x^2-2x+3)(x+1)}{(x^2+2x-3)^2} \\ &= \frac{2(2x^2-6x)}{(x^2-2x+3)^2} \\ &= \frac{4x(x-4)}{(x^2-2x+3)^2}\end{aligned}$$



1 Calculs de limites

RAPPEL:

Soient f et g deux fonctions et $a \in \mathbb{R} \cup \{-\infty, +\infty\}$.

On ne connaît pas, à l'avance, les limites de

- $f(x) - g(x)$ si $\begin{cases} f(x) \xrightarrow{x \rightarrow a} +\infty \\ g(x) \xrightarrow{x \rightarrow a} +\infty \end{cases}$ (“ $\infty - \infty$ ”)
- $\frac{f(x)}{g(x)}$ si $\begin{cases} f(x) \xrightarrow{x \rightarrow a} 0 \\ g(x) \xrightarrow{x \rightarrow a} 0 \end{cases}$ (“ $\frac{0}{0}$ ”)
- $\frac{f(x)}{g(x)}$ si $\begin{cases} f(x) \xrightarrow{x \rightarrow a} \pm \infty \\ g(x) \xrightarrow{x \rightarrow a} \pm \infty \end{cases}$ (“ $\frac{\infty}{\infty}$ ”)
- $f(x) \times g(x)$ si $\begin{cases} f(x) \xrightarrow{x \rightarrow a} 0 \\ g(x) \xrightarrow{x \rightarrow a} \pm \infty \end{cases}$ (“ $0 \times \infty$ ”)

EXEMPLE:

$$\lim_{n \rightarrow +\infty} \left(1 + \frac{1}{n}\right)^n ?$$

$$\forall n \in \mathbb{N}, \left(1 + \frac{1}{n}\right)^n = e^{n \ln\left(1 + \frac{1}{n}\right)}$$

et

$$\begin{cases} \ln\left(1 + \frac{1}{n}\right) \xrightarrow{n \rightarrow +\infty} 0 \\ n \xrightarrow{n \rightarrow +\infty} +\infty \end{cases}$$

donc c'est une forme indéterminée.

Proposition:

Si $\begin{cases} f(x) \xrightarrow{x \rightarrow a} 1 \\ g(x) \xrightarrow{x \rightarrow a} \pm\infty \end{cases}$ alors, on ne sait pas à l'avance calculer $\lim_{x \rightarrow a} (f(x))^{g(x)}$. \square

Définition: Soient f et g deux fonctions et $a \in \overline{\mathbb{R}}$ où $\overline{\mathbb{R}} = \mathbb{R} \cup \{+\infty, -\infty\}$.

On dit que f et g sont équivalentes au voisinage de a (ou équivalentes en a) s'il existe une fonction u telle que

$$\begin{cases} f = g \times u \\ u(x) \xrightarrow{x \rightarrow a} 1 \end{cases}$$

On note alors $f \underset{a}{\sim} g$ ou $f(x) \underset{x \rightarrow a}{\sim} g(x)$.

Proposition: Un polynôme est équivalent en $\pm\infty$ à son terme de plus haut degré.

Preuve:

Soit $P : x \mapsto \sum_{k=0}^n a_k x^k$ avec $a_n \neq 0$. On pose $Q : x \mapsto a_n x^n$.

$$\begin{aligned} \forall x \in \mathbb{R}, P(x) &= a_n x^n \left(\sum_{k=0}^n \frac{a_k x^k}{a_n x^n} \right) \\ &= Q(x) \left(1 + \sum_{k=0}^{n-1} \frac{a_k}{a_n} \times \underbrace{\left(\frac{1}{x^{n-k}} \right)}_{u(x)} \right) \\ &= Q(x) u(x) \end{aligned}$$

On a $u(x) \xrightarrow{x \rightarrow \pm\infty} 1$ donc $P(x) \underset{x \rightarrow \pm\infty}{\sim} Q(x)$. \square

Proposition: Un polynôme est équivalent en 0 à son terme de plus bas degré.

Preuve:

À faire \square

REMARQUE:

Soient f et g deux fonctions définies au voisinage de a tel que

$$\forall x \in I, g(x) \neq 0$$

où I est un intervalle

- qui contient a si $a \in \mathbb{R}$,
- dont une borne est a si $a = \pm\infty$.

Alors,

$$f \underset{a}{\sim} g \iff \frac{f(x)}{g(x)} \xrightarrow[x \neq a]{x \rightarrow a} 1.$$

EXEMPLE:

$$x^2 + x^3 \underset{x \rightarrow 0}{\sim} x^2 \text{ car } \frac{x^2 + x^3}{x^2} = 1 + x \xrightarrow{x \rightarrow 0} 1.$$

EXEMPLE:

Soit f une fonction.

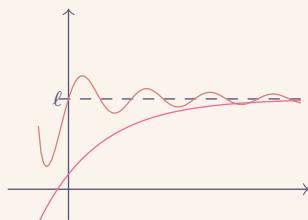
$$f \underset{0}{\sim} 0 \iff \exists I \text{ voisinage de } 0, \forall x \in I, f(x) = 0.$$

2 Asymptotes, branches paraboliques et prolongement par continuité

Cas1

Limite en $+\infty$:

$$f(x) \xrightarrow{x \rightarrow +\infty} \ell \in \mathbb{R}.$$



On dit que la droite d'équation $y = \ell$ est une asymptote horizontale.

Cas2

$$f(x) \xrightarrow{x \rightarrow +\infty} \pm\infty \quad \text{dans ce cas, on cherche } \lim_{x \rightarrow +\infty} \frac{f(x)}{x}.$$

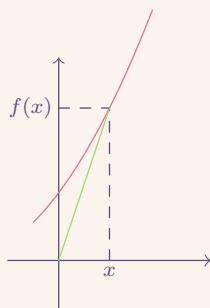
Sous cas 1

$$\frac{f(x)}{x} \text{ n'a pas de limite en } +\infty.$$

?

Sous cas 2

$$\frac{f(x)}{x} \xrightarrow{x \rightarrow +\infty} +\infty.$$

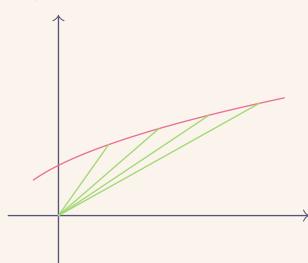


On dit que la courbe de f présente une branche parabolique de direction asymptotique l'axe des ordonnées.

$\frac{f(x)}{x}$ est la pente de la droite verte.

Sous cas 3

$$\frac{f(x)}{x} \xrightarrow{x \rightarrow +\infty} 0.$$



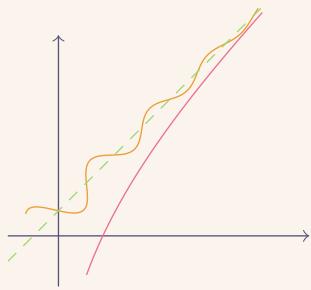
On dit que la courbe de f présente une

branche parabolique de direction asymptotique l'axe des ordonnées.

$\frac{f(x)}{x}$ est la pente de la droite verte.

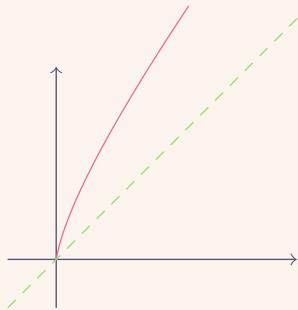
Sous cas 4 $\frac{f(x)}{x} \xrightarrow[x \rightarrow +\infty]{} \ell \in \mathbb{R}^+$. On cherche $\lim_{x \rightarrow +\infty} (f(x) - \ell x)$.

Sous-souscas1 $f(x) - \ell x \xrightarrow[x \rightarrow +\infty]{} a \in \mathbb{R}$



Asymptote oblique d'équation $y = \ell x + a$.

Sous-souscas2 $f(x) - \ell x \xrightarrow[x \rightarrow +\infty]{} \pm \infty$



Branche parabolique de direction asymptotique la droite d'équation $y = \ell x$.

Sous-souscas2 $f(x) - \ell x$ n'a pas de limite

?

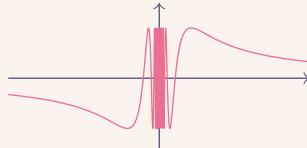
Limite en $a \in \mathbb{R}$:

On cherche $\lim_{x \rightarrow a} f(x)$.

Cas1

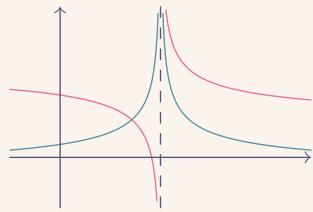
Pas de limite

[ex] $x \mapsto \sin\left(\frac{1}{x}\right)$ en 0 :



Cas2

$f(x) \xrightarrow[x \rightarrow a]{} \pm \infty$



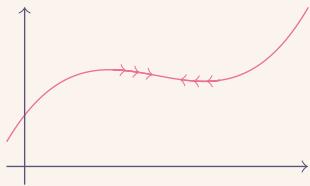
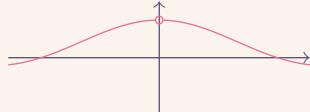
Asymptote verticale d'équation $x = a$.

Cas 3

$$f(x) \xrightarrow[x \rightarrow a]{} \ell \in \mathbb{R}.$$

[ex] $f : x \mapsto \frac{\sin x}{x}$ $f(x) \xrightarrow[x \rightarrow 0]{} 1$, dans ce cas,
on pose

$$f(x) = \begin{cases} \frac{\sin x}{x} & \text{si } x \neq 0 \\ 1 & \text{si } x = 0 \end{cases}$$



On pose $f(a) = \ell$. On dit que l'on a prolongé par continuité la fonction f .

CHAPITRE

4

FONCTIONS USUELLES

1 Logarithme népérien

Théorème (théorème fondamental de l'analyse): Soit f une fonction continue sur un intervalle I . Alors il existe F dérivable sur I telle que

$$\forall x \in I, F'(x) = f(x).$$

Preuve (c.f. chapitre 5 : calcul intégral):

□

Définition: La fonction ln est l'unique primitive sur \mathbb{R}_*^+ de $x \mapsto \frac{1}{x}$ qui s'annule en 1.

Proposition: 1. $\ln 1 = 0$;

2. \ln est dérivable sur \mathbb{R}_+^* et

$$\forall x > 0, \ln' x = \frac{1}{x}.$$

□

Corollaire:

$$\forall x > 0, \ln x = \int_1^x \frac{dt}{t}.$$

Preuve:

Soit

$$\begin{aligned}\varphi : \mathbb{R}_*^+ &\longrightarrow \mathbb{R} \\ x &\longmapsto \int_1^x \frac{dt}{t}.\end{aligned}$$

On a

$$\begin{aligned}\forall x > 0, \varphi(x) &= [\ln t]_1^x \\ &= \ln x - \ln 1 \\ &= \ln x\end{aligned}$$

□

REMARQUE:

$$\begin{aligned}u : \mathbb{R}_*^- &\longrightarrow \mathbb{R} \\ x &\longmapsto \ln(-x)\end{aligned}$$

u est dérivable sur \mathbb{R}_*^- et

$$\forall x < 0, u'(x) = \ln'(-x) \times (-1) = \frac{-1}{-x} = \frac{1}{x}.$$

Donc u est une primitive de $x \mapsto \frac{1}{x}$ sur \mathbb{R}_*^- .

Soit $v : \begin{array}{ccc} \mathbb{R}^* & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \ln(|x|). \end{array}$ $|x|$ est dérivable sur \mathbb{R}^* donc v aussi.

$$\begin{aligned}\forall x > 0, v(x) &= \ln x \\ \text{donc } \forall x > 0, v'(x) &= \frac{1}{x}.\end{aligned}$$

$$\forall x < 0, v(x) = \ln(-x) = u(x)$$

$$\text{donc } \forall x < 0, v'(x) = \frac{1}{x}.$$

Donc, $\forall x \in \mathbb{R}^*, v'(x) = \frac{1}{x}$. Ainsi, v est une primitive de $x \mapsto \frac{1}{x}$ sur \mathbb{R}^* mais cette primitive n'est pas unique :

$$\begin{aligned}w : \mathbb{R}^* &\longrightarrow \mathbb{R} \\ x &\longmapsto \begin{cases} 1 + \ln x & \text{si } x > 0 \\ \ln(-x) - 3 & \text{si } x < 0 \end{cases}\end{aligned}$$

est une autre primitive de $x \mapsto \frac{1}{x}$ sur \mathbb{R}^* .

|| **Corollaire:** \ln est strictement croissante sur \mathbb{R}_*^+ .

Preuve:

$$\forall x > 0, \ln' x = \frac{1}{x} > 0.$$

□

Proposition: Soit f une fonction croissante sur $]a, b[$ avec $\begin{cases} a \in \mathbb{R} \cup \{-\infty\} \\ b \in \mathbb{R} \cup \{+\infty\}. \end{cases}$ et $a < b$.

1. Si f est majorée, $\lim_{x \rightarrow b^-} f(x) \in \mathbb{R}$.
2. Si f n'est pas majorée, $\lim_{x \rightarrow b^-} f(x) = +\infty$.
3. Si f est minorée, $\lim_{x \rightarrow a^+} f(x) \in \mathbb{R}$.
4. Si f n'est pas minorée, $\lim_{x \rightarrow a^+} f(x) = -\infty$.

□

Proposition:

$$\forall a, b \in \mathbb{R}_*^+, \ln(ab) = \ln a + \ln b.$$

Preuve:

Soit $a > 0$ et $u : \begin{array}{ccc} \mathbb{R}_*^+ & \longrightarrow & \mathbb{R} \\ x & \mapsto & \ln(ax). \end{array}$

u est dérivable sur \mathbb{R}_*^+ et

$$\forall x > 0, u'(x) = \ln'(ax) \times a = \frac{a}{ax} = \frac{1}{x}$$

Donc u est une primitive de $x \mapsto \frac{1}{x}$ sur \mathbb{R}_*^+ . Comme \mathbb{R}_*^+ est un intervalle, il existe $C \in \mathbb{R}$ telle que

$$\forall x \in \mathbb{R}_*^+, u(x) = \ln x + C.$$

En particulier,

$$u(1) = \ln 1 + C$$

$$\ln a = C$$

Donc

$$\forall x > 0, \ln(ax) = \ln x + \ln a.$$

□

Corollaire: Soit $a > 0$ et $n \in \mathbb{Z}$. Alors $\ln(a^n) = n \ln(a)$.

Preuve (par récurrence sur n):

Pour $n \in \mathbb{N}$, on pose

$$\mathcal{P}(n) : \text{"}\ln(a^n) = n \ln a\text{"}.$$

- Avec $n = 0$, $\ln(a^n) = \ln 1 = 0 = 0 \times \ln a$
- Soit $n \in \mathbb{N}$. On suppose $\mathcal{P}(n)$ vraie.

$$\begin{aligned}\ln(a^{n+1}) &= \ln(a \times a^n) \\ &= \ln a + \ln(a^n) \\ &= \ln a + n \ln a \\ &= (n+1) \ln a\end{aligned}$$

Donc

$$\forall n \in \mathbb{N}, \ln(a^n) = n \ln a.$$

-
- $\ln\left(\frac{1}{a}\right) + \ln a = \ln\left(\frac{1}{a} \times a\right) = \ln 1 = 0$
- donc $\ln \frac{1}{a} = -\ln a$
- Soit $n \in \mathbb{Z}^-$. Alors,

$$\ln(a^n) = \ln\left(\left(\frac{1}{a}\right)^{-n}\right) = -n \ln \frac{1}{a} = n \ln a.$$

□

Corollaire:

$$\begin{cases} \lim_{x \rightarrow +\infty} \ln x = +\infty \\ \lim_{x \rightarrow 0} \ln x = -\infty \end{cases}$$

Preuve:

Comme \ln est croissante sur $]0, +\infty[$, on sait que $\lim_{x \rightarrow +\infty} \ln x$ existe. C'est un réel ou $+\infty$.

Supposons cette limite réelle : on pose $\lim_{x \rightarrow +\infty} \ln x = \ell \in \mathbb{R}$. Alors $\lim_{n \rightarrow +\infty} \ln(2^n) = \ell$ car $2^n \xrightarrow[n \rightarrow +\infty]{} +\infty$.

Or,

$$\forall x \in \mathbb{N}, \ln(2^n) = n \ln 2$$

et $2 > 1$ donc $\ln 2 > \ln 1 = 0$ donc $n \ln 2 \xrightarrow[n \rightarrow +\infty]{} +\infty$: une contradiction.

Donc $\ln x \xrightarrow[x \rightarrow +\infty]{} +\infty$.

$$\forall x > 0, \ln x = -\ln \frac{1}{x} \xrightarrow[x \rightarrow 0]{>} -\infty$$

car $\frac{1}{x} \xrightarrow[x \rightarrow 0]{>} +\infty$.

□

Proposition:

$$\lim_{x \rightarrow +\infty} \frac{\ln x}{x} = 0.$$

Preuve:

Soit $x \geq 1$. On a

$$0 = \ln 1 \leq \ln x = \int_1^x \frac{1}{t} dt.$$

et

$$\forall t \in [1, x], t \geq \sqrt{t}$$

donc

$$\forall t \in [1, x], \frac{1}{t} \leq \frac{1}{\sqrt{t}}.$$

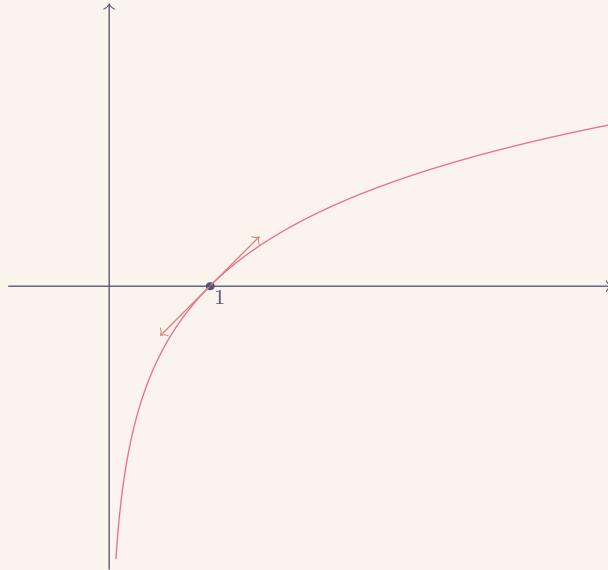
Par croissance de l'intégrale, on en déduit que

$$\ln x = \int_0^1 \frac{1}{t} dt \leq \int_1^x \frac{1}{\sqrt{t}} dt = \left[2\sqrt{t} \right]_1^x = 2\sqrt{x} - 2.$$

Ainsi,

$$\forall x \geq 1, 0 \leq \frac{\ln x}{x} \leq 2 \underbrace{\left(\frac{1}{\sqrt{x}} - \frac{1}{x} \right)}_{x \rightarrow +\infty \rightarrow 0}.$$

Par encadrement, on a donc $\frac{\ln x}{x} \xrightarrow[x \rightarrow +\infty]{} 0$. □



2 Exponentielle

Proposition: $\ln : \mathbb{R}_+^* \rightarrow \mathbb{R}$ est bijective.

Preuve:

\ln est continue sur \mathbb{R}_+^* (car elle est dérivable) et strictement croissante, donc elle établit

une bijection de $]0, +\infty[$ dans $\lim_{\substack{x \rightarrow 0 \\ >}} \ln x, \lim_{x \rightarrow +\infty} \ln x =]-\infty, +\infty[= \mathbb{R}$. \square

Définition: La fonction exponentielle est la réciproque du logarithme népérien. On la note \exp .

Proposition:

1. $\exp : \mathbb{R} \rightarrow \mathbb{R}_+^*$ est dérivable et $\forall x \in \mathbb{R}, \exp'(x) = \exp(x)$;
2. $\begin{cases} \lim_{x \rightarrow +\infty} \exp(x) = +\infty; \\ \lim_{x \rightarrow -\infty} \exp(x) = 0; \end{cases}$
3. $\lim_{x \rightarrow +\infty} \frac{\exp(x)}{x} = +\infty$;
4. $\forall a, b \in \mathbb{R}, \exp(a+b) = \exp(a) \times \exp(b)$.

Preuve:

1. Soit $x \in \mathbb{R}$.

$$\ln'(\exp(x)) = \frac{1}{\exp(x)} \neq 0$$

donc \exp est dérivable sur \mathbb{R} et

$$\forall x \in \mathbb{R}, \exp'(x) = \frac{1}{\ln'(\exp(x))} = \exp(x).$$

2. — $\ln u \xrightarrow[u \rightarrow 0]{} -\infty$ donc $\exp(x) \xrightarrow[x \rightarrow -\infty]{} 0$
 — $\ln u \xrightarrow[u \rightarrow +\infty]{} +\infty$ donc $\exp(x) \xrightarrow[x \rightarrow +\infty]{} +\infty$.

3. Pour $x \in \mathbb{R}$, on pose $x = \ln u \iff u = \exp(x)$. Donc

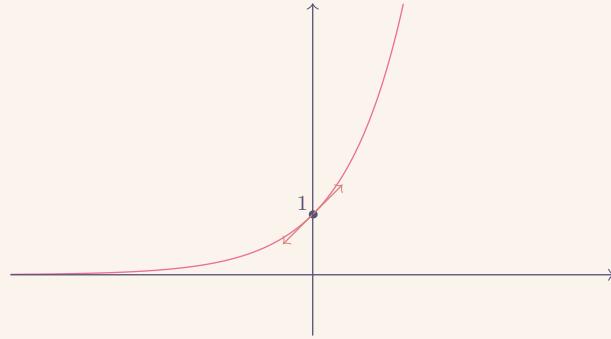
$$\frac{\exp(x)}{x} = \frac{u}{\ln u} = \frac{1}{\frac{\ln u}{u}} \xrightarrow[u \rightarrow +\infty]{} +\infty.$$

4. Soient $a, b \in \mathbb{R}$. On pose $\begin{cases} a = \ln \alpha, \\ b = \ln \beta. \end{cases}$

On a $\exp(a) \times \exp(b) = \alpha \beta$ et

$$\begin{aligned} \exp(a+b) &= \exp(\ln(\alpha) + \ln(\beta)) \\ &= \exp(\ln(\alpha \beta)) \\ &= \alpha \beta \end{aligned}$$

\square



3 Fonctions puissances

REMARQUE (Rappel):

$$\forall a \in \mathbb{R}, \forall x > 0, x^a = \exp(a \ln x).$$

En particulier, en posant $x = e = \exp(1)$, on a donc

$$\forall a \in \mathbb{R}, e^a = \exp(a).$$

REMARQUE (Notation):

Soit $a \in \mathbb{R}$. Pour ce chapitre, on note $p_a : \begin{array}{ccc} \mathbb{R}_+^* & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^a \end{array}$.

Proposition: Soit $a \in \mathbb{R}$. p_a est dérivable sur \mathbb{R}_+^* et

$$\forall x > 0, p'_a(x) = ax^{a-1}.$$

Preuve:

$$\forall x \in \mathbb{R}_+^*, p_a(x) = e^{a \ln x}.$$

Or, \ln , \exp , $x \mapsto ax$ sont dérивables sur leur domaine de définition donc p_a aussi et

$$\forall x > 0, p'_a(x) = \frac{a}{x} e^{a \ln x} = \frac{a}{x} x^a = ax^{a-1}.$$

□

Corollaire:

1. $\forall a \in \mathbb{R}_-^*$, p_a est strictement décroissante.
2. $\forall a \in \mathbb{R}_+^*$, p_a est strictement croissante.
3. p_0 est la fonction constante égale à 1.

Preuve:

Pour tout $x > 0$, $p'_a(x)$ est du signe de a puisque

$$x^{a-1} = e^{(a-1) \ln x} > 0.$$

□

Proposition: 1. Si $a > 0$, $\begin{cases} p_a(x) \xrightarrow[x \rightarrow +\infty]{} +\infty, \\ p_a(x) \xrightarrow[x \rightarrow 0]{} 0; \\ > \end{cases}$

2. Si $a < 0$, $\begin{cases} p_a(x) \xrightarrow[x \rightarrow +\infty]{} 0, \\ p_a(x) \xrightarrow[x \rightarrow 0]{} +\infty; \\ > \end{cases}$

3. Si $a = 0$, $\begin{cases} p_a(x) \xrightarrow[x \rightarrow +\infty]{} 1, \\ p_a(x) \xrightarrow[x \rightarrow 0]{} 1. \\ > \end{cases}$

Preuve:
À faire

□

Proposition: On suppose $a > 0$.

1. Si $a > 1$, alors $\frac{p_a(x)}{x} \xrightarrow[x \rightarrow +\infty]{} +\infty$;
2. Si $a < 1$, alors $\frac{p_a(x)}{x} \xrightarrow[x \rightarrow +\infty]{} 0$;
3. Si $a = 1$, alors $\forall x > 0, p_a(x) = x$.

Preuve:

$$\forall x > 0, \frac{p_a(x)}{x} = \frac{x^a}{x} = x^{a-1}.$$

□

Proposition: On suppose $a > 0$. On peut prolonger p_a par continuité en 0 en posant $p_a(0) = 0$.

1. Si $a > 1$, alors $p'_a(x) \xrightarrow[x \rightarrow 0]{} 0$;
2. Si $a < 1$, alors $p'_a(x) \xrightarrow[x \rightarrow 0]{} +\infty$;

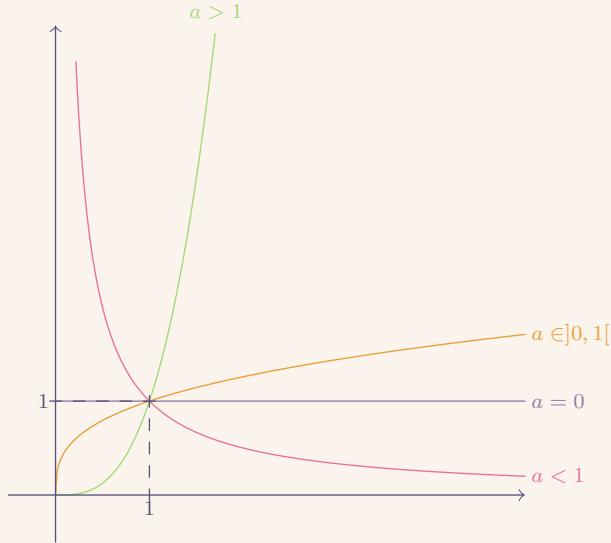
Preuve: 1. On suppose $a > 1$. Alors,

$$\forall x > 0, p'_a(x) = ax^{a-1} \xrightarrow[x \rightarrow 0]{} 0.$$

2. On suppose $a < 1$.

$$\forall x > 0, p'_a(x) = ax^{a-1} \xrightarrow[x \rightarrow 0]{} +\infty.$$

□



Proposition (croissances comparées): Soient $a, b \in \mathbb{R}_*^+$. Alors,

$$\lim_{x \rightarrow +\infty} \frac{\ln^a(x)}{x^b} = 0.$$

EXEMPLE:

Si on ne dispose pas de la formule :

$$\lim_{x \rightarrow +\infty} \frac{\ln x}{\sqrt{x}} = ?$$

On a

$$\frac{\ln x}{\sqrt{x}} = \frac{2 \ln(\sqrt{x})}{\sqrt{x}} = \underbrace{\frac{2 \ln u}{u}}_{u \rightarrow +\infty \rightarrow 0} \text{ avec } u = \sqrt{x} \xrightarrow{x \rightarrow +\infty} +\infty.$$

Preuve:

$$\forall x > 1, \frac{\ln^a(x)}{x^b} = \frac{e^{a \ln(\ln x)}}{e^{b \ln x}} = e^{a \ln(\ln x) - b \ln x}.$$

$$\text{Or } \ln(\ln x) = \underset{x \rightarrow +\infty}{\underset{\circ}{\lim}} (\ln x) \text{ car } \frac{\ln(\ln x)}{\ln x} = \underbrace{\frac{\ln u}{u}}_{u \rightarrow +\infty \rightarrow 0} \text{ avec } u = \ln x \xrightarrow{x \rightarrow +\infty} +\infty.$$

Donc,

$$\frac{\ln^a(x)}{x^b} = e^{a \ln(\ln x) - b \ln x} = e^{\ln(x)(-b + o(1))} \xrightarrow{x \rightarrow +\infty} 0.$$

$$\text{car } \begin{cases} -b + o(1) \xrightarrow{x \rightarrow +\infty} -b < 0 \\ \ln x \xrightarrow{x \rightarrow +\infty} +\infty. \end{cases}$$

□

Corollaire:

$$x \ln x \xrightarrow[x \rightarrow 0]{>} 0.$$

Preuve:

Pour $x \in]0, 1[$, on pose $u = \frac{1}{x} \xrightarrow{x \rightarrow 0} +\infty$.

Donc,

$$\begin{aligned} \forall x \in]0, 1[, x \ln x &= \frac{\ln(\frac{1}{u})}{u} \\ &= -\frac{\ln u}{u} \xrightarrow{u \rightarrow +\infty} 0. \end{aligned}$$

□

Corollaire: Soit $a > 0$. Alors

$$\lim_{x \rightarrow +\infty} \frac{x^a}{e^x} = 0.$$

Preuve:

On fait le changement de variables $u = e^x \xrightarrow{x \rightarrow +\infty} +\infty$.

$$\forall x > 0, \frac{x^a}{e^x} = \frac{\ln^a u}{u} \xrightarrow{u \rightarrow +\infty} 0.$$

□

4 Exponentielle et logarithme de base a

Définition: Soit $a > 0$. L'application $\exp_a : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R}_*^+ \\ x & \mapsto & a^x = e^{x \ln a} \end{array}$ est appelée exponentielle de base a .

REMARQUE:

L'exponentielle de base e est l'exponentielle classique.

Proposition: \exp_a est dérivable sur \mathbb{R} et

$$\forall x \in \mathbb{R}, \exp'_a(x) = \ln(a) \exp_a(x) = a^x \ln a.$$

□

Corollaire: 1. Si $a \in]0, 1[$, alors \exp_a est strictement décroissante.

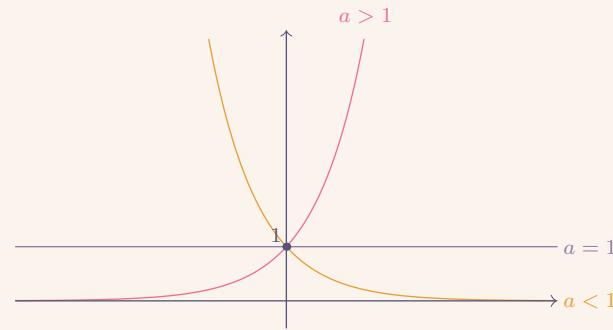
2. Si $a > 1$, alors \exp_a est strictement croissante.

3. Si $a = 1$, alors $\exp_a(x) = 1$ pour tout $x \in \mathbb{R}$.

]]

□

- Proposition:**
1. Si $a \in]0, 1[$,
 - $\exp_a(x) \xrightarrow{x \rightarrow +\infty} 0$,
 - $\exp_a(x) \xrightarrow{x \rightarrow -\infty} +\infty$,
 - $\frac{\exp_a(x)}{x} \xrightarrow{x \rightarrow -\infty} -\infty$;
 2. Si $a > 1$,
 - $\exp_a(x) \xrightarrow{x \rightarrow +\infty} +\infty$,
 - $\frac{\exp_a(x)}{x} \xrightarrow{x \rightarrow +\infty} +\infty$,
 - $\exp_a(x) \xrightarrow{x \rightarrow -\infty} 0$;



- Proposition:** Si $a \in \mathbb{R}_*^+ \setminus \{1\}$, alors \exp_a est bijective.

Définition: Soit $a > 0$ et $a \neq 1$.

La réciproque de \exp_a est appelé logarithme de base a et est noté \log_a .

- Proposition:** Si $a \in \mathbb{R}_*^+ \setminus \{1\}$, alors

$$\forall x > 0, \log_a(x) = \frac{\ln x}{\ln a}.$$

Preuve:

Soit $a \in \mathbb{R}_*^+ \setminus \{1\}$.

- Soit $x > 0$,

$$\exp_a\left(\frac{\ln x}{\ln a}\right) = e^{\frac{\ln x}{\ln a} \times \ln a} = e^{\ln x} = x$$

- Soit $x \in \mathbb{R}$,

$$\frac{\ln(\exp_a(x))}{\ln a} = \frac{\ln(e^{x \ln a})}{\ln a} = \frac{x \ln a}{\ln a} = x.$$

Donc, $\log_a : x \mapsto \frac{\ln x}{\ln a}$ est bien la réciproque de \exp_a . □

EXEMPLE:

Combien y a-t-il de chiffres dans la représentation décimale de 2^{2021} ?

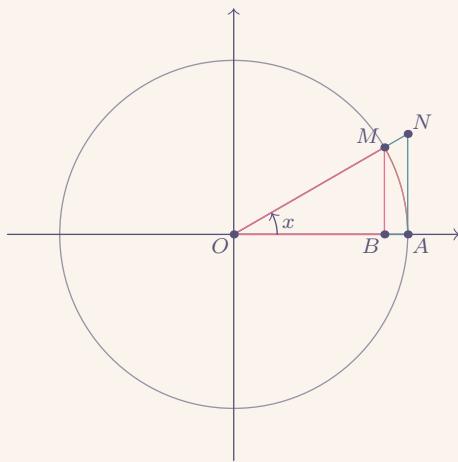
Soit $N \in \mathbb{N}$. La représentation décimale de 2^{2021} a N chiffres si et seulement si

$$\begin{aligned} 10^{N-1} &\leq 2^{2021} < 10^N \\ \iff N-1 &\leq \log_{10}(2^{2021}) < N \\ \iff N-1 &\leq 2021 \log_{10} 2 < N \\ \iff N &> 2021 \log_{10} 2 \text{ et } N \leq 2021 \log_{10}(2) + 1 \\ \iff \underbrace{2021 \log_{10} 2}_{\simeq 608,3} &< N \leq 2021 \log_{10}(2) + 1 \implies N = 609. \end{aligned}$$

5 Fonctions trigonométriques

Proposition:

$$\lim_{x \rightarrow 0} \frac{\sin x}{x} = 1$$



Preuve:

Soit $x \in \left]0, \frac{\pi}{2}\right[$. On pose $M(\cos x, \sin x)$ et $N(1, \tan x)$.

Le triangle OBM est contenu dans le secteur OAM donc

$$\frac{\cos(x)\sin(x)}{2} \leq \frac{x}{2}.$$

Le secteur OAM est contenu dans le triangle OAN donc

$$\frac{x}{2} \leq \frac{\tan x}{2} = \frac{\sin x}{2 \cos x}.$$

D'où,

$$\cos x \leq \frac{\sin x}{x} \leq \frac{1}{\cos x}$$

Or, $\cos x \xrightarrow[x \rightarrow 0]{>} 1$ et $\frac{1}{\cos x} \xrightarrow[x \rightarrow 0]{>} 1$.

Par encadrement, on en déduit que

$$\frac{\sin x}{x} \xrightarrow[x \rightarrow 0]{>} 1$$

et

$$\forall x \in \left] -\frac{\pi}{2}, 0 \right[, \frac{\sin x}{x} = \frac{\sin(-x)}{-x} \xrightarrow[x \rightarrow 0]{>} 1 \text{ d'après le calcul précédent.}$$

□

Corollaire: sin et cos sont dérivables sur \mathbb{R} et $\begin{cases} \sin' = \cos, \\ \cos' = -\sin. \end{cases}$

Preuve:

Soit $x \in \mathbb{R}$ et $h \in \mathbb{R}^*$.

$$\begin{aligned} \frac{\sin(x+h) - \sin x}{h} &= \frac{\sin(x)\cos(h) + \cos(x)\sin(h) - \sin(x)}{h} \\ &= \frac{-1 + \cos h}{h} \sin x + \frac{\sin h}{h} \cos x \\ &= \sin x \times \frac{-2 \sin^2 \frac{h}{2}}{h} + \cos x \frac{\sin h}{h} \end{aligned}$$

Or, $\sin^2 \frac{h}{2} \underset{h \rightarrow 0}{\sim} \left(\frac{h}{2}\right)^2 = \frac{h^2}{4}$. Alors

$$\frac{\sin^2 \frac{h}{2}}{h} \underset{h \rightarrow 0}{\sim} \frac{h}{4} \xrightarrow[h \rightarrow 0]{>} 0.$$

Donc,

$$\frac{\sin(x+h) - \sin x}{h} \xrightarrow[h \rightarrow 0]{>} \cos x.$$

Également, $\forall x \in \mathbb{R}, \cos x = \sin\left(\frac{\pi}{2} - x\right)$ donc

$$\forall x \in \mathbb{R}, \cos'(x) = \cos\left(\frac{\pi}{2} - x\right) \times (-1) = -\sin x.$$

□

Proposition: La fonction tan est dérivable sur $\left\{ x \in \mathbb{R} \mid x \neq \frac{\pi}{2} [\pi] \right\} = D$ et

$$\forall x \in D, \tan' x = 1 + \tan^2 x = \frac{1}{\cos^2 x}.$$

Preuve:

$$\forall x \in D, \tan x = \frac{\sin x}{\cos x}; \sin \text{ et } \cos \text{ sont dérивables sur } \mathbb{R} \text{ donc } \tan \text{ est dérivable sur } D.$$

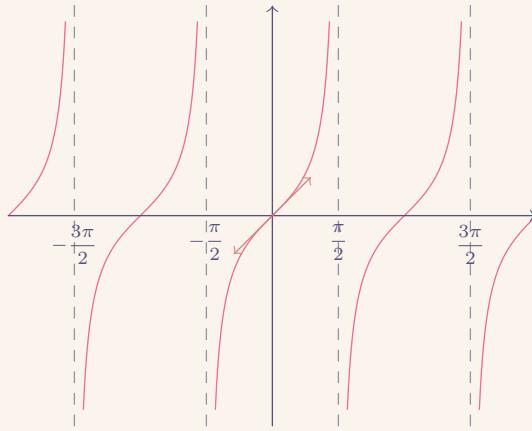
$$\forall x \in D, \tan' x = \frac{\cos^2 x + \sin^2 x}{\cos^2 x} = \frac{1}{\cos^2 x}$$

$$= \frac{1}{1 + \tan^2 x}$$

□

Proposition: $\lim_{\substack{x \rightarrow \frac{\pi}{2} \\ <}} \tan x = +\infty$ et $\lim_{\substack{x \rightarrow \frac{\pi}{2} \\ >}} \tan x = -\infty$.

□



Proposition: cotan est dérivable sur $D = \{x \in \mathbb{R} \mid x \equiv 0 \ [\pi]\}$ et

$$\forall x \in D, \cotan' x = -\frac{1}{\sin^2 x} = -1 - \cotan^2 x.$$

Preuve:

On a

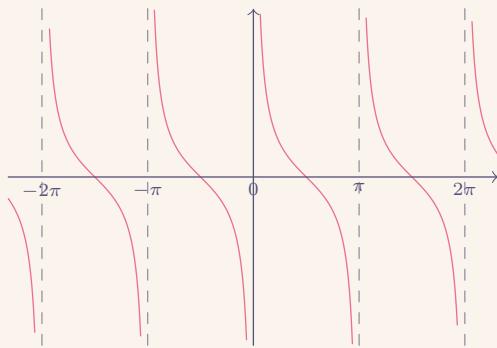
$$\forall x \in D, \cotan x = \frac{\cos x}{\sin x}.$$

Donc,

$$\begin{aligned} \forall x \in D, \cotan' x &= \frac{-\sin^2 x - \cos^2 x}{\sin^2 x} = -\frac{1}{\sin^2 x} \\ &= -1 - \cotan^2 x. \end{aligned}$$

□

Proposition: $\lim_{x \rightarrow -\pi^-} \cotan x = -\infty$ et $\lim_{x \rightarrow \pi^+} \cotan x = +\infty$. □



6 Fonctions trigonométriques réciproques

Proposition – Définition: L'application $\begin{array}{ccc} \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] & \longrightarrow & [-1, 1] \\ x & \mapsto & \sin x \end{array}$ est bijective.

On appelle arcsinus la réciproque de cette bijection et on la note Arcsin.

Pour tout $x \in [-1, 1]$, Arcsin x est le seul angle compris entre $-\frac{\pi}{2}$ et $\frac{\pi}{2}$ donc le sinus vaut x . □

EXEMPLE: — Arcsin 0 = 0,

$$\text{— Arcsin } 1 = \frac{\pi}{2},$$

$$\text{— Arcsin} \left(\sin \frac{3\pi}{2} \right) \neq \frac{3\pi}{2} \text{ car Arcsin}(-1) = -\frac{\pi}{2}.$$

$$\text{— Arcsin} \left(\sin \frac{7\pi}{5} \right) = -\frac{2\pi}{5} \text{ car } \sin \frac{7\pi}{5} = \sin \left(\pi - \frac{7\pi}{5} \right) = \sin \left(-\frac{2\pi}{5} \right) \text{ et } -\frac{2\pi}{5} \in \left[-\frac{\pi}{2}, \frac{\pi}{2} \right].$$

Proposition: 1. $\forall x \in [-1, 1], \text{Arcsin } x \in \left[-\frac{\pi}{2}, \frac{\pi}{2} \right]$

$$2. \forall \theta \in \left[-\frac{\pi}{2}, \frac{\pi}{2} \right], \text{Arcsin}(\sin \theta) = \theta$$

$$3. \forall x \in [-1, 1], \sin(\text{Arcsin } x) = x$$

$$4. \forall x \in [-1, 1], \cos(\text{Arcsin } x) = \sqrt{1 - x^2}$$

Preuve: 1., 2. et 3. correspondent à la définition de Arcsin.

4. Soit $x \in [-1, 1]$. On pose $\theta = \text{Arcsin } x \in \left[-\frac{\pi}{2}, \frac{\pi}{2} \right]$. On sait que $\cos^2 \theta + \sin^2 \theta = 1$ donc $\cos^2 \theta = 1 - \sin^2 \theta = 1 - (\text{Arcsin } x)^2 = 1 - x^2$. On en déduit que $|\cos \theta| = \sqrt{1 - x^2}$. Comme $\theta \in \left[-\frac{\pi}{2}, \frac{\pi}{2} \right]$, $\cos \theta \geq 0$ et donc

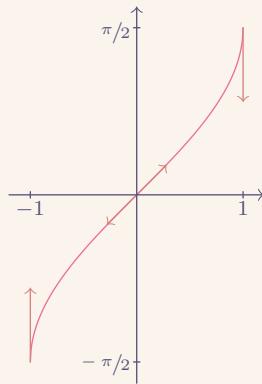
$$\cos(\text{Arcsin } x) = \sqrt{1 - x^2}.$$

□

- Proposition:**
1. Arcsin est impaire
 2. Arcsin est continue sur $[-1, 1]$
 3. Arcsin est dérivable sur $] -1, 1[$ et

$$\forall x \in] -1, 1[, \text{Arcsin}' x = \frac{1}{\sqrt{1-x^2}} > 0$$

4. Arcsin n'est pas dérivable en 1 et en -1.



Preuve:

1. Soit $x \in [-1, 1]$. Alors $-x \in [-1, 1]$. On pose $\theta = \text{Arcsin}(-x)$. θ est le seul nombre compris entre $-\frac{\pi}{2}$ et $\frac{\pi}{2}$ vérifiant $\sin \theta = -x$.
- Arcsin $x \in \left[-\frac{\pi}{2}, \frac{\pi}{2} \right]$ donc $-\text{Arcsin} x \in \left[-\frac{\pi}{2}, \frac{\pi}{2} \right]$. On a

$$\sin(-\text{Arcsin } x) = -\sin(\text{Arcsin } x) = -x$$

donc

$$\theta = \text{Arcsin}(-x) = -\text{Arcsin } x.$$

2. sin est continue et strictement croissante sur $[-\pi/2, \pi/2]$ à valeurs dans $[-1, 1]$ donc Arcsin est continue sur $[-1, 1]$.
3. Soit $x \in [-1, 1]$. $\sin'(\text{Arcsin } x) = \cos(\text{Arcsin } x) = \sqrt{1-x^2}$ donc

$$\forall x \in] -1, 1[, \sin'(\text{Arcsin } x) \neq 0.$$

Donc Arcsin est dérivable sur $] -1, 1[$ et

$$\forall x \in] -1, 1[, \text{Arcsin}' x = \frac{1}{\sqrt{1-x^2}}$$

4. Arcsin est continue sur $[-1, 1]$, dérivable sur $] -1, 1[$, et

$$\forall x \in] -1, 1[, \text{Arcsin}' x = \frac{1}{\sqrt{1-x^2}} \xrightarrow[x \rightarrow \pm 1]{} +\infty.$$

D'après le théorème de la limite de la dérivée, Arcsin n'est pas dérivable en ± 1 .

□

REMARQUE:

Une primitive de $x \mapsto \frac{1}{\sqrt{1-x^2}}$ est Arcsin.

Proposition – Définition: L'application $\begin{array}{ccc} [0, \pi] & \longrightarrow & [-1, 1] \\ x & \mapsto & \cos x \end{array}$ est bijective. On note sa réciproque Arccos.

En d'autres termes, pour $x \in [-1, 1]$, Arccos x est le seul angle compris entre 0 et π dont le cosinus vaut x .

Preuve:

Théorème de la bijection continue. \square

EXEMPLE:

$$\text{Arccos } 0 = \frac{\pi}{2}, \text{ Arccos } \frac{1}{2} = \frac{\pi}{3}, \text{ Arccos } \left(-\frac{1}{2}\right) = \frac{2\pi}{3},$$

$$\text{Arccos} \left(\cos \frac{75\pi}{67}\right) = \frac{59\pi}{67} \in [0, \pi] \text{ car } \cos \frac{75\pi}{67} = \cos \left(\frac{75\pi}{67} - 2\pi\right) = \cos \left(-\frac{59\pi}{67}\right) = \cos \frac{59\pi}{67}.$$

- Proposition:**
1. $\forall x \in [-1, 1], \text{Arccos } x \in [0, \pi],$
 2. $\forall \theta \in [0, \pi], \text{Arccos}(\cos \theta) = \theta,$
 3. $\forall x \in [-1, 1], \cos(\text{Arccos } x) = x,$
 4. $\forall x \in [-1, 1], \sin(\text{Arccos } x) = \sqrt{1 - x^2}.$

Preuve: 1., 2. et 3. correspondent à la définition de Arccos.

4. Soit $x \in [-1, 1]$.

$$\sin^2(\text{Arccos } x) = 1 - \cos^2(\text{Arccos } x) = 1 - x^2$$

donc $|\sin(\text{Arccos } x)| = \sqrt{1 - x^2}$.

Or, $\text{Arccos } x \in [0, \pi]$ donc $\sin(\text{Arccos } x) \geq 0$ et donc

$$\sin(\text{Arccos } x) = \sqrt{1 - x^2}.$$

\square

- Proposition:**
1. Arccos est continue sur $[-1, 1]$,
 2. Arccos est dérivable sur $] -1, 1[$ et

$$\forall x \in] -1, 1[, \text{Arccos}' x = -\frac{1}{\sqrt{1 - x^2}}.$$

Preuve: 1. cos est continue et strictement décroissante sur $[0, \pi]$ à valeurs dans $[-1, 1]$ donc Arccos continue dans $[-1, 1]$.

2.

$$\begin{aligned} \forall x \in] -1, 1[, \cos'(\text{Arccos } x) &= -\sin(\text{Arccos } x) \\ &= -\sqrt{1 - x^2} \neq 0 \end{aligned}$$

donc Arccos est dérivable sur $] -1, 1[$ et

$$\text{Arccos}' x = -\frac{1}{\sqrt{1-x^2}} < 0.$$

□

Corollaire:

$$\forall x \in [-1, 1], \text{Arccos } x + \text{Arcsin } x = \frac{\pi}{2}$$

Preuve: MÉTHODE1 Soit $f : \begin{cases} [-1, 1] & \longrightarrow \mathbb{R} \\ x & \mapsto \text{Arcsin } x + \text{Arccos } x \end{cases}$ continue sur $[-1, 1]$ et dérivable sur $] -1, 1[$. On a

$$\forall x \in] -1, 1[, f'(x) = \frac{1}{\sqrt{1-x^2}} - \frac{1}{\sqrt{1-x^2}} = 0.$$

donc f est constante sur $] -1, 1[$:

$$\exists C \in \mathbb{R}, \forall x \in] -1, 1[, f(x) = C.$$

En particulier,

$$f(0) = \text{Arccos } 0 + \text{Arcsin } 0 = \frac{\pi}{2} + 0 = \frac{\pi}{2}.$$

MÉTHODE2 Soit $x \in [0, 1]$.

$$\begin{aligned} \sin(\text{Arccos } x) &= \sqrt{1-x^2} = \cos(\text{Arcsin } x) \\ &= \sin\left(\frac{\pi}{2} - \text{Arcsin } x\right) \end{aligned}$$

donc

$$\text{Arccos } x \equiv \frac{\pi}{2} - \text{Arcsin } x \quad [2\pi] \quad \text{ou} \quad \pi - \text{Arccos } x \equiv \frac{\pi}{2} - \text{Arcsin } x \quad [2\pi]$$

donc

$$\exists k \in \mathbb{Z}, \text{Arccos } x + \text{Arcsin } x = \frac{\pi}{2} + 2k\pi$$

$$\text{ou } \exists k \in \mathbb{Z}, -\text{Arccos } x + \text{Arcsin } x = -\frac{\pi}{2} + 2k\pi.$$

Or, $\begin{cases} 0 \leqslant \text{Arccos } x \leqslant \pi \\ 0 \leqslant \text{Arcsin } x \leqslant \frac{\pi}{2} \end{cases}$ donc $0 \leqslant \text{Arccos } x + \text{Arcsin } x \leqslant \pi$

$$\Leftrightarrow \begin{cases} -\frac{\pi}{2} \leqslant -\text{Arccos } x \leqslant 0 \\ 0 \leqslant \text{Arcsin } x \leqslant \frac{\pi}{2} \end{cases} \quad \text{donc } -\frac{\pi}{2} \leqslant -\text{Arccos } x + \text{Arcsin } x \leqslant \frac{\pi}{2}$$

D'où

$$\text{Arccos } x + \text{Arcsin } x = \frac{\pi}{2} \quad \text{ou} \quad -\text{Arccos } x + \text{Arcsin } x = -\frac{\pi}{2}$$

— Si $-\text{Arccos } x > -\frac{\pi}{2}$ ou $\text{Arcsin } x > 0$, alors $-\text{Arccos } x + \text{Arcsin } x > -\frac{\pi}{2}$ et donc

$$\text{Arccos } x + \text{Arcsin } x = \frac{\pi}{2}.$$

— Si $-\operatorname{Arccos} x = \frac{\pi}{2}$ et $\operatorname{Arcsin} x = 0$, alors $x = 0$ et donc

$$\operatorname{Arccos} x + \operatorname{Arcsin} x = \frac{\pi}{2} + 0 = \frac{\pi}{2}.$$

Soit $x \in [-1, 0[$. On pose $y = -x \in [0, 1]$

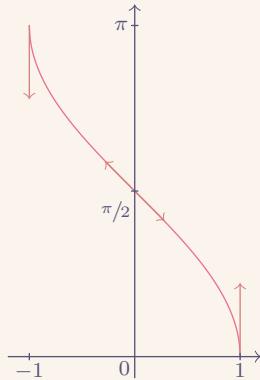
— $\operatorname{Arcsin} x = -\operatorname{Arcsin} y$,

— $\operatorname{Arccos} x = \pi - \operatorname{Arccos} y$: en effet, $\cos(\pi - \operatorname{Arccos} y) = -\cos(\operatorname{Arccos} y) = -y = x$ et $0 \leq \operatorname{Arccos} y \leq \pi$ donc $-\pi \leq \operatorname{Arccos} y \leq 0$ et donc $0 \leq \pi - \operatorname{Arccos} y \leq \pi$

D'où,

$$\begin{aligned}\operatorname{Arccos} x + \operatorname{Arcsin} x &= \pi - \operatorname{Arccos} y - \operatorname{Arcsin} y \\ &= \pi - (\operatorname{Arccos} y + \operatorname{Arcsin} y) \\ &= \pi - \frac{\pi}{2} \\ &= \frac{\pi}{2}.\end{aligned}$$

□



Proposition – Définition: L'application $\begin{array}{ccc} \left] -\frac{\pi}{2}, \frac{\pi}{2} \right[& \longrightarrow & \mathbb{R} \\ x & \mapsto & \tan x \end{array}$ est bijective. On note Arctan la réciproque de cette bijection.

C'est à dire, pour tout $x \in \mathbb{R}$, Arctan x est le seul angle compris entre $-\frac{\pi}{2}$ et $\frac{\pi}{2}$ (exclus) dont la tangente vaut x .

Preuve:

Théorème de la bijection continue.

□

EXEMPLE:

$\operatorname{Arctan} 0 = 0$, $\operatorname{Arctan} 1 = \frac{\pi}{4}$, $\operatorname{Arctan} \sqrt{3} = \frac{\pi}{3}$,

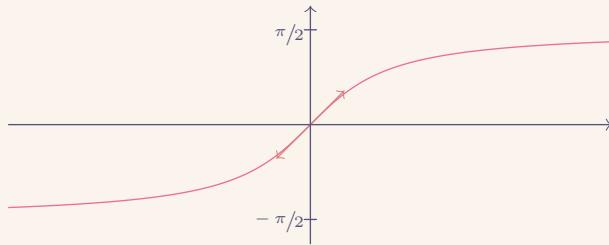
$\operatorname{Arctan}(\tan \frac{9\pi}{7}) = \frac{2\pi}{7} \in \left] -\frac{\pi}{2}, \frac{\pi}{2} \right[$ car $\tan \frac{9\pi}{7} = \tan \left(\frac{9\pi}{7} - \pi \right) = \tan \frac{2\pi}{7}$.

Proposition: 1. Arctan est dérivable sur \mathbb{R} et

$$\forall x \in \mathbb{R}, \text{Arctan}' x = \frac{1}{1+x^2},$$

2. $\begin{cases} \lim_{x \rightarrow +\infty} \text{Arctan } x = \frac{\pi}{2}, \\ \lim_{x \rightarrow -\infty} \text{Arctan } x = -\frac{\pi}{2}, \end{cases}$

3. Arctan est impaire.



Preuve: 1. $\forall x \in \mathbb{R}, \tan'(\text{Arctan } x) = 1 + \tan^2(\text{Arctan } x) = 1 + x^2 \neq 0$ donc Arctan est dérivable sur \mathbb{R} et

$$\forall x \in \mathbb{R}, \text{Arctan}'(x) = \frac{1}{1+x^2}.$$

2. On déduit des limites de tan les limites de Arctan.

3. Comme pour Arcsin.

□

Proposition:

$$\forall x \in \mathbb{R}^*, \text{Arctan } x + \text{Arctan } \frac{1}{x} = \begin{cases} \frac{\pi}{2} & \text{si } x > 0 \\ -\frac{\pi}{2} & \text{si } x < 0 \end{cases}$$

Preuve:

On pose $f : \begin{array}{ccc} \mathbb{R}^* & \longrightarrow & \mathbb{R} \\ x & \mapsto & \text{Arctan } x + \text{Arctan } \frac{1}{x} \end{array}$ dérivable sur \mathbb{R}^* par

$$\begin{aligned} f'(x) &= \frac{1}{1+x^2} - \frac{1}{1+(\frac{1}{x})^2} \times \frac{1}{x^2} \\ &= \frac{1}{1+x^2} - \frac{1}{1+x^2} \\ &= 0 \end{aligned}$$

⚠ \mathbb{R}^* n'est pas un intervalle !

- \mathbb{R}_*^+ est un intervalle donc $\exists C^+ \in \mathbb{R}, \forall x \in \mathbb{R}_*^+, f(x) = C^+$
- \mathbb{R}_*^- est un intervalle donc $\exists C^- \in \mathbb{R}, \forall x \in \mathbb{R}_*^-, f(x) = C^-$

$$\begin{aligned} f(1) &= \frac{\pi}{4} + \frac{\pi}{4} = \frac{\pi}{2} \text{ donc } C^+ = \frac{\pi}{2}, \\ f(-1) &= -\frac{\pi}{4} - \frac{\pi}{4} = -\frac{\pi}{2} \text{ donc } C^- = -\frac{\pi}{2}. \end{aligned}$$

□

7 Trigonométrie hyperbolique

Définition: Pour tout $x \in \mathbb{R}$, on pose

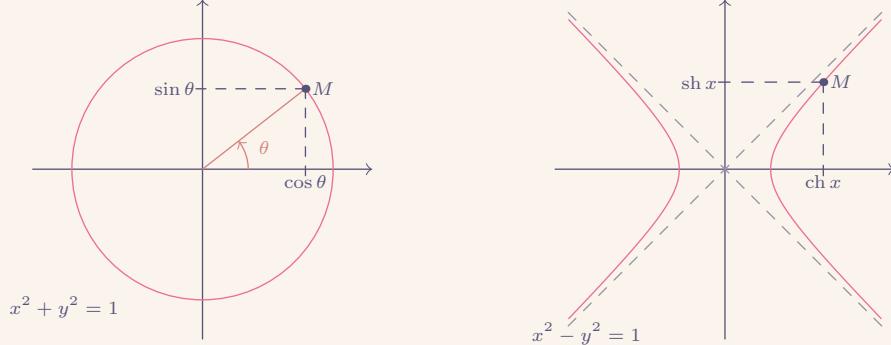
$$\begin{cases} \operatorname{ch} x = \frac{e^x + e^{-x}}{2}, \\ \operatorname{sh} x = \frac{e^x - e^{-x}}{2}, \\ \operatorname{th} x = \frac{\operatorname{sh} x}{\operatorname{ch} x}. \end{cases}$$

ch est appelé cosinus hyperbolique, sh est appelé sinus hyperbolique et th est appelé tangente hyperbolique.

REMARQUE:

Ces formules rappellent les formules d'Euler : pour tout $x \in \mathbb{R}$,

$$\begin{aligned} \cos x &= \frac{e^{ix} + e^{-ix}}{2} &\longleftrightarrow \operatorname{ch} x &= \frac{e^x + e^{-x}}{2} \\ \sin x &= \frac{e^{ix} - e^{-ix}}{2i} &\longleftrightarrow \operatorname{sh} x &= \frac{e^x - e^{-x}}{2} \end{aligned}$$



Proposition:

$$\forall t \in \mathbb{R}, \operatorname{ch}^2 t - \operatorname{sh}^2 t = 1.$$

Preuve:

Soit $t \in \mathbb{R}$.

$$\begin{aligned} \operatorname{ch}^2 t - \operatorname{sh}^2 t &= \left(\frac{e^t + e^{-t}}{2} \right)^2 - \left(\frac{e^t - e^{-t}}{2} \right)^2 \\ &= \frac{e^t + e^{-t} - e^t + e^{-t}}{2} \times \frac{e^t + e^{-t} + e^t - e^{-t}}{2} \\ &= \frac{2e^{-t}}{2} \times \frac{2e^t}{2} \\ &= e^{-t} \times e^t \\ &= 1 \end{aligned}$$

□

EXERCICE:

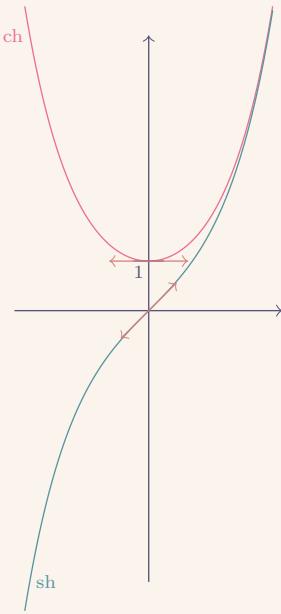
Expliciter $\operatorname{ch}(a+b)$ avec $(a, b) \in \mathbb{R}^2$.

$$\begin{aligned} \operatorname{ch}(a) \operatorname{ch}(b) + \operatorname{sh}(a) \operatorname{sh}(b) &= \frac{2e^{a+b} + e^{b-a} + e^{a-b}}{4} + \frac{2e^{-(a+b)} - e^{a-b} - e^{b-a}}{4} \\ &= \frac{1}{4} (2e^{a+b} + 2e^{-(a+b)}) \\ &= \frac{e^{a+b} + e^{-(a+b)}}{2} \\ &= \operatorname{ch}(a+b). \end{aligned}$$

Expliciter $\operatorname{sh}(a+b)$ avec $(a, b) \in \mathbb{R}^2$.

$$\begin{aligned} \operatorname{sh}(a) \operatorname{ch}(b) + \operatorname{sh}(b) \operatorname{ch}(a) &= \frac{1}{4} (2e^{a+b} + e^{a-b} - e^{b-a} + e^{b-a} - e^{a-b} - 2e^{-(a+b)}) \\ &= \frac{e^{a+b} - e^{-(a+b)}}{2} \\ &= \operatorname{sh}(a+b) \end{aligned}$$

- Proposition:**
1. ch est paire, sh est impaire ;
 2. ch et sh sont dérivables sur \mathbb{R} et $\begin{cases} \operatorname{ch}' = \operatorname{sh}, \\ \operatorname{sh}' = \operatorname{ch}; \end{cases}$
 3. sh est strictement croissante sur \mathbb{R} , ch est strictement croissante sur \mathbb{R}^+ ;
 4. $\lim_{x \rightarrow +\infty} \operatorname{ch} x = +\infty$, $\lim_{x \rightarrow +\infty} \operatorname{sh} x = +\infty$ et $\lim_{x \rightarrow -\infty} \operatorname{sh} x = -\infty$;
 5. $\operatorname{ch} x \underset{x \rightarrow +\infty}{\sim} \frac{1}{2} e^x$ et $\operatorname{sh} x \underset{x \rightarrow +\infty}{\sim} \frac{1}{2} e^x$.



Preuve: 1.

$$\begin{cases} \operatorname{ch}(-x) = \frac{e^{-x} + e^{-(-x)}}{2} = \frac{e^x + e^{-x}}{2} = \operatorname{ch} x; \\ \operatorname{sh}(-x) = \frac{e^{-x} - e^{-(-x)}}{2} = \frac{e^{-x} - e^x}{2} = -\frac{e^x - e^{-x}}{2} = -\operatorname{sh} x. \end{cases}$$

2. $x \mapsto e^x$ et $x \mapsto e^{-x}$ sont dérivables sur \mathbb{R} donc ch et sh aussi. On a donc

$$\forall x \in \mathbb{R}, \begin{cases} \operatorname{ch}'(x) = \frac{e^x - e^{-x}}{2} = \operatorname{sh}(x); \\ \operatorname{sh}'(x) = \frac{e^x + e^{-x}}{2} = \operatorname{ch}(x). \end{cases}$$

3. $\forall x \in \mathbb{R}, \operatorname{sh}' x = \operatorname{ch} x = \frac{e^x + e^{-x}}{2} > 0$ donc sh strictement croissante sur \mathbb{R} .

$\forall x \in \mathbb{R}_*^+, \operatorname{ch}' x = \operatorname{sh} x > \operatorname{sh} 0 = 0$ (car sh strictement croissante) et $\operatorname{ch}' 0 = \operatorname{sh} 0 = 0$. Donc, ch est strictement croissante sur \mathbb{R}^+ .

4. et 5.

$$\forall x \in \mathbb{R}, \begin{cases} \operatorname{ch} x = \frac{1}{2} (e^x + e^{-x}) = \frac{e^x}{2} (1 + e^{-2x}) \underset{x \rightarrow +\infty}{\sim} \frac{e^x}{2} \rightarrow +\infty; \\ \operatorname{sh} x = \frac{1}{2} (e^x - e^{-x}) = \frac{e^x}{2} (1 - e^{-2x}) \underset{x \rightarrow +\infty}{\sim} \frac{e^x}{2} \rightarrow +\infty; \end{cases}$$

□

REMARQUE:

La courbe représentative de ch est appelée "chaînette".

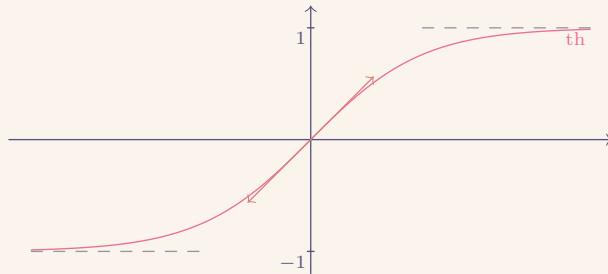
Proposition: 1. th est impaire;

2. th est dérivable sur \mathbb{R} et

$$\forall x \in \mathbb{R}, \operatorname{th}' x = \frac{1}{\operatorname{ch}^2 x} = 1 - \operatorname{th}^2 x;$$

3. th est strictement croissante sur \mathbb{R} ;

4. $\lim_{x \rightarrow +\infty} \operatorname{th} x = 1$ et $\lim_{x \rightarrow -\infty} \operatorname{th} x = -1$.



Preuve: 1. Soit $x \in \mathbb{R}$.

$$\operatorname{th}(-x) = \frac{\operatorname{sh}(-x)}{\operatorname{ch}(-x)} = -\frac{\operatorname{sh} x}{\operatorname{ch} x} = -\operatorname{th} x.$$

2. sh et ch sont dérivables sur \mathbb{R} et $\forall x \in \mathbb{R}, \operatorname{ch} x \neq 0$ donc th est dérivable sur \mathbb{R} et

$$\begin{aligned} \forall x \in \mathbb{R}, \operatorname{th}' x &= \frac{\operatorname{ch}^2 x - \operatorname{sh}^2 x}{2} = \frac{1}{\operatorname{ch}^2 x} \\ &= 1 - \frac{\operatorname{sh}^2 x}{\operatorname{ch}^2 x} = 1 - \operatorname{th}^2 x. \end{aligned}$$

3. $\forall x \in \mathbb{R}, \operatorname{th}' x = \frac{1}{\operatorname{ch}^2 x} > 0$ donc th est strictement croissante sur \mathbb{R} .

4. On a

$$\forall x \in \mathbb{R}, \operatorname{th} x = \frac{\operatorname{sh} x}{\operatorname{ch} x} \sim \frac{e^x/2}{e^x/2} = 1 \xrightarrow{x \rightarrow +\infty} 1$$

et, comme th est impaire,

$$\lim_{x \rightarrow -\infty} \operatorname{th} x = -\lim_{x \rightarrow +\infty} \operatorname{th} x = -1.$$

□

EXERCICE:

Résoudre $\operatorname{sh} x = y$ d'inconnue x et y étant un paramètre réel.

Soit $x \in \mathbb{R}$.

$$\begin{aligned} \operatorname{sh} x = y &\iff \frac{e^x - e^{-x}}{2} = y \\ &\iff (e^x)^2 - 1 = 2ye^x \\ &\iff (e^x - y)^2 - \underbrace{(y^2 + 1)}_{>0} = 0 \\ &\iff (e^x - y - \sqrt{y^2 + 1})(e^x - y + \sqrt{y^2 + 1}) = 0 \\ &\iff e^x = y + \sqrt{y^2 + 1} \text{ ou } e^x = y - \sqrt{y^2 + 1} \end{aligned}$$

Or, $(y + \sqrt{1 + y^2})(y - \sqrt{1 + y^2}) = -1 < 0$ donc $y + \sqrt{1 + y^2}$ et $y - \sqrt{1 + y^2}$ sont de signes opposés.

Comme $y + \sqrt{1 + y^2} > y - \sqrt{1 + y^2}$, on a $\begin{cases} y + \sqrt{1 + y^2} > 0 \\ y - \sqrt{1 + y^2} < 0 \end{cases}$ d'où

$$\operatorname{sh} x = y \iff e^x = y + \sqrt{1 + y^2} \iff x = \ln(y + \sqrt{1 + y^2}).$$

On a trouvé la réciproque de sh :

$$\begin{aligned} \operatorname{Argsh} : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \ln(x + \sqrt{1 + x^2}) \end{aligned}$$

CHAPITRE

5

CALCUL INTÉGRAL

1 Généralités

Définition: Soient I un intervalle de \mathbb{R} , f une fonction continue et $a, b \in I$.

On définit l'intégrale de f de a à b par

$$\int_a^b f(x) \, dx = [F(x)]_a^b = F(b) - F(a)$$

où F est une primitive quelconque de f .

La variable x est muette :

$$\int_a^b f(x) \, dx = \int_a^b f(u) \, du = \int_a^b f(t) \, dt = \int_a^b f(\mathbb{x}) \, d\mathbb{x} \neq \int_a^b f(\textcolor{brown}{x}) \, dt$$

Proposition (Croissance): Soient f et g continues sur I , $a, b \in I^2$ tels que $\begin{cases} \forall x \in I, f(x) \leq g(x), \\ a \leq b. \end{cases}$

Alors

$$\int_a^b f(x) \, dx \leq \int_a^b g(x) \, dx.$$

Preuve:

On pose, pour tout $x \in I$, $h(x) = g(x) - f(x) \geq 0$. h est continue sur I .

Soit H une primitive de h sur I . Donc

$$\begin{aligned}\int_a^b f(x) \, dx - \int_a^b g(x) \, dx &= \int_a^b (f(x) - g(x)) \, dx \\ &= - \int_a^b h(x) \, dx \\ &= H(a) - H(b)\end{aligned}$$

Or, $h = H' \geq 0$ donc H est croissante sur I . Comme $b \geq a$, $H(b) \geq H(a)$ et donc

$$\int_a^b f(x) \, dx - \int_a^b g(x) \, dx \leq 0.$$

□

Proposition (Linéarité): Soient f et g continues sur I , $\alpha, \beta \in \mathbb{R}$ et $a, b \in \mathbb{R}$. Alors,

$$\int_a^b (\alpha f(x) + \beta g(x)) \, dx = \alpha \int_a^b f(x) \, dx + \beta \int_a^b g(x) \, dx.$$

Preuve:

Soient F et G deux primitives sur I de f et g respectivement.

$\alpha F + \beta G$ est un primitive de $\alpha f + \beta g$ sur I car

$$(\alpha F + \beta G)' = \alpha F' + \beta G' = \alpha f + \beta g.$$

D'où

$$\begin{aligned}\int_a^b (\alpha f(x) + \beta g(x)) \, dx &= (\alpha F + \beta G)(b) - (\alpha F + \beta G)(a) \\ &= \alpha F(b) + \beta G(b) - \alpha F(b) - \beta G(a) \\ &= \alpha(F(b) - F(a)) + \beta(G(b) - G(a)) \\ &= \alpha \int_a^b f(x) \, dx + \beta \int_a^b g(x) \, dx.\end{aligned}$$

□

Proposition (Chasles): Soit f continue sur un interval I , $a, b, c \in I$. Alors

$$\int_a^b f(x) \, dx = \int_a^c f(x) \, dx + \int_c^b f(x) \, dx.$$

Preuve:

Soit F une primitive de f sur I . Alors,

$$\begin{aligned} \int_a^c f(x) \, dx + \int_b^c f(x) \, dx &= F(c) - F(a) + F(b) - F(c) \\ &= F(b) - F(a) \\ &= \int_a^b f(x) \, dx. \end{aligned}$$

□

Proposition: Soit f positive et continue sur un interval I , $(a, b) \in I^2$ avec $a \leq b$. Alors

$$\int_a^b f(x) \, dx = 0 \iff \forall x \in [a, b], f(x) = 0.$$

Preuve:

Soit F une primitive de f .

“ \implies ” On suppose que $\int_a^b f(x) \, dx = 0$. Donc $F(b) = F(a)$.

Comme $F' = f \geq 0$, F est croissante.

□

CHAPITRE

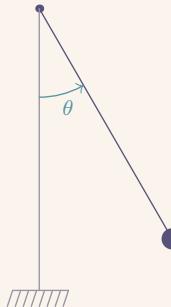
6

ÉQUATIONS DIFFÉRENTIELLES LINÉAIRES

Définition: Une équation différentielle est une égalité faisant intervenir une fonction inconnue y ainsi que ses dérivées successives $y', y'', y^{(3)}, \dots, y^{(n)}$.

EXEMPLE: 1. $y^{(3)} + \ln(y') = e^y$

2.



On a $\ddot{\theta} + \sin(\theta) = 0$ i.e. $\frac{d^2\theta}{dt^2} + \sin(\theta) = 0$
Pour les "petits angles", $\sin(\theta) \simeq 0$. On résout donc

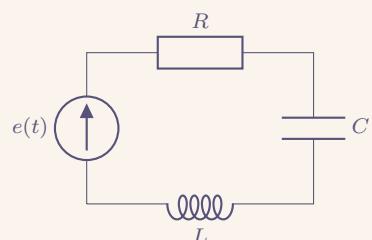
$$\ddot{\theta} = -\theta$$

3.

$$L \frac{d^2q}{dt^2} + R \frac{dq}{dt} + \frac{1}{C} q = e(t)$$

$$L \ddot{q} + R \dot{q} + \frac{1}{C} q = e(t)$$

4. Modèle de population : $\frac{dN}{dt} = \lambda N(1 - N)$



Définition: Une équation différentielle linéaire d'ordre n est de la forme

$$a_n y^{(n)} + a_{n-1} y^{(n-1)} + \dots + a_0 y = b(t)$$

où b, a_0, a_1, \dots, a_n sont des fonctions connues et continues sur un intervalle I . On dit que b est le second membre de l'équation.

EXEMPLE ($\cos(t)y'' + \sin(t)y' = \tan(t)$):

Proposition (Principe de superposition): Soient b_1 et b_2 continues sur I . Soient a_0, a_1, \dots, a_n également continues sur I .

$$(E_1) : \sum_{k=0}^n a_k y^{(k)} = b_1$$

$$(E_2) : \sum_{k=0}^n a_k y^{(k)} = b_2$$

Soient $(\lambda_1, \lambda_2) \in \mathbb{C}^2$.

$$(E) : \sum_{k=1}^n a_k y^{(k)} = \lambda_1 b_1 + \lambda_2 b_2$$

$$\left. \begin{array}{l} y_1 \text{ solution de } (E_1) \\ y_2 \text{ solution de } (E_2) \end{array} \right\} \implies \lambda_1 y_1 + \lambda_2 y_2 \text{ solution de } (E)$$

Preuve:

On pose $y = \lambda_1 y_1 + \lambda_2 y_2$ dérivable n fois car c'est le cas de y_1 et y_2 . Donc,

$$\forall k \in \llbracket 0, n \rrbracket, y^{(k)} = \lambda_1 y_1^{(k)} + \lambda_2 y_2^{(k)}$$

D'où,

$$\begin{aligned} \sum_{k=0}^n a_k y^{(k)} &= \sum_{k=0}^n a_k (\lambda_1 y_1^{(k)} + \lambda_2 y_2^{(k)}) \\ &= \lambda_1 \sum_{k=1}^n a_k y_1^{(k)} + \lambda_2 \sum_{k=1}^n a_k y_2^{(k)} \\ &= \lambda_1 b_1 + \lambda_2 b_2 \end{aligned}$$

□

Proposition: Soit (E) l'équation différentielle $\sum_{k=0}^n a_k y^{(k)} = b$ où a_0, a_1, \dots, a_n sont des fonctions homogènes. L'équation homogène associée à (E) est

$$(H) : \sum_{k=0}^n a_k y^{(k)} = 0$$

Les solutions de (E) sont toutes de la forme $h + y_0$ où h est solution de (H) et y_0 solution de (E) .

Preuve:

Soit y une solution de (E) et y_0 une solution particulière de (E) . On pose $h = y - y_0$. D'après le principe de superposition, h est une solution de (H) .

Réiproquement, si h est une solution de (H) et y_0 une solution de (E) alors $h + y_0$ est aussi solution de (E) . \square

Théorème (Théorème de Cauchy): Soit (E) une équation linéaire différentielle.

$$(E) : y^{(n)} + \sum_{k=0}^{n-1} a_k y^{(k)} = b$$

où a_0, a_1, \dots, a_n sont continues sur un intervalle I .

Soit $t_0 \in I$ et $(\alpha_0, \alpha_1, \dots, \alpha_n) \in \mathbb{C}^n$.

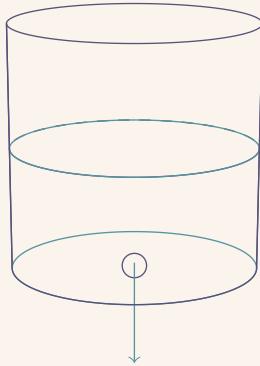
Il existe une et une seule fonction y telle que

$$\begin{cases} y \text{ solution de } (E) \\ \forall i \in \llbracket 0, n-1 \rrbracket, y^{(i)}(t_0) = \alpha_i \end{cases}$$

EXEMPLE:

On ne peut pas déduire le passé d'un sceau percé, son équation est non-linéaire.

$$h' = -c\sqrt{h} \text{ avec } c \in \mathbb{R}_*^+$$



1

Soit (E) l'équation $y' + ay = b$ où a et b sont continues sur un intervalle I .

Proposition: Soit A une primitive de a sur un intervalle I .

$$(H) : y' + ay = 0$$

Les solutions de (H) sont $t \mapsto \lambda e^{-A(t)}$ avec $\lambda \in \mathbb{C}$

Preuve:

Soit y une fonction dérivable sur I . On pose

$$z : t \mapsto y(t)e^{A(t)}$$

dérivable sur I et

$$\begin{aligned}\forall t \in I, z'(t) &= y'(t)e^{A(t)} + y(t)A'(t)e^{A(t)} \\ &= (y'(t) + a(t)y(t))e^{A(t)}\end{aligned}$$

$$\begin{aligned}y \text{ solution de } (H) &\iff \forall t \in I, y'(t) + a(t)y(t) = 0 \\ &\iff \forall t \in I, z'(t) = 0 \\ &\iff \exists \lambda \in \mathbb{C}, \forall t \in I, z(t) = \lambda \\ &\iff \exists \lambda \in \mathbb{C}, \forall t \in I, y(t) = \lambda e^{-A(t)}\end{aligned}$$

□

REMARQUE (pseudo preuve):

$$\begin{aligned}\frac{dy}{dt} + a(t)y = 0 &\iff \frac{dy}{y} = -a(t)dt \\ &\iff \int \frac{dy}{y} = \int -a(t)dt \\ &\iff \ln(y) = -A(t) + K \\ &\iff y = e^{-A(t)+K} \\ &\iff y = \lambda e^{-A(t)} \text{ avec } \lambda = e^K\end{aligned}$$

2 Annexe

$y : I \rightarrow E$ où E est un \mathbb{K} -espace vectoriel.

$$\begin{aligned}(*)&: y' + a(x)y = 0 \text{ et } y(x_0) = 0 \\ &\iff \forall x \in I, y(x) = - \int_{x_0}^x a(u)y(u) du\end{aligned}$$

$$\begin{aligned}T : E^I &\longrightarrow E^I \\ y &\longmapsto \left(x \mapsto - \int_{x_0}^x a(u)y(u) du \right)\end{aligned}$$

donc $(*) \iff T(y) = y$

CHAPITRE

7

DÉVELOPPEMENTS LIMITÉS

Définition: Soit f une fonction définie au voisinage d'un point $a \in \mathbb{R}$.

On dit que f possède un développement limité d'ordre n au voisinage de a s'il existe des réels $(c_0, \dots, c_n) \in \mathbb{R}^{n+1}$ tels que

$$f(x) = c_0 + c_1(x - a) + c_2(x - a)^2 + \cdots + c_n(x - a)^n + \underbrace{\underset{x \rightarrow a}{\circ}}_{\text{reste}}((x - a)^n).$$

En particulier, avec $a = 0$, on a

$$f(x) = \underbrace{c_0 + c_1x + c_2x^2 + \cdots + c_nx^n}_{\text{développement de Taylor}} + \underbrace{\underset{x \rightarrow 0}{\circ}}_{\text{reste}}(x^n).$$

Théorème (Taylor-Young): Si f est de classe \mathcal{C}^n (i.e. f définie et dérivable n fois et $f^{(n)}$ est continue) au voisinage de a , alors f admet un développement limité d'ordre n au voisinage de a est

$$f(x) = f(a) + (x - a)f'(a) + (x - a)^2 \frac{f''(a)}{2!} + \cdots + (x - a)^n \frac{f^{(n)}(a)}{n!} + \underset{x \rightarrow a}{\circ}((x - a)^n).$$

□

REMARQUE:

Cette formule est à éviter en pratique : il est bien trop difficile de calculer $f^{(n)}$ pour tout n .

Cependant, on peut quand même en déduire le développement limité de \exp , \cos , \sin et $x \mapsto (1 + x)^\alpha$ en 0.

Corollaire:

$$\begin{aligned}
 e^x &= 1 + x + \frac{x^2}{2} + \cdots + \frac{x^n}{n!} + \underset{x \rightarrow 0}{\mathcal{O}}(x^n), \\
 \cos x &= 1 - \frac{x^2}{2} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots + (-1)^n \frac{x^{2n}}{(2n)!} + \underset{x \rightarrow 0}{\mathcal{O}}(x^{2n}), \\
 \sin x &= x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots + (-1)^n \frac{x^{2n+1}}{(2n+1)!} + \underset{x \rightarrow 0}{\mathcal{O}}(x^{2n+1}), \\
 \forall \alpha \in \mathbb{R}, (1+x)^\alpha &= 1 + \alpha x + \alpha(\alpha-1) \frac{x^2}{2!} + \alpha(\alpha-1)(\alpha-2) \frac{x^3}{3!} + \cdots \\
 &\quad + \alpha(\alpha-1) \cdots (\alpha-(\alpha-1)) \frac{x^n}{n!} + \underset{x \rightarrow 0}{\mathcal{O}}(x^n).
 \end{aligned}$$

REMARQUE:

Avec $\alpha = -1$, on obtient le développement limité de $\frac{1}{1+x}$ en 0 :

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 + \cdots + (-1)^n x^n + \underset{x \rightarrow 0}{\mathcal{O}}(x^n).$$

On en déduit donc le développement limité en 0 de $\frac{1}{1-x}$:

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots + x^n + \underset{x \rightarrow 0}{\mathcal{O}}(x^n)$$

Avec $\alpha = \frac{1}{2}$, on obtient le développement limité à l'ordre 2 de $\sqrt{1+x}$:

$$\sqrt{1+x} = 1 + \frac{x}{2} - \frac{x^2}{8} + \underset{x \rightarrow 0}{\mathcal{O}}(x^2).$$

Théorème (primitivation): Soit f une fonction continue en a ayant un développement limité d'ordre n au voisinage de a . Soient $(c_0, c_1, \dots, c_n) \in \mathbb{R}^{n+1}$ tels que

$$f(x) = c_0 + c_1(x-a) + c_2(x-a)^2 + \cdots + c_n(x-a)^n + \underset{x \rightarrow a}{\mathcal{O}}((x-a)^n).$$

Soit F une primitive de f . Alors F a un développement limité d'ordre $n+1$ au voisinage de a et

$$F(x) = F(a) = c_0(x-a) + c_1 \frac{(x-a)^2}{2} + \cdots + c_n \frac{(x-a)^{n+1}}{n+1} + \underset{x \rightarrow a}{\mathcal{O}}((x-a)^{n+1}).$$

□

Corollaire: En primitivant le développement limité de $\frac{1}{x+1}$, on obtient le développement limité de $\ln(1+x)$:

$$\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} + \cdots + (-1)^n \frac{x^{n+1}}{n+1} + \underset{x \rightarrow 0}{\mathcal{O}}(x^{n+1}).$$

On en déduit aussi le développement limité de Arctan :

$$\text{Arctan } x = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \cdots + (-1)^n \frac{x^{2n+1}}{2n+1} + \underset{x \rightarrow 0}{\mathcal{O}}(x^{2n+1}).$$

||

□

EXERCICE (*Calculer $DL_5(0)$ de \tan*):

MÉTHODE 1 (quotient) : $\tan x = \frac{\sin x}{\cos x}$.

On a

$$\begin{cases} \sin x = x - \frac{x^3}{6} + \frac{x^5}{120} + o(x^5), \\ \cos x = 1 - \frac{x^2}{2} + \frac{x^4}{24} + o(x^5). \end{cases}$$

On calcule d'abord le développement limité de $\frac{1}{\cos x}$:

$$\begin{aligned} \frac{1}{\cos x} &= \frac{1}{1 - \frac{x^2}{2} + \frac{x^4}{24} + o(x^5)} \\ &= \frac{1}{1+u} \text{ avec } u = -\frac{x^2}{2} + \frac{x^4}{24} + o(x^5) \xrightarrow{x \rightarrow 0} 0 \\ &= 1 - u + u^2 + o(u^2) \\ &= 1 - \left(-\frac{x^2}{2} + \frac{x^4}{24} + o(x^5) \right) \\ &\quad + \left(-\frac{x^2}{2} + \frac{x^4}{24} + o(x^5) \right) \\ &\quad + o\left(\left(-\frac{x^2}{2} + \frac{x^4}{24} + o(x^5)\right)^2\right) \\ &= 1 + \frac{x^2}{2} - \frac{x^4}{24} + \frac{x^4}{4} + o(x^5) \\ &= 1 + \frac{x^2}{2} + \frac{5x^4}{24} + o(x^5). \end{aligned}$$

On en déduit le développement limité de $\tan x$:

$$\begin{aligned} \tan x &= \left(x - \frac{x^3}{6} + \frac{x^5}{120} + o(x^5) \right) \left(1 + \frac{x^2}{2} + \frac{5x^4}{24} + o(x^5) \right) \\ &= x + \frac{x^3}{2} + \frac{5x^5}{24} - \frac{x^3}{6} - \frac{x^5}{12} + \frac{x^5}{120} + o(x^5) \\ &= x + \frac{x^3}{3} + \frac{2x^5}{15} + o(x^5). \end{aligned}$$

À connaître :

$$\boxed{\tan x = x + \frac{x^3}{3} + \underset{x \rightarrow 0}{o}(x^3).}$$

MÉTHODE 2 (déterminer les coefficients)

On identifie les coefficients :

$$\begin{aligned} \sin x &= (\tan x)(\cos x) \\ &= (c_0 + c_1 x + c_2 x^2 + c_3 x^3 + c_4 x^4 + c_5 x^5 + o(x^5)) \\ &\quad \times \left(1 - \frac{x^2}{2} + \frac{x^4}{24} + o(x^5) \right) \\ &= c_0 + c_1 x + c_2 x^2 + c_3 x^3 + c_4 x^4 + c_5 x^5 + o(x^5) \\ &\quad - c_0 \frac{x^2}{2} - c_1 \frac{x^3}{2} - c_2 \frac{x^4}{2} - c_3 \frac{x^5}{2} + c_0 \frac{x^4}{24} + c_1 \frac{x^5}{24} \end{aligned}$$

Par unicité du développement limité,

$$\begin{cases} c_0 = 0 \\ c_1 = 1 \\ c_2 - \frac{c_0}{2} = 0 \\ c_3 - \frac{c_1}{2} = -\frac{1}{6} \\ c_4 - \frac{c_2}{2} + \frac{c_0}{24} = 0 \\ c_5 - \frac{c_3}{2} + \frac{c_1}{24} = \frac{1}{120} \end{cases}$$

et donc

$$\begin{cases} c_0 = c_2 = c_4 = 0 \\ c_1 = 1 \\ c_3 = \frac{1}{2} \\ c_5 = \frac{1}{15} \end{cases}$$

MÉTHODE 3 (primitivation)

On sait que

$$\frac{\tan x - \tan 0}{x - 0} \xrightarrow{x \rightarrow 0} \tan'(0) = 1$$

donc $\tan x \sim x$ et donc $\tan x = x + o(x)$.

D'où

$$\begin{aligned} \tan'(x) &= 1 + \tan^2(x) = 1 + (x + o(x))^2 \\ &= 1 + x^2 + o(x^2). \end{aligned}$$

En intégrant, on en déduit que

$$\tan x = \tan 0 + x + \frac{x^3}{3} + o(x^3)$$

Donc,

$$\begin{aligned} \tan'(x) &= 1 + \tan^2 x \\ &= 1 + \left(x + \frac{x^3}{3} + o(x^3) \right)^2 \\ &= 1 + x^2 + \frac{x^6}{9} + o(x^6) + 2 \frac{x^4}{3} + o(x^4) + o(x^6) \\ &= 1 + x^2 + \frac{2}{3} x^4 + o(x^4) \end{aligned}$$

On en déduit donc le développement limité à l'ordre 5 de \tan :

$$\tan x = \underbrace{\tan 0}_{0} + \frac{x^3}{3} + \frac{2}{15} x^5 + o(x^5)$$

CHAPITRE

8

ENSEMBLES, APPLICATIONS, RELATIONS ET LOIS DE COMPOSITION

1 Théorie naïve des ensembles

Définition: Un ensemble est une collection finie ou infinie d'objets de même nature ou non. L'ordre de ces objets n'a pas d'importance.

EXEMPLE: 1. $\{1, x \mapsto x^2, \{1\}\}$ est un ensemble : ses éléments sont l'entier 1, la fonction $x \mapsto x^2$ et un ensemble contenant uniquement 1 (un singleton).

2. \mathbb{N} est un ensemble infini

REMARQUE (Notation):

Soit E un ensemble et x un objet de E .
On écrit $x \in E$ ou bien $x \ni E$.

REMARQUE (Δ Paradoxe):

On note Ω l'ensemble de tous les ensembles. Alors, $\Omega \in \Omega$.
Ce n'est pas le cas de tous les ensembles :

$\mathbb{N} \not\in \mathbb{N}$ car \mathbb{N} n'est pas un entier

On distingue donc 2 types d'ensembles :

- ceux qui vérifient $E \not\in E$, on dit qu'ils sont ordinaires
- ceux qui vérifient $E \in E$, on dit qu'ils sont extra-ordinaires

On note O l'ensemble de tous les ensembles ordinaires.

- Supposons O ordinaire. Alors, $O \not\in O$
Or, O est ordinaire et donc $O \in O \not\in O$
- Supposons O extra-ordinaire.
Alors $O \in O$ et donc O ordinaire $\not\in O$

C'est un paradoxe

Pour éviter ce type de paradoxe, on a donné une définition axiomatique qui explique quelles sont les opérations permettant de combiner des ensembles pour en faire un autre.

Définition: Soit E un ensemble et F un autre ensemble. On dit que E et F sont égaux (noté $E = F$) si E et F contiennent les mêmes objets.

EXEMPLE: 1. $E = \{1, 2, 3\}$ et $F = \{3, 2, 1, 2\}$

On a bien $E = F$.

2. $\mathbb{N} \neq \mathbb{Z}$ car $\begin{cases} -1 \in \mathbb{Z} \\ -1 \notin \mathbb{N} \end{cases}$

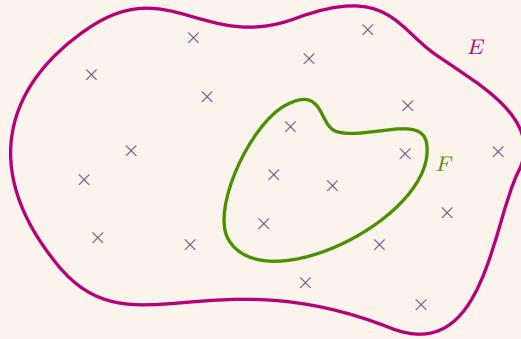
3. $E = \{0, \{0\}\} \neq \{0\} = F$

car $\begin{cases} \{0\} \in E \\ \{0\} \notin F \\ \text{mais, } F \in E \end{cases}$

Définition: L'ensemble vide, noté \emptyset est le seul ensemble à n'avoir aucun élément.

Définition: Soient E et F deux ensembles. On dit que F est inclus dans E , noté $F \subset E$ ou $E \supset F$ si tous les éléments de F sont aussi des éléments de E .

$$\forall x \in F, x \in E$$



Proposition: Pour tout ensemble E , $\emptyset \subset E$

Preuve (par l'absurde):
Si $\emptyset \not\subset E$ alors $\exists x \in \emptyset, x \notin E$: une contradiction \square

EXEMPLE: 1. $E = \{1, 2, 3\}$ et $F = \{1, 3\}$

On a $F \subset E$ mais pas $E \subset F$ car $\begin{cases} 2 \in E \\ 2 \notin F \end{cases}$

2. $F = \{0\}$ et $E = \{0, \{0\}\}$

- $F \in E$ car $\{0\} \in E$
- $F \subset E$ car $0 \in E$

3. $E = \{\{0\}\}; F = \{0\}$

- $F \not\subset E$ car $0 \notin E$
- $F \in E$

4. $E = \{\{\{0\}\}\}; F = \{0\}$

- $F \not\subset E$
- $F \not\subset E$
- $\emptyset \subset F$
- $\emptyset \subset E$

Définition: Soit E un ensemble. On peut former l'ensemble de toutes les parties de E (une partie de E est un ensemble F avec $F \subset E$). On le note $\mathcal{P}(E)$

$$A \in \mathcal{P}(E) \iff A \subset E$$

EXEMPLE: 1. $E = \{42\}$

Les sous-ensembles de E sont \emptyset et $\{42\} = E$ donc

$$\mathcal{P}(E) = \{\emptyset, \{42\}\}$$

2. $\mathcal{P}(\emptyset) = \{\emptyset\}$

3. $E = \{0, 1\}$ donc $\mathcal{P}(E) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$

4. $E = \{\emptyset, \{\emptyset\}\}$ donc $\mathcal{P}(E) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$

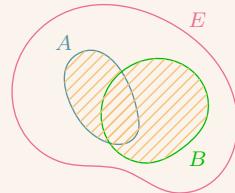
5. $E = \{\emptyset, \{\emptyset\}\}$

$$\begin{aligned} \mathcal{P}(\mathcal{P}(E)) &= \mathcal{P}(\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, E\}) \\ &= \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \{E\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\{\emptyset\}\}\}, \{\emptyset, E\}, \{\{\emptyset\}, \\ &\quad \{\{\emptyset\}\}, \{\{\{\emptyset\}\}, E\}, \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}, \{\emptyset, \{\emptyset\}, E\}, \\ &\quad \{\emptyset, \{\{\emptyset\}\}, E\}, \{\{\emptyset\}, \{\{\emptyset\}\}, E\}, \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, E\} \} \end{aligned}$$

Définition: Soit E un ensemble et $A, B \in \mathcal{P}(E)$

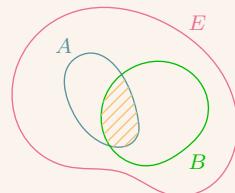
1. La réunion de A et B est

$$A \cup B = \{x \in E \mid x \in A \text{ ou } x \in B\}$$



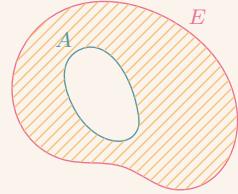
2. L'intersection de A et B est

$$A \cap B = \{x \in E \mid x \in A \text{ et } x \in B\}$$



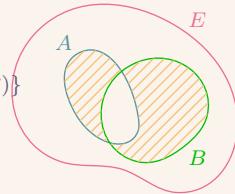
3. Le complémentaire de A dans E est

$$E \setminus A = \{x \in E \mid x \notin A\} = C_E A$$



4. La différence symétrique de A et B est

$$\begin{aligned} A \Delta B &= \{x \in E \mid (x \in A \text{ et } x \notin B) \text{ ou } (x \notin A \text{ et } x \in B)\} \\ &= (A \cup B) \setminus (A \cap B) \end{aligned}$$



Proposition: Soit E un ensemble et $A, B, C \in \mathcal{P}(E)$

- | | |
|--|---|
| 1. $A \cap A = A$ | 10. $A \cup E = E$ |
| 2. $B \cap A = A \cap B$ | 11. $(E \setminus A) \setminus A = E \setminus A$ |
| 3. $A \cap (B \cap C) = (A \cap B) \cap C$ | 12. $E \setminus (E \setminus A) = A$ |
| 4. $A \cap \emptyset = \emptyset$ | 13. $E \setminus \emptyset = E$ |
| 5. $A \cap E = A$ | 14. $E \setminus E = \emptyset$ |
| 6. $A \cup A = A$ | 15. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ |
| 7. $B \cup A = A \cup B$ | 16. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ |
| 8. $A \cup (B \cup C) = (A \cup B) \cup C$ | 17. $E \setminus (A \cup B) = (E \setminus A) \cap (E \setminus B)$ |
| 9. $A \cup \emptyset = A$ | 18. $E \setminus (A \cap B) = (E \setminus A) \cup (E \setminus B)$ |

Preuve: 16. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

— Soit $x \in A \cap (B \cup C)$ donc $x \in A$ et $x \in B \cup C$

CAS1 $x \in B$, alors $x \in A \cap B$ et donc $x \in (A \cap B) \cup (A \cap C)$

CAS2 $x \in C$, alors $x \in A \cap C$ et donc $x \in (A \cap B) \cup (A \cap C)$

On a prouvé

$$A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$$

— Soit $x \in (A \cap B) \cup (A \cap C)$

CAS1 $x \in A \cap B$ donc $x \in A$ et $x \in B$ donc $x \in B \cup C$ et donc $x \in A \cap (B \cup C)$

CAS2 $x \in A \cap C$ donc $x \in A$ et $x \in C$ donc $x \in B \cup C$ et donc $x \in A \cap (B \cup C)$

On a prouvé

$$A \cap (B \cup C) \supset (A \cap B) \cup (A \cap C)$$

17. $E \setminus (A \cup B) = (E \setminus A) \cap (E \setminus B)$

— Montrons que $x \in E \setminus (A \cup B) \implies x \in (E \setminus A) \cap (E \setminus B)$

Soit $x \in E \setminus (A \cup B)$ donc $x \notin A \cup B$

— Si $x \in A$, alors $x \in A \cup B \not\in$

donc $x \notin A$ i.e. $x \in E \setminus A$

— Si $x \in B$ alors, $x \in A \cup B \not\in$

Donc $x \notin B$ i.e. $x \in E \setminus B$

On en déduit que $x \in (E \setminus A) \cap (E \setminus B)$

- $x \in (E \setminus A) \cap (E \setminus B)$. Montrons que $x \in E \setminus (A \cup B)$
On suppose que $x \notin E \setminus (A \cup B)$ donc $x \in A \cup B$
 - Si $x \in A$, on a une contradiction car $x \in E \setminus A$
 - Si $x \in B$, on a une contradiction car $x \in E \setminus B$
donc $x \in E \setminus (A \cup B)$

□

2 Applications

Définition: Une application f est la donnée de

- un ensemble E appelé ensemble de départ
- un ensemble F appelé ensemble d'arrivée
- une fonction qui associe à tout élément x de E un unique élément de F noté $f(x)$

L'application est notée

$$\begin{aligned} f : E &\longrightarrow F \\ x &\longmapsto f(x) \end{aligned}$$

EXEMPLE: 1. Soit \mathcal{P} le plan (affine) et $A \in \mathcal{P}$. Soit \mathcal{D} l'ensemble des droites.

$$\begin{aligned} f : \mathcal{P} \setminus \{A\} &\longrightarrow \mathcal{D} \\ B &\longmapsto (AB) \end{aligned}$$

2. $E = \mathcal{C}^1([0, 1], \mathbb{R})$ l'ensemble des fonctions à valeurs réelles de classe \mathcal{C}^1 sur $[0, 1]$
 $F = \mathcal{C}^0([0, 1], \mathbb{R})$

$$\begin{aligned} \varphi : E &\longrightarrow F \\ f &\longmapsto f' \end{aligned}$$

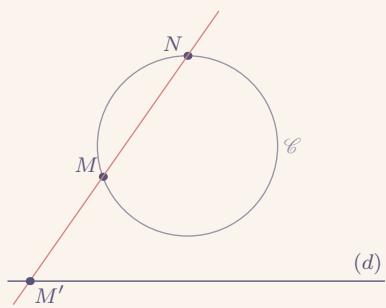
3. $E = \mathcal{C}^1([0, 1], \mathbb{R})$ et $F = \mathbb{R}$

$$\begin{aligned} \varphi : E &\longrightarrow F \\ f &\longmapsto f'\left(\frac{1}{2}\right) \end{aligned}$$

4. $E = [0, 1]$ et $F = \mathcal{C}^0([0, 1], \mathbb{R})$

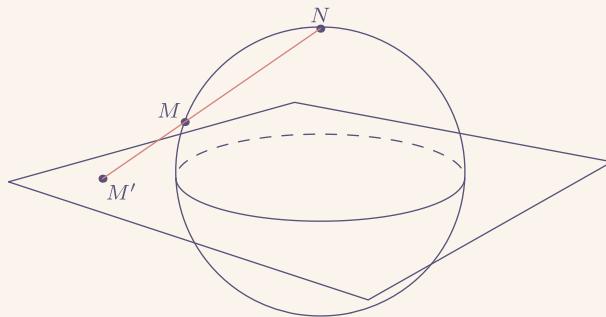
$$\begin{aligned} \varphi : E &\longrightarrow F \\ x &\longmapsto \int_a^x t^2 \ln(t) dt \end{aligned}$$

5.



$$\begin{aligned}\varphi : \mathcal{C} \setminus \{N\} &\longrightarrow (d) \\ M &\longmapsto M'\end{aligned}$$

6.

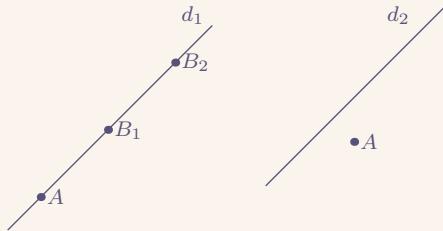


Définition: Soit $f : E \rightarrow F$ une application. On dit que f est

- injective si tout élément de F a au plus un antécédent par f
- bijective si tout élément de F a un unique antécédent par f
- surjective si tout élément de F a au moins un antécédent par f

EXAMPLE (suite des exemples précédents):

1. L'application n'est ni injective ni surjective



B_1 et B_2 sont deux antécédents de d_1
 d_2 n'a pas d'antécédant par f

2. L'application n'est pas injective :
 - $f : x \mapsto x$ est continue
 - $x \mapsto \frac{x^2}{2}$ et $x \mapsto \frac{x^2}{2} + 42$ sont deux antécédents de f .
 Mais, l'application est surjective d'après le théorème fondamental de l'analyse
3. L'application n'est pas injective ($x \mapsto 0$ et $x \mapsto 42$ sont deux antécédents de 0) mais elle est surjective ($\forall x \in \mathbb{R}, x \mapsto ax$ est un antécédent de a).
4. L'application est injective mais pas surjective (les images sont des primitives de $x \mapsto x^2 \ln(x)$)
5. et 6. sont bijectives

Définition: Soit $f : E \rightarrow F$ et $g : F \rightarrow G$. L'application notée $g \circ f$ est définie par

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

On dit que c'est la composée de f et g .

Proposition: Soient $f : E \rightarrow F, g : F \rightarrow G, h : G \rightarrow G$. Alors, $h \circ (g \circ f) = (h \circ g) \circ f$

Preuve:

Par définition, $g \circ f : E \rightarrow F$ donc $h \circ (g \circ f) : E \rightarrow H$ et $h \circ g : F \rightarrow H$ donc $(h \circ g) \circ f : E \rightarrow H$. Soit $x \in E$.

$$\begin{aligned} h \circ (g \circ f)(x) &= h(g \circ f(x)) \\ &= h(g(f(x))) \end{aligned}$$

$$\begin{aligned} (h \circ g) \circ f(x) &= h \circ g(f(x)) \\ &= h(g(f(x))) \end{aligned}$$

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

□

REMARQUE (Δ Attention):

En général, $g \circ f \neq f \circ g$

Par exemple, $f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R}^+ \\ x & \longmapsto & x^2 \end{array}$ et $g : \begin{array}{ccc} \mathbb{R}^+ & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \sqrt{x} \end{array}$

Alors, $f \circ g : \begin{array}{ccc} \mathbb{R}^+ & \longrightarrow & \mathbb{R}^+ \\ x & \longmapsto & x \end{array}$ et $g \circ f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & |x| \end{array}$

donc $f \circ g \neq g \circ f$

Proposition: Soient $f : E \rightarrow F$ et $g : F \rightarrow G$

1. Si $g \circ f$ est injective, alors f est injective
2. Si $g \circ f$ est surjective, alors g est surjective
3. Si f et g sont surjectives, alors $g \circ f$ est surjective
4. Si f et g sont injectives, alors $g \circ f$ est injective

Preuve: 1. On suppose $g \circ f$ injective. On veut montrer que f est injective. Soient $(x, y) \in E^2$. On suppose $f(x) = f(y)$. Montrons que $x = y$.

Comme $f(x) = f(y)$, $g(f(x)) = g(f(y))$ i.e. $g \circ f(x) = g \circ f(y)$
Or, $g \circ f$ injective donc $x = y$

2. On suppose $g \circ f$ surjective. On veut montrer que g est surjective. Soit $y \in G$.
On cherche $x \in F$ tel que $g(x) = y$.

Comme $g \circ f : E \rightarrow G$ surjective, y a un antécédant $z \in E$ par $g \circ f$.
On pose $x = f(z) \in F$ et on a bien $g(x) = y$

3. On suppose f et g injectives. Montrons que $g \circ f$ injective. Soient $x, y \in E$. On suppose $g \circ f(x) = g \circ f(y)$. Montrons $x = y$
On sait que $g(f(x)) = g(f(y))$. Comme g est injective, $f(x) = f(y)$ et comme f est injective, $x = y$

4. On suppose f et g surjectives. Soit $y \in G$. On cherche $x \in E$ tel que $g \circ f(x) = y$
Comme g est surjective, y a un antécédant $z \in F$ par g
Comme f est surjective, z a un antécédant $x \in E$ par f
On en déduit $g \circ f(x) = g(f(x)) = g(z) = y$

□

REMARQUE:

$$f : E \longrightarrow F$$

$$f \text{ injective} \iff \left(\forall (x, y) \in E^2, f(x) = f(y) \implies x = y \right)$$

Définition: Soit $f : E \rightarrow F$ une bijection. L'application $\begin{cases} F & \longrightarrow E \\ y & \mapsto \text{l'unique antécédent de } y \text{ par } f \end{cases}$ est la réciproque de f notée f^{-1}

Définition: L'identité de E est $\text{id}_E : \begin{cases} E & \longrightarrow E \\ x & \mapsto x \end{cases}$

Proposition: Soient $f : E \rightarrow F$ et $g : F \rightarrow E$

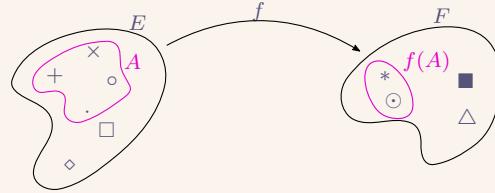
$$\begin{cases} f \circ g = \text{id}_F \\ g \circ f = \text{id}_E \end{cases} \iff \begin{cases} f \text{ bijective} \\ f^{-1} = g \end{cases}$$

Preuve (déjà faite): □

Définition: Soit $f : E \rightarrow F$

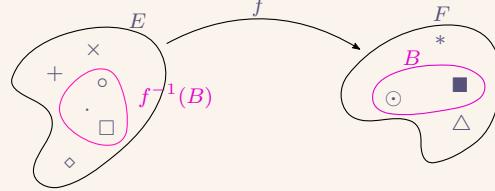
1. Soit $A \in \mathcal{P}(E)$. L'image directe de A par f est

$$f(A) = \{f(x) \mid x \in A\}$$



2. Soit $B \in \mathcal{P}(F)$. L'image réciproque de B par f est

$$f^{-1}(B) = \{x \in E \mid f(x) \in B\}$$



REMARQUE:

- $y \in f(A) \iff \exists x \in A, y = f(x),$
- $x \in f^{-1}(B) \iff f(x) \in B.$

Proposition: Soient $f : E \rightarrow F$, $A \in \mathcal{P}(E)$ et $F \in \mathcal{P}(F)$.

1. $f^{-1}(f(A)) \supset A$,
2. Si f est injective alors $f^{-1}(f(A)) = A$,
3. $f(f^{-1}(B)) \subset B$,
4. Si f est surjective, alors $f(f^{-1}(B)) = B$.

Preuve: 1. Soit $x \in A$. Montrons que $x \in f^{-1}(f(A))$ i.e. montrons que $f(x) \in f(A)$.

Comme $x \in A$, $f(x) \in f(A)$.

2. On suppose f injective. Montrons que $f^{-1}(f(A)) = A$. Soit $x \in f^{-1}(f(A))$, montrons que $x \in A$. On sait que $f(x) \in f(A)$. Donc, il existe $a \in A$ tel que $f(x) = f(a)$. Or, f est injective et donc $x = a$. On en déduit que $x \in A$.

D'après 1., on sait que $f^{-1}(f(A)) \supset A$. On a montré $f^{-1}(f(A)) \subset A$. Donc

$$f^{-1}(f(A)) = A.$$

3. Soit $y \in f(f^{-1}(B))$. Montrons $y \in B$. On sait qu'il existe $x \in f^{-1}(B)$ tel que $y = f(x)$. On a donc $f(x) \in B$ et donc $y \in B$.

4. On suppose f surjective, montrons $B \subset f(f^{-1}(B))$. Soit $y \in B$, montrons $y \in f(f^{-1}(B))$. On cherche $x \in f^{-1}(B)$ tel que $y = f(x)$. C'est à dire, on cherche $x \in E$ tel que $f(x) \in B$ et $y = f(x)$. On sait que f est surjective donc y a un antécédant $x \in E$ tel que $B \ni y = f(x)$.

On vient de montrer $B \subset f(f^{-1}(B))$ et on a montré dans 3. que $B \supset f(f^{-1}(B))$.

On en déduit que

$$f(f^{-1}(B)) = B.$$

□

Proposition: Soit $f : E \rightarrow F$ et $(A, B) \in \mathcal{P}(F)^2$. Alors

$$\begin{cases} f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B), & (1) \\ f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B). & (2) \end{cases}$$

Preuve:

Soit $x \in E$.

$$\begin{aligned} x \in f^{-1}(A \cup B) &\iff f(x) \in A \cup B \\ &\iff f(x) \in A \text{ ou } f(x) \in B \\ &\iff x \in f^{-1}(A) \text{ ou } x \in f^{-1}(B) \\ &\iff x \in f^{-1}(A) \cup f^{-1}(B). \end{aligned}$$

$$\begin{aligned} x \in f^{-1}(A \cap B) &\iff f(x) \in A \cap B \\ &\iff f(x) \in A \text{ et } f(x) \in B \\ &\iff x \in f^{-1}(A) \text{ et } x \in f^{-1}(B) \\ &\iff x \in f^{-1}(A) \cap f^{-1}(B). \end{aligned}$$

□

Proposition: Soient $f : E \rightarrow F$ et $(A, B) \in \mathcal{P}(E)^2$.

1. $f(A \cap B) \subset f(A) \cap f(B)$
2. Si f est injective, $f(A \cap B) = f(A) \cap f(B)$
3. $f(A \cup B) = f(A) \cup f(B)$.

Preuve: 1. Soit $y \in f(A \cap B)$. Soit $x \in A \cap B$ tel que $y = f(x)$. Comme $x \in A$, $f(x) \in f(A)$ et comme $x \in B$, $f(x) \in f(B)$ et donc $y \in f(A) \cap f(B)$

2. On suppose f injective. Soit $y \in f(A) \cap f(B)$.
Comme $y \in f(A)$, il existe $a \in A$ tel que $y = f(a)$.
Comme $y \in f(B)$, il existe $b \in B$ tel que $y = f(b)$.
Comme f est injective, $a = b$ et donc $a \in A \cap B$. On en déduit que

$$y = f(a) \in f(A \cap B).$$

3. Soit $y \in F$. Alors

$$\begin{aligned} y \in f(A \cup B) &\iff \exists x \in A \cup B; y = f(x) \\ &\iff (\exists x \in A \text{ ou } \exists x \in B), y = f(x) \\ &\iff y \in f(A) \text{ ou } y \in f(B) \\ &\iff y \in f(A) \cup f(B). \end{aligned}$$

□

REMARQUE (Contre-exemple pour 2.):

Cas d'une application qui n'est pas injective

On pose $A = \mathbb{R}_*^+$, $B = \mathbb{R}_*^-$ et

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R}^+ \\ x &\longmapsto x^2 \end{aligned}$$

On a $A \cap B = \emptyset$ donc $f(A \cap B) = \emptyset$.

$$\text{Or, } \left. \begin{array}{l} f(A) = \mathbb{R}_*^+ \\ f(B) = \mathbb{R}_*^+ \end{array} \right\} \text{ donc } f(A) \cap f(B) = \mathbb{R}_*^+.$$

On a

$$f(A \cap B) \neq f(A) \cap f(B).$$

Définition: Soit $f : E \rightarrow F$ et $A \in \mathcal{P}(E)$.

La restriction de f à A est

$$\begin{aligned} f|_A : A &\longrightarrow F \\ x &\longmapsto f(x)a \end{aligned}$$

On dit aussi que f est un prolongement de $f|_A$.

REMARQUE (Notation):

L'ensemble des applications de E dans F est noté F^E .

EXEMPLE:

$$\text{On pose } f : \begin{array}{ccc} \mathbb{R}^* & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \frac{1}{x} \end{array} \text{ et } g : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \begin{cases} \frac{1}{x} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases} \end{array}$$

$g|_{\mathbb{R}^*} = f.$

$$\text{L'application } h : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \begin{cases} \frac{1}{x} & \text{si } x \neq 0 \\ 1 & \text{si } x = 0 \end{cases} \end{array}$$

est un autre prolongement de f .

3 Relations binaires

Définition: Soit E un ensemble. Un relation (binaire) sur E est un prédicat défini sur E^2 .

EXEMPLE: 1. Avec $E = \mathbb{C}$, $=$ est une relation binaire,

- 2. Avec $E = \mathbb{R}$, \leq est une relation binaire,
- 3. Avec E l'humanité et la relation binaire \wedge :

$$x \wedge y \iff x \text{ et } y \text{ ont la même mère.}$$

Définition: Soit E un ensemble, \diamond une relation sur E . On dit que \diamond est un relation d'équivalence si

- 1. $\forall x \in E, x \diamond x$, (réflexivité)
- 2. $\forall x, y \in E, x \diamond y \implies y \diamond x$, (symétrie)
- 3. $\forall x, y, z \in E, \begin{cases} x \diamond y \\ y \diamond z \end{cases} \implies x \diamond z$ (transitivité)

EXEMPLE:

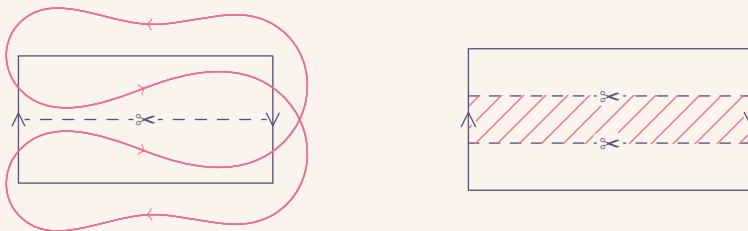
Avec $E = \mathbb{Z}$ et

$$x \diamond y \iff x \equiv y [3]$$

“ \diamond ” est une relation d'équivalence.

REMARQUE:

Le but d'une relation d'équivalence est d'identifier des objets différents.



Définition: Soit E un ensemble et \diamond une relation d'équivalence sur E . Soit $x \in E$. La classe de x (modulo \diamond) est

$$\mathcal{C}\ell_{\diamond}(x) = \mathcal{C}\ell(x) = \bar{x} = \{y \in E \mid y \diamond x\}.$$

EXEMPLE: 1. Avec $E = \mathbb{C}$ et $\diamond = “=”$,

$$\forall z \in \mathbb{C}, \bar{z} = \mathcal{E}\ell(z) = \{z\}.$$

2. Avec $E = \mathbb{Z}$ et $\diamond = \text{congruence modulo } 5$, on a

$$\begin{array}{ll} \bar{0} = \{5k \mid k \in \mathbb{Z}\} & \bar{1} = \{5k + 1 \mid k \in \mathbb{Z}\} \\ \bar{2} = \{5k + 2 \mid k \in \mathbb{Z}\} & \bar{3} = \{5k + 3 \mid k \in \mathbb{Z}\} \\ \bar{4} = \{5k + 4 \mid k \in \mathbb{Z}\} & \bar{5} = \bar{0} \end{array}$$

On constate que

$$x \equiv y \pmod{5} \iff \bar{x} = \bar{y}.$$

Proposition: Soit E un ensemble muni d'une relation d'équivalence \diamond . Alors

$$\forall x, y \in E, x \diamond y \iff \bar{x} = \bar{y}.$$

Preuve:

Soient $x, y \in E$.

- On suppose $x \diamond y$. Soit $z \in \bar{x}$. On sait que $z \diamond x$ et $y \diamond x$. Par transitivité, on en déduit que $z \diamond y$ et donc $z \in \bar{y}$.
- Soit $z \in \bar{y}$, donc $y \diamond z$. Or $x \diamond y$. Comme \diamond est symétrique, on a $y \diamond x$ et par transitivité, on a donc $z \diamond x$. Donc $z \in \bar{x}$.
- On suppose $\bar{x} = \bar{y}$. \diamond réfléctive donc $x \diamond x$ et donc $x \in \bar{x} = \bar{y}$ donc $x \in \bar{y}$ et donc $x \diamond y$.

□

HORS-PROGRAMME

Définition: Soit E un ensemble et \diamond une relation d'équivalence.

L'ensemble

$$\{\bar{x} \mid x \in E\} = E/\diamond$$

est appelé quotient de E modulo \diamond .

EXEMPLE: 1. $E = \mathbb{Z}$ et $\diamond = \text{congruence modulo } 5$:

$$E/\diamond = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\} = \mathbb{Z}/5\mathbb{Z}$$

2. *Construction de \mathbb{Q}*

On suppose avoir déjà construit \mathbb{Z} mais pas \mathbb{Q} : on veut donc donner une définition de p/q sans parler de division.

On pose

$$E = \mathbb{Z} \times \mathbb{N}^* = \{(p, q) \mid p \in \mathbb{Z}, q \in \mathbb{N}^*\}.$$

Soit \sim la relation définie par

$$(p, q) \sim (p', q') \iff pq' = p'q$$

Montrons que \sim est une relation d'équivalence.

- Soient $(p, q) \in E$. \sim est réfléctive car $(p, q) \sim (p, q) \iff pq = pq$.

— Soient $(p, q), (p', q') \in E$. On suppose $(p, q) \sim (p', q')$.

$$\begin{aligned} (p, q) \sim (p', q') &\iff pq' = p'q \\ &\iff p'q = pq' \\ &\iff (p', q') \sim (p, q) \end{aligned}$$

Donc \sim est symétrique.

— Soient $(p, q), (p', q'), (p'', q'') \in E$. On suppose

$$\begin{cases} (p, q) \sim (p', q') \\ (p', q') \sim (p'', q'') \end{cases}$$

On sait que

$$(p, q) \sim (p'', q'') \iff pq'' = p''q$$

Or,

$$\begin{cases} pq' = qp' \\ p'q'' = p''q' \end{cases} \quad \text{donc } pq'p'q'' = p'q'p''q'$$

Donc

$$p'q'(pq'' - p''q) = 0$$

et donc

$$p' = 0 \text{ ou } pq'' - p''q = 0$$

Si $p' = 0$, alors $\begin{cases} pq' = 0 \\ p''q' = 0 \end{cases}$ et donc $\begin{cases} p = 0 \\ p'' = 0 \end{cases}$. On a donc

$$pq'' = 0 = p''q$$

Si $p' \neq 0$, on a $pq'' - p''q = 0$ et donc

$$pq'' = p''q$$

On a donc $(p, q) \sim (p'', q'')$.

On pose $\mathbb{Q} = E/\sim$ et

$$\forall (p, q) \in E, \frac{p}{q} = \mathcal{C}\ell((p, q)).$$

Ainsi,

$$\begin{aligned} \frac{p}{q} = \frac{p'}{q'} &\iff \mathcal{C}\ell((p, q)) = \mathcal{C}\ell((p', q')) \\ &\iff (p, q) \sim (p', q') \\ &\iff pq' = p'q \end{aligned}$$

3. Construction de \mathbb{Z} à partir de \mathbb{N}

On pose $E = \mathbb{N} \times \mathbb{N}^*$ et \sim la relation $(p, q) \sim (p', q') \iff p + q' = p' + q$. \sim est une relation d'équivalence. On pose donc $\mathbb{Z} = \mathbb{N}/\sim$ et pour $n \in \mathbb{N}$, on définit n par $\mathcal{C}\ell((n, 0))$ et $-n$ par $\mathcal{C}\ell((0, n))$.

4. Construction de \mathbb{C} à partir de \mathbb{R}

On pose E l'ensemble des polynômes à coefficients réels ($E = \mathbb{R}[X]$) et \diamond la relation d'équivalence

$$P \diamond Q \iff P \equiv Q [x^2 + 1]$$

On pose $\mathbb{C} = E/\diamond$.

Il manque une partie du cours ici

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

On dit que $(A_i)_{i \in I}$ est une partition de E si

$$\begin{cases} E = \bigcup_{i \in I} A_i \\ \forall i \neq j, A_i \cap A_j = \emptyset \end{cases}$$

On a donc

$$\forall x \in E, \exists ! i \in I, x \in A_i.$$

Proposition: Soit E un ensemble muni d'une relation d'équivalence \diamond . Les classes d'équivalences de E modulo \diamond forment une partition de E .

Preuve: — Soit $x \in E$. On sait que $x \diamond x$ donc $\bar{x} \ni x$. On a montré $E \subset \bigcup_{y \in E} \bar{y}$.

$$— \forall y \in E, \bar{y} \subset E \text{ donc } E \supset \left(\bigcup_{y \in E} \bar{y} \right).$$

— Soit $x, y \in E$ tel que $\bar{x} \neq \bar{y}$. Montrons que $\bar{x} \cap \bar{y} = \emptyset$. Soit $z \in \bar{x} \cap \bar{y}$. $z \in \bar{x}$ donc $z \diamond x$. De même, $z \in \bar{y}$ donc $z \diamond y$. Par transitivité, $x \diamond y$ et donc $\bar{x} = \bar{y}$: une contradiction.

□

Proposition: Soit E un ensemble et $(A_i)_{i \in I}$ une partition de E telle que

$$\forall i \in I, A_i \neq \emptyset.$$

Alors il existe une relation d'équivalence \diamond telle que pour tout $i \in I$, A_i est une classe d'équivalence modulo \diamond .

Preuve:

Soit \diamond la relation définie par

$$x \diamond y \iff \exists i \in I, \begin{cases} x \in A_i \\ y \in A_i \end{cases}$$

— Soit $x \in E$. Comme $E = \bigcup_{i \in I} A_i$, il existe $i \in I$ tel que $x \in A_i$ donc $x \diamond x$.

— Soient $x, y \in E$. On suppose $x \diamond y$. Soit $i \in I$ tel que $\begin{cases} x \in A_i \\ y \in A_i \end{cases}$ donc $\begin{cases} y \in A_i \\ x \in A_i \end{cases}$ et donc $y \diamond x$.

— Soit $x, y, z \in E$. On suppose $x \diamond y$ et $y \diamond z$.

Soit $i \in I$ tel que $\begin{cases} x \in A_i \\ y \in A_i \end{cases}$.

Soit $j \in I$ tel que $\begin{cases} y \in A_j \\ z \in A_j \end{cases}$.

On a donc $y \in A_i \cap A_j$. Si $i \neq j$, alors $y \in \emptyset$: une contradiction. Donc $i = j$ et

donc $\begin{cases} x \in A_i \\ z \in A_i \end{cases}$. On en déduit que $x \diamond z$.

Ainsi \diamond est une relation d'équivalence.

— Soit $i \in I$ et soit $x \in A_i \neq \emptyset$.

$$\bar{x} = \{y \in E \mid y \diamond x\} = \{y \in E \mid y \in A_i\} = A_i.$$

□

Définition: Soit E un ensemble et \diamond . On dit que \diamond est une relation d'ordre sur E si

1. \diamond est réfléctive ($\forall x \in E, x \diamond x$),
2. \diamond est anti-symétrique :

$$\forall x, y \in E, \quad \begin{cases} x \diamond y \\ y \diamond x \end{cases} \implies x = y,$$

3. \diamond est transitive ($\forall x, y, z \in E, (x \diamond y \text{ et } y \diamond z) \implies x \diamond z$).

En général, la relation \diamond est notée \leqslant ou \preccurlyeq . On dit aussi que (E, \diamond) est un ensemble ordonné.

EXEMPLE: 1. (\mathbb{R}, \leqslant) est un ensemble ordonné.

2. $(\mathcal{P}(E), \subset)$ est un ensemble ordonné.

3. $(\mathbb{N}, |)$ est un ensemble ordonné.

4. $(MP2I, \preccurlyeq)$ avec

$$x \preccurlyeq y \iff \text{note de } x \leqslant \text{note de } y$$

n'est un ensemble ordonné car \preccurlyeq n'est pas anti symétrique.

5. $E = \mathbb{N}^2$ et \preccurlyeq définie par

$$(x, y) \preccurlyeq (x', y') \iff x < x' \text{ ou } \begin{cases} x = x' \\ y \leqslant y' \end{cases}$$

(E, \preccurlyeq) est un ensemble ordonné.

Définition: Soit (E, \leqslant) un ensemble ordonné. Soient $x, y \in E$. On dit que x et y sont comparables si

$$x \leqslant y \text{ ou } y \leqslant x.$$

On dit que \leqslant est un ordre total si tous les éléments de E sont comparables 2 à 2.

EXEMPLE: — (\mathbb{R}, \leqslant) est totalement ordonné

— $(\mathcal{P}(E), \subset)$ n'est pas totalement ordonné en général :

Soient $a, b \in E$ avec $a \neq b$. $\{a\}$ et $\{b\}$ ne sont pas comparables.

— $(\mathbb{N}, |)$ n'est pas totalement ordonné :

$2 \nmid 5$ et $5 \nmid 2$ donc 2 et 5 ne sont pas comparables.

Définition: Soit (E, \leqslant) un ensemble ordonné, $A \in \mathcal{P}(E)$ et $M \in E$. On dit que A est majorée par M , que M majore A ou que M est un majorant de A si

$$\forall a \in A, a \leqslant M.$$

Soit $m \in E$. On dit que A est minorée par m , que m minore A ou que m est un minorant de A si

$$\forall a \in A, m \leqslant a.$$

Il manque une partie du cours ici

EXEMPLE: 1. $E = \mathbb{R}$ muni de \leq et $A = [2, 5]$.

On sait que $\sup A = 5$ car

$$\forall x \in A, x \leq 5$$

et

$$\forall y \leq 5, \quad 5 > \frac{y+5}{2} > y$$

donc y ne majore pas A .

2. $E = \mathbb{R}$ avec \leq et $A =]2, 5[$. $A \not\ni \sup A = 5$ par le même raisonnement.

3. $E = \mathbb{N}^*$ avec $|$ et $A = \{p, q\}$ avec $p \neq q \in E$. $\sup A = \text{PPCM}(p, q) = p \vee q$ (c.f. chapitre 10 arithmétique)

4. $\mathcal{P}(E)$ avec \subset et $A = \{P, Q\}$ avec $P, Q \in \mathcal{P}(E)$ et $P \neq Q$. $\sup A = P \cup Q$.

5. $E = \{0, 1\} \times \mathbb{Z}$ muni de \leq défini par

$$(x_1, y_1) \leq (x_2, y_2) \iff x_1 < x_2 \text{ ou } \begin{cases} x_1 = x_2 \\ y_1 \leq y_2 \end{cases}$$

et $A = \{0\} \times \mathbb{Z}$. (x, y) majore $A \iff x = 1$ donc A est majorée mais n'a pas de borne supérieure.

Proposition: Soit (E, \leq) un ensemble ordonné et $A \in \mathcal{P}(E)$. Si A a une borne supérieure, alors celle-ci est unique. On la note $\sup A$.

Preuve:

Soit M_1 et M_2 deux bornes supérieures de A .

Donc M_2 majore A . Comme M_1 est une borne supérieure de A , on a $M_1 \leq M_2$.

De même, on en déduit que $M_2 \leq M_1$.

Comme \leq est antisymétrique, $M_1 = M_2$. \square

Proposition – Définition: Soit (E, \leq) un ensemble ordonné et $A \in \mathcal{P}(E)$ minorée par $m \in E$. On dit que m est une borne inférieure de A si

$$\begin{cases} \forall a \in A, m \leq a, \\ \forall x \in E, (\forall a \in A, x \leq a) \implies x \leq m. \end{cases}$$

Dans ce cas, m est unique et on la note $\inf(A)$. \square

Définition: Soit (E, \leq) un ensemble ordonné et $A \in \mathcal{P}(E)$.

1. Soit $M \in E$. On dit que M est le plus grand élément de A ou que M est le maximum de A si

$$\begin{cases} \forall a \in A, a \leq M, \\ M \in A. \end{cases}$$

Dans ce cas, on le note $M = \max(A)$.

2. Soit $m \in E$. On dit que m est le plus petit élément de A ou que m est le minimum de A si

$$\forall a \in A, a \geq m \in A$$

Dans ce cas, on le note $m = \min(A)$.

Proposition: En cas d'existence, il y a unicité du minimum et du maximum.

Preuve:

Soient M_1 et M_2 deux maxima. On a $M_1 \in A$ donc $M_1 \leq M_2$. Or, $M_2 \in A$ donc $M_2 \leq M_1$. On en déduit que $M_1 = M_2$. \square

Proposition: Soit (E, \leq) un ensemble ordonné, $A \in \mathcal{P}(E)$ et $M \in E$.

$$\begin{aligned} M = \max(A) &\iff \begin{cases} M = \sup(A), \\ M \in A; \end{cases} \\ M = \min(A) &\iff \begin{cases} M = \inf(A), \\ M \in A. \end{cases} \end{aligned}$$

Preuve: “ \implies ” On suppose $M = \max(A)$. On sait déjà que $M \in A$ et que M est un majorant de A .

Soit M' un majorant de A . $M \in A$ donc $M' \geq M$. On en déduit que $M = \sup(A)$.

“ \impliedby ” On suppose $M = \sup(A) \in A$. Alors M majore A et $M \in A$ donc $M = \max(A)$.

\square

EXEMPLE:

$E = \mathbb{N}^*$ muni de $|$ et $A = \{3, 5\}$. $\sup(A) = 3 \vee 5 = 15 \notin A$ donc A n'a pas de maximum.

Définition: Soit (E, \leq) un ensemble ordonné, $A \in \mathcal{P}(E)$ et $M \in E$.

On dit que M est un élément maximal de A si aucun élément de A n'est strictement supérieur à M :

$$\nexists a \in A, \begin{cases} M \leq a, \\ M \neq a. \end{cases}$$

On dit que M est un élément minimal de A si aucun élément de A n'est strictement inférieur à M :

$$\nexists a \in A, \begin{cases} M \geq a, \\ M \neq a. \end{cases}$$

EXEMPLE:

$E = \{n \in \mathbb{N} \mid n \geq 2\} = \mathbb{N} \setminus \{0, 1\}$ muni de $|$ et $A = E$. Les éléments minimaux de E sont les nombres premiers, il y en a une infinité. Il n'y a donc pas d'élément maximal.

Proposition: Avec les notations précédentes, si A a un maximum M alors M est le seul élément maximal de A .

Preuve:

Soit $M = \max(A)$. Soit $a \in A$ tel que $M \leq a$ et $M \neq a$. Comme $a \in A$ et $M = \max(A)$, on sait que $a \leq M$. Par antisymétrie, on en déduit que $a = M$: une contradiction.

Donc M est un élément maximal de A .

Soit M' un élément maximal de A . $M' \in A$ donc $M' \leq M$ et donc $M = M'$. \square

Définition: Soient (E, \leq) et (F, \preceq) deux ensembles ordonnés et $f : E \rightarrow F$. On dit que

1. f est croissante si

$$\forall (x, y) \in E^2, x \leq y \implies f(x) \preceq f(y);$$

2. f est décroissante si

$$\forall (x, y) \in E^2, x \leq y \implies f(x) \succ f(y).$$

EXEMPLE:

$$E = \mathbb{N}^* \text{ muni de } |, F = \mathbb{N}^* \text{ muni de } \leq \text{ et } f : \begin{array}{ccc} E & \longrightarrow & F \\ x & \longmapsto & x. \end{array}$$

Soit $(x, y) \in E^2$ tels que $x \mid y$. Alors $x \leq y$ donc f est croissante.

On pose

$$\begin{aligned} g : F &\longrightarrow E \\ n &\longmapsto n. \end{aligned}$$

$2 \leq 3$ mais $2 \nmid 3$ donc g n'est pas croissante et $2 \leq 5$ mais $5 \nmid 2$ donc g n'est pas décroissante.

Définition: Soit (E, \leq) un ensemble ordonné et $A \in \mathcal{P}(E)$. On dit que A est bornée si A est à la fois majorée et minorée.

Définition: Avec les notations précédentes, un extremum de A (sous réserve d'existence) est un maximum ou un minimum de A .

4 Lois de composition

Définition: Une loi de composition interne est une application f de $E \times E$ dans E .

On la note $x * y$ au lieu de $f(x, y)$ (on est libre de choisir le symbole).

Définition: Soit E un ensemble muni d'une loi de composition interne \boxtimes .

On dit que \boxtimes est associative si

$$\forall (x, y, z) \in E^3, (x \boxtimes y) \boxtimes z = x \boxtimes (y \boxtimes z).$$

Dans ce cas, on écrit plutôt $x \boxtimes y \boxtimes z$.

EXEMPLE: — + et \times dans \mathbb{C} sont associatives ;
— \circ est associative ;

- la multiplication matricielle est aussi associative.

Définition: On dit que \boxtimes est commutative si

$$\forall (x, y) \in E^2, x \boxtimes y = y \boxtimes x.$$

EXEMPLE: — + et \times dans \mathbb{C} sont commutatives;

- \circ n'est pas commutative;
- la multiplication matricielle n'est pas commutative.

Définition: Soit $e \in E$. On dit que e est un
— élément neutre à gauche si

$$\forall x \in E, e \boxtimes x = x;$$

— élément neutre à droite si

$$\forall x \in E, x \boxtimes e = x;$$

— élément neutre si

$$\forall x \in E, e \boxtimes x = x \boxtimes e = x.$$

Proposition: Sous réserve d'existence, il y a unicité de l'élément neutre.

Preuve:

Soient e et e' deux éléments neutre.

- $e \boxtimes e' = e'$ car e est neutre,
- $e \boxtimes e' = e$ car e' est neutre.

On a donc $e = e'$. □

Axiome (axiome du choix): Soit E un ensemble non vide. Il existe $f : \mathcal{P}(E) \setminus \{\emptyset\} \rightarrow E$ telle que

$$\forall A \in \mathcal{P}(E) \setminus \{\emptyset\}, f(A) \in A.$$

Définition: Soit $f : E \rightarrow F$. Le **graphe** de f est

$$\{(x, f(x)) \mid x \in E\} \subset E \times F.$$

Proposition: Soit $G \subset E \times F$. G est le graphe d'une application si et seulement si

$$\forall x \in E, \exists ! y \in F, (x, y) \in G.$$

Preuve: “ \implies ” par définition d'une application

“ \impliedby ” On pose $f(x)$ le seul élément y de F qui vérifie $(x, y) \in G$. Alors $f \in F^E$ et son graphe vaut G .

□

Définition: Soit $A \in \mathcal{P}(E)$. L'indicatrice de A est

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

EXEMPLE: 1. Dans \mathbb{C} , le neutre de $+$ est 0 et le neutre de \times est 1.

- 2. Dans E^E , le neutre de \circ est id_E .
- 3. Dans $\mathcal{M}_n(\mathbb{C})$ (l'ensemble des matrices carrées $n \times n$ à valeurs dans \mathbb{C}), le neutre de \times est I_n :

$$I_n = \begin{pmatrix} 1 & & & & (0) \\ & \ddots & \ddots & \ddots & \\ & & \ddots & \ddots & \\ (0) & & & & 1 \end{pmatrix}$$

Définition: Soit E un ensemble muni d'une loi de composition interne \boxtimes et $x \in E$.

- 1. On dit que x est simplifiable à gauche si

$$\forall (y, z) \in E^2, (x \boxtimes y = x \boxtimes z) \implies x = z.$$

et que x est simplifiable à droite si

$$\forall (y, z) \in E^2, (y \boxtimes x = z \boxtimes x) \implies x = z.$$

- 2. On dit que x est symétrisable à gauche s'il existe $y \in E$ tel que $y \boxtimes x = e$ où e est l'élément neutre de \boxtimes .

De même, on dit que x est symétrisable à droite s'il existe $y \in E$ tel que $x \boxtimes y = e$. On dit que x est symétrisable s'il est symétrisable à gauche et à droite, donc s'il existe $y \in E$ tel que $x \boxtimes y = y \boxtimes x = e$.

EXEMPLE:

$E = \mathbb{N}$ muni de la loi $+$, tous les éléments de E sont simplifiables. 0 est le seul élément de E symétrisable.

Proposition: Avec les notations précédentes, si \boxtimes est associative, et x est symétrisable, alors x est simplifiable.

Preuve:

Soient $y, z \in E$.

- On suppose $x \boxtimes y = x \boxtimes z$. Soit $a \in E$ tel que $a \boxtimes x = e$. Alors

$$a \boxtimes (x \boxtimes y) = a \boxtimes (x \boxtimes z).$$

Or,

$$\begin{aligned} a \boxtimes (x \boxtimes y) &= (a \boxtimes x) \boxtimes y \\ &= e \boxtimes y \\ &= y. \end{aligned}$$

De même, $a \boxtimes (x \boxtimes z) = z$.

Donc $y = z$.

— De même, si $y \boxtimes x = z \boxtimes x$, on “multiplie” x à droite par a et on obtient $y = z$. \square

Proposition – Définition: On suppose \boxtimes associative. Soit $x \in E$ symétrisable. Alors

$$\exists ! y \in E, x \boxtimes y = y \boxtimes x = e.$$

On dit que y est le symétrique de x et on le note $y = x^*$.

Preuve:

Soient $x, y, z \in E$ tels que

$$\begin{cases} x \boxtimes y = y \boxtimes x = e \\ x \boxtimes z = z \boxtimes x = e \end{cases}$$

Alors, $x \boxtimes y = x \boxtimes z$ et, en simplifiant par x , on a $y = z$. \square

EXEMPLE:

Les fonctions symétrisables de (E^E, \circ) sont les bijections et le symétrique d'une bijection est sa réciproque.

REMARQUE: 1. Si la loi est notée $+$, on parle d'opposé plutôt que de symétrique et on le note $-x$ au lieu de x^* . L'élément neutre est noté 0_E .

2. Si la loi est notée \times , on parle d'élément inversible au lieu de symétrisable, d'inverse au lieu de symétrique et on note x^{-1} au lieu de x^* . On note le neutre 1_E .

EXERCICE:

Soient $x, y \in E = \mathbb{R}_*^+$. On définit la loi de composition interne \oplus :

$$x \oplus y = \frac{1}{\frac{1}{x} + \frac{1}{y}}.$$

Cette loi peut-être utile en physique pour le calcul de résistances équivalentes en parallèles.

— **ASSOCIATIVITÉ** : soient $x, y, z \in E$.

D'une part, on a

$$x \oplus (y \oplus z) = \frac{1}{\frac{1}{x} + \frac{1}{\frac{1}{y} + \frac{1}{z}}} = \frac{1}{\frac{1}{x} + \frac{1}{y} + \frac{1}{z}}.$$

D'autre part, on a

$$(x \oplus y) \oplus z = \frac{1}{\frac{1}{\frac{1}{x} + \frac{1}{y}} + \frac{1}{z}} = \frac{1}{\frac{1}{x} + \frac{1}{y} + \frac{1}{z}}.$$

La loi \oplus est associative.

— **COMMUTATIVITÉ** : soient $x, y \in E$.

$$x \oplus y = \frac{1}{\frac{1}{x} + \frac{1}{y}} = \frac{1}{\frac{1}{y} + \frac{1}{x}} = y \oplus x.$$

Donc la loi \oplus est commutative.

— **ÉLÉMENT NEUTRE** : soit e l'élément neutre de \oplus .

$$\forall x \in E, x \oplus e = e \oplus x = x.$$

Comme la loi est commutative, seul l'égalité $x \oplus e = x$ est utile.

Soit $x \in E$. On a donc $\frac{1}{\frac{1}{x} + \frac{1}{e}} = x$ donc $\frac{ex}{e+x} = x$ donc $ex = x(e+x)$ et donc $ex = ex + x^2$. On en déduit que $x^2 = 0$, ce qui n'est pas possible car $x \in \mathbb{R}_*^+$. Donc, il n'y a pas d'élément neutre pour \oplus .

5 Divers

Définition: Soient E et F deux ensembles. Un couple (x, y) est la donnée d'un élément x de E et d'un élément y de F où

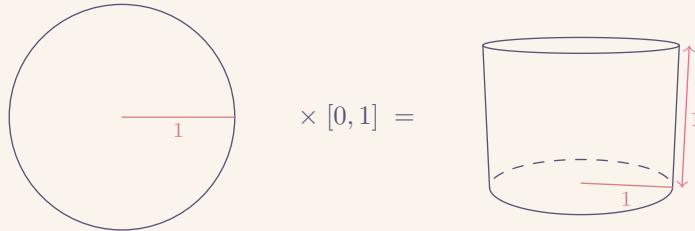
$$\forall x, x' \in E, \forall y, y' \in F, \quad (x, y) = (x', y') \iff \begin{cases} x = x', \\ y = y'. \end{cases}$$

On note $E \times F$ l'ensemble des couples ; c'est le produit cartésien de E et F .

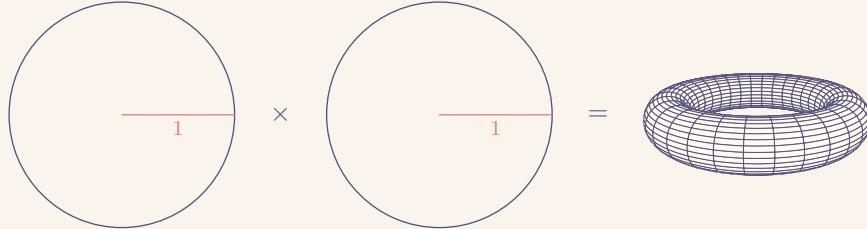
EXEMPLE:

$D \times [0, 1]$ est un cylindre plein où D est le disque unité fermé i.e.

$$D = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}.$$



$C \times C$ où $C = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ est un tore (creu).



Définition: Soient E et F deux ensembles. On dit que E et F sont équipotents s'il existe une bijection de E dans F .

EXEMPLE: 1. \mathbb{N} et \mathbb{N}^* sont équipotents car $f : \frac{\mathbb{N}}{k} \xrightarrow{\quad} \frac{\mathbb{N}^*}{k+1}$ est bijective.

2. $P = \{n \in \mathbb{N} \mid n \text{ pair}\}$ et $I = \{n \in \mathbb{N} \mid n \text{ impair}\}$ sont équipotents car $f : \frac{P}{x} \xrightarrow{\quad} \frac{I}{x+1}$ est bijective.

3. \mathbb{N} et P sont équipotents car $f : \frac{\mathbb{N}}{k} \xrightarrow{\quad} \frac{P}{2k}$ est bijective.

4. $[0, 1]$ et $[0, 1[$ sont équipotents car

$$f : [0, 1] \longrightarrow [0, 1[$$

$$x \longmapsto \begin{cases} \frac{1}{n+1} & \text{si } x = \frac{1}{n} \text{ avec } n \in \mathbb{N}^* \\ x & \text{sinon} \end{cases}$$

est bijective.

5. De même, $]0, 1[$ et $]0, 1]$ sont équipotents.
 6. $]0, 1[$ et $[0, 1[$ sont équipotents : $f : \begin{matrix}]0, 1] \\ x \end{matrix} \longrightarrow \begin{matrix} [0, 1[\\ 1 - x \end{matrix}$ est bijective.
 7. $\forall a < b$, $[a, b]$ et $[0, 1]$ sont équipotents :

$$\begin{aligned} f : [0, 1] &\longrightarrow [a, b] \\ \alpha &\longmapsto \alpha b + (1 - \alpha)a \end{aligned}$$

est bijective (interpolation linéaire).

8. \mathbb{R} et $]0, 1[$ sont équipotents :

$$\begin{aligned} f : \mathbb{R} &\longrightarrow]0, 1[\\ x &\longmapsto \frac{1}{2} + \frac{\text{Arctan } x}{\pi} \end{aligned}$$

est bijective.

9. $[0, 1[$ et \mathbb{N} ne sont pas équipotents (argument de Cantor). Soit $f : \mathbb{N} \rightarrow [0, 1[$ une bijection :

k	$f(k)$
0	0, 0 0 0 0 ...
1	0, $a_1 a_2 a_3 a_4$...
2	0, $b_1 b_2 b_3 b_4$...
\vdots	\vdots ...

On considère le nombre

$$x = 0, (a_0 + 1)(b_1 + 1)(c_2 + 1) \dots$$

$f(1) \neq x$ car ils n'ont pas le même chiffre des dizaines.

$f(2) \neq x$ car ils n'ont pas le même chiffre des centaines.

Par le même raisonnement, on en déduit que

$$\forall n \in \mathbb{N}, f(n) \neq x$$

donc x n'a pas d'antécédant : une contradiction.

10. On verra en exercice que E et $\mathcal{P}(E)$ ne sont pas équipotents. \mathbb{R} et $\mathcal{P}(\mathbb{R})$ ne sont pas équipotents mais \mathbb{R} et $\mathcal{P}(\mathbb{N})$ le sont (développement dyadique).
 11. \mathbb{R}^2 et \mathbb{R} sont équipotents ; \mathbb{C} et \mathbb{R} sont équipotents.

EXERCICE:

Soit E un ensemble. L'application

$$\begin{aligned} f : \mathcal{P}(E) &\longrightarrow 0, 1^E \\ A &\longmapsto \mathbb{1}_A \end{aligned}$$

est bijective.

Soit $g : E \rightarrow \{0, 1\}$.

ANALYSE Soit $A \in \mathcal{P}(E)$ tel que $f(A) = g$. Alors $g = \mathbb{1}_A$. donc

$$\forall x \in E, g(x) = \mathbb{1}_A(x)$$

et donc

$$\begin{cases} \forall x \in A, g(x) = 1 \\ \forall x \in E \setminus A, g(x) = 0 \end{cases}$$

On en déduit que

$$A = \{x \in E \mid g(x) = 1\} = g^{-1}(\{1\}).$$

SYNTHÈSE On pose $A = g^{-1}(\{1\})$. Montrons que $f(A) = g$.

$$\forall x \in E, g(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases} = \mathbb{1}_A$$

donc $g = \mathbb{1}_A$.

On aurait aussi pu rédiger de la façon suivante : on pose

$$\begin{aligned} u : \{0, 1\}^E &\longrightarrow \mathcal{P}(E) \\ g &\longmapsto g^{-1}(\{1\}). \end{aligned}$$

On montre que u est la réciproque de f :

$$\begin{cases} f \circ u = \text{id}_{\{0,1\}^E}, \\ u \circ f = \text{id}_{\mathcal{P}(E)}. \end{cases}$$

Définition: Soit $f : E \rightarrow F$. L'image de f est

$$\text{Im}(f) = f(E) = \{f(x) \mid x \in E\}.$$

Proposition: Soit $f : E \rightarrow F$.

$$f \text{ est surjective} \iff f(E) = F.$$

Définition: Une suite de E est une application de \mathbb{N} dans E .

REMARQUE (Notation):

Soit $u \in E^{\mathbb{N}}$. Pour $n \in \mathbb{N}$, on écrit u_n à la place de $u(n)$.

Définition: Soient E et I deux ensembles. Une famille de E indéxée par I est une application de I dans E .

À la place de $u(i)$ (avec $i \in I$), on écrit u_i .

Définition: Soit E un ensemble et $(A_i)_{i \in I}$ une famille de parties de E . On suppose $I \neq \emptyset$. On pose

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

et

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

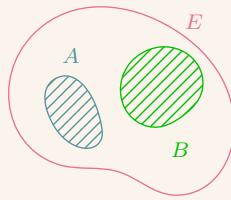
On pose aussi $\bigcup_{i \in \emptyset} A_i = \emptyset$ et $\bigcap_{i \in \emptyset} A_i = E$.

REMARQUE:

De même que pour les sommes et produits de complexes, on peut intervertir des réunions doubles.

Proposition: Soit E un ensemble, $(A, B) \in \mathcal{P}(E)^2$.

$$A \subset (E \setminus B) \iff A \cap B = \emptyset.$$



Preuve: “ \implies ” Soit $x \in A \cap B$. Alors $x \in A$ et $x \in B$. Comme $x \in A \subset (E \setminus B)$, alors $x \in E \setminus B$ i.e. $x \notin B$: une contradiction. Donc $A \cap B = \emptyset$.
 “ \impliedby ” On suppose $A \cap B = \emptyset$. Soit $x \in A$. Si $x \in B$, alors $x \in A \cap B = \emptyset$: faux.
 Donc $x \notin B$ et donc $x \in E \setminus B$.

□

Proposition: Si $f : E \rightarrow F$ et $g : F \rightarrow G$ sont bijectives, alors $g \circ f$ est bijective et

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

□

REMARQUE (⚠️ Attention):
 $g \circ f$ peut-être bijective alors que f et g ne le sont pas.

CHAPITRE

9

INÉGALITÉS DANS \mathbb{R}

1

2

3

4 Bornes supérieures

Proposition (borne inférieure): Toute partie minorée non vide de \mathbb{R} admet une borne inférieure.

Preuve:

Soit $A \subset \mathbb{R}$ non vide minorée. On pose $B = \{-a \mid a \in A\} \neq \emptyset$. Soit m un minorant de A :

$$\forall a \in A, m \leq a.$$

D'où,

$$\forall a \in A, -a \leq -m$$

donc B est majorée par $-m$.

D'après la propriété de la borne supérieure, B admet une borne supérieure. On pose $\beta = \sup(B)$, donc β majore B et donc

$$\forall a \in A, -a \leq \beta$$

et donc

$$\forall a \in A, \beta \geq a.$$

Donc $-\beta$ est un minorant de A .

Soit x un minorant de A . Montrons que $x \leq -\beta$. On sait que $-x$ majore B et donc $-x \geq \beta$. On en déduit que $x \leq -\beta$ et donc $-\beta = \inf(A)$. \square

Proposition (caractérisation de la borne supérieure): Soit $A \subset \mathbb{R}$ non vide majorée et $M \in \mathbb{R}$.

$$M = \sup(A) \iff \begin{cases} \forall a \in A, a \leq M, \\ \forall \varepsilon > 0, \exists a_0 \in A, a_0 > M - \varepsilon. \end{cases}$$

Preuve: “ \implies ” On suppose $M = \sup(A)$. M est un majorant de A :

$$\forall a \in A, a \leq M.$$

Soit $\varepsilon > 0$, comme M est le plus petit majorant de A et que $M - \varepsilon < M$, $M - \varepsilon$ ne majore pas A . Donc

$$\exists a_0 \in A, a_0 > M - \varepsilon.$$

— On suppose

$$\begin{cases} \forall a \in A, a \leq M; & (1) \\ \forall \varepsilon > 0, \exists a_0 \in A, M - \varepsilon < a_0. & (2) \end{cases}$$

D'après (1), M est un majorant de A . Soit M' un majorant de A . Montrons que $M' \geq M$.

On suppose $M' < M$ et on pose $\varepsilon = M - M' > 0$. D'après (2), il existe $a_0 \in A$ tel que

$$a_0 > M - \varepsilon = M' \geq a_0$$

une contradiction. Donc $M' \geq M$ et donc M est le plus petit majorant de A : $M = \sup(A)$.

□

Proposition (caractérisation de la borne inférieure): Soit $A \subset \mathbb{R}$, non vide minorée et $m \in \mathbb{R}$.

$$m = \inf(A) \iff \begin{cases} \forall a \in A, m \leq a; \\ \forall \varepsilon > 0, \exists a_0 \in A, a_0 < m + \varepsilon. \end{cases}$$

□

Proposition: Soit $A \subset \mathbb{R}$ non vide majorée et $M \in \mathbb{R}$.

$$M \geq \sup(A) \iff \forall a \in A, a \leq M.$$

Preuve: “ \implies ” On suppose $M = \sup(A)$. Soit $a \in A$. On sait que $a \leq \sup(A)$ car $\sup(A)$ majore A . Donc $a \leq M$.

“ \impliedby ” On suppose $\forall a \in A, a \leq M$. Donc M majore A . Or, $\sup(A)$ est le plus petit majorant et donc $M \geq \sup(A)$.

□

Proposition: Soit $A \subset \mathbb{R}$ non vide minorée et $m \in \mathbb{R}$.

$$m \leq \inf(A) \iff \forall a \in A, m \leq a.$$

□

Proposition – Définition: \mathbb{R} est archimédien :

$$\forall x \in \mathbb{R}_+^*, \forall y \in \mathbb{R}, \exists n \in \mathbb{N}, nx \geq y.$$

Preuve:

Soit $x \in \mathbb{R}_+^*$ et $y \in \mathbb{R}$. Supposons

$$(H) : \quad \forall n \in \mathbb{N}, nx < y.$$

On pose $A = \{nx \mid n \in \mathbb{N}\} \subset \mathbb{R}$. Comme $0 \in A$, $A \neq \emptyset$. D'après (H) , A est majorée par y .

Soit $\alpha = \sup(A)$ et $n \in \mathbb{N}$. On sait que $(n+1)x \in A$ donc $(n+1)x \leq \alpha$ et donc $nx \geq \alpha - x$. On remarque que $\alpha - x$ majore A mais que $\alpha - x < \alpha$: une contradiction car α est le plus petit majorant de A . Donc,

$$\exists n \in \mathbb{N}, nx \geq y.$$

□

Théorème: Toute fonction continue sur un segment est bornée et atteint ses bornes : si $f : [a, b] \rightarrow \mathbb{R}$ (avec $a < b \in \mathbb{R}$) est continue, alors

$$\exists(\alpha, \beta) \in [a, b]^2, \forall x \in [a, b], f(\alpha) \leq f(x) \leq f(\beta).$$

Preuve:

c.f. Chapitre 14 : Continuité.

□

Proposition: Soit $A \subset \mathbb{R}$ non vide majorée. Il existe une suite $(a_n) \in A^{\mathbb{N}}$ telle que $\lim_{n \rightarrow +\infty} a_n = \sup(A)$.

Preuve:

On sait que

$$\forall \varepsilon > 0, \exists a \in A, a > \sup(A) - \varepsilon.$$

Donc,

$$\forall n \in \mathbb{N}^*, \exists a_n \in A, a_n > \sup(A) - \frac{1}{n}.$$

On a

$$\forall n \in \mathbb{N}^*, a_n \in A \text{ et } a_n \leq \sup(A).$$

Or

$$\forall n \in \mathbb{N}^*, \sup(A) - \frac{1}{n} < a_n \leq \sup(A),$$

par encadrement, on en déduit que $a_n \xrightarrow{n \rightarrow +\infty} \sup(A)$.

□

Proposition: Soit $A \subset \mathbb{R}$ non vide minorée. Il existe une suite $(a_n) \in A^{\mathbb{N}}$ telle que $\lim_{n \rightarrow +\infty} a_n = \inf(A)$.

□

5 Partie entière

Proposition – Définition: Soit $x \in \mathbb{R}$. Il existe un unique entier $n \in \mathbb{N}$ tel que

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

Cet entier n est appelé partie entière de x et est noté $\lfloor x \rfloor$.

Preuve:

Soit $A = \{p \in \mathbb{Z} \mid p > x\}$. $A \neq \emptyset$ car \mathbb{R} est archimédien.

Soit α la borne inférieure de A . Alors $\alpha \geq x$. Montrons que $\alpha \in A$. Soit $n \geq 2$. On a $\alpha + \frac{1}{n} > \alpha$ donc, il existe $a_n \in A$ tel que

$$\alpha < a_n < \alpha + \frac{1}{n}.$$

On sait que $\frac{1}{n} < 1$ donc, il y a au plus un entier dans le segment $\left[\alpha, \alpha + \frac{1}{n} \right]$. Donc, tous les a_n sont égaux et $a_n \xrightarrow[n \rightarrow +\infty]{} \alpha$. On en déduit que

$$\forall n \geq 2, a_n = \alpha$$

et donc $\alpha \in A$. Ainsi, $\alpha = \min(A)$ et alors $\alpha - 1 \notin A$. On a donc

$$\alpha - 1 \leq x < \alpha$$

et, en posant $n = \alpha - 1$, on en déduit que

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

□

6 Densité

Définition: Soit $A \in \mathcal{P}(\mathbb{R})$. On dit que A est dense dans \mathbb{R} si, pour tout intervalle I ouvert non vide de \mathbb{R} , $A \cap I \neq \emptyset$.

Théorème: \mathbb{Q} est dense dans \mathbb{R} .

Preuve:

Soit I un intervalle ouvert non vide. Soient $a < b$ deux éléments de I . On cherche $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que

$$a \leq \frac{p}{q} \leq b.$$

Comme \mathbb{R} est archimédien, il existe $q \in \mathbb{N}^*$ tel que

$$q(b - a) \geq 2 > 1.$$

Donc, l'intervalle $[qa, qb]$ a une longueur supérieure à 1, il contient donc au moins un entier p .

En effet, sinon on a $\lfloor qa \rfloor = \lfloor qb \rfloor$ et alors

$$\begin{cases} \lfloor qa \rfloor \leq qb < \lfloor qa \rfloor + 1 \\ \lfloor qa \rfloor \leq qa < \lfloor qa \rfloor + 1 \end{cases}$$

et alors

$$-1 < qb - qa < 1$$

une contradiction. On a donc $qa \leq p \leq qb$ et finalement

$$a \leq \frac{p}{q} \leq b.$$

□

Théorème: $\mathbb{R} \setminus \mathbb{Q}$ est dense dans \mathbb{R} .

Il manque une partie du cours ici

7

8

Il manque une partie du cours ici

Preuve:

Soit $a \in I$ et

$$\begin{aligned} \tau_a : I \setminus \{a\} &\longrightarrow \mathbb{R} \\ x &\longmapsto \frac{f(x) - f(a)}{x - a}. \end{aligned}$$

D'après le lemme des pentes, τ_a est croissante. En effet, soient $x, y \in I \setminus \{a\}$ tels que $x < y$.

CAS 1 $a < x < y$. On a alors

$$\frac{f(x) - f(a)}{x - a} \leq \frac{f(y) - f(a)}{y - a}$$

et donc $\tau_a(x) \leq \tau_a(y)$.

CAS 2 $x < a < y$. On a alors

$$\frac{f(x) - f(a)}{x - a} \leq \frac{f(x) - f(y)}{x - y} \leq \frac{f(y) - f(a)}{y - a}$$

et donc $\tau_a(x) \leq \tau_a(y)$.

CAS 3 $x < y < a$. On a alors

$$\frac{f(x) - f(y)}{x - y} \leq \frac{f(x) - f(a)}{x - a} \leq \frac{f(y) - f(a)}{y - a}$$

et donc $\tau_a(x) \leq \tau_a(y)$.

Soit $x > a$ avec $x \in I$. On fixe $z_0 < a$ un élément de I . z_0 existe car I est ouvert. On a alors... □

Il manque une partie du cours ici

La suite du cours provient d'Aubin. Je ne suis pas responsable pour les éventuelles bêtises qu'il a pu taper.

9 Propriétés de (\mathbb{R}, \leq)

Axiome (Propriétés de (\mathbb{R}, \leq)): \mathbb{R} est muni d'une addition notée $+$ associative, commutative, d'élément neutre 0 et tout réel x a un symétrique pour $+$ noté $-x$
 \mathbb{R} est muni d'une multiplication notée \times , associative, commutative, d'élément neutre 1 et tout réel x a un symétrique pour \times noté x^{-1} ou $\frac{1}{x}$ (on la notera $*$ dans ce document)
La multiplication est distributive sur l'addition
 $\forall(a, b, c) \in \mathbb{R}^3, a(b + c) = ab + ac$

\leq est un ordre total sur \mathbb{R}
 $\forall(x, y, a) \in \mathbb{R}^3, (x \leq y \implies a + x \leq a + y)$
 $\forall a \in \mathbb{R}_+^*, \forall(x, y) \in \mathbb{R}^2, x \leq y \implies ax \leq ay$

$$\mathbb{Q} \subset \mathbb{R}$$

Propriété de la borne supérieure : Tout partie non vide majorée de \mathbb{R} admet une borne supérieure

Lemme (Opposé d'un réel): $\forall a \in \mathbb{R}, -a = -1 * a$

Proposition (Inverse de \leq): Soient $(x, y) \in \mathbb{R}^2$
 $x \leq y \implies -y \leq -x$

Preuve:

$$\begin{aligned} x \leq y &\implies -x + x \leq -x + y \\ &\implies 0 \leq -x + y \\ &\implies -y \leq -x \end{aligned}$$

□

Corollaire (\times et \leq): $\forall a \in \mathbb{R}_-^*, \forall(x, y) \in \mathbb{R}^2, x \leq y \implies ay \leq ax$

Preuve:

Soient $a < 0, (x, y) \in \mathbb{R}^2$

$$\begin{aligned} \text{On pose } b &= -a \\ a < 0 &\implies -0 \leq -a \implies 0 \leq b \end{aligned}$$

$$\begin{aligned} \text{Si } b &= 0, a = 0 \\ x \leq y &\implies bx \leq by \\ &\implies -by \leq -bx \\ &\implies -1(by) \leq -1(bx) \\ &\implies (-1 * b) * y \leq (-1 * b) * x \\ &\implies -by \leq -bx \end{aligned}$$

$$\implies ay \leq ax$$

□

Proposition (Elément Symétrique pour la Multiplication): Soit $a \in \mathbb{R}$, $-a$ est le seul réel qui vérifie $a + (-a) = 0$

Preuve:

$$\begin{aligned} a + (-a) &= a + (-1) * a \\ &= a * (1 + -1) \\ &= a * 0 = 0 \end{aligned}$$

On a bien $a * 0 = 0$ car :

$$\begin{aligned} a * 0 &= a * (0 + 0) \\ 0 + 0 &= (a * 0) + (a * 0) = 0 \end{aligned}$$

□

Proposition (+ et \leq): Soient $(a, b, x, y) \in \mathbb{R}^4$ tels que $\begin{cases} x \leq y \\ a \leq b \end{cases}$

Alors $a + x \leq b + y$

Preuve:

$$\begin{aligned} a \leq b &\implies a + x \leq b + x \\ x \leq y &\implies b + x \leq b + y \\ \leq \text{ est transitive donc } a + x &\leq b + y \end{aligned}$$

□

REMARQUE (Soustraire des Inégalités):

On ne peut pas soustraire directement des inégalités

Si $\begin{cases} x \leq y \\ a \leq b \end{cases}$, alors $\begin{cases} x \leq y \\ -b \leq -a \end{cases}$

et alors, $x - b \leq y - a$

Proposition (\times et \leq dans \mathbb{R}^4): Soient $(x, y, a, b) \in (\mathbb{R}^+)^4$

$$\begin{cases} 0 \leq x \leq y \\ 0 \leq a \leq b \end{cases} \implies xa \leq yb$$

Preuve:

$$\left\{ \begin{array}{l} x \leq y \\ 0 \leq a \end{array} \right. \implies ax \leq ay \text{ et } \left\{ \begin{array}{l} a \leq b \\ 0 \leq y \end{array} \right. \implies ay \leq bx$$

□

Proposition (Inégalité des Inverses): $\forall (x, y) \in (\mathbb{R}_*)^2, x \leq y \implies \frac{1}{x} \leq \frac{1}{y}$

Preuve:

Soient $(x, y) \in (\mathbb{R}_*)^2$

On suppose $x \leq y$

Si $\frac{1}{x} \leq 0$, alors $x \frac{1}{x} \leq 0 * x$, alors $1 \leq 0$

Donc $\frac{1}{x} \geq 0$ donc $\frac{1}{x}x \leq \frac{1}{x}y$

Donc $\frac{1}{x} \leq \frac{1}{y}$

□

REMARQUE (Diviser des Inégalités):

On ne peut pas diviser des inégalités

10 Inégalités Classiques

Proposition (Inégalité Triangulaire dans \mathbb{R}): $\forall (x, y) \in \mathbb{R}^2, \left\{ \begin{array}{l} |x + y| \leq |x| + |y| \\ |x| - |y| \leq |x - y| \end{array} \right.$

En changeant y en $-y$, on a aussi

$$\left\{ \begin{array}{l} |x - y| \leq |x| + |y| \\ |x| - |y| \leq |x + y| \end{array} \right.$$

Preuve:

1 - Soient $(x, y) \in \mathbb{R}^2$

$$|x| = \max(-x, x) \geq x$$

$$|y| \geq y$$

$$\text{Donc } x + y \leq |x + y|$$

$$\text{Si } x + y \leq 0, \text{ alors } |x + y| \leq |x| + |y|$$

$$\text{On a aussi } |x| \geq -x \text{ et } |y| \geq -y$$

$$\text{Donc } -(x + y) \leq |x| + |y|$$

$$\text{Si } x + y \leq 0, \text{ alors } |x| + |y| \geq |x + y|$$

2 - Soient $(x, y) \in \mathbb{R}^2$

$$|x| = |x - y + y| \leq |x - y| + |y| \\ \text{Donc } |x| - |y| \leq |x + y|$$

$$\text{Si } |x| - |y| \geq 0, |x| - |y| \leq |x - y|$$

$$\text{On a aussi } |y| = |y - x + x| \leq |y - x| + |x| \\ \text{Donc } |y| - |x| \leq |y - x|$$

$$\text{Si } |x| - |y| \leq 0, |x| - |y| \leq |x - y|$$

□

Proposition (Inégalité Triangulaire dans \mathbb{C}): $\forall (x, y) \in \mathbb{C}, \begin{cases} |x + y| \leq |x| + |y| \\ |x| - |y| \leq |x - y| \end{cases}$

Preuve:

$$\begin{aligned} |x + y| \leq |x| + |y| &\iff |x + y|^2 \leq (|x| + |y|)^2 \\ &\iff (x + y)(\bar{x} + \bar{y}) \leq |x|^2 + |y|^2 + 2|xy| \\ &\iff |x|^2 + |y|^2 + (x\bar{y} + \bar{x}y) \leq |x|^2 + |y|^2 + 2|xy| \\ &\iff 2\Re(xy) \leq 2|xy| \end{aligned}$$

Or, pour tout $z \in \mathbb{C}, \Re(z) \leq |z|$

$$\text{En effet : } |z| = \sqrt{\Re(z)^2 + \Im(z)^2} \geq \sqrt{\Re(z)^2} = |\Re(z)| \geq \Re(z)$$

□

Proposition (Inégalité Triangulaire à n Coefficients): Soient $(z_1 \dots z_n) \in \mathbb{C}^n$

$$\text{Alors, } \left| \sum_{k=1}^n z_k \right| \leq \sum_{k=1}^n |z_k|$$

Preuve:

$$\text{Pour } n \in \mathbb{N}^*, P(n) : \forall (z_1 \dots z_n) \in \mathbb{C}^n, \left| \sum_{k=1}^n z_k \right| \leq \sum_{k=1}^n |z_k|$$

$P(1)$ et $P(2)$ sont vraies

Soit $n \in \mathbb{N}^*$, on suppose $P(n)$ vraie

Soient $(z_1 \dots z_n + 1) \in \mathbb{C}^n + 1$

$$\left| \sum_{k=1}^{n+1} z_k \right| = \left| \sum_{k=1}^n z_k + z_{n+1} \right| \leq \sum_{k=1}^n |z_k| + |z_{n+1}| = \sum_{k=1}^{n+1} |z_k|$$

Donc $P(n + 1)$ vraie

Par récurrence, $\forall n \in N^*, P(n)$ vraie

□

Proposition (Inégalité Triangulaire des Intégrales): Soit $f : [a, b] \rightarrow \mathbb{R}$ continue
Alors $|\int_a^b f(x)dx| \leq \int_a^b |f(x)|dx$

Preuve:
 $\forall x \in [a, b], -|f(x)| \leq f(x) \leq |f(x)|$

□

Proposition (Inégalité Triangulaire des Intégrales sur \mathbb{C}): Soit $f : [a, b] \rightarrow \mathbb{C}$ continue

Alors $|\int_a^b f(x)dx| \leq \int_a^b |f(x)|dx$

Preuve:
Cas 1 : $|\int_a^b f(x)dx| = 0$

On a $\forall x \in [a, b], |f(x)| \geq 0$
donc $\int_a^b |f(x)|dx \geq 0 = |\int_a^b f(x)dx|$

Cas 2 : $|\int_a^b f(x)dx| \neq 0$

On pose $r = |\int_a^b f(x)dx| \in \mathbb{R}_+^*$

Soit θ un argument de $\int_a^b f(x)dx$

D'où $\int_a^b f(x)dx = re^{i\theta}$

$$\begin{aligned} r &= e^{-i\theta} \int_a^b f(x)dx = \int_a^b f(x)e^{-i\theta} dx \\ &= \Re(\int_a^b f(x)e^{-i\theta} dx) \\ &= \int_a^b \Re(f(x)e^{-i\theta}) dx \leq \int_a^b |f(x)e^{-i\theta}| dx \\ \text{car } \forall x, \Re(f(x)e^{-i\theta}) &\leq |f(x)e^{-i\theta}| \end{aligned}$$

$$\leq \int_a^b |f(x)| |e^{-i\theta}| dx = \int_a^b |f(x)| dx$$

□

Proposition (Inégalité de Cauchy-Schwartz): Soient $f, g : [a, b] \rightarrow \mathbb{R}$ continues

$$\left(\int_a^b f(t)g(t)dt \right)^2 \leq \int_a^b f^2(t)dt \int_a^b g^2(t)dt$$

Proposition (Inégalité des Accroissements Finis sur \mathbb{R}): Soit $f : I \rightarrow \mathbb{R}$ dérivable sur I telle qu'il existe $M \in \mathbb{R}$ vérifiant
 $\forall t \in I, |f'(t)| \leq M$

Alors $\forall (a, b) \in I^2, |f(a) - f(b)| \leq M|a - b|$

Proposition (Inégalité des Accroissements Finis sur \mathbb{C}): Soit $f : I \rightarrow \mathbb{C}$ de classe C^1 et M tel que
 $\forall t \in I, |f'(t)| \leq M$

Alors $\forall (a, b) \in I^2, |f(a) - f(b)| \leq M|a - b|$

Preuve:

On suppose $a \leq b$

$$\begin{aligned} |f(a) - f(b)| &= |f(b) - f(a)| = \left| \int_a^b f'(t)dt \right| \\ &\leq \int_a^b |f'(t)| dt \\ &\leq \int_a^b M dt = M(b - a) = M|b - a| \end{aligned}$$

□

11 Valeur Absolue

Proposition (Inégalités avec la Valeur Absolue): Soient $(a, b) \in \mathbb{R}^2$
 $|a| \leq b \iff -b \leq a \leq b$
 $|a| \geq b \iff a \geq b$ ou $a \leq -b$

Proposition (Partie Bornée et Valeur Absolue): Soit $A \in \mathcal{P}(\mathbb{R})$

A est bornée $\iff \exists M \in \mathbb{R}, \forall a \in A, |a| \leq M$

Preuve:

“ \Leftarrow ” :

On suppose qu'il existe $M \in \mathbb{R}$ tel que $\forall a \in A, |a| \leq M$

Donc $\forall a \in A, -M \leq a \leq M$

Donc A est majorée par M et minorée par $-M$

Donc A est bornée

“ \Rightarrow ” :

On suppose A bornée

Soit M un majorant de A et m un minorant de A

On pose $\alpha = \max(M, -m)$

$\alpha \geq M$ et $\forall a \in A, a \leq \alpha$

On a aussi $\alpha \geq m$ donc $-a \leq -m$
donc $-m$ est un majorant

$\forall a \in A, -\alpha \leq a \leq \alpha$
donc $\forall a \in A, |a| \leq \alpha$

□

12 Bornes Inférieure / Supérieure

Proposition (Existence de la Borne Inférieure): Toute partie minorée, non vide de \mathbb{R} admet une borne inférieure

Preuve:

Soit $A \in \mathcal{P}(\mathbb{R})$ non vide et minorée

Soit $B = \{-a \mid a \in A\} \neq \emptyset$

Soit m un minorant de A

$\forall a \in A, m \leq a$
donc $\forall a \in A, -a \geq -m$
donc B est majoré par m

D'après la propriété de la borne supérieure, B admet une borne supérieure
On suppose $\beta = \sup(B)$

β majore B donc $\forall a \in A, -a \leq \beta$
donc $\forall a \in A, -\beta \leq a$
donc $-\beta$ est un majorant de A

Soit x un minorant de A
Montrons que $x \leq -\beta$

$-x$ majore B donc $-x \geq \beta$ donc $x \leq -\beta$

Donc $-\beta = \inf(A)$

□

Proposition (Caractérisation de la Borne Supérieure): Soient $A \in \mathcal{P}(\mathbb{R})$ non vide majorée et $M \in \mathbb{R}$

$$M = \sup(A) \iff \begin{cases} \forall a \in A, a \leq M \\ \forall \varepsilon > 0, \exists a_0 \in A, a_0 > M - \varepsilon \end{cases}$$

Preuve:

“ \implies ” : On suppose $M = \sup(A)$

M est un majorant de A donc $\forall a \in A, a \leq M$
et c'est le plus petit majorant

Soit $\varepsilon > 0$

$M - \varepsilon > M$ donc $M - \varepsilon$ ne majore pas A
 $\exists a_0 \in A, a_0 > M - \varepsilon$

$$\text{“ \impliedby ” : On suppose } \begin{cases} \forall a \in A, a \leq M \\ \forall \varepsilon > 0, \exists a_0 \in A, a_0 > M - \varepsilon \end{cases} \quad \begin{matrix} 1 \\ 2 \end{matrix}$$

D'après 1, M est un majorant de A

Soit M' un majorant de A , montrons $M' \geq M$
On suppose $M' \leq M$, on pose $\varepsilon = M - M' \geq 0$

D'après 2, il existe $a_0 \in A$ tel que
 $a_0 > M - \varepsilon = M' \geq a_0$ contradiction

Donc $M' \geq M$

Donc M est le plus petit majorant de A
Donc $M = \sup(A)$

□

Proposition (Caractérisation de la Borne Inférieure): Soient $A \in \mathcal{P}(\mathbb{R})$ non vide minorée et $M \in \mathbb{R}$

$$M = \inf(A) \iff \begin{cases} \forall a \in A, a > M \\ \forall \varepsilon > 0, \exists a_0 \in A, a_0 < M + \varepsilon \end{cases}$$

Proposition (Inégalité et Borne Supérieure): Soit $A \in \mathcal{P}(\mathbb{R})$ non vide majorée et $M \in \mathbb{R}$

$$M \geq \sup(A) \iff \forall a \in A, M \geq a$$

Preuve:

“ \implies ” : On suppose $M \geq \sup(A)$
 Soit $a \in A$, on sait que $a \leq \sup(A)$ car $\sup(A)$ majore A
 Donc $a \leq M$

“ \impliedby ” : On suppose $\forall a \in A, a \leq M$
 Donc M majore A
 Or, $\sup(A)$ est le plus petit majorant de A donc $M \geq \sup(A)$

□

Proposition (Inégalité et Borne Inférieure): Soit $A \in \mathcal{P}(\mathbb{R})$ non vide minorée et $m \in \mathbb{R}$
 $m \leq \inf(A) \iff \forall a \in A, a > m$

Proposition (\mathbb{R} est archimédien): \mathbb{R} est archimédien :
 $\forall x \in \mathbb{R}_*^+, \forall y \in \mathbb{R}, \exists n \in \mathbb{N}, nx \geq y$

Preuve:

Soient $(x, y) \in \mathbb{R}_*^+ \times \mathbb{R}$
 Supposons $(H) : \forall n \in \mathbb{N}, nx \leq y$

On pose $A = \{nx | n \in \mathbb{N}\} \subset \mathbb{R}$
 $A \neq \emptyset$ car $0 \in A$
 D'après (H) , A est majoré par y
 Soit $\alpha = \sup(A)$

Soit $n \in \mathbb{N}$
 $(n+1)x \in A$ donc $(n+1)x \leq \alpha$
 donc $nx \leq \alpha$

Donc $\begin{cases} \alpha - x \geq nx \\ \alpha - x < \alpha \end{cases}$ Contradiction avec le fait que α soit le plus petit majorant de A

Donc $\exists n \in \mathbb{N}, nx \geq y$

□

Proposition (Théorème des Valeurs Extrêmes): Toute fonction continue sur un segment est bornée et atteint ses bornes

Si $f : [a, b] \rightarrow \mathbb{R}$ est continue, alors
 $\exists (\alpha, \beta) \in [a, b]^2, \forall x \in [a, b], f(\alpha) \leq f(x) \leq f(\beta)$

Preuve:
Voir Chapitre 12 : Suites

□

Proposition (Limite de Suite et Borne Supérieure): Soit $A \in \mathcal{P}(\mathbb{R})$ non vide majorée
Il existe une suite $(a_n) \subset A$ telle que
 $\lim a_n = \sup(A)$

Preuve:
On sait que $\forall \varepsilon > 0, \exists a \in A, a > \sup(A) - \varepsilon$

Donc $\forall n \in \mathbb{N}^*, \exists a_n > \sup(A) - \frac{1}{n}$
 $\forall n \in \mathbb{N}, a_n \in A$ donc $a_n < \sup(A)$
 $\forall a \in \mathbb{N}^*, \sup(A) - \frac{1}{n} < a_n < \sup(A)$

Par encadrement, $a_n \xrightarrow{n \rightarrow +\infty} \sup(A)$

□

Proposition (Limite de Suite et Borne Inférieure): Soit $A \in \mathcal{P}(\mathbb{R})$ non vide minorée
Il existe une suite $(a_n) \subset A$ telle que
 $\lim a_n = \inf(A)$

13 Partie Entière

Proposition (Définition): Soit $x \in \mathbb{R}$
 $\exists! n \in \mathbb{Z}, n \leq x < n + 1$
Cet entier est appelé partie entière de x et noté $\lfloor x \rfloor$

Preuve:
Soit $A = \{p \in \mathbb{Z} | p > x\}$
 $A \neq \emptyset$ car \mathbb{R} est archimédien
 A est minoré par x

Soit α la borne inférieure de A , alors $\alpha \geq x$
Montrons que $\alpha \in \mathbb{Z}$

Soit $n \geq 2, \alpha + \frac{1}{n} \geq \alpha$
donc $\exists a_n \in A, \alpha \leq a_n \leq \alpha + \frac{1}{n}$
 $\frac{1}{n} < 1$ car la distance entre deux entiers est ≥ 1

Il y a au plus 1 entier dans $[\alpha, \alpha + \frac{1}{n}]$

Donc tous les a_n sont égaux et $a_n \rightarrow \alpha$ donc $\forall n \geq 2, a_n = \alpha$
 donc $\alpha \in A$, donc $\alpha = \min(A)$, alors $\alpha - 1 \notin A$
 donc $\alpha - 1 \leq x \leq \alpha$
 On pose $n = \alpha - 1$

□

14 Densité

Définition (Densité): Soit $A \in \mathcal{P}(\mathbb{R})$
 On dit que A est dense dans \mathbb{R} si :
 Pour tout intervalle I ouvert non vide de \mathbb{R} , $A \cap I \neq \emptyset$

Théorème (Densité de \mathbb{Q}): \mathbb{Q} est dense dans \mathbb{R}

Preuve:

Soit I un intervalle ouvert non vide de \mathbb{R}
 Soient $a < b$ deux éléments de I

On cherche $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que $a < \frac{p}{q} < b$

Comme \mathbb{R} est archimédien, $\exists q \in \mathbb{N}^*, q(b - a) \geq 2 > 1$
 Donc l'intervalle $[qa, qb]$ a une longueur supérieure à 1
 Il contient donc au moins 1 entier p

En effet, sinon on a $\lfloor qa \rfloor = \lfloor qb \rfloor$ et alors
 $\begin{cases} \lfloor qa \rfloor \leq qb \leq \lfloor qa \rfloor + 1 \\ \lfloor qa \rfloor \leq qa \leq \lfloor qa \rfloor + 1 \end{cases}$
 et alors $-1 < qb - qa < 1$ contradiction

On a donc $qa \leq p \leq qb$
 et finalement $a \leq \frac{p}{q} \leq b$

□

Théorème (Densité de $\mathbb{R}\mathbb{Q}$): $\mathbb{R}\mathbb{Q}$ est dense dans \mathbb{R}

Preuve:

Soit I un intervalle ouvert non vide de \mathbb{R}

On pose $J = \{x - \sqrt{2}|x \in I\}$, J est ouvert et non vide
 \mathbb{Q} est dense dans \mathbb{R} donc $J \cap \mathbb{Q} \neq \emptyset$

Soit $r \in J \cap \mathbb{Q}$, alors $r + \sqrt{2} \in I$
 Soit $s \in Q = r + \sqrt{2}$, alors $\sqrt{2} = s - r \in \mathbb{Q}$
 ce qui n'est pas le cas
 Ainsi, $r + \sqrt{2} \in I \cap (\mathbb{R} \setminus \mathbb{Q})$

□

REMARQUE (Suite de Rationnels):

Soit $x \in \mathbb{R}, \forall n \in \mathbb{N}^*, I_n =]x - \frac{1}{n}, x + \frac{1}{n}[$

Pour tout $n \in \mathbb{N}^*$, on choisit $r_n \in Q \cap I$

On a défini une suite de rationnels (r_n)

$\forall n \in \mathbb{N}^*, x - \frac{1}{n} \leq r_n \leq x + \frac{1}{n}$

Par encadrement, $r_n \rightarrow x$

Proposition (Approximation par Défaut et par Excès): Soit $x \in \mathbb{R}$

Alors, $\forall n \in \mathbb{N}, \frac{\lfloor 10^n x \rfloor}{10^n} \leq x < \frac{\lfloor 10^n x \rfloor}{10^n} + \frac{1}{10^n}$

On démontrera que $\frac{\lfloor 10^n x \rfloor}{10^n} \xrightarrow{n \rightarrow +\infty} x$

Preuve:

$\forall n \in \mathbb{N}, \lfloor 10^n x \rfloor \leq 10^n x < \lfloor 10^n x \rfloor + 1$

□

Corollaire (Densité de D): Soit D l'ensemble des nombres décimaux

$D = \left\{ \frac{p}{10^n} \mid p \in \mathbb{Z}, n \in \mathbb{N} \right\}$

D est dense dans \mathbb{R}

15 Intervalles

Définition (Intervalle de \mathbb{R}): Un intervalle de \mathbb{R} est une partie de \mathbb{R} d'une de ces formes :

$\{x \in \mathbb{R} \mid a \leq x \leq b\}, (a, b) \in \mathbb{R}^2$

$\{x \in \mathbb{R} \mid a \leq x < b\}, a \in \mathbb{R}, b \in \mathbb{R} \cup \{+\infty\}$

$\{x \in \mathbb{R} \mid a < x \leq b\}, a \in \mathbb{R} \cup \{-\infty\}, b \in \mathbb{R}$

$\{x \in \mathbb{R} \mid a < x < b\}, a \in \mathbb{R} \cup \{-\infty\}, b \in \mathbb{R} \cup \{+\infty\}$

Définition (Partie Convexe): Soit D une partie de \mathbb{R}

On dit que D est convexe si $\forall (x, y) \in D^2, x \leq y \implies [x, y] \in D$

Théorème (Intervalle et Convexité): Soit $D \in \mathcal{P}(\mathbb{R})$
 D est un intervalle $\iff D$ est convexe

Preuve:

“ \implies ” : On suppose que D est un intervalle

Cas 1 : On suppose $D = [a, b]$ avec $(a, b) \in \mathbb{R}^2$ et $a \leq b$
 Soient $(x, y) \in D^2$ avec $x \leq y$
 Soit $z \in [x, y]$
 On a donc $a \leq x \leq z \leq y \leq b$ donc $z \in [a, b]$
 Donc D est convexe

Cas 2 : On suppose $D = [a, b[$ avec $a \in \mathbb{R}, b \in \mathbb{R} \cup \{+\infty\}$ et $a < b$
 Soient $(x, y) \in D^2$ avec $x \leq y$
 Soit $z \in [x, y]$
 On a donc $a \leq x \leq z \leq y < b$ donc $z \in [a, b]$
 Donc D est convexe

Les deux autres cas se traitent de la même façon

“ \iff ” : On suppose que D est convexe et non vide

On pose $M = \begin{cases} \sup(D) & \text{si } D \text{ est majorée} \\ +\infty & \text{sinon} \end{cases}$ et $m = \begin{cases} \inf(D) & \text{si } D \text{ est minorée} \\ -\infty & \text{sinon} \end{cases}$

Montrons que
 $]m, M[\subset D \subset [m, M]$ si $(m, M) \in \mathbb{R}^2$
 $]m, M[\subset D \subset [m, M[$ si $m \in \mathbb{R}, M = +\infty$
 $]m, M[\subset D \subset]m, M]$ si $m = -\infty, M \in \mathbb{R}$
 $]m, M[\subset D \subset]m, M[$ si $m = -\infty, M = +\infty$

Soit $z \in]m, M[$
 Si $M \in \mathbb{R}$, z ne majore pas D car $z \leq M$
 Si $M = +\infty$, D n'est pas majorée donc z n'est pas un majorant
 Donc $\exists y \in D, y \geq z$

Si $m \in \mathbb{R}$, z ne minore pas D car $m \leq z$
 Si $m = -\infty$, D n'est pas minorée donc z n'est pas un minorant
 Donc $\exists x \in D, x \leq z$

Donc $z \in [x, y] \subset D$ car $\begin{cases} (x, y) \in D^2 \\ D \text{ convexe} \end{cases}$

Donc $z \in D$, on a bien $]m, M[\subset D$

Cas 1 : On suppose $(m, M) \in \mathbb{R}^2$

Soit $z \in D$, $\begin{cases} m \text{ minore } D \text{ donc } m \leq z \\ M \text{ majore } D \text{ donc } z \leq M \end{cases}$ donc $z \in [m, M]$

Donc $D \in \{]m, M[, [m, M[,]m, M], [m, M]\}$
 Donc D est un intervalle

Cas 2 : On suppose $m \in \mathbb{R}, M = +\infty$

Soit $z \in D$, $\begin{cases} m \text{ minore } D \text{ donc } m \leq z & \text{donc } z \in [m, +\infty[\\ M = +\infty \end{cases}$

Donc $D \in \{]m, M[, [m, M[\}$
Donc D est un intervalle

Cas 3 : On suppose $m = -\infty, M \in \mathbb{R}$

Soit $z \in D$, $\begin{cases} m = -\infty \\ M \text{ majore } D \text{ donc } z \leq M \end{cases} \text{ donc } z \in]-\infty, M]$

Donc $D \in \{]m, M[,]m, M[\}$
Donc D est un intervalle

Cas 4 : On suppose $m = -\infty, M = +\infty$

Soit $z \in \mathbb{R}$ donc $z \in]-\infty, +\infty[$

$D = \mathbb{R}$ donc D est un intervalle

□

Proposition (Bornes, Min et Max): Soient $a, b \in \mathbb{R}$

$$\inf([a, b]) = \min([a, b]) = a$$

$$\sup([a, b]) = \max([a, b]) = b$$

$$\inf(]a, b[) = a$$

$$\sup(]a, b[) = b$$

$$\inf([a, b[) = \min([a, b[) = a$$

$$\sup([a, b[) = b$$

$$\inf(]a, b]) = a$$

$$\sup(]a, b]) = \max(]a, b]) = b$$

Proposition (Intersection d'Intervalles): Un intersection quelconque d'intervalles est convexe

Preuve:

Soit $(I_a)_{a \in A}$ une famille d'intervalles et $I = \bigcap_{a \in A} I_a$

Montrons que I est un intervalle
Montrons que I est convexe

Soit $(x, y) \in I^2$, $x \leq y$, montrons $[x, y] \subset I$

Soit $z \in [x, y]$
Soit $a \in A$

$x \in I$ donc $x \in I_a$
 $y \in I$ donc $y \in I_a$

I_a est convexe
Donc $z \in I_a$

□

REMARQUE (Réunion d'Intervalles):
Un réunion d'intervalles n'est pas nécessairement un intervalle

16 Fonction Convexes

Définition (Fonction Convexe): Soit $f : I \rightarrow \mathbb{R}$ avec I un intervalle
On dit que f est convexe si
 $\forall (x, y) \in I^2, \forall \lambda \in [0, 1], f((1 - \lambda)x + \lambda y) \leq (1 - \lambda)f(x) + \lambda f(y)$

Proposition (Expression d'un Élément d'un Intervalle selon les Bornes): Soit $(a, b) \in \mathbb{R}^2$ avec $a \leq b$
Soit $x \in \mathbb{R}$
 $x \in [a, b] \iff \exists \lambda \in [0, 1], x = (1 - \lambda)a + \lambda b$

Preuve:
 $x \in [a, b] \iff a \leq x \leq b$
 $\iff 0 \leq x - a \leq b - a$
 $\iff 0 \leq \frac{x - a}{b - a} \leq 1$
 $\iff \exists \lambda \in [0, 1], \lambda = \frac{x - a}{b - a}$
 $\iff \exists \lambda \in [0, 1], x = \lambda(b - a) + a$
 $\iff \exists \lambda \in [0, 1], x = \lambda b - \lambda a + a$
 $\iff \exists \lambda \in [0, 1], x = (1 - \lambda)a + \lambda b$

□

Proposition (Inégalité de Jansen): Soit $f : I \rightarrow \mathbb{R}$ convexe
et $(x_1, \dots, x_n) \in I^n$, $(\lambda_1, \dots, \lambda_n) \in [0, 1]^n$ tels que $\sum_{i=1}^n \lambda_i = 1$ et $n \geq 2$

Alors $f\left(\sum_{i=1}^n \lambda_i x_i\right) \leq \sum_{i=1}^n \lambda_i f(x_i)$

Preuve:

Soit $n \geq 2$

$$\forall (x_1 \dots x_n) \in I^n, (\lambda_1 \dots \lambda_n) \in [0, 1]^n \text{ tels que } \sum_{i=1}^n \lambda_i = 1$$

$$\text{On a } f\left(\sum_{i=1}^n \lambda_i x_i\right) \leq \sum_{i=1}^n \lambda_i f(x_i)$$

$$\text{Soient } (x_1 \dots x_{n+1}) \in I^{n+1}, (\lambda_1 \dots \lambda_{n+1}) \in [0, 1]^{n+1}$$

$$\text{On suppose } \sum_{i=1}^{n+1} \lambda_i = 1$$

$$\text{On suppose } \lambda_{n+1} \neq 1$$

$$\text{On pose } \begin{cases} \lambda = \sum_{i=1}^n \lambda_i = 1 - \lambda_{n+1} \neq 0 \\ x = \frac{1}{\lambda} \sum_{i=1}^n \lambda_i x_i = \sum_{i=1}^n \frac{\lambda_i}{\lambda} x_i \in I \end{cases}$$

$$\begin{aligned} \text{Ainsi, } f\left(\sum_{i=1}^{n+1} \lambda_i x_i\right) &= f\left(\lambda_{n+1} x_{n+1} + \sum_{i=1}^n \lambda_i x_i\right) \\ &= f((1 - \lambda)x_{n+1} + \lambda x) \leq (1 - \lambda)f(x_{n+1}) + \lambda f(x) \end{aligned}$$

$$\text{De plus, } f(x) = f\left(\sum_{i=1}^n \mu_i x_i\right) \text{ avec } \forall i \in \llbracket 1, n \rrbracket, \mu_i = \frac{\lambda_i}{\lambda}$$

$$\sum_{i=1}^n \mu_i = \sum_{i=1}^n \frac{\lambda_i}{\lambda} = \frac{1}{\lambda} + \lambda = 1$$

D'après l'hypothèse de récurrence,

$$f(x) \leq \sum_{i=1}^n \frac{\lambda_i}{\lambda} f(x_i)$$

D'où

$$f\left(\sum_{i=1}^{n+1} \lambda_i x_i\right) = \lambda_{n+1} f(x_{n+1}) + \sum_{i=1}^n \lambda_i f(x_i)$$

Montrons que $x \in I$

$$\text{On pose } \begin{cases} \alpha = \min\{x_i | i \in \llbracket 1, n \rrbracket\} \in I \\ \beta = \max\{x_i | i \in \llbracket 1, n \rrbracket\} \in I \end{cases}$$

$$\forall i \in \llbracket 1, n \rrbracket, \alpha \leq x_i \leq \beta$$

$$\text{donc } \forall i \in \llbracket 1, n \rrbracket, \frac{\lambda_i}{\lambda} \alpha \leq \frac{\lambda_i}{\lambda} x_i \leq \frac{\lambda_i}{\lambda} \beta$$

$$\text{donc } \sum_{k=1}^n \frac{\lambda_i}{\lambda} \alpha \leq \sum_{k=1}^n \frac{\lambda_i}{\lambda} x_i \sum_{k=1}^n \frac{\lambda_i}{\lambda} \beta$$

$$\text{donc } \alpha \leq x \leq \beta$$

Donc, par convexité de I ,

$$\text{On suppose } \lambda_{n+1} = 1, \text{ alors } \sum_{i=1}^n \lambda_i = 0$$

$$\text{Or, } \forall i \in \llbracket 1, n \rrbracket, \lambda_i \geq 0$$

$$\text{Donc } \forall i \in \llbracket 1, n \rrbracket, \lambda_i = 0$$

$$f\left(\sum_{i=1}^n \lambda_i x_i\right) = f(x_{n+1}) \leq \sum_{i=1}^{n+1} \lambda_i f(x_i) = f(x_{n+1})$$

□

Proposition (Lemme des Pentes): Soit $f : I \rightarrow \mathbb{R}$ convexe
Soient $x_1 < x_2 < x_3 \in I^3$
Alors $\frac{f(x_1) - f(x_2)}{x_1 - x_2} \leq \frac{f(x_1) - f(x_3)}{x_1 - x_3} \leq \frac{f(x_2) - f(x_3)}{x_2 - x_3}$

Preuve:

$$\begin{aligned} \text{Soit } \lambda \in]0, 1[\text{ tel que } x_2 = (1 - \lambda)x_1 + \lambda x_3 \\ f(x_2) - f(x_1) &\leq (1 - \lambda)f(x_1) + \lambda f(x_3) - f(x_1) \\ &\leq \lambda(f(x_3) - f(x_1)) \\ x_2 - x_1 &= \lambda(x_3 - x_1) > 0 \end{aligned}$$

$$\text{D'où } \frac{f(x_2) - f(x_1)}{x_2 - x_1} \leq \frac{\lambda(f(x_3) - f(x_1))}{\lambda(x_3 - x_1)} \leq \frac{f(x_3) - f(x_1)}{x_3 - x_1}$$

$$\begin{aligned} f(x_2) - f(x_3) &\leq (1 - \lambda)f(x_1) + \lambda f(x_3) - f(x_3) \\ &\leq (1 - \lambda)(f(x_1) - f(x_3)) \end{aligned}$$

$$\begin{aligned} x_2 - x_3 &= (1 - \lambda)(x_1 - x_3) < 0 \\ \frac{f(x_2) - f(x_3)}{x_2 - x_3} &\geq \frac{(1 - \lambda)(f(x_1) - f(x_3))}{(1 - \lambda)(x_1 - x_3)} \geq \frac{f(x_1) - f(x_3)}{x_1 - x_3} \end{aligned}$$

□

Proposition (Réciproque du Lemme des Pentes): Soit $f : I \rightarrow \mathbb{R}$

Si, $\forall x_1 < x_2 < x_3 \in I^3$, $\frac{f(x_1) - f(x_2)}{x_1 - x_2} \leq \frac{f(x_1) - f(x_3)}{x_1 - x_3}$
Alors f est convexe

Preuve:

Soient $x \leq y \in I^2$
Soient $\lambda \in]0, 1[$ et $z = (1 - \lambda)x + \lambda y$

Montrons que $f(z) \leq (1 - \lambda)f(x) + \lambda f(y)$

On pose $\begin{cases} x_1 = x \\ x_2 = z \\ x_3 = y \end{cases}$ Ainsi, $x_1 < x_2 < x_3$

Donc $\frac{f(x) - f(z)}{x - z} \leq \frac{f(x) - f(y)}{x - y}$ (*) et $\lambda = \frac{z - x}{y - x}$

(*) $\implies \frac{f(z) - f(x)}{z - x} \leq \frac{f(y) - f(x)}{y - x}$

$\implies f(z) - f(x) \leq \frac{f(y) - f(x)}{y - x}(z - x)$

$\implies f(z) \leq \lambda(f(y) - f(x)) + f(x) = \lambda f(y) + (1 - \lambda)f(x)$

□

REMARQUE (Autres Preuves Possible):

Si on remplace (*) par $\frac{f(x_1) - f(x_3)}{x_1 - x_3} \leq \frac{f(x_2) - f(x_3)}{x_2 - x_3}$ ou par $\frac{f(x_1) - f(x_2)}{x_1 - x_2} \leq \frac{f(x_2) - f(x_3)}{x_2 - x_3}$

On peut aussi conclure que f est convexe

Proposition (Théorème Convexité / Dérivabilité): Soit $f : I \rightarrow \mathbb{R}$ convexe sur I ouvert

Alors f est dérivable à gauche et à droite en tout point de I et

$\forall x \in I, f'_{gauche}(x) \leq f'_{droite}(x)$

Preuve:

Soit $a \in I$ et $\tau_a : I \setminus \{a\} \rightarrow \mathbb{R}$

$$x \mapsto \frac{f(x) - f(a)}{x - a}$$

D'après le Lemme des Pentes, τ_a est croissante

En effet, soient $(x, y) \in (I \setminus \{a\})^2$ et $x < y$

Cas 1 : $a < x < y$

$$\text{On a alors } \frac{f(x) - f(a)}{x - a} \leq \frac{f(y) - f(a)}{y - a}$$

Donc $\tau_a(x) \leq \tau_a(y)$

Cas 2 : $x \leq a \leq y$

$$\text{On a alors } \frac{f(x) - f(a)}{x - a} \leq \frac{f(x) - f(y)}{x - y} \leq \frac{f(y) - f(a)}{y - a}$$

Donc $\tau_a(x) \leq \tau_a(y)$

Cas 3 : $x \leq y \leq a$

$$\text{On a alors } \frac{f(x) - f(y)}{x - y} \leq \frac{f(x) - f(a)}{x - a} \leq \frac{f(y) - f(a)}{y - a}$$

Donc $\tau_a(x) \leq \tau_a(y)$

Donc $\tau_a(x) \leq \tau_a(y)$

Soit $x > a$ avec $x \in I$

On fixe $z_0 < a$ avec $z_0 \in I$

Alors $\tau_a(x) \geq \tau_a(z_0)$

τ_a est minorée sur $I \cap]a, +\infty[$ et croissante

Donc τ_a a une limite finie quand x tend vers a par valeur supérieure

Donc f est dérivable à droite et $f'_{droite}(a) \geq \tau_a(z_0)$

Soit $z_1 > a$ fixé

$\forall x \in I \cap]-\infty, a[, \tau_a(x) \leq \tau_a(z_1)$

Donc τ_a est majorée sur $I \cap]-\infty, a[$

Donc τ_a a une limite finie que x tend vers a par valeur inférieure

Donc f est dérivable à gauche et $f'_{gauche}(a) \leq \tau_a(z_1)$

De plus, $\forall x \in I \cap]-\infty, a[, \forall y \in]a, +\infty[, \tau_a(x) \leq \tau_a(y)$

Donc, si on fait tendre x vers a par valeur inférieure :

$$\forall y \in I \cap]a, +\infty[, f'_{gauche}(a) \leq \tau_a(y)$$

Si on fait tendre y par valeur supérieure :

$$f'_{gauche}(x) \leq f'_{droite}(x)$$

□

Corollaire: Soit $f : I \rightarrow \mathbb{R}$ convexe où I est ouvert
Alors f est continue sur I

Preuve:

Soit $a \in I$

$$\forall x \in I \cap]-\infty, a[, \frac{f(x) - f(a)}{x - a} = f'_g(a) + \underset{x \rightarrow a^-}{o}(1)$$

$$\text{Donc } f(x) = f(a) + f'_g(a)(x - a) + \underset{x \rightarrow a^-}{o}(x - a)$$

$$\text{Donc } f(x) \xrightarrow{x \rightarrow a^-} f(a)$$

$$\text{De même, } \forall x \in I \cap]a, +\infty[, f(x) = f(a) + f'_d(a)(x - a) + \underset{x \rightarrow a^+}{o}(x - a)$$

$$\text{Donc } f(x) \xrightarrow{x \rightarrow a^+} f(a)$$

Donc f est continue en a

□

Proposition (Théorème Convexité / Croissance Dérivée): Soit $f : I \rightarrow \mathbb{R}$ dérivable
 f est dérivable $\iff f'$ est croissante

Preuve:

“ \implies ” : On suppose que I a au moins 2 éléments distincts, sinon le résultat est trivial
On suppose f convexe

Soient $(x, y) \in I^2$, on suppose $x < y$

Soit $u \in]x, y[$

$$\text{Soit } \tau_x : u \mapsto \frac{f(u) - f(x)}{u - x}$$

Comme τ_x est croissante sur $I \setminus \{x\}$, $f'(x) \leq \tau_x(u)$

D'après le Lemme des Pentes,

$$\frac{f(u) - f(x)}{u - x} \leq \frac{f(x) - f(y)}{x - y} \leq \frac{f(y) - f(u)}{y - u}$$

et donc $\tau_x(u) \leq \tau_y(u)$

Comme τ_y est croissante, $\tau_y(u) \leq f'(y)$

D'où $f'(x) \leq \tau_x(u) \leq \tau_y(u) \leq f'(y)$

Donc f' est croissante

“ \Leftarrow ” : On va exploiter le Théorème des Accroissements Finis

Soit $f : [a, b] \rightarrow \mathbb{R}$ continue dérivable sur $]a, b[$

$$\text{Alors } \exists c \in]a, b[, f'(c) = \frac{f(a) - f(b)}{a - b}$$

Soient $x_1 < x_2 < x_3 \in I^3$

f est continue sur $[x_1, x_2]$ et dérivable sur $]x_1, x_2[$

$$\exists c_1 \in]x_1, x_2[, \frac{f(x_1) - f(x_2)}{x_1 - x_2} = f'(c_1)$$

f est continue sur $[x_2, x_3]$ et dérivable sur $]x_2, x_3[$

$$\exists c_2 \in]x_2, x_3[, \frac{f(x_2) - f(x_3)}{x_2 - x_3} = f'(c_2)$$

On remarque que $c_1 < x < c_2$

Comme f' est croissante, $f'(c_1) \leq f'(c_2)$

□

Corollaire: Soit $f : I \rightarrow \mathbb{R}$ deux fois dérivable
 f convexe sur $I \iff \forall x \in I, f''(x) > 0$

Proposition (Inégalité Image / Taux de Variation): Soit $f : I \rightarrow \mathbb{R}$ convexe, dérivable
 $\forall (x, a) \in I^2, f(x) \geq f'(a)(x - a) + f(a)$

Preuve:

Soit $a \in I$

On pose $g : I \rightarrow \mathbb{R}$

$$x \mapsto f(x) - f'(a)(x - a) + f(a)$$

g est dérivable sur I et $g'(x) = f'(x) - f'(a)$

On sait que f' est croissante sur I

g est décroissante pour $x < a$, croissante pour $x > a$ et $g(a) = 0$
 $\forall x \in I, g(x) \geq 0$

□

Définition (Concavité): On dit que f est concave si $-f$ est convexe

Proposition (Concavité): Soit $f : I \rightarrow \mathbb{R}$
 f concave $\iff \forall (x, y) \in I^2, \forall \lambda \in [0, 1], f((1 - \lambda)x + \lambda y) \geq (1 - \lambda)f(x) + \lambda f(y)$

Si f est concave sur un intervalle I ouvert, f est continue

Si f est dérivable, f concave $\iff f'$ décroissante

Si f est deux fois dérivable, f concave $\iff f''$ négative

Si f est dérivable et concave, $\forall(x, a) \in I^2, f(x) < f'(a)(x - a) + f(a)$

CHAPITRE

10

NOMBRES ENTIERS - \mathbb{N}

1 Axiomatique de \mathbb{N}

Axiome: (\mathbb{N}, \leq) est un ensemble non vide totalement ordonné vérifiant

- Toute partie non vide de \mathbb{N} a un plus petit élément ;
- Toute partie non vide majorée de \mathbb{N} a un plus grand élément ;
- \mathbb{N} n'est pas majoré.

Définition: — 0 est le plus petit élément de \mathbb{N} : $0 = \min(\mathbb{N})$.

— $1 = \min(\mathbb{N}^*) = \min(\mathbb{N} \setminus \{0\})$.

— Soit $n \in \mathbb{N}$. On pose $n + 1 = \min(\{k \in \mathbb{N} \mid k > n\})$. On dit que $n + 1$ est le successeur de n .

— Soit $n \in \mathbb{N}^*$. On pose $n - 1 = \max(\{k \in \mathbb{N} \mid k < n\})$. On dit que $n - 1$ est le prédécesseur de n .

Proposition:

$$\begin{cases} \forall n \in \mathbb{N}, (n + 1) - 1 = n; \\ \forall n \in \mathbb{N}^*, (n - 1) + 1 = n. \end{cases}$$

Preuve:

Soit $n \in \mathbb{N}$. On pose $p = n + 1$ et $q = p - 1$. On a donc $n < p$ et $q < p$ et donc $n \leq q$ car $q = \max(\{k \in \mathbb{N} \mid k < p\})$.

Si $q > n$, alors $q \geq p$ car $p = \min(\{k \in \mathbb{N} \mid k > n\})$: une contradiction.

On a donc $q = n$. □

Proposition: Pour tout $n \in \mathbb{N}$, $\mathbb{N} \cap]n, n + 1[= \emptyset$.

Preuve:

Soit $n \in \mathbb{N}$. On sait que $n + 1 > n$. Soit $p \in \mathbb{N}$ tel que $n < p < n + 1$. Comme $p > n$, $p \geq n + 1$: une contradiction. \square

Théorème (référence): Soit P un prédicat sur \mathbb{N} et $n_0 \in \mathbb{N}$. Si

$$\begin{cases} P(n_0) \text{ est vrai ,} \\ \forall n \geq n_0, P(n) \implies P(n+1), \end{cases}$$

alors

$$\forall n \geq n_0, P(n) \text{ est vrai.}$$

Preuve:

Soit $A = \{n \in \mathbb{N} \mid n \geq n_0 \text{ et } P(n) \text{ faux}\}$. Supposons $A \neq \emptyset$; A a donc un plus petit élément. On pose $N = \min(A)$.

CAS 1 $N = 0$, alors, comme $N \in A$, on a $n_0 \leq 0$ et $P(0)$ fausse. On en déduit que $n_0 = 0$: une contradiction car $P(n_0) = P(0)$ est vraie.

CAS 2 $N \neq 0$. Alors $N - 1 \in \mathbb{N}$ et $N - 1 \notin A$ (car $N - 1 < N$). On en déduit que $N - 1 < n_0$ ou $P(N - 1)$ vraie.

— Supposons $N - 1 < n_0$. $N \in A$ donc $N \geq n_0$ et donc $N - 1 < n_0 \leq N$ donc $N = n_0$. Or, $N \in A$ donc $P(N)$ fausse alors que $P(n_0)$ est vraie.

— Supposons $N - 1 > n_0$ et $P(N - 1)$ vraie. Comme $N - 1 \geq n_0$, $P(N - 1) \implies P(N)$ et donc $P(N)$ est vraie. Or, $N \in A$ et donc $P(N)$ est fausse.

On en déduit que $A = \emptyset$. \square

2 Référence

Proposition (référence double): Soit P un prédicat sur \mathbb{N} et $n_0 \in \mathbb{N}$. Si

$$\begin{cases} P(n_0) \text{ vraie} \\ P(n_0 + 1) \text{ vraie} \\ \forall n \in \mathbb{N} \text{ avec } n \geq n_0, P(n) \text{ et } P(n+1) \implies P(n+2) \end{cases}$$

Alors

$$\forall n \in \mathbb{N} \text{ avec } n \geq n_0, P(n) \text{ vraie.}$$

Preuve:

On pose, pour tout $n \geq n_0$,

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

— $Q(0)$ est vraie.

— Soit $n \geq n_0$. On suppose $Q(n)$ vraie. On sait alors que $P(n+2)$ est vraie. De plus, par hypothèse de récurrence, $P(n+1)$ est vraie. Donc $Q(n+1)$ est vraie. \square

EXEMPLE:

On pose $u_0 = 0$, $u_1 = 1$ et

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

Montrons que $\forall n \in \mathbb{N}, u_n \geq 0$.

- $u_0 = 0 \geq 0$;
 - $u_1 = 1 \geq 0$;
 - Soit $n \in \mathbb{N}$. On suppose que $u_n \geq 0$ et $u_{n+1} \geq 0$. Alors $u_{n+2} = u_n + u_{n+1} \geq 0$.
- Par récurrence double,

$$\forall n \in \mathbb{N}, u_n \geq 0.$$

Proposition: Soit P un prédictat, $p \in \mathbb{N}^*$ et $n_0 \in \mathbb{N}$. Si

$$\begin{cases} \forall k \in \llbracket 0, p-1 \rrbracket, P(n_0+k) \text{ vraie;} \\ \forall n \geq n_0, (P(n) \text{ et } P(n+1) \text{ et } \dots \text{ et } P(n+p-1)) \implies P(n+p). \end{cases}$$

Alors,

$$\forall n \geq n_0, P(n) \text{ vraie.}$$

□

EXEMPLE:

On pose $u_0 = 0$, $u_1 = 1$, $u_2 = 2$, $u_3 = 3$ et

$$\forall n \in \mathbb{N}, u_{n+4} = u_n + 2u_{n+1} + 3u_{n+2} + u_{n+3}.$$

Montrons que $\forall n \in \mathbb{N}, u_n \geq 0$.

- $u_0 \geq 0$, $u_1 \geq 0$, $u_2 \geq 0$ et $u_3 \geq 0$.
- Soit $n \in \mathbb{N}$. On suppose $u_n \geq 0$, $u_{n+1} \geq 0$, $u_{n+2} \geq 0$ et $u_{n+3} \geq 0$. Comme u_{n+4} est la somme de réels positifs, $u_{n+4} \geq 0$.

Proposition (référence forte): Soit P un prédictat sur \mathbb{N} et $n_0 \in \mathbb{N}$. Si $P(n_0)$ est vrai et

$$\forall n \geq n_0, (P(n_0) \text{ et } \dots \text{ et } P(n-1) \text{ et } P(n)) \implies P(n+1).$$

Alors,

$$\forall n \geq n_0, P(n) \text{ est vraie.}$$

Preuve:

On pose, pour tout $n \in \mathbb{N}$,

$$Q(n) : \text{"}\forall k \in \llbracket n_0, n \rrbracket, P(k) \text{ vraie"}$$

- $Q(n_0)$ est vraie car $P(n_0)$ est vraie.
- Soit $n \geq n_0$. On suppose $Q(n)$ vraie. On sait donc que $\forall k \in \llbracket n_0, n \rrbracket, P(k)$ vraie.
Alors, $P(n+1)$ est vraie et donc

$$\forall k \in \llbracket n_0, n+1 \rrbracket, P(k) \text{ est vraie.}$$

Ainsi, $Q(n+1)$ est vraie.

□

EXEMPLE:

Montrer que tout entier supérieur ou égal à 2 peut s'écrire comme un produit de nombres premiers. On prouve ce résultat par référence forte.

- Le nombre 2 est un nombre premier : $2 = 2$.
- Soit $n \geq 2$. On suppose que, tout entier $k \in \llbracket 2, n \rrbracket$ est un produit de nombres premiers.
On pose $N = n+1$.
- CAS 1 N est premier et donc, on peut l'exprimer comme un produit de nombres premiers : $N = N$.
- CAS 2 N n'est pas un nombre premier. Alors, il existe p, q tels que $N = p \times q$ avec $1 < p < N$ et $1 < q < N$. Comme $p \in \llbracket 2, n \rrbracket$, p est un produit de nombres premiers. De même pour q . Donc, le produit $N = p \times q$ est un produit de nombres premiers.

EXEMPLE:

Avec $u_0 = 0$, $u_1 = 1$, $u_2 = 2$, $u_3 = 3$ et, pour tout $n \in \mathbb{N}$, $u_{n+4} = u_n + 2u_{n+1} + 3u_{n+2} + u_{n+3}$, montrer que, pour tout $n \in \mathbb{N}$, $u_n \geq 0$. On prouve ce résultat par récurrence forte.

- $u_0 = 0 \geq 0$.
- Soit $n \in \mathbb{N}$. On suppose que $\forall k \in \llbracket 1, n \rrbracket$, $u_k \geq 0$.
 - Si $n = 0$, $u_{n+1} = u_1 = 1 \geq 0$.
 - Si $n = 1$, $u_{n+1} = u_2 = 2 \geq 0$.
 - Si $n = 2$, $u_{n+1} = u_3 = 3 \geq 0$.
 - Si $n \geq 3$, $u_{n+1} = \underbrace{u_{n-3}}_{\geq 0} + 2 \underbrace{u_{n-2}}_{\geq 0} + 2 \underbrace{u_{n-1}}_{\geq 0} + 3 \underbrace{u_n}_{\geq 0} \geq 0$.

3 Divisibilité

Définition: Soient $a, b \in \mathbb{Z}$. On dit que a divise b s'il existe $k \in \mathbb{Z}$ tel que $b = k \times a$. Dans ce cas, on écrit $a \mid b$. On dit aussi que a est un diviseur de b ; et que b est un multiple de a .

EXEMPLE: — $\forall x \in \mathbb{Z}$, $1 \mid x$.

- $0 \mid 0$ mais $\forall x \in \mathbb{Z}^*, 0 \nmid x$.
- $\forall x \in \mathbb{Z}$, $x \mid 0$.

Proposition: “ \mid ” est une relation d'ordre sur \mathbb{Z} .

□

Proposition: Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$.

$$a \mid b \implies |a| \leq |b|.$$

□

Proposition: Soient $a, b, c \in \mathbb{Z}$.

$$\left. \begin{array}{l} a \mid b \\ a \mid c \end{array} \right\} \implies (\forall (k, \ell) \in \mathbb{Z}^2, a \mid (kb + \ell c)).$$

Preuve:

On pose $u, v \in \mathbb{Z}$ tels que

$$\left\{ \begin{array}{l} b = au, \\ c = av. \end{array} \right.$$

Soient $k, \ell \in \mathbb{Z}$.

$$bk + \ell c =aku + a\ell v = a \underbrace{ku + \ell v}_{\in \mathbb{Z}}.$$

et donc $a \mid (ku + \ell v)$.

□

EXEMPLE:

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

$$\left. \begin{array}{l} a \mid n \\ a \mid n+1 \end{array} \right\} \implies a \mid ((n+1) - n) \implies a \mid 1 \implies a = \pm 1.$$

Définition: Soient $a, b \in \mathbb{Z}$. On dit que a et b sont associés si

$$a = b \text{ ou } a = -b.$$

Proposition: Soient $a, b \in \mathbb{Z}$.

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

Proposition (division euclidienne dans \mathbb{N}): Soient $(a, b) \in \mathbb{N} \times \mathbb{N}^*$.

$$\begin{array}{c} a \\ \hline q \\ \hline r \end{array}$$

$$\exists! (q, r) \in \mathbb{N}^2, \begin{cases} a = bq + r, \\ 0 \leq r < q. \end{cases}$$

Preuve: EXISTENCE On considère $A = \{q \in \mathbb{N} \mid qb \leq a\}$. $A \neq \emptyset$ car $0 \in A$: $0 \times b = 0 \leq a$. A est majoré :

$$\forall q \in A, a \geq qb \geq q \text{ car } b \geq 1.$$

Soit $q = \max(A)$. On pose $r = a - bq$. Comme a, b et q sont des entiers positifs, $r \in \mathbb{Z}$. On sait que $q \in A$, donc $qb \leq a$ et donc $r \geq 0$. $q + 1 > \max A$ donc $q + 1 \notin A$ i.e. $(q + 1)b > a$ et donc $r < b$.

UNICITÉ Soient $(q', r') \in \mathbb{N}^2$ tels que $\begin{cases} a = q'b + r', \\ 0 \leq r' < b. \end{cases}$ Or, $a = bq + r$ et donc, en soustrayant les deux égalités, on a

$$0 = b(q' - q) + r' - r.$$

De plus, $0 \leq r < b$ et $-b < -r' \leq 0$, et donc

$$r - r' = b(\underbrace{q' - q}_{\in \mathbb{Z}}).$$

On en déduit que $-b < r - r' < b$. Le seul multiple de b dans $[-b, b]$ est 0. Ainsi, $r' = r$ et donc $b(q' - q) = 0$. Or, $b > 0$, donc $q' = q$.

□

Proposition (division euclidienne dans \mathbb{Z}): Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$.

$$\exists! (q, r) \in \mathbb{Z}^2, \begin{cases} a = bq + r, \\ 0 \leq r \leq |b|. \end{cases}$$

Preuve: EXISTENCE Cas1 $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. D'après la proposition précédente,

$$\exists!(q, r) \in \mathbb{N}^2, \begin{cases} a = bq + r \\ 0 \leq r < b. \end{cases}$$

Comme $b > 0$, on a bien $0 \leq r < |b| = b$. et $q \in \mathbb{N} \subset \mathbb{Z}$.
Cas2 $a \in \mathbb{Z}^-$ et $b \in \mathbb{N}^*$. Comme $-a \in \mathbb{N}$,

$$\exists(q', r') \in \mathbb{N}^2, \begin{cases} -a = bq' + r' \\ 0 \leq r' < b \end{cases}$$

donc

$$\begin{aligned} a &= b(-q') - r' \\ &= b(q' - 1) + b - r'. \end{aligned}$$

En posant,

$$\begin{aligned} q &= \begin{cases} -q' - 1 & \text{si } r' \neq 0, \\ -q' & \text{si } r' = 0; \end{cases} \\ r &= \begin{cases} b - r' & \text{si } r' \neq 0, \\ -r' & \text{si } r' = 0; \end{cases} \end{aligned}$$

on a bien

$$\begin{cases} a = bq + r, \\ q \in \mathbb{Z}, \\ 0 \leq r < b. \end{cases}$$

Cas3 $a \in \mathbb{N}$ et $b \in \mathbb{Z}_-^*$. On sait que

$$\exists(q', r') \in \mathbb{N}^2, \begin{cases} a = (-b)q' + r' \\ 0 \leq r' < -b. \end{cases}$$

En posant $q = -q'$ et $r = r'$, on a bien $a = bq + r$ et $0 \leq r < |b|$.
Cas4 $a \in \mathbb{Z}^-$ et $b \in \mathbb{Z}_-^*$. On sait que

$$\exists(q', r') \in \mathbb{N}^2, \begin{cases} -a = -bq' + r' \\ 0 \leq r' < -b. \end{cases}$$

Donc,

$$\begin{aligned} a &= bq' - r' \\ &= b(q' + 1) - r' - b. \end{aligned}$$

En posant

$$\begin{aligned} q &= \begin{cases} q' & \text{si } r' = 0, \\ q' + 1 & \text{si } r' \neq 0; \end{cases} \\ r &= \begin{cases} r' & \text{si } r' = 0, \\ -r' - b & \text{si } r' \neq 0; \end{cases} \end{aligned}$$

on a bien

$$\begin{cases} a = bq + r \\ q \in \mathbb{Z} \\ 0 \leq r < |b|. \end{cases}$$

UNICITÉ Soient $(q', r') \in \mathbb{Z}^2$ tels que

$$\begin{cases} a = bq' + r' \\ 0 \leq r' < |b|. \end{cases}$$

Or, on sait que $a = bq + r$ et $0 \leq r < |b|$. D'où

$$\begin{cases} b(q' - q) = r' - r \\ -|b| < r - r' < |b| \end{cases}$$

donc $r - r' = 0$ et donc $q = q'$.

□

Définition: Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. D'après le théorème précédent, il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$\begin{cases} a = bq + r \\ 0 \leq r < |b|. \end{cases}$$

On dit que r est le quotient, et r le reste dans la division (euclidienne) de a par b .

EXEMPLE:

Soit $n \in \mathbb{N}$ impair. On divise n par 2 : soient $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que $\begin{cases} n = 2q + r \\ 0 \leq r < 2. \end{cases}$

Si $r = 0$, n est pair : une contradiction. Ainsi, $r \neq 0$ et donc $r = 1$. On a donc $n = 2q + 1$.

Proposition: Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. On note r le reste de la division euclidienne de a par b .

$$r = 0 \iff a \mid b.$$

Preuve:

On pose $a = bq + r$ avec $q \in \mathbb{Z}$.

“ \implies ” Si $r = 0$, alors $a = bq$ avec $q \in \mathbb{Z}$ et donc $b \mid a$.

“ \impliedby ” Si $b \mid a$, il existe $k \in \mathbb{Z}$ tel que $a = bk$. Donc, $a = bk + 0$ et $0 \leq 0 < |b|$. Par unicité de la division euclidienne, $r = 0$.

□

4 Arithmétique modulaire

Définition: Soient $a, b \in \mathbb{Z}$ et $c \in \mathbb{N}^*$. On dit que a est congrus à b modulo c si a et b ont le même reste dans la division euclidienne par c . Dans ce cas, on écrit $a \equiv b \pmod{c}$.

Proposition: La congruence modulo c est une relation d'équivalence.

□

REMARQUE (Notation):

On note \mathbb{Z}/cz l'ensemble des classes d'équivalences modulo c .

Par exemple, $\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$.

Proposition: Soient $a, b \in \mathbb{Z}$ et $c \in \mathbb{N}^*$.

$$a \equiv b \pmod{c} \iff c \mid (b - a).$$

Preuve: “ \implies ” Soient $q, q' \in \mathbb{Z}$ et $r \in \mathbb{N}$ tels que

$$\begin{cases} a = cq + r \\ b = cq' + r \end{cases}$$

avec $0 < r < c$. En soustrayant les égalités, on obtient

$$b - a = c \underbrace{(q' - q)}_{\in \mathbb{Z}}.$$

Ainsi, $c \mid (b - a)$.

“ \impliedby ” On pose $\begin{cases} a = cq + r \\ b = cq' + r' \end{cases}$ avec $(q, q') \in \mathbb{Z}$ et $\begin{cases} 0 \leq r < c \\ 0 \leq r' < c \end{cases}$. En soustrayant les égalités et inégalités, on obtient

$$\begin{cases} b - a = c(q' - q) + r' - r \\ -c < r' - r < c. \end{cases}$$

□

La suite du cours provient d'Aubin. Je ne suis pas responsable pour les éventuelles bêtises qu'il a pu taper.

5 Axiomatique de \mathbb{N}

Axiome (Axiomatique de Von Neumann): (\mathbb{N}, \leq) est un ensemble totalement ordonné vérifiant

- Toute partie non vide de \mathbb{N} a un plus petit élément
- Toute partie non vide majorée de \mathbb{N} a un plus grand élément
- \mathbb{N} n'est pas majoré

Définition (0): $0 = \min(\mathbb{N})$

Définition (1): $1 = \min(\mathbb{N} \setminus \{0\})$

Définition ($n+1$): Soit $n \in \mathbb{N}$
On pose $n+1 = \min(\{k \in \mathbb{N} \mid k > n\})$
On dit que $n+1$ est le successeur de n

Proposition (+1-1): $\forall n \in \mathbb{N}, (n+1)-1 = n$
 $\forall n \in \mathbb{N}, (n-1)+1 = n$

Preuve:

Soient $n \in \mathbb{N}$, $p = n+1$, $q = p-1$

$n < p$ et $q < p$
Donc $n \leq q$ car $q = \max(\{k \in \mathbb{N} \mid k < p\})$
Si $q > n$, alors $q \geq p$ car $p = \min(\{k \in \mathbb{N} \mid k > n\})$
Donc $q = n$

□

Proposition (Ensemble Ouvert Vide): $\forall n \in \mathbb{N},]n, n+1[= \emptyset$

Preuve:

Soit $n \in \mathbb{N}$, on sait que $n+1 > n$
Soit $p > n$, on suppose $n < p < n+1$
Comme $p > n$, $p \geq n+1$ Contradiction

□

Proposition (Théorème de Récurrence): Soit P un prédictat sur \mathbb{N} et $n \in \mathbb{N}$

Si $\begin{cases} P(n_0) \text{ est vrai} \\ \forall n \geq n_0, P(n) \implies P(n+1) \end{cases}$
 Alors $\forall n \geq n_0, P(n)$ est vrai

Preuve:

Soit $A = \{n \in \mathbb{N} \mid n \geq n_0\}$ et $P(n)$ faux

Supposons $A \neq \emptyset$

A a donc un plus petit élément, soit $N = \min(A)$

Cas 1 : $N = 0$

Alors, comme $N \in A$, on a $n_0 \leq 0$ et $P(0)$ est faux

Alors $n_0 = 0$ Contradiction avec “ $P(n)$ est vrai”

Cas 2 : $N \neq 0$

Alors $N - 1 \in \mathbb{N}$

$N - 1 \notin A$ car $N - 1 < N$

Donc $N - 1 < n_0$ ou $P(n)$ vrai

Supposons $N - 1 < n_0$

$N \in A$ donc $N \geq n_0$

$N - 1 < n_0 < N$

Donc $N = n_0$

Or, $N \in A$ donc $P(n)$ est faux alors que $P(n)$ est vrai

Supposons $\begin{cases} P(n-1) \text{ vrai} \\ N - 1 \geq n_0 \end{cases}$ Comme $N - 1 \geq n_0, P(N-1) \implies P(N)$

Donc $P(N)$ est vrai

Or, $N \in A$ donc $P(N)$ est faux

Donc $A = \emptyset$

□

6 Récurrences

Proposition (Récurrence Double): Soient P un prédictat sur \mathbb{N} et $n_0 \in \mathbb{N}$

Si $\begin{cases} P(n_0) \text{ est vrai} \\ P(n_0 + 1) \text{ est vrai} \\ \forall n > n_0, P(n) \text{ et } P(n+1) \implies P(n+2) \end{cases}$
 Alors $\forall n \geq n_0, P(n)$ est vrai

Preuve:

On pose $\forall n \in \mathbb{N}, Q(n) : "P(n) \text{ et } P(n+1) \text{ vrais}"$

$Q(n_0)$ est vrai

Soit $n \geq n_0$, on suppose $Q(n)$ vrai

On sait alors que $P(n+2)$ est vrai

On sait par hypothèse de récurrence que $P(n+1)$ est vrai
Donc $Q(n+1)$ est vrai

□

Proposition (Récurrence Multiple): Soient P un prédicat sur \mathbb{N} et $(p, n_0) \in \mathbb{N}^2$
Si $\begin{cases} \forall k \in \llbracket 0, p \rrbracket, P(n_0 - k) \text{ est vrai} \\ \forall n \geq n_0, (P(n) \text{ et } \dots \text{ } P(n+p-1)) \implies P(n+p) \end{cases}$
Alors $\forall n \geq n_0, P(n)$ est vrai

Proposition (Récurrence Forte): Soient P un prédicat sur \mathbb{N} et $n_0 \in \mathbb{N}$
Si $\begin{cases} P(n_0) \text{ est vrai} \\ \forall n \geq n_0, (P(n_0) \text{ et } \dots \text{ } P(n-1)) \implies P(n) \end{cases}$
Alors $\forall n \geq n_0, P(n)$ est vrai

Preuve:
On pose $\forall n \in N, Q(n) : \text{"}\forall k \in \llbracket n_0, n \rrbracket, P(k) \text{ vrai"}$
 $Q(n_0)$ est vrai car $P(n_0)$ est vrai

Soit $n \geq n_0$, on suppose $Q(n)$ vrai
On sait que $\forall k \in \llbracket n_0, n \rrbracket, P(k)$ est vrai
Alors $P(n+1)$ est vrai
Donc $\forall k \in \llbracket n_0, n+1 \rrbracket, P(k)$ est vrai
Donc $Q(n+1)$ est vrai

□

7 Divisibilité

Définition (Divisibilité): Soient $(a, b) \in \mathbb{Z}^2$
On dit que a divise b si il existe $k \in \mathbb{Z}$ tel que $b = ka$
On écrit $a|b$ et on dit que $\begin{cases} a \text{ est un diviseur de } b \\ b \text{ est un multiple de } a \end{cases}$

Proposition (Caractéristiques de la Divisibilité): $|$ est une relation d'ordre sur \mathbb{Z}
Ce n'est pas une relation totale

Proposition (Ordonnancement et Divisibilité): Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$
Si $a|b, |a| \leq |b|$

Proposition (Divisibilité et Combinaison Linéaire): Soient $(a, b, c) \in (\mathbb{Z}^*)^3$

$$\left| \begin{array}{l} \left\{ \begin{array}{l} a|b \\ a|c \end{array} \right. \implies \forall (k, l) \in \mathbb{Z}^2, a|(bk + cl) \end{array} \right.$$

Preuve:
 $\left\{ \begin{array}{l} b = au \text{ avec } u \in \mathbb{Z} \\ c = av \text{ avec } v \in \mathbb{Z} \end{array} \right.$

Soient $(k, l) \in \mathbb{Z}^2$

$$bk + cl = auk + avl = a(uk + vl)$$

Donc $a|(bk + cl)$

□

Définition (Nombres Associés): Soient $(a, b) \in \mathbb{Z}^2$

a et b sont associés si $a = b$ ou $a = -b$

Proposition (Nombres Associés et Divisibilité): Soient $(a, b) \in \mathbb{Z}^2$
 $a|b \iff -a|b \iff a|-b \iff -a|-b$

8 Division Euclidienne

Proposition (Division Euclidienne dans \mathbb{N}): Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$
 $\exists! (q, r) \in \mathbb{N}^2, \left\{ \begin{array}{l} a = bq + r \\ r \in [0, b[\end{array} \right.$

Preuve:

Existence : On considère $A = \{q \in \mathbb{N} | qb \leq a\}$ A est non vide car $0 \in A$
 A est majoré : $\forall q \in A, q \leq a$ car $a \geq qb \geq q$

Soit $q = \max(A)$, on pose $r = a - bq$

Comme a, b et $q \in \mathbb{N}, r \in \mathbb{Z}$

$q \in A$ donc $qb \leq a$ donc $r \geq 0$

$q + 1 > \max(A)$ donc $q + 1 \notin A$ donc $(q + 1)b > a$

Donc $r < b$

Unicité : Soit $(q', r') \in \mathbb{N}^2$ tel que $\left\{ \begin{array}{l} a + bq' + r' \\ 0 \leq r' < b \end{array} \right.$

On sait aussi que $a = bq + r$

Donc $0 = b(q' - q) + r' - r$

$$-r' + r = b(q' - q)$$

De plus, $\left\{ \begin{array}{l} 0 \leq r < b \\ -b < -r \leq 0 \end{array} \right.$
 Donc $-b < r' - r < b$

Le seul multiple de b dans $[-b, b[$ est 0

Donc $r' - r = 0$, donc $r = r'$
et $b(q' - q) = 0$
Or, $b \neq 0$ donc $q' - q = 0$ donc $q = q'$

□

Proposition (Division Euclidienne dans \mathbb{Z}): Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$

$$\exists!(q, r) \in \mathbb{Z}^2, \begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$$

Preuve:

Existence :

Cas 1 : $a \in \mathbb{N}, b \in \mathbb{N}^*$

D'après ce qui précède, $\exists!(q, r) \in \mathbb{N}^2, \begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$

Comme $b \in \mathbb{N}^*$, on a bien $0 \leq r < |b|$
 $q \in \mathbb{N} \subset \mathbb{Z}$

Cas 2 : $a \in \mathbb{Z}, b \in \mathbb{N}^*$

Comme $-a \in \mathbb{N}, \exists!(q', r') \in \mathbb{N}^2, \begin{cases} -a = bq' + r' \\ 0 \leq r' < b \end{cases}$

$$\begin{aligned} \text{Donc } a &= b(-q') - r' \\ &= b(-q' - 1) - r' + b \end{aligned}$$

On pose $q = \begin{cases} -q' - 1 & \text{si } r' \neq 0 \\ -q' & \text{si } r' = 0 \end{cases}$ et $r = \begin{cases} -r' + b & \text{si } r' \neq 0 \\ r' & \text{si } r' = 0 \end{cases}$

On a bien $\begin{cases} a = bq + r \\ q \in \mathbb{Z} \\ 0 \leq r < |b| \end{cases}$

Cas 3 : $a \in \mathbb{N}, b \in \mathbb{Z}_-^*$

$\exists!(q', r') \in \mathbb{N}^2, \begin{cases} a = (-b)q' + r' \\ 0 \leq r' < -b \end{cases}$

On pose $\begin{cases} q = -q' \\ r = r' \end{cases}$

Et on a bien $\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$

Cas 4 : $a \in \mathbb{Z}_-^*, b \in \mathbb{Z}_-^*$

$\exists!(q', r') \in \mathbb{N}^2, \begin{cases} -a = -bq' + r' \\ 0 \leq r' < -b \end{cases}$

$$\begin{aligned} \text{Donc } a &= bq' - r' \\ &= b(q' + 1) - r' - b \end{aligned}$$

On pose $q = \begin{cases} q' + 1 & \text{si } r' \neq 0 \\ q' & \text{si } r' = 0 \end{cases}$ et $r = \begin{cases} -r - b' & \text{si } r' \neq 0 \\ r' & \text{si } r' = 0 \end{cases}$

On a bien $\begin{cases} a = bq + r \\ q \in \mathbb{Z} \\ 0 \leq r < |b| \end{cases}$

Unicité :

Soit $(q', r') \in \mathbb{Z}^2$ tel que $\begin{cases} a = bq' + r' \\ 0 \leq r' < |b| \end{cases}$ et $\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$

D'où $\begin{cases} b(q' - q) = r' - r \\ -|b| < r - r' < |b| \end{cases}$
Donc $r - r' = 0$

Donc $r' = r$ et $q' = q$

□

Définition (Quotient et Reste): Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$

D'après le théorème précédent, $\exists!(q, r) \in \mathbb{Z} \times \mathbb{N}$, $\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$

On dit que q est le quotient et r le reste dans la division (euclidienne) de a par b

Proposition (Reste et Divisibilité): Soient $a \in \mathbb{Z}, b \in \mathbb{Z}^*$

On note r le reste de la division de a par b

$r = 0 \iff b|a$

Preuve:

On pose $a = bq + r, q \in \mathbb{Z}$

“ \implies ” : Si $r = 0$, alors $\begin{cases} a = bq \\ q \in \mathbb{Z} \end{cases}$ donc $b|a$

“ \impliedby ” : Si $b|a$, $\exists k \in \mathbb{Z}, a = bk$

Donc $\begin{cases} a = bk \\ 0 \leq 0 < |b| \end{cases}$

Par unicité du reste, $r = 0$

□

9 Arithmétique Modulaire

Définition (Congruences): Soient $(a, b) \in \mathbb{Z}^2, c \in \mathbb{N}^*$

On dit que a et b sont congrus modulo c si a et b ont le même reste dans ma division par c

On note $a = b[c]$

Proposition (Congruence et Relation D'Équivalence): La relation de congruence modulo c est une relation d'équivalence

REMARQUE (Classes d'Équivalence Modulo c):

On note $\mathbb{Z}/c\mathbb{Z}$ l'ensemble des classes d'équivalence modulo c
 $\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

Proposition (Modulo et Divisibilité): Soient $(a, b) \in \mathbb{Z}^2$ et $c \in \mathbb{N}^*$

$$a \equiv b[c] \iff c|b - a$$

Preuve:

$$\begin{aligned} \text{“}\Rightarrow\text{” : On pose } & \begin{cases} a = cq + r, q \in \mathbb{Z}, 0 \leq r < c \\ b = cq' + r, q' \in \mathbb{Z} \end{cases} \\ \text{Donc } b - a &= c(q' - q) \end{aligned}$$

Donc $c|b - a$

$$\begin{aligned} \text{“}\Leftarrow\text{” : On pose } & \begin{cases} a = cq + r, q \in \mathbb{Z}, 0 \leq r < c \\ b = cq' + r', q' \in \mathbb{Z}, 0 \leq r' < c \end{cases} \\ b - a &= c(q' - q) + r' - r \\ -c &\leq r' - r \leq c \end{aligned}$$

Si $r' - r \geq 0$, $r' - r$ est le reste de la division de $a - b$ par c
Donc $r' = r$ donc $a \equiv b[c]$

Si $r' - r < 0$, $r - r'$ est le reste de la division de $a - b$ par c
Donc $r' = r$ donc $a \equiv b[c]$

□

Proposition (Addition et Multiplication de Congruences): Soient $(a, b, x, y) \in \mathbb{Z}^4$ et $c \in \mathbb{N}^*$

$$\text{On suppose } \begin{cases} a \equiv b[c] \\ x \equiv y[c] \end{cases}$$

$$\text{Alors } \begin{cases} a + x \equiv b + y[c] \\ ax \equiv by[c] \end{cases}$$

Preuve:

$$\begin{aligned} c|b - a \text{ et } c|y - x \\ \text{Donc } c|(b - a + y - x) \\ \text{Donc } c|(b + y - (a + x)) \\ \text{Donc } a + x \equiv b + y[c] \end{aligned}$$

$$\begin{aligned} \text{On pose } & \begin{cases} a = ck + b, k \in \mathbb{Z} \\ x = cl + y, l \in \mathbb{Z} \end{cases} \\ ax &= (ck + b)(cl + y) \\ &= by + cky + clk + c^2kl \\ &= by + c(ky + bl + clk) \\ \text{Donc } ax &\equiv by[c] \end{aligned}$$

□

Proposition (Critères de Divisibilité en Base 10): Soit $N \in \mathbb{N}$, on notera ses chiffres

$$N = \sum_{k=0}^{a_0 \dots a_n} 10^k a_k$$

Divisibilité par 2 :

$$N \text{ pair} \iff N \equiv 0[2]$$

$$\iff \sum_{k=0}^n 10^k a_k \equiv 0[2]$$

$$\iff a_0 \equiv 0[2] \text{ car } \forall k \geq 1, 10^k \equiv 0[2]$$

$$10^0 = 1 \equiv 1[2]$$

Divisibilité par 3 :

$$\forall k \in \mathbb{N}, 10^k \equiv 1^k \equiv 1[3] \text{ car } 10 \equiv 1[3]$$

$$3|N \iff N \equiv 0[3]$$

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

Divisibilité par 9 :

$$\forall k \in \mathbb{N}, 10^k \equiv 1[9]$$

$$9|N \iff N \equiv 0[9]$$

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

Divisibilité par 5 :

$$\begin{cases} 10^0 \equiv 1[5] \\ \forall k \in \mathbb{N}^*, 10^k \equiv 0[5] \end{cases}$$

$$5|N \iff a_0 \equiv 0[5]$$

$$\iff a_0 \in \{0, 5\}$$

Divisibilité par 11 :

$$10^0 \equiv -1[11]$$

$$\text{Donc } \forall k \in \mathbb{N}, 10^k \equiv (-1)^k[11]$$

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

$$\iff a_0 - a_1 + a_2 \dots + (-1)^n a_n \equiv 0[11]$$

REMARQUE (Réécriture en Classes d'Équivalence):

On peut réécrire le calcul précédent dans $\mathbb{Z}/11\mathbb{Z}$

$$\overline{N} = \sum_{k=0}^n \overline{10^k a_k} = \sum_{k=0}^n \overline{10^k} \overline{a_k} = \sum_{k=0}^n \overline{(-1)^k} \overline{a_k}$$

REMARQUE (Opération dans $\mathbb{Z}/n\mathbb{Z}$):

$$\text{Dans } \mathbb{Z}/n\mathbb{Z}, \text{ on dispose } \begin{cases} \text{d'une addition : } & \overline{a} + \overline{b} = \overline{a+b} \\ \text{d'une multiplication : } & \overline{a} * \overline{b} = \overline{a*b} \end{cases}$$

L'addition est commutative, associative, n'élément neutre $\bar{0}$ et l'opposé de \bar{a} est $\overline{-a}$

La multiplication est commutative, associative, d'élément neutre $\bar{1}$ et distributive par rapport à $+$

10 PCGD et PPCM

Définition (PGCD): Soient $(a, b) \in \mathbb{Z}^2$

Le PGCD de a et b est le plus grand diviseur commun à a et b
Il existe car $\mathcal{D} = \{d \in \mathbb{N} | d|a \text{ et } d|b\}$ est non vide car $a \in \mathcal{D}$
 \mathcal{D} est majoré par $|a|$
On le note $\text{PGCD}(a, b)$ ou $a \wedge b$

Proposition (Théorème d'Euclide): Soient $a \in \mathbb{Z}, b \in \mathbb{N}^*$
Soit r le reste de la division de a par b
 $a \wedge b = b \wedge r$

Preuve:

On pose $\begin{cases} d = a \wedge b \\ \varsigma = b \wedge r \\ a = bq + r \end{cases}$

$$\begin{cases} d|a \\ d|b \end{cases} \implies \begin{cases} d|a - bq \\ d|b \end{cases} \implies \begin{cases} d|r \\ d|b \end{cases} \implies d \leq \varsigma$$

$$\begin{cases} \varsigma|b \\ \varsigma|r \end{cases} \implies \begin{cases} \varsigma|bq + r \\ \varsigma|r \end{cases} \implies \begin{cases} \varsigma|a \\ \varsigma|r \end{cases} \implies \varsigma \leq d$$

Donc $d = \varsigma$

□

Proposition (PGCD et Diviseurs): Soient $(a, b) \in \mathbb{Z}^2$ et $d = a \wedge b$
 $\mathcal{D} = \{k \in \mathbb{Z} | k|a, k|b\}$
 $\forall k \in \mathbb{Z}, k \in \mathcal{D} \iff k|d$

Preuve:

“ \Leftarrow ” : Soit $k \in \mathbb{Z}$, on suppose $k|d$
 $d|a$ donc $k|a$
 $d|b$ donc $k|b$

Donc $k \in \mathcal{D}$

“ \Rightarrow ” : Soit $k \in \mathcal{D}$
On pose r_0 le reste de la division de a par b ,
 r_1 le reste de la division de b par r_0
et $\forall n \in \mathbb{N}, r_{n+1}$ le reste de la division de r_{n-1} par r_n si $r_n \neq 0$

La suite (r_n) est décroissante, minorée par 0 et à valeurs entières
Soit $N \in \mathbb{N}$ tel que $r_N = 0$ (si $N = 0$, on pose $r_{-1} = b$)

D'après la proposition précédente,
 $d = a \wedge b = b \wedge r_0 = r_0 \wedge r_1 \dots r_{N-1} \wedge r_N$
 $= r_{N-1} \wedge 0 = r_N$

On pose aussi $\forall n \in \llbracket 1, N-1 \rrbracket$, $r_{n-1} = r_n q_n + r_{n+1}$
 On en déduit que $\exists (\alpha_n, \beta_n) \in \mathbb{Z}^2$, $r_{N-1} = a\alpha_N + b\beta_N$

$$\begin{cases} k|a \\ k|b \end{cases} \implies k|a\alpha_N + b\beta_N \implies k|r_{N-1} \implies k|d$$

□

Définition (PPCM): Soit $(a, b) \in \mathbb{Z}^2$, on pose $M = \{k \in \mathbb{N} \mid a|k, b|k\}$
 $M \neq \emptyset$ car $ab \in M$

$M \neq \emptyset$ donc admet un plus petit élément noté $\text{PPCM}(a, b)$ ou $a \vee b$

Proposition (Produit PGCD PPCM): $\forall (a, b) \in \mathbb{Z}^2, (a \wedge b)(a \vee b) = ab$

Preuve:

Voir paragraphe Facteurs Premiers

□

Proposition (Propriétés de \wedge et \vee): \wedge est commutative, associative sur \mathbb{Z}^*
 \vee est commutative, associative sur \mathbb{Z}^*

Preuve:

Soient $(a, b, c) \in (\mathbb{Z}^*)^3$, $d = (a \wedge b) \wedge c$, $\varsigma = a \wedge (b \wedge c)$

$$\begin{cases} d|c \\ d|a \wedge b \end{cases} \implies \begin{cases} d|c \\ d|a \\ d|b \end{cases}$$

$$\begin{cases} \varsigma|a \\ \varsigma|b \wedge c \end{cases} \implies \begin{cases} \varsigma|a \\ \varsigma|b \\ \varsigma|c \end{cases}$$

On pose $\varepsilon = \text{PGCD}(a, b, c)$

$$\text{On a } \begin{cases} d \leq \varepsilon \\ \varsigma \leq \varepsilon \end{cases}$$

$$\begin{cases} \varepsilon|a \\ \varepsilon|b \\ \varepsilon|c \end{cases} \implies \begin{cases} \varepsilon|a \\ \varepsilon|b \\ \varepsilon|b \wedge c \end{cases} \implies \varepsilon|a \wedge (b \wedge c) \implies \varepsilon \leq d$$

De même, on $\varepsilon \leq \varsigma$

Donc $d = \varepsilon = \varsigma$

□

Proposition (Théorème de Bézout): Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, $d = a \wedge b$
 $\exists (u, v) \in \mathbb{Z}^2, d = au + bv$

Preuve:

On pose $A = \{au + bv | (u, v) \in \mathbb{Z}^2\}$

On veut montrer que $d \in A$

$a = a * 1 + b * 0$ donc $a \in A$

$b = a * 0 + b * 1$ donc $b \in A$

$0 = a * 0 + b * 0$ donc $0 \in A$

Soit $(x, y) \in A^2$

$x = au_1 + bv_1, (u_1, v_1) \in \mathbb{Z}^2$

$y = au_2 + bv_2, (u_2, v_2) \in \mathbb{Z}^2$

$x + y = a(u_1 + u_2) + b(v_1 + v_2) \in A$

Soit $x \in A, k \in \mathbb{Z}$

$x = au + bv, (u, v) \in \mathbb{Z}^2$

$kx = akau + bkv \in A$

Soit $n = \min(A \cap \mathbb{N}^*)$ ($|b| \in A \cap \mathbb{N}^*$)

Soit $x \in A$

Par division euclidienne de x par n :

$$\begin{cases} x = nq + r \\ q \in A, 0 \leq r < n \end{cases}$$

$$\begin{cases} x \in A \\ n \in A \end{cases} \implies \begin{cases} x \in A \\ -qn \in A \end{cases} \implies x - qn \in A \implies r \in A$$

$$\begin{cases} r < n \\ r \in A \end{cases} \implies r \leq 0$$

Donc $r = 0$

Donc $n|x$

D'où $A = n\mathbb{Z}$

$$\text{Or, } \begin{cases} a \in A \\ b \in A \end{cases} \implies \begin{cases} n|a \\ n|b \end{cases}$$

Cas particulier : $a \wedge b = d = 1$, alors 1 est le seul diviseur positif de a et b

Donc $n = 1$ donc $A = \mathbb{Z}$ donc $1 \in \mathbb{Z}$

Cas général : On pose $a' = \frac{a}{d} \in \mathbb{Z}$, $b' = \frac{b}{d} \in \mathbb{Z}$, $a' \wedge b' = 1$

D'après le cas particulier, $\exists (u, v) \in \mathbb{Z}^2, a'u + b'v = 1$

D'où $au + bv = d$

□

Proposition (Réciproque du Théorème de Bézout): Soient $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$
 On suppose qu'il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$

Alors $a \wedge b = 1$

Preuve:

On pose $d = a \wedge b$

$$\begin{cases} d|a \\ d|b \end{cases} \implies d|au + bv \implies d|1 \implies d = 1$$

□

Proposition (Théorème de Gauß): Soient $(a, b, c) \in \mathbb{Z}^3$ tels que $\begin{cases} a \wedge b = 1 \\ a|bc \end{cases}$

Alors $a|c$

Preuve:

D'après le théorème de Bézout,

$au + bv = 1$ avec $(u, v) \in \mathbb{Z}^2$

D'où $acu + bcv = c$

$$\begin{cases} a|acu \\ a|bcv \end{cases}$$

Donc $a|acu + bcv$

Donc $a|c$

□

REMARQUE (Inversion Modulo n):

Soit $x \in \mathbb{Z}$

$\exists y \in \mathbb{Z}, xy \equiv 1[n]$

(\iff dans $\mathbb{Z}/n\mathbb{Z}$, $\bar{x} + \bar{y} = \bar{1}$)

Avec $n = 4$:

x 0123

0 0000

1 0123 $\begin{cases} 1 \text{ et } 3 \text{ sont inversibles modulo 4} \\ 2 \text{ n'est pas inversible modulo 4} \end{cases}$

2 0202

3 0321

$$3x \equiv 2[4]$$

$$\iff 3 * 3x \equiv 3 * 2[4]$$

$$\iff x \equiv 2[4]$$

$$2x \equiv 1[4]$$

$$\implies 2 * 2x \equiv 2[4]$$

$$\implies 0 \equiv 2[4]$$

Proposition (Congruences et Nombres Premiers): Soit p un nombre premier

Alors $\forall x \in \mathbb{Z}, x \not\equiv 0[p] \implies \exists y \in \mathbb{Z}, xy \equiv 1[p]$

Preuve:

Soit $x \in \mathbb{Z}$ tel que $x \not\equiv 0[p]$

Soit $y \in \mathbb{Z}$

$$\begin{aligned} xy \equiv 1[p] &\iff \exists u \in \mathbb{Z}, xy = 1 + pu \\ &\iff \exists u \in \mathbb{Z}, xy - pu = 1 \end{aligned}$$

$$\begin{aligned} y \text{ existe} &\iff x \wedge p = 1 \\ &\iff p \nmid x \end{aligned}$$

□

Proposition (Inversibilité Modulo n): Soit $n \in \mathbb{N}^*, x \in \mathbb{Z}$
 x inversible modulo $n \iff x \wedge n = 1$

Preuve:

Voir précédent

□

Proposition (Petit Théorème de Fermat): Soit p premier, $a \in \mathbb{Z}$
 $a^p \equiv a[p]$

Preuve:

Cas 1 : $a \equiv 0[p]$

$a^p \equiv 0^p[p]$

$a^p \equiv 0[p] \equiv a[p]$

Cas 2 : $a \not\equiv 0[p]$

Alors $a \wedge p = 1$

On pose $\forall i \in \mathbb{N}^*, r_i$ le reste de la division de ia par p

Soit $i \in [1, p-1]$

$r_i = 0 \implies p|ia \implies p|i$ Contradiction

$\forall i \in \mathbb{N}^*, r_i \neq 0$

Soit $(i, j) \in [1, p-1]^2, i \neq j$

On suppose $r_i = r_j$, alors $ia \equiv ja[p]$

Or, $a \wedge p = 1$ donc a est inversible modulo p

Donc $a \equiv j[p]$ donc $i = j$ Contradiction

Ainsi, $r_1 \dots r_{p-1} \in [1, p-1]$ distincts donc ils prennent toutes les valeurs de $[1, p-1]$

$i \mapsto r_i$ est injective

$\{r_1 \dots r_{p-1}\} = [1, p-1]$

$$\text{Donc } \prod_{k=1}^{p-1} r_i = (p-1)!$$

$$\begin{aligned} \text{Donc } \prod_{k=1}^{p-1} ia &\equiv (p-1)![p] \\ \text{Donc } (p-1)!a^{p-1} &\equiv (p-1)![p] \end{aligned}$$

D'où $(p-1)! \equiv 0[p] \iff p|1 * 2 * 3 * \dots * (p-1)$
 $\iff \exists i \in \llbracket 1, p-1 \rrbracket, p|i$
 Donc $(p-1)! \not\equiv 0[p]$
 Donc $(p-1)!$ est inversible modulo p
 Donc $a^p \equiv 1[p]$
 Donc $a^p \equiv a[p]$

□

11 Décomposition en Facteurs Premiers

Définition (Nombre Premier): Soit $n \in \mathbb{N}$

On dit que n est premier si

$n \geq 2$

les seuls diviseurs entiers de n sont 1 et n

Proposition (Infinité de Nombres Premiers): Il y a une infinité de nombres premiers

Preuve:

On suppose qu'il n'y a qu'un nombre fini de nombres premiers
 $p_1 < \dots < p_n$

On pose $N = p_n * \dots * p_1 + 1$
 $N > p_n$ donc N n'est pas premier
 N a d'autres diviseurs positifs que 1 et N
 N est divisible par un nombre entre 2 et $N - 1$

Soit $p = \min(\{k \in \llbracket 2, N-1 \rrbracket \mid k|N\})$
 p est premier (Tout diviseur de p divise aussi N)
 $\exists i \in \llbracket 1, n \rrbracket, p_i = p$
 $p_i|N$
 $p_i|N - p_1 \dots p_n$
 $p_i|1$ Contradiction

Donc il y a une infinité de nombres premiers

□

Proposition (Théorème Fondamental de l'Arithmétique): "Tout entier se décompose en un unique produit de nombres premiers"

Soient $n \in \mathbb{N}$ tel que $n \geq 2$ et \mathcal{P} l'ensemble des nombres premiers

$$\left| \begin{array}{l} \exists! \nu : \mathcal{P} \longrightarrow \mathbb{N} \text{ telle que } \left\{ \begin{array}{l} \{p \in \mathcal{P} | \nu(p) \neq 0\} \text{ est fini} \\ n = \prod_{p \in \mathcal{P}} p^{\nu(p)} \end{array} \right. \end{array} \right.$$

Preuve:

Existence : Déjà vue : Récurrence Forte (Chapitre 9)

Unicité : Soit $n \geq 2$ et $\nu : \mathcal{P} \longrightarrow \mathbb{N}$ telle que

$$(*) \prod_{p \in \mathcal{P}} p^{\mu(p)} = \prod_{p \in \mathcal{P}} p^{\nu(p)} \text{ avec } \left\{ \begin{array}{l} \mu \neq \nu \\ M = \{p \in \mathcal{P} | \mu(p) \neq 0\} \text{ fini} \\ M = \{p \in \mathcal{P} | \nu(p) \neq 0\} \text{ fini} \\ n \text{ minimale pour cette propriété} \end{array} \right.$$

Soit $p \in M, \mu(p) \neq 0$ donc $p|n$

Si $\nu(p) = 0, \forall q \in \mathbb{N}, p \wedge q = 1$ donc $p|1$ Contradiction avec le théorème de Gauß

Donc on peut simplifier $(*)$ par $\frac{p}{n}$

On a alors 2 décompositions de $\frac{n}{p} < n$ Contradiction

Donc n n'existe pas

□

Proposition (Divisibilité et Nombres Premiers): Soient $(a, b, c) \in \mathbb{N}^3$ supérieurs à 2

$$\text{On pose } a = \prod_{p \in \mathcal{P}} p^{\alpha(p)} \text{ et } b = \prod_{p \in \mathcal{P}} p^{\beta(p)}$$

$$a|b \iff \forall p \in \mathcal{P}, \alpha(p) \leq \beta(p)$$

Preuve:

“ \implies ” : On suppose $a|b, \exists k, b = ak$

$$\text{On pose } k = \prod_{p \in \mathcal{P}} p^{\kappa(p)}$$

$$\text{et donc } b = \prod_{p \in \mathcal{P}} p^{\alpha(p)} \prod_{p \in \mathcal{P}} p^{\kappa(p)} = \prod_{p \in \mathcal{P}} p^{\alpha(p)+\kappa(p)}$$

Par unicité de la décomposition en facteurs premiers,
 $\forall p \in \mathcal{P}, \beta(p) = \alpha(p) + \kappa(p) \geq \alpha(p)$

“ \impliedby ” : On suppose $\forall p \in \mathcal{P}, \beta(p) \geq \alpha(p)$

On pose $\forall p \in \mathcal{P}, \kappa(p) = \beta(p) - \alpha(p) \in \mathbb{N}$

Tous les $\alpha(p)$ et $\beta(p)$ sont nuls à partir d'un certain rang
C'est donc le cas aussi pour les $\kappa(p)$

Donc on a le droit de former le produit

$$\prod_{p \in \mathcal{P}} p^{\kappa(p)} \in \mathbb{N}$$

$$\text{On pose } k = \prod_{p \in \mathcal{P}} p^{\kappa(p)} \text{ et } ak = \prod_{p \in \mathcal{P}} p^{\alpha(p)} \prod_{p \in \mathcal{P}} p^{\kappa(p)} = \prod_{p \in \mathcal{P}} p^{\alpha(p)+\kappa(p)} = \prod_{p \in \mathcal{P}} p^{\beta(p)} = b$$

□

Proposition (Produit de Facteurs Premiers, PGCD et PPCM): Avec les notations précédentes,

$$a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(\alpha(p), \beta(p))} \text{ et } a \vee b = \prod_{p \in \mathcal{P}} p^{\max(\alpha(p), \beta(p))}$$

Corollaire: $(a \wedge b)(a \vee b) = ab$

Preuve:

$$\begin{aligned} (a \wedge b)(a \vee b) &= \prod_{p \in \mathcal{P}} p^{\min(\alpha(p), \beta(p))} \prod_{p \in \mathcal{P}} p^{\max(\alpha(p), \beta(p))} \\ &= \prod_{p \in \mathcal{P}} p^{\min(\alpha(p), \beta(p)) + \max(\alpha(p), \beta(p))} \\ &= \prod_{p \in \mathcal{P}} p^{\alpha(p) + \beta(p)} = ab \end{aligned}$$

□

CHAPITRE

11

SUITES NUMÉRIQUES

1 Modes de définition

Définition: Une suite peut être définie

- Explicitement On dispose pour tout $n \in \mathbb{N}$ de l'expression de u_n en fonction de n .

[ex] $\forall n \in \mathbb{N}_*, u_n = \frac{\ln(n)}{n} e^{-n}$

- Par récurrence On connaît u_{n+1} en fonction de u_0, u_1, \dots, u_n

[ex] $\begin{cases} u_0 = 1 \\ \forall n \in \mathbb{N}, u_{n+1} = \sin(u_n) \end{cases}$

- Implicitement $\forall n \in \mathbb{N}, u_n$ est le seul nombre vérifiant une certaine propriété

[ex] u_n est le seul réel vérifiant $x^5 + nx - 1 = 0$

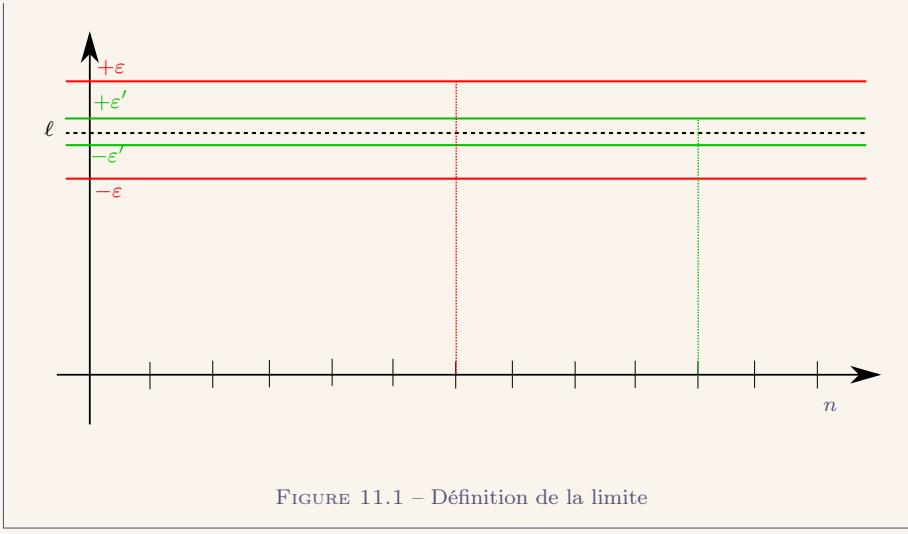
2 Limites

Définition: Soit u une suite réelle et $\ell \in \mathbb{R}$. On dit que

- u converge vers ℓ
- u_n tends vers ℓ quand n tends vers $+\infty$
- ℓ est une limite de u

si

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, |u_n - \ell| \leq \varepsilon$$
$$(\ell - \varepsilon \leq u_n \leq \ell + \varepsilon)$$



EXEMPLE:

Montrer que $\left(\frac{1}{n}\right)_{n \in \mathbb{N}}$ converge vers 0.

Soit $\varepsilon > 0$ quelconque. On cherche $N \in \mathbb{N}$ tel que

$$\forall n \geq N, -\varepsilon \leq \frac{1}{n} \leq \varepsilon$$

Analyse Soit $N \in \mathbb{N}^*$ tel que $\forall n \geq N, -\varepsilon \leq \frac{1}{n} \leq \varepsilon$.

En particulier, $\frac{1}{N} \leq \varepsilon$ donc $N \geq \frac{1}{\varepsilon}$.

Synthèse On pose $N = \left\lfloor \frac{1}{\varepsilon} \right\rfloor + 1 \in \mathbb{N}^*$ et $N > \frac{1}{\varepsilon}$. Soit $n \geq N$.

$$\frac{1}{n} > 0 > -\varepsilon \text{ donc } \frac{1}{n} \geq -\varepsilon$$

$$n \geq N > \frac{1}{\varepsilon} \text{ donc } n \geq \frac{1}{\varepsilon} \iff \frac{1}{n} \leq \varepsilon$$

Définition: Soit u une suite réelle.

On dit que u tends vers $+\infty$ si

$$\forall M \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \geq N, u_n \geq M$$

On dit que u tends vers $-\infty$ si

$$\forall m \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \geq N, u_n \leq m$$

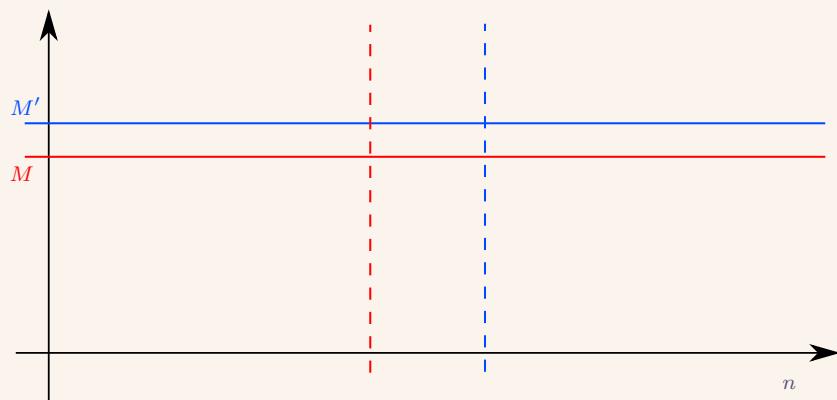


FIGURE 11.2 – Limites infinies

EXEMPLE:

Montrons que $n^2 \xrightarrow[n \rightarrow +\infty]{} +\infty$.Soit $M \in \mathbb{R}$, on cherche $N \in \mathbb{N}$ tel que $\forall n \geq N, n^2 \geq M$.Analyse Soit $N \in \mathbb{N}$ tel que $\forall n \geq N, n^2 \geq M$.En particulier, $N^2 \geq M$ et donc $N \geq \sqrt{M}$ si $M \geq 0$ Synthèse On pose $N = \begin{cases} 0 & \text{si } M \leq 0 \\ \lfloor \sqrt{M} \rfloor + 1 & \text{sinon} \end{cases}$ Ainsi $N \in \mathbb{N}$ et $N^2 \geq M$. Soit $n \geq N$. On a $n^2 \geq N^2 \geq M$.

Définition: Une suite qui ne converge pas est dite divergente (on dit qu'elle diverge). C'est le cas si cette suite n'a pas de limite quand elle tends vers $\pm\infty$.

Théorème (Unicité de la limite (réelle)): Soit $u \in \mathbb{R}^{\mathbb{N}}$, $(\ell_1, \ell_2) \in \overline{\mathbb{R}}^2$

Si $\begin{cases} u_n \xrightarrow[n \rightarrow +\infty]{} \ell_1 \\ u_n \xrightarrow[n \rightarrow +\infty]{} \ell_2 \end{cases}$ alors $\ell_1 = \ell_2$

Preuve: **Cas 1** $(\ell_1, \ell_2) \in \mathbb{R}^2$.

On suppose $\begin{cases} \ell_1 \neq \ell_2 \\ u_n \rightarrow \ell_1 \\ u_n \rightarrow \ell_2 \end{cases}$

Sans perte de généralité, on peut supposer $\ell_1 < \ell_2$

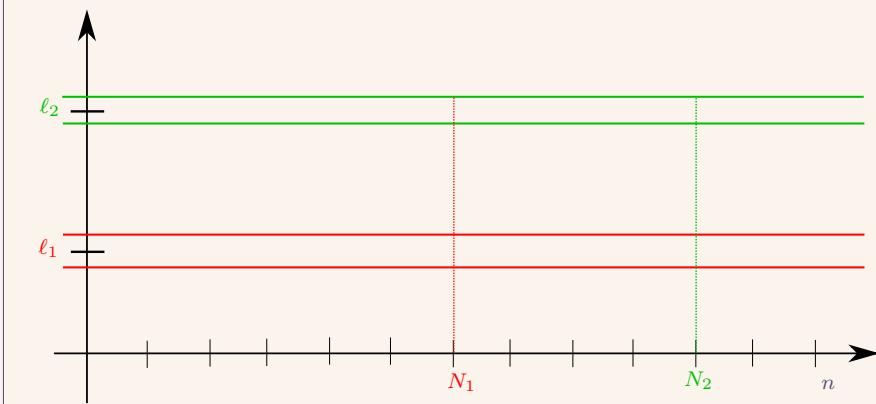


FIGURE 11.3 – Preuve unicité de la limite (cas 1)

On pose $\varepsilon = \frac{\ell_2 - \ell_1}{3} > 0$. On sait qu'il existe $N_1 \in \mathbb{N}$ tel que

$$\forall n \geq N_1, \ell_1 - \varepsilon \leq u_n \leq \ell_1 + \varepsilon$$

et il existe $N_2 \in \mathbb{N}$ tel que

$$\forall n \geq N_2, \ell_2 - \varepsilon \leq u_n \leq \ell_2 + \varepsilon$$

On pose $N = \max(N_1, N_2)$. On a alors

$$u_n \leq \ell_1 + \varepsilon < \ell_2 + \varepsilon \leq u_n$$

une contradiction ($u_n < u_n$). En effet,

$$\begin{aligned} \ell_1 + \varepsilon < \ell_2 + \varepsilon &\iff 2\varepsilon < \ell_2 - \ell_1 \\ &\iff \frac{2}{3}(\ell_2 - \ell_1) < \ell_2 - \ell_1 \\ &\iff \frac{2}{3} < 1 \end{aligned}$$

Ainsi $\ell_1 = \ell_2$

Cas 2 $\ell_1 \in \mathbb{R}, \ell_2 = +\infty$

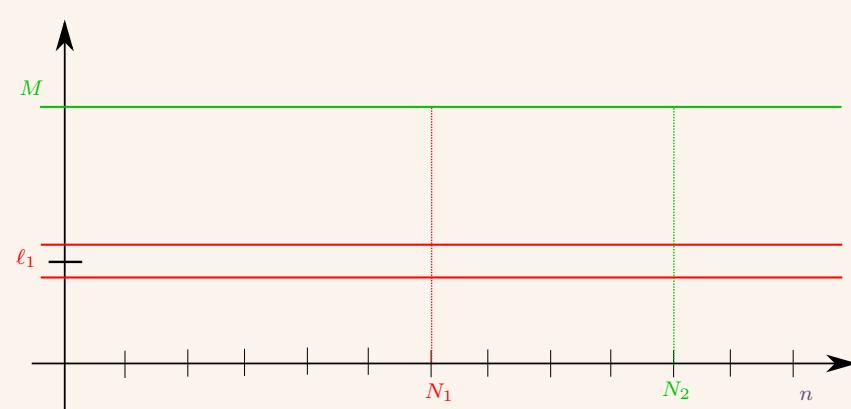


FIGURE 11.4 – Preuve unicité de la limite (cas 2)

$u_n \rightarrow \ell_1$ donc il existe $N_1 \in \mathbb{N}$ tel que

$$\forall n \geq N_1, \ell_1 - 1 \leq u_n \leq \ell_1 + 1$$

$u_n \rightarrow +\infty$ donc il existe $N_2 \in \mathbb{N}$ tel que

$$\forall n \geq N_2, u_n \geq \ell_1 + 2$$

On pose $N = \max(N_1, N_2)$. Ainsi

$$u_n \geq \ell_1 + 2 > \ell_1 + 1 \geq u_n$$

une contradiction

De la même manière, on peut prouver pour $(\mathbb{R}, -\infty)$ et $(+\infty, -\infty)$

□

REMARQUE:

Si u_n tends vers ℓ quand n tends vers $+\infty$, on écrit $u_n \xrightarrow{n \rightarrow +\infty} \ell$ ou $\lim_{n \rightarrow +\infty} u_n = \ell$ ou $\lim u_n = \ell$

Proposition: Toute suite convergente est bornée

Preuve:

On pose $\ell = \lim u_n \in \mathbb{R}$. Il existe $N \in \mathbb{N}$ tel que

$$\forall n \geq N, \ell - 1 \leq u_n \leq \ell + 1$$

L'ensemble $\{u_n \mid n \leq N\}$ est fini, il a donc un plus grand élément et un plus petit élément. On pose

$$\begin{cases} M_1 = \max\{u_n \mid n \leq N\} \\ m_1 = \min\{u_n \mid n \leq N\} \end{cases}$$

et

$$\begin{cases} M = \max(\ell_1 + 1, M_1) \\ m = \min(\ell_1 - 1, m_1) \end{cases}$$

Ainsi,

$$\forall n \in \mathbb{N}, \begin{cases} m \leq m_1 \leq u_n \leq M_1 \leq M & \text{si } n \leq N \\ m \leq \ell_1 - 1 \leq u_n \leq \ell_1 + 1 \leq M & \text{si } n > N \end{cases}$$

Donc

$$\forall n \in \mathbb{N}, m \leq u_n \leq M$$

□

Proposition: Soient $u \in \mathbb{R}^{\mathbb{N}}$ et $v \in \mathbb{R}^{\mathbb{N}}$. On pose $\ell_1 = \lim u_n$ et $\ell_2 = \lim v_n$

1. si $\ell_1 \in \mathbb{R}$ et $\ell_2 \in \mathbb{R}$ alors $u_n + v_n \rightarrow \ell_1 + \ell_2$
2. si $\ell_1 \in \mathbb{R}$ et $\ell_2 = +\infty$ alors $u_n + v_n \rightarrow +\infty$
3. si $\ell_1 \in \mathbb{R}$ et $\ell_2 = -\infty$ alors $u_n + v_n \rightarrow -\infty$
4. si $\ell_1 = \ell_2 = +\infty$, alors $u_n + v_n \rightarrow +\infty$
5. si $\ell_1 = \ell_2 = -\infty$, alors $u_n + v_n \rightarrow -\infty$

Preuve: 1. On suppose $(\ell_1, \ell_2) \in \mathbb{R}^2$, on pose $\ell = \ell_1 + \ell_2$.

Soit $\varepsilon > 0$ quelconque. On cherche $N \in \mathbb{N}$ tel que

$$\forall n \geq N, \ell - \varepsilon \leq u_n + v_n \leq \ell + \varepsilon$$

$\frac{\varepsilon}{2} > 0$ donc il existe $N_1 \in \mathbb{N}$ tel que

$$\forall n \geq N_1, \ell_1 - \frac{\varepsilon}{2} \leq u_n \leq \ell_1 + \frac{\varepsilon}{2}$$

Il existe $N_2 \in \mathbb{N}$ tel que

$$\forall n \geq N_2, \ell_2 - \frac{\varepsilon}{2} \leq v_n \leq \ell_2 + \frac{\varepsilon}{2}$$

On pose $N = \max(N_1, N_2)$. Soit $n \geq N$ quelconque.

$$n \geq N \geq N_1 \text{ donc } \ell_1 - \frac{\varepsilon}{2} \leq u_n \leq \ell_1 + \frac{\varepsilon}{2}$$

$$n \geq N \geq N_2 \text{ donc } \ell_2 - \frac{\varepsilon}{2} \leq v_n \leq \ell_2 + \frac{\varepsilon}{2}$$

D'où, en additionnant les inégalités

$$\ell - \varepsilon = \ell_1 + \ell_2 - \varepsilon \leq u_n + v_n \leq \ell_1 + \ell_2 + \varepsilon = \ell + \varepsilon$$

2. On suppose $\ell_1 \in \mathbb{R}$ et $\ell_2 = +\infty$. Soit $M \in \mathbb{R}$ quelconque.

Il existe $N_1 \in \mathbb{N}$ tel que

$$\forall n \geq N_1, \ell_1 - 1 \leq u_n \leq \ell_1 + 1$$

et il existe $N_2 \in \mathbb{N}$ tel que

$$\forall n \geq N_2, v_n \geq M - \ell_1 + 1$$

On pose $N = \max(N_1, N_2)$. Soit $n \geq N$ quelconque

$$\begin{cases} n \geq N_1 \text{ donc } u_n \geq \ell_1 - 1 \\ n \geq N_2 \text{ donc } v_n \geq M - \ell_1 + 1 \end{cases}$$

D'où, $u_n + v_n \geq M$

□

Proposition: Soient u et v deux suites réelles. On pose $\ell_1 = \lim u_n$ et $\ell_2 = \lim v_n$

1. si $\ell_1 \in \mathbb{R}$ et $\ell_2 \in \mathbb{R}$, alors $u_n v_n \rightarrow \ell_1 \ell_2$
2. si $\begin{cases} \ell_1 \in \mathbb{R}_*, \ell_2 = +\infty \text{ alors } u_n v_n \rightarrow +\infty \\ \ell_1 \in \mathbb{R}_*, \ell_2 = -\infty \text{ alors } u_n v_n \rightarrow -\infty \end{cases}$
3. si $\begin{cases} \ell_1 \in \mathbb{R}_*, \ell_2 = -\infty \text{ alors } u_n v_n \rightarrow -\infty \\ \ell_1 \in \mathbb{R}_*, \ell_2 = +\infty \text{ alors } u_n v_n \rightarrow +\infty \end{cases}$
4. si $\begin{cases} \ell_1 = -\infty, \ell_2 = +\infty \text{ alors } u_n v_n \rightarrow -\infty \\ \ell_1 = -\infty, \ell_2 = -\infty \text{ alors } u_n v_n \rightarrow +\infty \\ \ell_1 = +\infty, \ell_2 = +\infty \text{ alors } u_n v_n \rightarrow +\infty \end{cases}$

Preuve: 1. $(\ell_1, \ell_2) \in \mathbb{R}^2$

Soit $\varepsilon > 0$ quelconque. On cherche $N \in \mathbb{N}$ tel que

$$\forall n \geq N, |u_n v_n - \ell_1 \ell_2| \leq \varepsilon$$

$$\begin{aligned} \forall n \in \mathbb{N}, |u_n v_n - \ell_1 \ell_2| &= |(u_n - \ell_1)v_n + \ell_1(v_n - \ell_2)| \\ &\leq |v_n| |u_n - \ell_1| + |\ell_1| |v_n - \ell_2| \end{aligned}$$

Comme v_n converge, elle est bornée,

$$\exists M \in \mathbb{R}, \forall n \in \mathbb{N}, |v_n| \leq M$$

donc

$$|u_n v_n - \ell_1 \ell_2| \leq M \times |u_n - \ell_1| + |\ell_1| |v_n - \ell_2|$$

Cas 1 On suppose $M \neq 0$ et $\ell_1 \neq 0$. Il existe $N_1 \in \mathbb{N}$ tel que

$$\forall n \geq N_1, |u_n - \ell_1| \leq \frac{\varepsilon}{2M}$$

Il existe $N_2 \in \mathbb{N}$ tel que

$$\forall n \geq N_2, |v_n - \ell_2| \leq \frac{\varepsilon}{2|\ell_1|}$$

On pose $N = \max(N_1, N_2)$.

$$\forall n \geq N, |u_n v_n - \ell_1 \ell_2| \leq \frac{\varepsilon}{2M} \times M + |\ell_1| \times \frac{\varepsilon}{2|\ell_1|} = \varepsilon$$

Cas 2 $M = 0, (\ell_1 \neq 0)$

Alors, $\forall n \in \mathbb{N}, v_n = 0$

Donc

$$\begin{cases} \forall n \in \mathbb{N}, u_n v_n = 0 \\ \ell_2 = 0 \\ \ell_1 \ell_2 = 0 = \lim_{n \rightarrow +\infty} u_n v_n \end{cases}$$

Cas 3 $M \neq 0$ et $\ell_1 = 0$

Alors, $\forall n \in \mathbb{N}, |u_n v_n - 0| \leq M |u_n|$
 $\frac{\varepsilon}{M} > 0$ donc il existe $N \in \mathbb{N}$ tel que

$$\forall n \geq N, |u_n| \leq \frac{\varepsilon}{M}$$

Donc,

$$\forall n \geq N, |u_n v_n| \leq M \times \frac{\varepsilon}{M} = \varepsilon$$

Donc, $u_n v_n \xrightarrow[n \rightarrow +\infty]{} 0 = \ell_1 \ell_2$

2. $\ell_1 > 0$ et $\ell_2 = +\infty$
Soit $M \in \mathbb{R}_*^+$ On cherche $N \in \mathbb{N}$ tel que

$$\forall n \geq N, u_n v_n \geq M$$

On pose $\varepsilon = \frac{\ell_1}{2} > 0$. Il existe $N_1 \in \mathbb{N}$ tel que

$$\forall n \geq N_1, u_n \geq \ell_1 - \varepsilon = \frac{\ell_1}{2} > 0$$

et il existe $N_2 \in \mathbb{N}$ tel que

$$\forall n \geq N_2, v_n \geq \frac{2M}{\ell_1} > 0$$

On pose $N = \max(N_1, N_2)$. Alors,

$$\forall n \geq N, u_n v_n \geq \frac{2M}{\ell_1} \times \frac{\ell_1}{2} = M$$

Donc $u_n v_n \xrightarrow[n \rightarrow +\infty]{} +\infty$

□

Proposition: Soit $(u_n)_{n \in \mathbb{N}}$ une suite de \mathbb{R}_* . Donc, $\forall n \in \mathbb{N}, u_n \neq 0$
On pose $\ell = \lim u_n$ (si elle existe).

1. si $\ell = +\infty$ alors, $\frac{1}{u_n} \rightarrow 0$
2. si $\ell = 0$ alors, $\left| \frac{1}{u_n} \right| \rightarrow +\infty$
 \triangleleft Si le signe de u_n ne se stabilise pas $\frac{1}{u_n}$ n'a pas de limite
 $\boxed{\text{ex}} u_n = \frac{(-1)^n}{n}$
3. si $\ell \in \mathbb{R}^*$, alors $\frac{1}{u_n} \xrightarrow[n \rightarrow +\infty]{} \frac{1}{\ell}$

Preuve: 3.

$$\forall n \in \mathbb{N}, \left| \frac{1}{u_n} - \frac{1}{\ell} \right| = \frac{|\ell - u_n|}{|u_n| |\ell|}$$

On pose $\varepsilon = \frac{|\ell|}{2} > 0$. Il existe $N \in \mathbb{N}$ tel que

$$\forall n \geq N, \ell - \varepsilon \leq u_n \leq \ell + \varepsilon$$

Si $\ell > 0$ alors

$$\forall n \geq N, u_n \geq \ell - \varepsilon = \frac{\ell}{2} > 0$$

et donc

$$\forall n \geq N, |u_n| \geq \frac{|\ell|}{2}$$

Si $\ell < 0$ alors

$$\forall n \in \mathbb{N}, u_n \leq \ell + \varepsilon = \frac{\ell}{2} < 0$$

et donc

$$\forall n \in \mathbb{N}, |u_n| \geq \frac{|\ell|}{2}$$

Donc,

$$\forall n \geq N, \left| \frac{1}{u_n} - \frac{1}{\ell} \right| \leq \frac{|u_n| - |\ell|}{|\ell| \times \frac{|\ell|}{2}} = \frac{2|u_n - \ell|}{|\ell|^2}$$

Soit $\varepsilon' > 0$ quelconque. $\frac{\varepsilon' |\ell|^2}{2}$ donc il existe $N' \in \mathbb{N}$ tel que

$$\forall n \geq N', |u_n - \ell| \leq \frac{\varepsilon'}{2} |\ell|^2$$

On pose N'' , $\left| \frac{1}{u_n} - \frac{1}{\ell} \right| \leq \frac{\varepsilon'}{2} |\ell|^2 \times \frac{2}{|\ell|^2} = \varepsilon'$

□

3 Limites et inégalités

Proposition: Soient u et v deux suites réelles convergentes de limites respectives ℓ_1 et ℓ_2 . On suppose que

$$\forall n \in \mathbb{N}, u_n \leq v_n$$

Alors, $\ell_1 \leq \ell_2$

Preuve:

On suppose $\ell_1 < \ell_2$. On pose $\varepsilon = \frac{\ell_1 - \ell_2}{3} > 0$.

Il existe $N_1 \in \mathbb{N}$ tel que

$$\forall n \geq N_1, u_n \geq \ell_1 - \varepsilon$$

Il existe $N_2 \in \mathbb{N}$ tel que

$$\forall n \geq N_2, v_n \leq \ell_2 + \varepsilon$$

Ainsi,

$$\forall n \geq \max(N_1, N_2), \ell_1 - \varepsilon \leq u_n \leq v_n \leq \ell_2 + \varepsilon$$

et donc

$$\ell_1 - \varepsilon \leq \ell_2 + \varepsilon$$

donc, $\ell_1 - \ell_2 \leq 2\varepsilon$

donc, $1 \leq \frac{2}{3}$ une contradiction

□

REMARQUE:

Si $\begin{cases} u_n \rightarrow \ell_1 \in \mathbb{R} \\ v_n \rightarrow \ell_2 \in \mathbb{R} \\ \forall n \in \mathbb{N}, u_n < v_n \end{cases}$
on n'a pas forcément $\ell_1 < \ell_2$
ex] $\forall n \in \mathbb{N}_*, \frac{1}{n+1} < \frac{1}{n}$ mais les deux convergent vers 0

Proposition: Soient u et v deux suites réelles telles que

$$\forall n \in \mathbb{N}, u_n < v_n$$

1. si $u_n \rightarrow +\infty, v_n \rightarrow +\infty$
2. si $v_n \rightarrow -\infty, u_n \rightarrow -\infty$

Preuve: 1. On suppose $u_n \rightarrow +\infty$. Soit $M \in \mathbb{R}$, il existe $N \in \mathbb{N}$ tel que

$$\forall n \geq N, u_n \geq M$$

Donc

$$\forall n \geq N, v_n \geq u_n \geq M$$

Donc $v_n \rightarrow +\infty$

□

Théorème (Théorème des "gendarmes"): Soient u, v et w trois suites réelles telles que

$$\forall n \in \mathbb{N}, u_n \leq v_n \leq w_n$$

On suppose que u et w convergent vers la même limite $\ell \in \mathbb{R}$. Alors, v converge vers ℓ

Preuve:

Soit $\varepsilon > 0$. Il existe $N_1 \in \mathbb{N}$ tel que

$$\forall n \geq N_1, w_n \leq \ell + \varepsilon$$

Il existe $N_2 \in \mathbb{N}$ tel que

$$\forall n \geq N_2, u_n \leq \ell - \varepsilon$$

On pose $N = \max(N_1, N_2)$. D'où,

$$\forall n \geq N, \ell - \varepsilon \leq u_n \leq v_n \leq w_n \leq \ell + \varepsilon$$

Donc, $v_n \xrightarrow[n \rightarrow +\infty]{} \ell$

□

Théorème (Limite monotone): 1. Soit u une suite croissante majorée par M .
Alors, u converge et $\lim u_n \leq M$

2. Soit u une suite croissante non majorée.

Alors, $u_n \xrightarrow{n \rightarrow +\infty} +\infty$

3. Soit u une suite décroissante minorée par m .

Alors, u converge et $\lim u_n \geq m$

4. Soit u une suite décroissante non minorée.

Alors, $u_n \xrightarrow[n \rightarrow +\infty]{} -\infty$

Preuve: 1. $\{u_n \mid n \in \mathbb{N}\} \neq \emptyset$ (u_0 y est) majorée (par hypothèse) par M .

On pose $\ell = \sup_{n \in \mathbb{N}} (u_n)$. Soit $\varepsilon > 0$ quelconque

$\ell - \varepsilon < \ell$ donc, $\exists N \in \mathbb{N}, u_N > \ell - \varepsilon$
 u est croissante donc

$$\forall n \geq N, u_n \geq u_N > \ell - \varepsilon$$

donc,

$$\forall n \geq N, \ell - \varepsilon \leq u_n \leq \ell \leq \ell + \varepsilon$$

Donc, $u_n \rightarrow \ell$

2. Soit $M \in \mathbb{R}$. M n'est pas un majorant de l'ensemble $\{u_n \mid n \in \mathbb{N}\}$ donc

$$\exists N \in \mathbb{N}, u_N > M$$

Comme u est croissante

$$\forall n \geq N, u_n \geq u_N \geq M$$

donc

$$u_n \xrightarrow[n \rightarrow +\infty]{} +\infty$$

□

EXEMPLE:

$$\begin{cases} u_0 = a \in]0, 1[\\ \forall n \in \mathbb{N}, u_{n+1} = u_n(1 - u_n) \end{cases}$$

(suite logistique)

$$u_{n+1} = f(u_n) \text{ avec } f : x \mapsto x(1 - x)$$

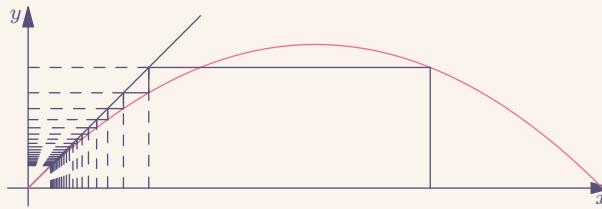


FIGURE 11.5 – Courbe logistique

— Soit $n \in \mathbb{N}$,

$$\begin{aligned} u_{n+1} - u_n &= u_n(1 - u_n) - u_n \\ &= -u_n^2 \leq 0 \end{aligned}$$

Donc, u est décroissante.

— Montrons par récurrence que

$$\forall n \in \mathbb{N}, u_n \in [0, 1]$$

— $u_0 = a \in]0, 1[$ donc $u_0 \in [0, 1]$

— Soit $n \in \mathbb{N}$. On suppose $u_n \in [0, 1]$

$$\begin{cases} 0 \leq u_n \leq 1 \\ 0 \leq 1 - u_n \leq 1 \end{cases}$$

donc

$$0 \leq u_{n+1} \leq 1$$

donc u minoré par 0

— D'après le théorème de la limite monotone, u converge. On pose ℓ sa limite :

$$\ell = \lim_{n \rightarrow +\infty} u_n$$

Alors, $u_{n+1} \xrightarrow{n \rightarrow +\infty} \ell$

$$u_n(1 - u_n) \xrightarrow{n \rightarrow +\infty} \ell(1 - \ell)$$

Par unicité de la limite,

$$\begin{aligned} \ell &= \ell(1 - \ell) \\ \iff 1 &= 1 - \ell \\ \iff 0 &= -\ell \iff \ell = 0 \end{aligned}$$

EXEMPLE:

$$\begin{cases} u_0 = a \in]0, 1[\\ u_{n+1} = 2u_n(1 - u_n) \end{cases}$$

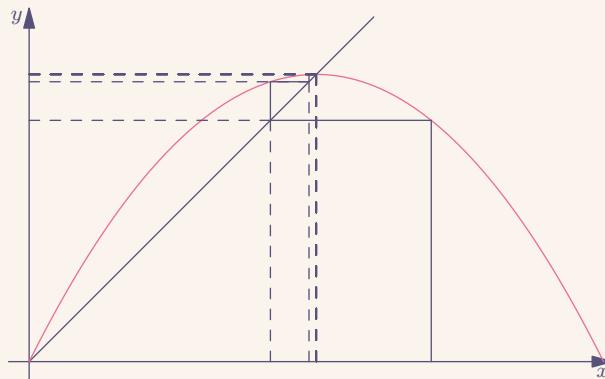


FIGURE 11.6 – Courbe logistique (2)

EXEMPLE:

$$\begin{cases} u_0 = a \in]0, 1[\\ u_{n+1} = 3u_n(1 - u_n) \end{cases}$$

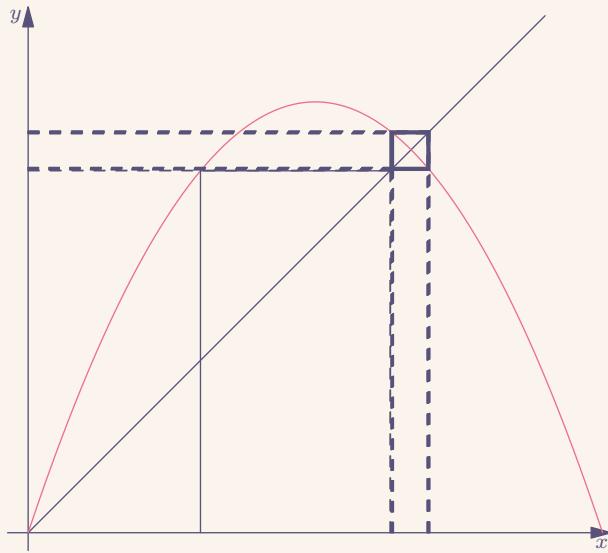


FIGURE 11.7 – Courbe logistique (3)

EXEMPLE:

$$\begin{cases} u_0 = a \in]0, 1[\\ u_{n+1} = 4u_n(1 - u_n) \end{cases}$$

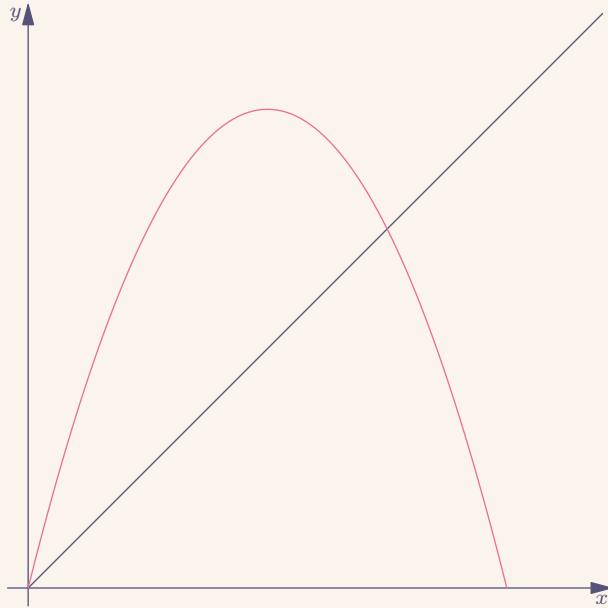


FIGURE 11.8 – Courbe logistique (4)

Définition: Soient u et v deux suites réelles. On dit que u et v sont adjacentes si
— u est croissante

- v est décroissante
- $u_n - v_n \xrightarrow{n \rightarrow +\infty} 0$

Théorème: Soient u et v deux suites adjacentes. Alors, u et v convergent vers la même limite.

Preuve:

$u - v$ est croissante donc,

$$\forall n \in \mathbb{N}, u_n - v_n \leq 0$$

v décroissante donc

$$\forall n \in \mathbb{N}, v_n \leq v_0$$

donc u majorée par v_0 donc u converge.

u est croissante donc,

$$\forall n \in \mathbb{N}, u_n \geq u_0$$

donc v est minorée par u_0 donc v converge.

Donc, $u_n - v_n \rightarrow \lim(u_n) - \lim(v_n)$ Par unicité de la limite,

$$\begin{aligned} \lim(u_n) - \lim(v_n) &= 0 \\ \iff \lim(u_n) &= \lim(v_n) \end{aligned}$$

□

Théorème (Théorème des segments emboîtés): Soit (I_n) une suite de segments (non vide) décroissante

$$\forall n \in \mathbb{N}, I_{n+1} \subset I_n$$

On note $\ell(I)$ la longueur d'un intervalle I .

Si $\ell(I_n) \xrightarrow{n \rightarrow +\infty} 0$ alors $\bigcap_{n \in \mathbb{N}} I_n$ est un singleton.

Preuve:

On pose $\forall n \in \mathbb{N}, I_n = [a_n, b_n]$ avec $\forall n \in \mathbb{N}, a_n \leq b_n$. Soit $n \in \mathbb{N}$.

$I_{n+1} \subset I_n$ donc $a_{n+1} \in I_{n+1} \subset I_n$

donc $a_{n+1} \geq a_n$. De même, $b_{n+1} \in I_{n+1}$ donc $b_{n+1} \in I_n$ donc $b_{n+1} \leq b_n$.

$$\forall n \in \mathbb{N}, b_n - a_n = \ell(I_n) \xrightarrow{n \rightarrow +\infty} 0$$

donc (a_n) et (b_n) sont adjacentes, elles convergent donc vers la même limite $\ell \in \mathbb{R}$.

(a_n) croissante de limite ℓ donc

$$\forall n \in \mathbb{N}, a_n \leq \ell$$

(b_n) est décroissante de limite ℓ donc

$$\forall n \in \mathbb{N}, b_n \geq \ell$$

Donc, $\forall n \in \mathbb{N}, \ell \in I_n$ donc $\ell \in \bigcap_{n \in \mathbb{N}} I_n$.

Soit $\ell' \neq \ell$.

— Si $\ell' < \ell = \sup_{n \in \mathbb{N}} (a_n)$ donc ℓ' ne majore pas (a_n)

$$\exists N \in \mathbb{N}, a_N > \ell'$$

$$\text{donc } \ell' \notin I_N \text{ donc } \ell' \notin \bigcap_{n \in \mathbb{N}} I_n$$

— Si $\ell' > \ell = \inf_{n \in \mathbb{N}} (b_n)$ donc ℓ' ne minore pas (b_n)

$$\exists N' \in \mathbb{N}, b_{N'} < \ell'$$

$$\text{et donc } \ell' \notin I_{N'} \text{ donc } \ell' \notin \bigcap_{n \in \mathbb{N}} I_n$$

□

4 Suites extraites

Définition: Soit $u \in \mathbb{R}^{\mathbb{N}}$ et $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ strictement croissante.

On dit que $(u_{\varphi(n)})$ est une **suite extraite** de u ou une **sous suite** de u . On dit alors que φ est une extractrice.

EXEMPLE:

$u_0 [u_1] u_2 u_3 [u_4] [u_5] u_6 u_7 \dots$

$$\begin{cases} \varphi(0) = 1 \\ \varphi(1) = 4 \\ \varphi(2) = 5 \end{cases}$$

Lemme: Soit $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ strictement croissante. Alors,

$$\forall n \in \mathbb{N}, \varphi(n) \geq n$$

Preuve (par récurrence): — $\varphi(0) \in \mathbb{N}$ donc $\varphi(0) \geq 0$

— Soit $n \in \mathbb{N}$. On suppose $\varphi(n) \geq n$.

$n + 1 > n$ donc $\varphi(n + 1) > \varphi(n) \geq n$ donc $\varphi(n + 1) > n$

Comme $\varphi(n + 1) \in \mathbb{N}$, $\varphi(n + 1) \geq n + 1$

□

Proposition: Soit $u \in \mathbb{R}^{\mathbb{N}}$ de limite $\ell \in \overline{\mathbb{R}}$ et $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ strictement croissante alors $u_{\varphi(n)} \xrightarrow{n \rightarrow +\infty} \ell$.

Preuve: CAS 1 $\ell \in \mathbb{R}$

Soit $\varepsilon > 0$ on sait qu'il existe $N \in \mathbb{N}$ tel que

$$\forall n \geq N, |u_n - \ell| \leq \varepsilon$$

Soit $n \geq N$ alors $\varphi(n) \geq n \geq N$ donc

$$|u_{\varphi(n)} - \ell| \leq \varepsilon$$

Donc, $u_{\varphi(n)} \xrightarrow[n \rightarrow +\infty]{} \ell$

CAS 2 $\ell = +\infty$

Soit $M \in \mathbb{R}$ et soit $N \in \mathbb{N}$ tel que

$$\forall n \geq N, u_n \geq M$$

Soit $n \geq N$, on a $\varphi(n) \geq n \geq N$ donc

$$u_{\varphi(n)} \geq M$$

Donc $u_{\varphi(n)} \xrightarrow[n \rightarrow +\infty]{} +\infty$

CAS 3 $\ell = -\infty$ similaire au CAS 2

□

EXEMPLE:

$$\forall n \in \mathbb{N}, u_n = (-1)^n$$

$$u_{2n} = 1 \xrightarrow[n \rightarrow +\infty]{} 1$$

$$u_{2n+1} = -1 \xrightarrow[n \rightarrow +\infty]{} -1$$

donc u_n n'a pas de limite.

Proposition: Si (u_{2n}) et (u_{2n+1}) ont la même limite ℓ alors $u_n \xrightarrow[n \rightarrow +\infty]{} \ell$

Preuve: CAS 1 $\ell \in \mathbb{R}$

Soit $\varepsilon > 0$. Soit $N_1 \in \mathbb{N}$ tel que

$$\forall n \geq N_1, |u_{2n} - \ell| \leq \varepsilon$$

Soit $N_2 \in \mathbb{N}$ tel que

$$\forall n \geq N_2, |u_{2n+1} - \ell| \leq \varepsilon$$

On pose $N = \max(2N_1, 2N_2 + 1)$. Soit $n \geq N$.

Si n pair alors $n = 2k$ avec $k \geq N_1$ et donc, $|u_{2k} - \ell| \leq \varepsilon$, i.e. $|u_n - \ell| \leq \varepsilon$

Si n impair alors $n = 2k+1$ avec $k \geq N_2$ et donc, $|u_{2k+1} - \ell| \leq \varepsilon$, i.e. $|u_n - \ell| \leq \varepsilon$

Donc,

$$\forall n \geq N, |u_n - \ell| \leq \varepsilon$$

Donc $u_n \xrightarrow[n \rightarrow +\infty]{} \ell$

□

Théorème (Théorème de Bolzano-Weierstrass): Soit (u_n) une suite réelle bornée. Alors, il existe $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ strictement croissante telle que $(u_{\varphi(n)})$ converge.

Preuve: MÉTHODE 1 par dichotomie

Soitent $m, M \in \mathbb{R}$ tel que

$$\forall n \in \mathbb{N}, m \leq u_n \leq M$$

On pose

$$\begin{aligned} A_1 &= \left\{ n \in \mathbb{N} \mid m \leq u_n \leq \frac{m+M}{2} \right\} \\ A_2 &= \left\{ n \in \mathbb{N} \mid \frac{m+M}{2} \leq u_n \leq M \right\} \end{aligned}$$

Comme $A_1 \cup A_2 = \mathbb{N}$, A_1 et A_2 ne peuvent pas être finis tous les deux.
On pose

$$B_0 = \begin{cases} A_1 & \text{si } A_1 \text{ est infini} \\ A_2 & \text{sinon} \end{cases}$$

B_0 est infini donc non vide. On pose $\varphi(0) = \min(B_0)$

On pose aussi

$$m_0 = \begin{cases} m & \text{si } B_0 = A_1 \\ \frac{m+M}{2} & \text{si } B_0 = A_2 \end{cases}$$

et

$$M_0 = \begin{cases} \frac{m+M}{2} & \text{si } B_0 = A_1 \\ M & \text{si } B_0 = A_2 \end{cases}$$

Ainsi, $B_0 = \{n \in \mathbb{N} \mid m_0 \leq u_n \leq M_0\}$. On pose

$$\begin{aligned} B'_1 &= \left\{ n \in B_0 \mid n > \varphi(0) \text{ et } m_0 \leq u_n \leq \frac{M_0 + m_0}{2} \right\} \\ B'_2 &= \left\{ n \in B_0 \mid n > \varphi(0) \text{ et } \frac{m_0 + M_0}{2} \leq u_n \leq M_0 \right\} \end{aligned}$$

$$B'_1 \cup B'_2 = \{n \in B \mid n > \varphi(0)\} = B_0 \setminus \{\varphi(0)\}$$

$B_0 \setminus \{\varphi(0)\}$ est infini donc B'_1 ou B'_2 est infini. On pose

$$B_1 = \begin{cases} B'_1 & \text{si } B'_1 \text{ est infini} \\ B'_2 & \text{sinon} \end{cases}$$

B_1 est infini donc non vide et admet un plus petit élément :

$$\varphi(1) = \min(B_1)$$

$\varphi(1) \in B_1$ donc $\varphi(1) > \varphi(0)$

On pose

$$\begin{aligned} m_1 &= \begin{cases} m_0 & \text{si } B_1 = B'_1 \\ \frac{m_0 + M_0}{2} & \text{si } B_1 = B'_2 \end{cases} \\ M_1 &= \begin{cases} \frac{m_0 + M_0}{2} & \text{si } B_1 = B'_1 \\ M_0 & \text{si } B_1 = B'_2 \end{cases} \end{aligned}$$

On construit une suite décroissante (B_n) , deux suites de réels (m_n) et (M_n) et une suite d'entiers $(\varphi(n))$ telles que

$$\forall n \in \mathbb{N}, \begin{cases} B_{n+1} = \{k \in B_n \mid k > \varphi(n) \text{ et } m_{n+1} \leq u_k \leq M_{n+1}\} \\ \varphi(n+1) = \min(B_{n+1}) > \varphi(n) \\ M_{n+1} - m_{n+1} = \frac{1}{2}(M_n - m_n) \end{cases}$$

La suite (m_n) est croissante, (M_n) est décroissante et

$$\lim_{n \rightarrow +\infty} M_n - m_n = \lim_{n \rightarrow +\infty} \left(\frac{1}{2}\right)^n (M_0 - m_0) = 0$$

Donc, (m_n) et (M_n) sont adjacentes donc convergentes avec la même limite $\ell \in \mathbb{R}$

$$\forall n \in \mathbb{N}, m_n \leq u_{\varphi(n)} \leq M_n$$

Par encadrement, $u_{\varphi(n)} \xrightarrow{n \rightarrow +\infty} \ell$

□

MÉTHODE 2 On pose $A = \{n \in \mathbb{N} \mid \forall k > n, u_k > u_n\}$

CAS 1 On suppose A infini.

On pose $\varphi(0) = \min(A)$. Soit $n \in \mathbb{N}$. On suppose $\varphi(0), \varphi(1), \dots, \varphi(n)$ soient déjà construits. On pose

$$\varphi(n+1) = \min(A \setminus \{\varphi(0), \varphi(1), \dots, \varphi(n)\})$$

Soit $n \in \mathbb{N}_*$

$$\varphi(n+1) \in A \setminus \{\varphi(0), \varphi(1), \dots, \varphi(n)\}$$

donc

$$\varphi(n+1) \in A \setminus \{\varphi(0), \varphi(1), \dots, \varphi(n-1)\}$$

donc

$$\varphi(n+1) \geq \varphi(n)$$

Or, par définition, $\varphi(n+1) \neq \varphi(n)$ donc $\varphi(n+1) > \varphi(n)$

On a aussi $\varphi(1) \in A$ donc $\varphi(1) \geq \varphi(0)$ Or, on sait que $\varphi(1) \neq \varphi(0)$. Donc, $\varphi(1) > \varphi(0)$ Soit $n \in \mathbb{N}$, $\varphi(n) \in A$ donc

$$\forall k > \varphi(n), u_k < u_{\varphi(n)}$$

or $\varphi(n+1) > \varphi(n)$ donc $u_{\varphi(n+1)} < u_{\varphi(n)}$.

La sous suite $(u_{\varphi(n)})$ est décroissante et minorée (car u est minorée) donc elle converge

CAS 2 On suppose A fini. Soit $N = \max(A)$,

$$\forall n > N, n \notin A$$

Donc $\forall n > N, \exists k > n, u_n \leq u_k$.

Par exemple, en posant $\varphi(0) = N+1$, on a

$$A_1 = \{k > N+1 \mid u_{N+1} \leq u_k\} \neq \emptyset$$

On pose $\varphi(1) = \min(A_1)$ donc $\begin{cases} \varphi(1) > N+1 = \varphi(0) \\ u_{\varphi(0)} < u_{\varphi(1)} \end{cases}$

Avec $n = \varphi(1)$

$$\exists k > n, u_{\varphi(1)} \leq u_k$$

Donc, $A_2 = \{k \in \mathbb{N} \mid k > \varphi(1) \text{ et } u_{\varphi(1)} \leq u_k\} \neq \emptyset$

On pose $\varphi(2) = \min(A_2)$. On a alors $\varphi(2) > \varphi(1)$. Soit $n \in \mathbb{N}$, on suppose $\varphi(n)$ déjà construit avec $\varphi(n) > N$. On sait alors que

$$A_{n+1} = \{k \in \mathbb{N} \mid k > \varphi(n) \text{ et } u_{\varphi(n)} \leq u_k\} \neq \emptyset$$

On pose $\varphi(n+1) = \min(A_{n+1})$. Donc,

$$\begin{cases} \varphi(n+1) > \varphi(n) > N \\ u_{\varphi(n)} \leq u_{\varphi(n+1)} \end{cases}$$

On vient de construire une sous suite croissante majorée (car u est majorée) donc convergente.

□

5 Suites récurrentes

Définition: On dit que u est une suite récurrente linéaire d'ordre 2 à coefficients constants s'il existe $(a, b) \in \mathbb{C}$ tels que

$$\forall n \in \mathbb{N}, u_{n+2} = au_{n+1} + bu_n$$

L'équation caractéristique associée est

$$(C) : z^2 = az + b \text{ avec } z \in \mathbb{C}$$

Proposition: Avec les notations précédentes,

1. Si (C) a 2 racines simples $r_1 \neq r_2$ alors

$$\exists (A, B) \in \mathbb{C}^2, \forall n \in \mathbb{N}, u_n = Ar_1^n + Br_2^n$$

2. Si (C) a une racine double $r \in \mathbb{C}$ alors

$$\exists (A, B) \in \mathbb{C}^2, \forall n \in \mathbb{N}, u_n = (An + B)r^n$$

Preuve (Récurrence double):

□

Proposition: avec les notations précédentes et avec $(a, b) \in \mathbb{R}^2$ et $(u_n) \in \mathbb{R}^{\mathbb{N}}$

1. Si (C) a deux racines simples $r_1 \neq r_2$ alors

$$\exists (A, B) \in \mathbb{R}^2, \forall n \in \mathbb{N}, u_n = Ar_1^n + Br_2^n$$

2. Si (C) a une racine simple $r \in \mathbb{R}$ alors

$$\exists (A, B) \in \mathbb{R}^2, \forall n \in \mathbb{N}, u_n = (An + B)r^n$$

3. Si (C) a deux racines complexes conjuguées $re^{i\theta}$ avec $r \in \mathbb{R}_*^+$ et $\theta \in [0, \frac{\pi}{2}[$ alors

$$\exists (A, B) \in \mathbb{R}^2, \forall n \in \mathbb{N}, u_n = r^n(A \cos(n\theta) + B \sin(n\theta))$$

□

REMARQUE:

Étude de $u_{n+1} = f(u_n)$

1. On choisit rapidement la fonction f (au moins le tableau de variation)
- 1'. (OPTIONNEL) on représente graphiquement la fonction f et la droite d'équation $y = x$ pour conjecturer sa limite
2. On utilise le tableau de variation pour vérifier que (u_n) est bien définie par récurrence

$$P(n) : "u_n \text{ existe et } u_n \in \mathcal{D}_f"$$

3. On étudie le signe de $f(x) - x$
4. On cherche les intervalles stables par f :

$$f(I) \subset I$$

les plus petits possible (c a permis de montrer que la suite est majorée (minorée) en particulier ceux sur lesquels $f(x) - x$ ne change pas de signe

- 4'. Donc on utilise le théorème de la limite monotone
 4''. Sinon, on essaie l'inégalité (voir théorème) des accroissements finis :
 Soit ℓ un point fixe de $f : f(\ell) = \ell$

$$\forall n \in \mathbb{N}, |u_{n+1} - \ell| = |f(u_n) - f(\ell)| = M |u_n - \ell|$$

où M est un majorant de $|f'|$

Si $0 \leq M \leq 1$ alors

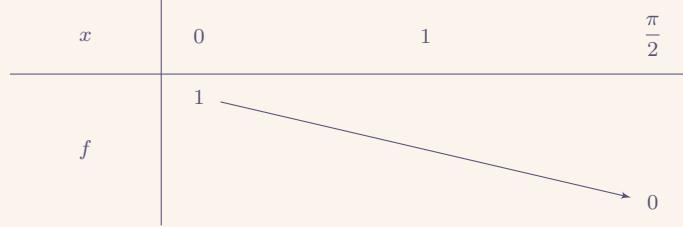
$$\forall n \in \mathbb{N}, |u_n - \ell| \leq M^n |u_0 - \ell| \xrightarrow[n \rightarrow +\infty]{} 0$$

donc $u_n \xrightarrow[n \rightarrow +\infty]{} \ell$

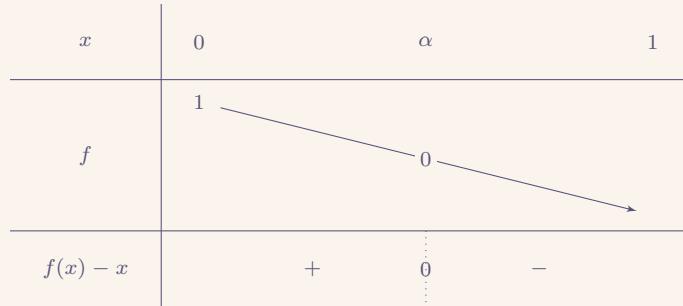
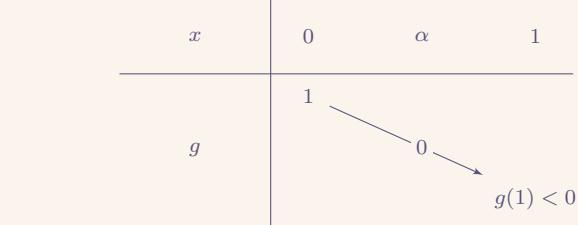
5. si (u_n) a une limite et si f continue alors $\lim(u_n)$ est une point fixe de f

EXEMPLE: 1.

$$\begin{cases} u_{n+1} = \cos(u_n) \\ u_0 \in]0, 1[\end{cases}$$



On pose $g : x \mapsto \cos(x) - x$ dérivable et
 $\forall x \in [0, 1], g'(x) = -\sin(x) - 1 \leq 0$



$$\begin{aligned} \forall x \in [0, 1], |f'(x)| &= |- \sin(x)| \\ &= \sin(x) \leq \sin(1) < 1 \end{aligned}$$

$$\forall n, |u_{n+1} - \alpha| = |f(u_n) - f(\alpha)| \leq \sin(1) |u_n - \alpha|$$

donc

$$\forall n, |u_n - \alpha| \leq \underbrace{\sin^n(1)}_{n \rightarrow +\infty} |u_0 - \alpha|$$

Donc, $u_n \xrightarrow[n \rightarrow +\infty]{} \alpha$

6 Comparaison de suites

Définition: Soient u et v deux suites réelles. On dit que u est dominée par v si

$$\exists M \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \geq N, |u_n| \leq M |v_n|$$

Dans ce cas, on note $u = O(v)$ ou $u_n = O(v_n)$ et on dit que "u est un grand o de v"

EXEMPLE:

En informatique, on dit qu'un algorithme a une complexité linéaire si son temps d'exécution est un $O(n)$. Par exemple, on calcule a^n

— Approche naïve Complexité linéaire $O(n)$

```

1:  $p \leftarrow 1$ 
2: for  $i \in \llbracket 0, n - 1 \rrbracket$  do
3:    $p \leftarrow p \times a$ 
4: end for
5: return  $p$ 
```

— Exponentiation rapide

On écrit n en binaire :

$$n = \overline{a_k a_{k-1} \dots a_0}^{(2)}$$

$$= \sum_{i=0}^k a_i 2^i$$

avec $(a_i) \in \{0, 1\}^{k+1}$

$$\begin{aligned} a^n &= a^{\sum_{i=0}^k a_i 2^i} \\ &= \prod_{i=0}^k a^{a_i 2^i} \end{aligned}$$

```

1:  $s \leftarrow 0$ 
2:  $p \leftarrow a$ 
3: for  $i \in \llbracket 0, \log_2(n) \rrbracket$  do
4:    $p \leftarrow p \times p$ 
5:   if  $a[i] = 1$  then
6:      $s \leftarrow s + p$ 
7:   end if
8: end for
9: return  $s$ 
```

Complexité logarithmique $O(\log_2(n))$

Proposition: O est une relation réfléctive et transitive.

Preuve: — Soit u une suite. On pose $M = 1$ et

$$\forall n \in \mathbb{N}, |u_n| \leq M |u_n|$$

Donc $u = O(u)$.

— Soient u, v, w trois suites telles que

$$\begin{cases} u = O(v) \\ v = O(w) \end{cases}$$

Soient $M_1, M_2 \in \mathbb{R}$ et $N_1, N_2 \in \mathbb{N}$ tels que

$$\begin{cases} \forall n \geq N_1, |u_n| \leq M_1 |v_n| \\ \forall n \geq N_2, |v_n| \leq M_2 |w_n| \end{cases}$$

Nécessairement, $M_1 \geq 0$ et $M_2 \geq 0$.

Soit $N = \max(N_1, N_2)$.

$$\forall n \geq N, |u_n| \leq M_1 |v_n| \leq M_1 M_2 |w_n|$$

Donc $u = O(w)$

□

Définition: Soient u et v deux suites. On dit que u est négligeable devant v si

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, |u_n| \leq \varepsilon |v_n|$$

Dans ce cas, on note $u = o(v)$ ou $u_n = o(v_n)$ ou on le lit "u est un petit o de v"

Proposition: o est une relation transitive, non-réfléctive

Preuve: — Soient u, v et w trois suites telles que

$$\begin{cases} u = o(v) \\ v = o(w) \end{cases}$$

Soit $\varepsilon > 0$. Soit $N_1 \in \mathbb{N}$ tel que

$$\forall n \geq N_1, |u_n| \leq \sqrt{\varepsilon} |v_n|$$

Soit $N_2 \in \mathbb{N}$ tel que

$$\forall n \geq N_2, |v_n| \leq \sqrt{\varepsilon} |w_n|$$

On pose $N = \max(N_1, N_2)$, alors

$$\forall n \geq N, |u_n| \leq \sqrt{\varepsilon} |v_n| \leq \underbrace{\sqrt{\varepsilon} \times \sqrt{\varepsilon}}_{\varepsilon} |w_n|$$

donc $u = o(w)$

— Soit u une suite tel qu'il existe $N \in \mathbb{N}$ tel que

$$\forall n \geq N, u_n > 0$$

On suppose que $u = o(u)$, alors

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, |u_n| \leq \varepsilon |u_n|$$

On pose $\varepsilon = \frac{1}{2}$ alors

$$\exists N \in \mathbb{N}, \forall n \geq N, |u_n| \leq \frac{1}{2} |u_n|$$

une contradiction

□

Proposition: Soient u et v deux suites.

- $o(u) + o(v) = o(u)$
- $v \times o(u) = o(vu)$
- $o(u) \times o(v) = o(vu)$
- $o(o(u)) = o(u)$

□

Définition: Soient u et v deux suites. On dit que u et v sont équivalentes si

$$u = v + o(v)$$

i.e.

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, |u_n - v_n| \leq \varepsilon |v_n|$$

Dans ce cas, on le note $u \sim v$

Proposition: \sim est une relation d'équivalence

□

Proposition: Soient $(u, v) \in \mathbb{R}^{\mathbb{N}}$. On suppose que v ne s'annule pas à partir d'un certain rang

1. $u = o(v) \iff \left(\frac{u_n}{v_n} \right)$ bornée
2. $u = o(v) \iff \frac{u_n}{v_n} \xrightarrow[n \rightarrow +\infty]{} 0$
3. $u \sim v \iff \frac{u_n}{v_n} \xrightarrow[n \rightarrow +\infty]{} 1$

□

Proposition (Suites de références): 1. $\ln^\alpha(n) = o(n^\beta)$ avec $(\alpha, \beta) \in (\mathbb{R}_*)^2$

2. $n^\beta = o(a^n)$ avec $\beta > 0$ et $a > 1$
3. $a^n = o(n!)$ avec $a > 1$
4. $n! = o(n^n)$

Lemme (Exercice 10 du TD): Soit $u \in (\mathbb{R}_*)^{\mathbb{N}}$

Si $\frac{u_{n+1}}{u_n} \xrightarrow[n \rightarrow +\infty]{} \ell < 1$ avec $\ell \in \mathbb{R}$,
alors $u_n \xrightarrow[n \rightarrow +\infty]{} 0$

Preuve (de la proposition): 1. par croissance comparée

2. On pose $\forall n \in \mathbb{N}^*, u_n = \frac{n^\beta}{a^n}$.

$$\begin{aligned}\forall n \in \mathbb{N}^*, \frac{u_{n+1}}{u_n} &= \left(\frac{n+1}{n}\right)^\beta \times \frac{1}{a} \\ &= \frac{1}{a} \left(1 + \frac{1}{n}\right)^\beta \\ &\xrightarrow[n \rightarrow +\infty]{} \frac{1}{a} < 1\end{aligned}$$

Donc, $u_n \xrightarrow[n \rightarrow +\infty]{} 0$

3. On pose $\forall n \in \mathbb{N}, u_n = \frac{a^n}{n!}$

$$\forall n \in \mathbb{N}, \frac{u_{n+1}}{u_n} = \frac{a}{n+1} \xrightarrow[n \rightarrow +\infty]{} 0 < 1$$

donc $u_n \xrightarrow[n \rightarrow +\infty]{} 0$

4. On pose $\forall n \in \mathbb{N}^*, u_n = \frac{n!}{n^n}$.

$$\begin{aligned}\forall n \in \mathbb{N}^*, \frac{u_{n+1}}{u_n} &= (n+1) \frac{n^n}{(n+1)^{n+1}} \\ &= \left(\frac{n}{n+1}\right)^n \\ &= e^{n \ln\left(\frac{n}{n+1}\right)} \\ &= e^{n \ln\left(1 + \frac{1}{n+1}\right)} \\ &= e^{n(-\frac{1}{n} + o(\frac{1}{n}))} \\ &= e^{-1 + o(1)} \\ &\xrightarrow[n \rightarrow +\infty]{} e^{-1} < 1\end{aligned}$$

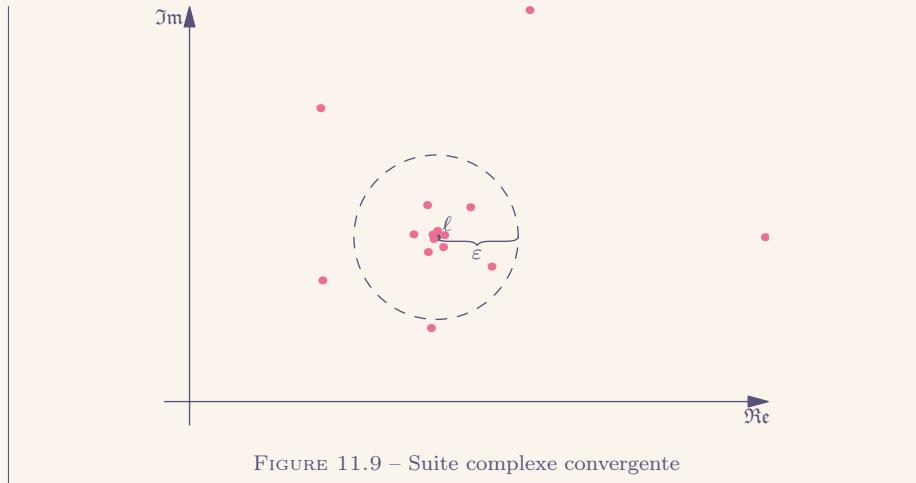
donc $u_n \xrightarrow[n \rightarrow +\infty]{} 0$

□

7 Suites complexes

Définition: Soit $(u_n) \in \mathbb{C}^{\mathbb{N}}$ et $\ell \in \mathbb{C}$. On dit que (u_n) converge vers ℓ si

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, |u_n - \ell| \leq \varepsilon$$



Proposition: Si ℓ_1 et ℓ_2 sont deux limites de u alors $\ell_1 = \ell_2$

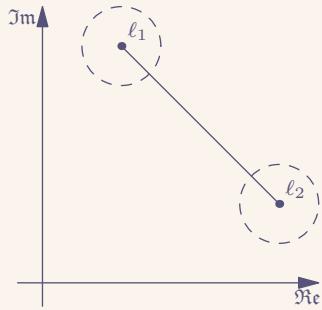


FIGURE 11.10 – Unicité de la limite de suites complexes

□

Proposition: Les limites de somme, produit, quotient de suites complexes respectent les mêmes lois que pour les suites réelles. □

Théorème: Soit $u \in \mathbb{C}^{\mathbb{N}}$ et $\ell \in \mathbb{C}$.

$$u_n \xrightarrow{n \rightarrow +\infty} \ell \iff \begin{cases} \Re(u_n) \xrightarrow{n \rightarrow +\infty} \Re(\ell) \\ \Im(u_n) \xrightarrow{n \rightarrow +\infty} \Im(\ell) \end{cases}$$

Preuve: \implies On suppose $u_n \rightarrow \ell$.
Soit $\varepsilon > 0$. Soit $N \in \mathbb{N}$ tel que

$$\forall n \geq N, |u_n - \ell| \leq \varepsilon$$

Or,

$$\forall n \geq N, \begin{cases} \Re(u_n) - \Re(\ell) = \Re(u_n - \ell) \leq |u_n - \ell| \leq \varepsilon \\ \Im(u_n) - \Im(\ell) = \Im(u_n - \ell) \leq |u_n - \ell| \leq \varepsilon \end{cases}$$

donc

$$\begin{cases} \Re(u_n) \rightarrow \Re(\ell) \\ \Im(u_n) \rightarrow \Im(\ell) \end{cases}$$

$$\Leftarrow \text{ On suppose } \begin{cases} \Re(u_n) \rightarrow \Re(\ell) \\ \Im(u_n) \rightarrow \Im(\ell) \end{cases}$$

Alors,

$$\forall n \in \mathbb{N}, u_n = \Re(u_n) + i\Im(u_n) \rightarrow \Re(\ell) + i\Im(\ell) = \ell$$

□

Proposition: Soit $u \in \mathbb{C}^{\mathbb{N}}$ et $\ell \in \mathbb{C}$.
Si $u_n \rightarrow \ell$ alors $|u_n| \rightarrow |\ell|$

Preuve:

On suppose $u_n \rightarrow \ell$

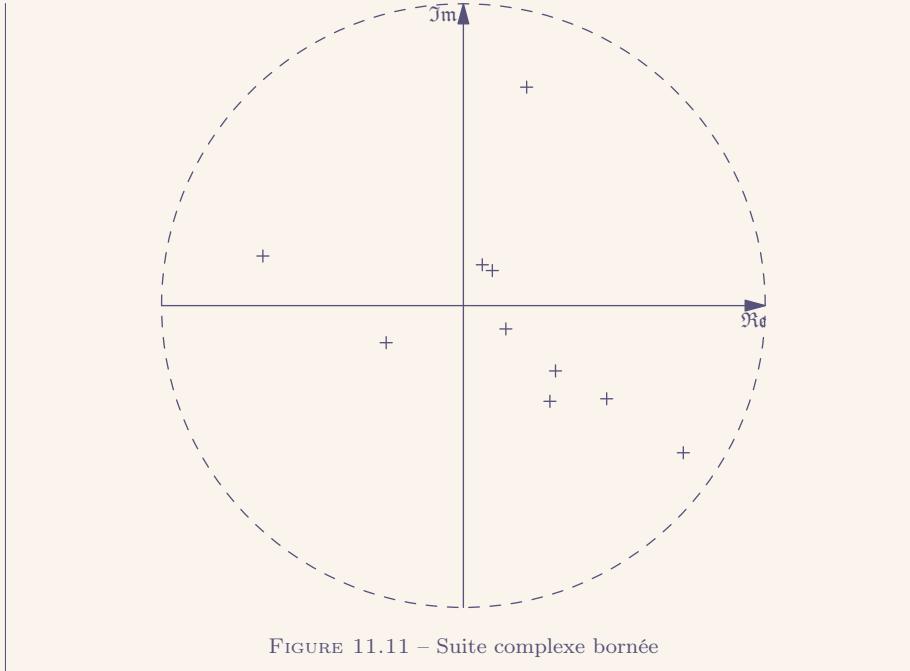
$$\forall n \in \mathbb{N}, |u_n| = \sqrt{\Re^2(u_n) + \Im^2(u_n)} \rightarrow \sqrt{\Re^2(\ell) + \Im^2(\ell)} = |\ell|$$

□

Proposition: Tous les résultats (sauf ceux avec des limites infinies!) concernant les suites extraits sont encore valables dans \mathbb{C} y compris le théorème de Bolzano-Weierstrass (mais avec une autre preuve).

Définition: Soit $u \in \mathbb{C}^{\mathbb{N}}$. On dit que u est bornée s'il existe $M \in \mathbb{R}^+$ tel que

$$\forall n \in \mathbb{N}, |u_n| \leq M$$



Théorème (Bolzano Weierstrass): Soit $u \in \mathbb{C}^{\mathbb{N}}$ bornée. Il existe $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ strictement croissante telle que $(u_{\varphi(n)})$ converge.

Preuve:

Soit $M \in \mathbb{R}^+$ tel que

$$\forall n \in \mathbb{N}, |u_n| \leq M$$

Donc, $\forall n \in \mathbb{N}, |\operatorname{Re}(u_n)| \leq |u_n| \leq M$. Donc $(\operatorname{Re}(u_n))_{n \in \mathbb{N}}$ est bornée. Donc, il existe $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ strictement croissante telle que $(\operatorname{Re}(u_{\varphi(n)}))$ converge.

$$\forall n \in \mathbb{N}, |\operatorname{Im}(u_{\varphi(n)})| \leq |u_{\varphi(n)}| \leq M$$

donc $(\operatorname{Im}(u_{\varphi(n)}))$ est bornée. Soit $\psi : \mathbb{N} \rightarrow \mathbb{N}$ strictement croissante telle que $(\operatorname{Im}(u_{\varphi(\psi(n))}))$ converge. Or, $(\operatorname{Re}(u_{\varphi(\psi(n))}))$ est une sous suite de la suite convergente $(\operatorname{Re}(u_{\varphi(n)}))$.

donc $(\operatorname{Re}(u_{\varphi(\psi(n))}))$ converge.

Donc, $(u_{\varphi(\psi(n))})$ converge.

Comme $\varphi \circ \psi$ est strictement croissante, $(u_{\varphi(\psi(n))})$ est une sous suite de (u_n)

□

8 Annexe

Proposition: Soit $f : I \rightarrow I$ continue et $(u_n)_{n \in \mathbb{N}}$ définie par

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

Si (u_n) converge vers $\ell \in \mathbb{R}$
alors $f(\ell) = \ell$ i.e. (ℓ est un point fixe de f)

Preuve:

On suppose que (u_n) converge vers ℓ .

$\lim_{n \rightarrow +\infty} u_{n+1} = \ell$ car (u_{n+1}) est une sous suite de (u_n) .

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

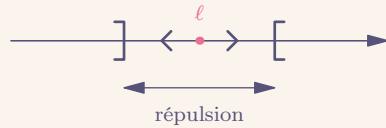
Comme f est continue alors $f(u_n) \xrightarrow{n \rightarrow +\infty} f(\ell)$. Par unicité de la limite, $\ell = f(\ell)$ \square

REMARQUE:

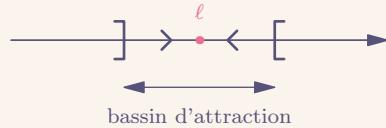
Soit $u \in \mathbb{R}^{\mathbb{N}}$ et $f : \mathbb{R} \rightarrow \mathbb{R}$ dérivable telle que $u_{n+1} = f(u_n)$.

Soit $\ell \in \mathbb{R}$ un point fixe de f . Donc, $f(\ell) = \ell$.

$|f'(\ell)| > 1$:



$|f'(\ell)| < 1$:



Par contre, si $|f'(\ell)| = 1$, on ne sait pas.

REMARQUE (Suite arithmético-géométrique):

$$(*) : \forall n \in \mathbb{N}, u_{n+1} = au_n + b = f(u_n)$$

MÉTHODE 1

— On cherche v une suite constante solution de $(*)$:

$$\exists C \in \mathbb{R}, \forall n \in \mathbb{N}, v_n = C$$

donc

$$\forall n \in \mathbb{N}, C = aC + b = f(C)$$

$$\text{Si } a \neq 1 : C = \frac{b}{1-a}$$

— Soit u qui vérifie $(*)$. On pose $w = u - v$.

$$\begin{aligned} \forall n \in \mathbb{N}, w_{n+1} &= u_{n+1} - v_{n+1} \\ &= au_n + b - av_n - b \\ &= a(u_n - v_n) \\ &= aw_n \end{aligned}$$

Donc $\forall n \in \mathbb{N}, w_{n+1} = aw_n + 0$: équation homogène associée à $(*)$
 (w_n) est géométrique donc

$$\forall n \in \mathbb{N}, w_n = w_0 a^n$$

et donc

$$\forall n \in \mathbb{N}, u_n = w_0 a^n + \frac{b}{1-a}$$

MÉTHODE 2

$$\begin{aligned}\varphi : \mathbb{R}^{\mathbb{N}} &\longrightarrow \mathbb{R}^{\mathbb{N}} \\ (u_n) &\longmapsto (u_{n+1} - au_n)\end{aligned}$$

φ morphisme de groupes additifs

$$\varphi(u) = (b) \iff u = v + w \text{ avec } w \in \text{Ker}(\varphi)$$

$$\begin{aligned}w \in \text{Ker}(\varphi) &\iff \varphi(w) = 0 \\ &\iff \forall n \in \mathbb{N}, w_{n+1} - aw_n = 0 \\ &\iff \forall n \in \mathbb{N}, w_{n+1} = aw_n\end{aligned}$$

CHAPITRE

12

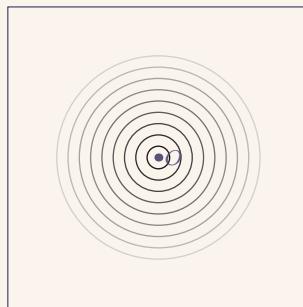
STRUCTURES ALGÉBRIQUES USUELLES

1 Groupes

Principe de symétrie (Pierre Curie)

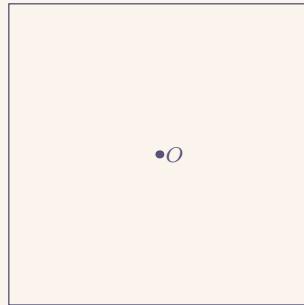
La symétrie des causes se retrouvent dans les effets.

On fait tomber un caillou dans un plan d'eau ce qui crée une onde qui se propage.

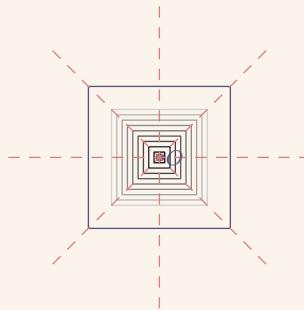
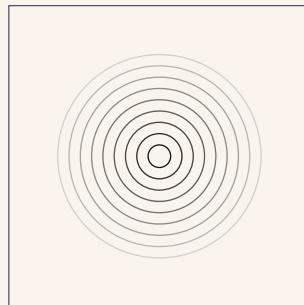


— Symétries des "causes"
(conserver O en place)

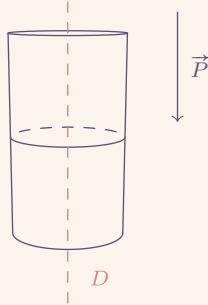
- translation de vecteur \vec{O}
- rotations de centre O d'angle quelconque
- symétries d'axe passant par O



- Symétries des "effets"
(conserver les ondes en place)
 - translation de vecteur $\vec{0}$
 - rotations de centre O d'angle quelconque
 - symétries d'axe passant par O



- translation de vecteur $\vec{0}$
- 4 rotations de centre O d'angle $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$
- 4 symétries axiales
- Causes
 - translations de vecteur $\vec{u} \in \vec{D}$
 - rotations d'axe D



— Effet



Définition: Soit G un ensemble, muni d'une loi de composition interne \diamond .
On dit que (G, \diamond) est un groupe si :

- \diamond est associative
- \diamond a un neutre $e \in G$
- $\forall x \in G, \exists y \in G, x \diamond y = y \diamond x = e$

EXEMPLE ((À connaître)): 1. E un ensemble. $S(E)$ l'ensemble des bijections de E dans E .
 $(S(E), \circ)$ est un groupe appelé groupe symétrique de E .

Si, $E = [[1, n]]$, alors noté $S(E)$ est noté S_n (ou parfois \mathfrak{S}_n)

2. $(\mathbb{Z}, +)$ est un groupe mais $(\mathbb{N}, +)$ n'est pas un groupe.
3. $(\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ sont des groupes
4. (\mathbb{R}, \times) n'est pas un groupe car 0 n'a pas d'inverse.
 $(\mathbb{Q}_*, \times), (\mathbb{R}_*, \times), (\mathbb{C}_*, \times)$ sont des groupes.
 (\mathbb{Z}_*, \times) n'est pas un groupe.
5. $(\mathcal{M}_n(\mathbb{C}), +)$ est un groupe
 $(\mathcal{M}_n(\mathbb{C}), \times)$ n'est pas un groupe

Définition: On dit que (G, \diamond) est un groupe commutatif ou abélien si c'est un groupe et \diamond est une loi commutative.

Définition: Soit (G, \cdot) un groupe (d'élément neutre e) et $H \subset G$. On dit que H est un sous groupe de G si

1. $\forall(x, y) \in H^2, x \cdot y \in H$
2. $e \in H$
3. $\forall x \in H, x^{-1} \in H$

Proposition: Soit H un sous groupe de (G, \cdot) . Alors, (H, \cdot) est un groupe.

□

Proposition: Soit (G, \cdot) un groupe et $H \subset G$.

$$H \text{ est un sous groupe de } G \iff \begin{cases} \forall (x, y) \in H, x \cdot y^{-1} \in H \\ H \neq \emptyset \end{cases}$$

Preuve: " \implies " $e \in H$ donc $H \neq \emptyset$.

Soit $(x, y) \in H^2$.

$y \in H$ donc $y^{-1} \in H$.

$x \in H$ donc $x \cdot y^{-1} \in H$.

" \iff " $H \neq \emptyset$.

Soit $a \in H$, $(a, a) \in H^2$ donc $a \cdot a^{-1} \in H$ donc $e \in H$.

Soit $x \in H$, $(e, x) \in H^2$ donc $e \cdot e^{-1} \in H$ donc $x^{-1} \in H$.

Soit $(x, y) \in H^2$. Comme $y \in H$, $y \in y^{-1} \in H$ donc $(x, y^{-1}) \in H^2$.

Donc, $x \cdot (y^{-1})^{-1} \in H$.

Donc, $x \cdot y \in H$.

□

EXEMPLE:

$2\mathbb{Z}$ est un sous groupe de $(\mathbb{Z}, +)$.

En effet,

— $2 \in 2\mathbb{Z}$ donc $2\mathbb{Z} \neq \emptyset$

— Soit $(x, y) \in (2\mathbb{Z})^2$, $\begin{cases} x \equiv 0 [2] \\ y \equiv 0 [2] \end{cases}$

donc $x - y \equiv 0 [2]$ donc $x - y \in 2\mathbb{Z}$

Proposition: Soit (G, \cdot) un groupe et $(H_i)_{i \in I}$ une famille non vide de sous groupes de G . Alors, $\bigcap_{i \in I} H_i$ est un sous groupe de G .

Preuve:

On sait que $\forall i \in I, e \in H_i$ et $I \neq \emptyset$

Donc, $e \in \bigcap_{i \in I} H_i$ donc $\bigcap_{i \in I} H_i \neq \emptyset$

Soit $(x, y) \in \left(\bigcap_{i \in I} H_i \right)^2$.

$$\forall i \in I, \begin{cases} x \in H_i \\ y \in H_i \end{cases}$$

donc,

$$\forall i \in I, x \cdot y^{-1} \in H_i$$

donc

$$x \cdot y^{-1} \in \bigcap_{i \in I} H_i$$

□

Proposition: Soit (G, \cdot) un groupe.
 $\{e\}$ et G sont des sous groupes de G

REMARQUE:

Une réunion de sous groupes n'est pas nécessairement un sous groupe.

$$(G, \cdot) = (\mathbb{Z}, +)$$

$$2\mathbb{Z} \cup 3\mathbb{Z} = A$$

$2 \in A$ et $3 \in A$ mais $2 + 3 = 5 \notin A$.

Donc, A n'est pas un sous groupe de \mathbb{Z}

Proposition – Définition: Soit (G, \cdot) un groupe et $A \subset G$. Alors,

$$\bigcap_{\substack{H \text{ sous groupe de } G \\ A \subset H}} H$$

est le plus petit (au sens de l'inclusion) sous groupe de G qui contient A . On dit que c'est le sous groupe engendré par A et on le note $\langle A \rangle$

Preuve:

On pose $\mathcal{G} = \{H \in \mathcal{P}(G) \mid H \text{ sous groupe contenant } A\}$.G ∈ \mathcal{G} donc $\mathcal{G} \neq \emptyset$ donc $\bigcap_{H \in \mathcal{G}} H$ est un sous groupe de G .Soit $a \in A$. Alors

$$\forall H \in \mathcal{G}, a \in A \subset H$$

et donc $a \in \bigcap_{H \in \mathcal{G}} H$.Donc, $A \subset \bigcap_{H \in \mathcal{G}} H$.Soit H un sous groupe de G qui contient A .Alors, $H \in \mathcal{G}$ alors $H \supset \bigcap_{H \in \mathcal{G}} H$

□

EXEMPLE:

$$(G, \cdot) = (\mathbb{Z}, +)$$

$$A = 2\mathbb{Z} \cup 3\mathbb{Z}$$

$$\langle A \rangle = \mathbb{Z}$$
 (d'après le théorème de Bézout).

On généralise $\langle a\mathbb{Z} \cup b\mathbb{Z} \rangle = (a \wedge b)\mathbb{Z}$

Définition: Soit (G, \cdot) un groupe et $A \subset G$.

On dit que A est une partie génératrice de G ou que A engendre G si $G = \langle A \rangle$

EXEMPLE (Rubik's cube):

EXEMPLE:

Soit (G, \cdot) un groupe.

- $\langle \emptyset \rangle = \{e\}$
- $\langle G \rangle = G$
- Soit $a \in G \setminus \{e\}$.
 $\langle a \rangle = \langle \{a\} \rangle = \{a^n \mid n \in \mathbb{Z}\}$
- Soit $a \neq b$ deux éléments de $G \setminus \{e\}$

$$\begin{aligned} \langle \{a, b\} \rangle &= \{x \in G \mid \exists n \in \mathbb{N}, \exists (a_1, a_2, \dots, a_n) \in \{a, b\}^n, \\ &\quad \exists (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) \in \{-1, 1\}^n, x = a_1^{\varepsilon_1} \times a_2^{\varepsilon_2} \times \dots \times a_n^{\varepsilon_n}\} \end{aligned}$$

REMARQUE (Notation):

Soit (G, \cdot) un groupe et $a \in G$.

Pour $n \in \mathbb{N}_*$, on pose $a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_{n \text{ fois}}$.

On pose $a^0 = e$ et pour $n \in \mathbb{Z}_*$,

$$a^n = (a^{-1})^{-n}$$

REMARQUE:

Si le groupe est noté additivement. On note na ($n \in \mathbb{Z}, a \in G$) à la place de a^n

Définition: On dit qu'un groupe (G, \cdot) est monogène s'il existe $a \in G$ tel que

$$G = \langle a \rangle$$

On dit alors que a est un générateur de G

EXEMPLE:

$(\mathbb{Z}, +)$ est engendré par 1.

$(2\mathbb{Z}, +)$ est engendré par 2

Définition: Un groupe monogène fini est cyclique.

Proposition: Soit (G, \cdot) un groupe monogène fini. Soit a un générateur de G . Il existe $k \in \mathbb{N}$ tel que

$$G = \{e, a, a^2, \dots, a^{k-1}\}$$

Preuve:

G est fini donc il existe $p < q$ tels que $a^p = a^q$. On a alors $e = a^{q-p}$.

On pose alors, $k = \min \{n \in \mathbb{N}_* \mid a^n = e\}$.

Soit $x \in G = \langle a \rangle$. Il existe $n \in \mathbb{Z}$ tel que $x = a^n$. On fait la division de n par k

$$\begin{cases} n = kq + r \\ q \in \mathbb{Z}, 0 \leq r < k \end{cases}$$

$$x = a^n = a^{kq+r} = (a^k)^q \times a^r = a^r$$

On a prouvé

$$G \subset \{e, a, \dots, a^{k-1}\}$$

On sait déjà que $\{e, a, \dots, a^{k-1}\} \subset G$. □

EXEMPLE:

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique :

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1}\}$$

Définition: Soit (G, \cdot) un groupe et $a \in G$. Si $\langle a \rangle$ est fini, le cardinal de $\langle a \rangle$ est appelé ordre de a : c'est le plus petit entier strictement positif n tel que $a^n = e$

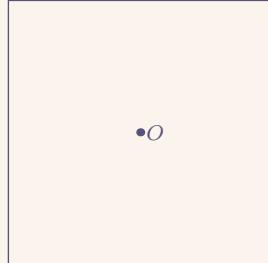
EXEMPLE:

$(S(\mathbb{C}_*), \circ)$ est un groupe
 $z \mapsto \bar{z}$ est d'ordre de 2
 $z \mapsto -z$ est d'ordre de 2
 $z \mapsto \frac{1}{z}$ est d'ordre de 2

EXEMPLE: — $G_1 = (\mathbb{U}_4, \times)$ où

$$\begin{aligned} \mathbb{U}_4 &= \{z \in \mathbb{C} \mid z^4 = 1\} \\ &= \{1, i, -1, -i\} \end{aligned}$$

$x \backslash y$	x	1	i	-1	$-i$
1	1	i	-1	$-i$	
i	i	-1	$-i$	1	
-1	-1	$-i$	1	i	
$-i$	$-i$	1	i	-1	



— G_2 l'ensemble des rotations planes qui laissent globalement invariant un carré.

$$G_2 = \left\{ id, \rho_{\frac{\pi}{2}}, \rho_{\pi}, \rho_{\frac{3\pi}{2}} \right\}$$

$y \backslash x$	x	id	$\rho_{\frac{\pi}{2}}$	ρ_{π}	$\rho_{\frac{3\pi}{2}}$
id	id	$\rho_{\frac{\pi}{2}}$	ρ_{π}	$\rho_{\frac{3\pi}{2}}$	
$\rho_{\frac{\pi}{2}}$	$\rho_{\frac{\pi}{2}}$	ρ_{π}	$\rho_{\frac{3\pi}{2}}$	id	
ρ_{π}	ρ_{π}	$\rho_{\frac{3\pi}{2}}$	id	$\rho_{\frac{\pi}{2}}$	
$\rho_{\frac{3\pi}{2}}$	$\rho_{\frac{3\pi}{2}}$	id	$\rho_{\frac{\pi}{2}}$	ρ_{π}	

—

$$G_3 = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$$

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$$

	$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\textcolor{orange}{0}, \textcolor{orange}{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\textcolor{orange}{0}, \textcolor{orange}{0})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\textcolor{orange}{0}, \textcolor{orange}{0})$	$(\bar{0}, \bar{1})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\textcolor{orange}{0}, \textcolor{orange}{0})$

Définition: Soient (G_1, \cdot) et $(G_2, *)$ deux groupes et $f : G_1 \rightarrow G_2$. On dit que f est un (homo)morphisme de groupes si

$$\forall (x, y) \in G_1, f(x \cdot y) = f(x) * f(y)$$

EXEMPLE:

$\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_*^+, \times)$ est un morphisme de groupes

Proposition: Avec les notations précédentes,

- l'image directe d'un sous groupe de G_1 est un sous groupe de G_2
- l'image réciproque d'un sous groupe de G_2 est un sous groupe de G_1

Preuve: — Soit H_1 un sous groupe de G_1 .

$e_1 \in H_1$ donc $f(e_1) \in f(H_1)$ donc $H_1 \neq \emptyset$ Soient $x \in f(H_1)$ et $y \in f(H_2)$.

On pose $\begin{cases} x = f(u) \text{ avec } u \in H_1 \\ y = f(v) \text{ avec } v \in H_1 \end{cases}$

$$\begin{aligned} x * y^{-1} &= f(u) * f(v)^{-1} \\ &= f(u) * f(v^{-1}) \\ &= f(u \cdot v^{-1}) \end{aligned}$$

$$\begin{cases} u \in H_1 \\ v \in H_1 \end{cases} \text{ donc } u \cdot v^{-1} \in H_1 \text{ donc } x * y^{-1} \in f(H_1)$$

— Soit H_2 un sous groupe de G_2 .

$$(x, y) \in f^{-1}(H_2)^2$$

$$\begin{aligned} x \cdot y^{-1} \in f^{-1}(H_2) &\iff f(x \cdot y^{-1}) \in H_2 \\ &\iff f(x) * f(y^{-1}) \in H_2 \\ &\iff f(x) * f(y)^{-1} \in H_2 \end{aligned}$$

Or, $\begin{cases} f(x) \in H_2 \\ f(y) \in H_2 \end{cases}$

Comme H_2 est un sous groupe de G_2 ,

$$f(x) * f(y)^{-1} \in H_2$$

et donc,

$$x \cdot y^{-1} \in f^{-1}(H_2)$$

□

Lemme:

$$\begin{cases} f(e_1) = e_2 \\ \forall u \in G_1, f(u^{-1}) = (f(u))^{-1} \end{cases}$$

Preuve:

$$f(e_1) = f(e_1 \cdot e_1) = f(e_1) * f(e_1)$$

On multiplie par $f(e_1)^{-1}$ (possible car G_2 est un groupe) et on trouve $f(e_1) = e_2$.
Soit $u \in G_1$.

$$f(u) * f(u^{-1}) = f(u \cdot u^{-1}) = f(e_1) = e_2$$

Donc, $f(u^{-1}) = (f(u))^{-1}$

□

Corollaire: Soit $f : (G_1, \cdot) \rightarrow (G_2, *)$ un morphisme de groupes. Alors, $\text{Im}(f)$ est un sous groupe de G_2 .

$$\text{Ker}(f) = \{x \in G_1 \mid f(x) = e_2\} = f^{-1}(\{e_2\})$$

est un sous groupe de G_1 .

□

Théorème: Avec les notations précédentes,

$$f \text{ injective} \iff \text{Ker}(f) = \{e_1\}$$

Preuve: " \implies " On suppose f injective.

$$\begin{aligned} f(e_1) = e_2 \text{ donc } e_1 \in \text{Ker}(f) \\ \text{donc } \{e_1\} \subset \text{Ker}(f) \end{aligned}$$

Soit $x \in \text{Ker}(f)$. On a alors $f(x) = e_2 = f(e_1)$

Comme f injective, $x = e_1$.

" \iff " On suppose $\text{Ker}(f) = \{e_1\}$

Soient $\begin{cases} x \in G_1 \\ y \in G_1 \end{cases}$. On suppose $f(x) = f(y)$

$$\begin{aligned} f(x) = f(y) &\implies f(x) * f(y)^{-1} = e_2 \\ &\implies f(x) * f(y^{-1}) = e_2 \\ &\implies f(x \cdot y^{-1}) && \implies x \cdot y^{-1} \in \text{Ker}(f) = \{e_1\} \\ &\implies x \cdot y^{-1} = e_1 \\ &\implies x = y \end{aligned}$$

Donc, f est injective

□

EXEMPLE ((équation diophantienne)):

$$\begin{cases} 2x + 5y = 1 \\ (x, y) \in \mathbb{Z}^2 \end{cases}$$

On trouve une solution particulière (Bézout) : $(-1, 1) = (x_0, y_0)$

$$\begin{aligned} 2x + 5y = 1 &\iff 2x + 5y = 2x_0 + 5y_0 \\ &\iff 2(x - x_0) + 5(y - y_0) = 0 \\ &\iff 2(x - x_0) = 5(y_0 - y) \end{aligned}$$

⋮
⋮ (Gauß)
⋮

$$\begin{aligned} f : \mathbb{Z}^2 &\longrightarrow \mathbb{Z} \\ (x, y) &\longmapsto 2x + 5y \end{aligned}$$

$(\mathbb{Z}^2, +)$ est un groupe avec $+$ qui est l'addition composante par composante.
 f est un morphisme de groupes.

$$\begin{aligned} f(x, y) = 1 = f(x_0, y_0) &\iff f(x, y) - f(x_0, y_0) = 0 \\ &\iff f(x - x_0, y - y_0) = 0 \\ &\iff (x - x_0, y - y_0) \in \text{Ker}(f) \end{aligned}$$

Théorème: Soit $f : (G_1, \cdot) \rightarrow (G_2, *)$ un morphisme de groupes, $y \in G_2$ et (\mathcal{E}) l'équation

$$f(x) = y$$

d'inconnue $x \in G_1$.

Si $y \notin \text{Im}(f)$, alors (\mathcal{E}) n'a pas de solution.

Sinon, soit $x_0 \in G_1$ tel que $f(x_0) = y$ (x_0 est une solution particulière de (\mathcal{E}))

$$f(x) = y \iff \exists h \in \text{Ker}(f), x = x_0 \cdot h$$

Preuve:

$$\begin{aligned} f(x) = y &\iff f(x) = f(x_0) \\ &\iff f(x_0)^{-1} * f(x) = e_2 \\ &\iff f(x_0^{-1}) * f(x) = e_2 \\ &\iff f(x_0^{-1} \cdot x) = e_2 \\ &\iff x_0^{-1} \cdot x \in \text{Ker}(f) \\ &\iff \exists h \in \text{Ker}(f), x_0^{-1} \cdot x = h \\ &\iff \exists h \in \text{Ker}(f), x = x_0 \cdot h \end{aligned}$$

□

Proposition: Soient $f : G_1 \rightarrow G_2$ et $g : G_2 \rightarrow G_3$ deux morphismes de groupes. Alors, $g \circ f$ est un morphisme de groupes.

Preuve:

Soient $x \in G_1$ et $y \in G_2$.

$$\begin{aligned} g \circ f(x \cdot y) &= g(f(x) * f(y)) = g(f(x)) \times g(f(y)) \\ &= g \circ f(x) \times g \circ f(y) \end{aligned}$$

□

Définition: Soit G un groupe.

- Un endomorphisme de G est un morphisme de groupes de G dans G .
- Un isomorphisme de G dans H un morphisme de groupes $f : G \rightarrow H$ bijectif.
- Un automorphisme de G est un endomorphisme de G bijectif.

Proposition: Soit $f : G \rightarrow H$ un isomorphisme de groupes.
Alors, $f^{-1} : H \rightarrow G$ est aussi un isomorphisme.

Preuve:

Soit $(x, y) \in H^2$. On pose $\begin{cases} f(u) = x, u \in G \\ f(v) = y, v \in G \end{cases}$

$$\begin{aligned} f(f^{-1}(x \cdot y^{-1})) &= x \cdot y^{-1} \\ &= f(u) \cdot f(v)^{-1} \\ &= f(u \cdot v^{-1}) \end{aligned}$$

Comme f injective,

$$f^{-1}(x \cdot y^{-1}) = u \cdot v^{-1} = f^{-1}(x)(f^{-1}(y))^{-1}$$

□

Corollaire: On note $\text{Aut}(G)$ l'ensemble des automorphismes de G .
 $\text{Aut}(G)$ est un sous groupe de $(S(G), \circ)$.

Définition: Soit (G, \cdot) un groupe et $g \in G$. L'application

$$\begin{aligned} c_g : G &\longrightarrow G \\ x &\longmapsto gxg^{-1} \end{aligned}$$

est appelée conjugaison par g . On dit aussi que c'est un automorphisme intérieur.

Proposition: Avec les notations précédentes,

$$c_g \in \text{Aut}(G)$$

Preuve:

Soient $x \in G$ et $y \in G$.

$$\begin{aligned} c_g(xy) &= g \cdot xy \cdot g^{-1} \\ c_g(x) \cdot c_g(y) &= gxg^{-1}gyg^{-1} = gxyg^{-1} = c_g(xy) \end{aligned}$$

Donc, c_g est un morphisme de groupes.

De plus,

$$\forall x \in G, c_{g^{-1}} \circ c_g(x) = g^{-1}(gxg^{-1}g) = x$$

Donc, $c_{g^{-1}} \circ c_g = id_G$.

De même, $c_g \circ c_{g^{-1}} = id_G$

Donc, c_g bijective et $(c_g)^{-1} = c_{g^{-1}}$

□

Corollaire:

$$\forall x \in G, \forall n \in \mathbb{Z}, c_g(x^n) = (c_g(x))^n$$

□

Proposition: L'application

$$\begin{aligned} G &\longrightarrow \text{Aut}(G) \\ g &\longmapsto c_g \end{aligned}$$

est un morphisme de groupes.

Preuve:

Soient $(g, h) \in G^2$.

$$\begin{aligned} \forall x \in G, c_g \circ c_h(x) &= g(hxh^{-1})g^{-1} \\ &= (gh)x(gh)^{-1} \\ &= c_{gh}(x) \end{aligned}$$

Donc, $c_g \circ c_h = c_{gh}$

□

Proposition (Rappel):

$$\forall g, h \in G, (gh)^{-1} = h^{-1}g^{-1}$$

Preuve:

$$(gh)(h^{-1}g^{-1}) = e$$

$$(h^{-1}g^{-1})(gh) = e$$

□

Proposition – Définition: Soient $(G_1, *)$ et $(G_2, *)$ deux groupes. On définit une loi sur $G_1 \times G_2$ en posant

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1, x_2 y_2)$$

Alors, $G_1 \times G_2$ est un groupe pour cette loi appelée **groupe produit**.

Preuve: — Soient $(x_1, y_1) \in G_1^2$ et $(x_2, y_2) \in G_2^2$.

On sait que $x_1 * y_1 \in G_1$ et que $x_2 * y_2 \in G_2$.

Donc, $(x_1, x_2) \cdot (y_1, y_2) = (x_1 x_2, y_1 y_2) \in G_1 \times G_2$

□

2 Anneaux

Définition: Un anneau $(A, +, \times)$ est un ensemble A muni de deux lois de compositions internes notées $+$ et \times vérifiant

1. $(A, +)$ est un groupe commutatif (son neutre est noté 0_A)
2. (A, \times) est un monoïde
 - (a) \times est associative
 - (b) \times a un neutre $1_A \in A$
3. distributivité à gauche et à droite :

$$\forall (a, b, c) \in A^3, \begin{cases} a \times (b + c) = (a \times b) + (a \times c) \\ (b + c) \times a = (b \times a) + (c \times a) \end{cases}$$

REMARQUE (Convention):

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

On convient que la multiplication est prioritaire sur l'addition.

$$(a \times b) + (a \times c) = a \times b + a \times c$$

et l'exponentiation est prioritaire sur la multiplication ($n \in \mathbb{N}$)

$$a \times b^n = a \times (\underbrace{b \times b \times \cdots \times b}_{n \text{ fois}}) \neq (a \times b)^n$$

Proposition: Soit $(A, +, \times)$ un anneau. Alors, 0_A est absorbant

$$\forall a \in A, a \times 0_A = 0_A \times a = 0_A$$

Preuve:

Soit $a \in A$. On pose $b = a \times 0_A \in A$.

$$\begin{aligned} b &= a \times 0_A = a \times (0_A + 0_A) = a \times 0_A + a \times 0_A \\ &= b + b (= 2b) \end{aligned}$$

Donc,

$$-b + b = -b + b + b$$

donc $0_A = b$

De même, $0_A \times a = 0_A$. □

REMARQUE:

On peut imaginer $\begin{cases} a \times b = 0_A \\ a \neq 0_A \\ b \neq 0_A \end{cases}$

EXEMPLE: — $(\mathbb{Z}/4\mathbb{Z}, +, \times)$ est un anneau

$$\begin{cases} \bar{2} \times \bar{2} = \bar{0} & \text{car } 4 \equiv 0 [4] \\ \bar{2} \neq \bar{0} & \text{car } 2 \not\equiv 0 [4] \end{cases}$$

— $(M_2(\mathbb{C}), +, \times)$ est un anneau (non commutatif)

$$\begin{aligned} A &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_A \\ A^2 &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

Définition: On dit qu'un anneau $(A, +, \times)$ est intègre si

$$\forall (a, b) \in A^2, (a \times b = 0_A \implies a = 0_A \text{ ou } b = 0_A)$$

EXEMPLE: — $(\mathbb{Z}, +, \times)$ est intègre

— $\forall p$ premier, $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est intègre (car tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible donc simplifiable)

EXEMPLE:

Soit $(A, +, \times)$ un anneau et $(a, b) \in A^2$.

$$\begin{aligned} (a + b)^2 &= (a + b) \times (a + b) \\ &= (a + b) \times a + (a + b) \times b \\ &= a^2 + b \times a + a \times b + b^2 \end{aligned}$$

Si a et b commutent, alors, $a \times b = b \times a$ et donc $(a + b)^2 = a^2 + b^2 + 2ab$

$$\begin{aligned} (a + b)^3 &= (a + b) \times (a + b) \times (a + b) \\ &= a^3 + a^2 \times b + a \times b \times a + b \times a^2 \\ &\quad + b^2 \times a + b \times a \times b + a \times b^2 + b^3 \end{aligned}$$

Si a et b commutent,

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Proposition: Soient $(A, +, \times)$ un anneau, $(a, b) \in A^2$, $n \in \mathbb{Z}$. Alors,

$$n(a \times b) = (na) \times b = a \times (nb)$$

Preuve: — Évident si $n = 0$

— On suppose $n > 0$.

$$\begin{aligned} n(a \times b) &= \underbrace{a \times b + \cdots + a \times b}_{n \text{ fois}} \\ &= \sum_{k=1}^n (a \times b) \\ &= a \times \sum_{k=1}^n = a \times (nb) \\ &= \left(\sum_{k=1}^n a \right) \times b = (na) \times b \end{aligned}$$

— On suppose $n < 0$. On pose $n = -p$ avec $p \in \mathbb{N}_*$.

$$\begin{aligned} n(a \times b) &= (-p)(a \times b) = -(p(a \times b)) \\ &= -((pa) \times b) = (-p)a \times b = (na) \times b \\ &= -(a \times (pb)) = a \times (-pb) = a \times (nb) \end{aligned}$$

En effet,

$$\forall (a', b') \in A^2 \quad (-a') \times b' + a' \times b' = (-a' + a') \times b' = 0_A \times b' = 0_A$$

$$\text{donc } - (a' \times b') = (-a') \times b'$$

□

Théorème (Formule du binôme de Newton): Soient $(A, +, \times)$ un anneau, $(a, b) \in A^2$, $n \in \mathbb{N}$.

Si a et b commutent alors

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

Preuve (par récurrence sur n):

□

Proposition: Soient $(A, +, \times)$ un anneau, $(a, b) \in A^2$ et $n \in \mathbb{N}_*$.

Si a et b commutent, alors

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

□

Proposition: On note A^\times l'ensemble des éléments inversibles d'un anneau $(A, +, \times)$. (A^\times, \times) est un groupe. □

EXEMPLE:

- $\mathbb{Z}^\times = \{-1, 1\}$
- $\mathcal{M}_n(\mathbb{C})^\times = GL_n(\mathbb{C})$
- $(\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}, \bar{3}\}$

Définition: Soit $(A, +, \times)$ un anneau commutatif.

1. Soient $(a, b) \in A^2$. On dit que a divide b s'il existe $k \in A$ tel que $b = a \times k$. On dit aussi que a est un diviseur de b et que b est un multiple de a .
2. On dit que a et b sont associés s'il existe $k \in A^\times$ tel que $ak = b$ (dans ce cas, $a \mid b$ et $b \mid a$)

REMARQUE:

Le théorème des deux carrés peut se démontrer en exploitant les propriétés arithmétiques de l'anneau $(\mathbb{Z}[i], +, \times)$ où $\mathbb{Z}[i] = \{a + ib \mid a \in \mathbb{Z}, b \in \mathbb{Z}\}$.
 $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$

Théorème des deux carrés :

1. Soit p un nombre premier.

$$\exists (a, b) \in \mathbb{N}^2, p = a^2 + b^2 \iff p \equiv 1 [4]$$

2. Soit $n \in \mathbb{N}_*$, $n = \prod_{p \in \mathcal{P}} p^{\alpha(p)}$

$$\exists (a, b) \in \mathbb{N}^2, n = a^2 + b^2 \iff \forall p \in \mathcal{P} \text{ tel que } \alpha(p) \neq 0, p \equiv 1 [4]$$

Définition: Soit $(A, +, \times)$ un anneau et $B \subset A$. On dit que B est un sous anneau de A si

1. B est un sous groupe de $(A, +)$
2. $\forall (a, b) \in B^2, a \times b \in B$
3. $1_A \in B$

EXEMPLE:

$\mathbb{Z}[i]$ est un sous anneau de $(\mathbb{C}, +, \times)$

Proposition: Soit $(A, +, \times)$ un anneau et B un sous anneau de A . Alors, $(B, +, \times)$ est un anneau. □

EXERCICE (Exercice à connaître):

Soit $(A, +, \times)$ un anneau. Le centre de A est

$$Z(A) = \{x \in A \mid \forall a \in A, a \times x = x \times a\}$$

$Z(A)$ est un sous anneau de A .

Proposition: Soit $(A, +, \times)$ un anneau.
Si $0_A = 1_A$ alors $A = \{0_A\}$. On dit alors que A est l'anneau nul.

Preuve:

Soit $a \in A$.

$$a = a \times 1_A = a \times 0_A = 0_A$$

□

Définition: Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux (les lois notés de la même façon mais ne sont pas forcément les mêmes!).

Soit $f : A \rightarrow B$. On dit que f est un (homo)morphisme d'anneaux si

1. $\forall (a, b) \in A^2, f(a + b) = f(a) + f(b)$
2. $\forall (a, b) \in A^2, f(a \times b) = f(a) \times f(b)$
3. $f(1_A) = 1_B$

Proposition: Avec les notations précédentes, si $a \in A^\times$ alors $f(a) \in B^\times$ et dans ce cas,

$$f(a)^{-1} = f(a^{-1})$$

Preuve:

On suppose $a \in A^\times$.

$$\begin{cases} f(a^{-1}) \times f(a) = f(a^{-1} \times a) = f(1_A) = 1_B \\ f(a) \times f(a^{-1}) = f(a \times a^{-1}) = f(1_A) = 1_B \end{cases}$$

Donc, $f(a) \in B^\times$ et $f(a)^{-1} = f(a^{-1})$

□

Définition: Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux et $f : A \rightarrow B$ un morphisme d'anneaux.

On dit que f est un

— isomorphisme d'anneaux si f est bijective

— endomorphisme d'anneaux si $\begin{cases} A = B \\ + = + \\ \times = \times \end{cases}$

— automorphisme d'anneaux si f est à la fois un isomorphisme et un endomorphisme d'anneaux

EXEMPLE: 1. Soit $a \in \mathbb{Z}$ et

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longmapsto ax \end{aligned}$$

f endomorphisme d'anneaux $\iff a = 1$

2.

$$\begin{aligned} f : \mathcal{M}_n(\mathbb{C}) &\longrightarrow \mathcal{M}_n(\mathbb{C}) \\ A &\longmapsto A^2 \end{aligned}$$

f n'est pas un morphisme d'anneaux car

$$(A + B)^2 \neq A^2 + B^2$$

3.

$$\begin{aligned} f : \mathbb{C} &\longrightarrow \mathbb{C} \\ z &\longmapsto \bar{z} \end{aligned}$$

est un automorphisme d'anneaux

4.

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{R} \\ x &\longmapsto x \end{aligned}$$

f est un morphisme d'anneaux mais ce n'est pas un endomorphisme.

5.

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ k &\longmapsto \bar{k} \end{aligned}$$

f est un morphisme d'anneaux surjectif.

Proposition: La composée de deux morphismes d'anneaux est un morphisme d'anneaux. \square

Proposition: La réciproque d'un isomorphisme d'anneaux est un isomorphisme d'anneaux. \square

Proposition: L'ensemble des automorphismes d'anneaux de A est un sous groupe de $(S(A), \circ)$. \square

Proposition: L'image directe ou réciproque d'un sous anneau par un morphisme d'anneaux est un sous anneaux.

Définition: Soit $f : A \rightarrow B$ un morphisme d'anneaux. Le noyau de f est

$$\text{Ker}(f) = \{a \in A \mid f(a) = 0_B\}$$

Proposition: Avec les notations précédents,

$$f \text{ injective} \iff \text{Ker}(f) = \{0_A\}$$

\square

REMARQUE:

$\text{Ker}(f)$ n'est pas un sous anneau en général (car $1_A \notin \text{Ker}(f)$ sauf si $A = \{0_A\}$)

Définition: Soit $(A, +, \times)$ un anneau et $a \in A \setminus \{0_A\}$.
On dit que a est un diviseur de zéro s'il existe $b \in A \setminus \{0_A\}$ tel que $a \times b = b \times a = 0_A$

Proposition: Les diviseurs de zéro ne sont pas inversibles. \square

EXEMPLE:

$A = \mathcal{M}_2(\mathbb{C})$

$M = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ est un diviseur de zéro

car $M \times M = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

3 Corps

EXEMPLE (Problème): — avec $A = \mathbb{Z}/9\mathbb{Z}$, résoudre $\bar{x}^2 = \bar{0}$

\bar{x}	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$
\bar{x}^2	$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{0}$	$\bar{7}$	$\bar{7}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{0}$

On a trouvé 3 solutions : $\bar{0}, \bar{3}, \bar{6}$.

— $\mathbb{Z}/8\mathbb{Z}$

\bar{x}	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
\bar{x}^2	$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{1}$

$\bar{x}^2 = \bar{7}$ a 4 solutions : $\bar{1}, \bar{7}, \bar{3}, \bar{5}$

— $A = \mathbb{H} = \{a + bi + cj + dk \mid (a, b, c, d) \in \mathbb{R}^4\}$
 $i^2 = j^2 = k^2 = -1$

$$\begin{array}{lll} ij = k & jk = i & ji = j \\ ji = -k & kj = -i & ik = -j \end{array}$$

Dans cet anneau, -1 a 6 racines !

Définition: Soit $(K, +, \times)$ un ensemble muni de deux lois de composition internes. On dit que c'est un corps si

1. (K, \times) est un groupe abélien
2. (K, \times) est un monoïde commutatif
3. $\forall x \in K \setminus \{0_K\}, \exists y \in K, xy = 1_K$
4. $0_K \neq 1_K$

EXEMPLE: — $(\mathbb{C}, +, \times)$ est un corps

— $(\mathbb{R}, +, \times)$ est un corps

— $(\mathbb{Q}, +, \times)$ est un corps

— $(\mathbb{Z}, +, \times)$ n'est pas un corps

Proposition: $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est premier.

Preuve:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \left\{ \bar{k} \mid k \wedge n = 1 \right\}$$

\square

Proposition: Tout corps est un anneau intègre.

Preuve:

Soit $(\mathbb{K}, +, \times)$ un corps. Soient $(a, b) \in \mathbb{K}^2$ tel que $a \times b = 0_{\mathbb{K}}$. On suppose $a \neq 0_{\mathbb{K}}$. Alors, a est inversible et donc

$$b = a^{-1} \times a \times b = a^{-1} \times 0_{\mathbb{K}} = 0_{\mathbb{K}}$$

□

EXEMPLE:

Soit $(\mathbb{K}, +, \times)$ un corps.

Résoudre

$$\begin{cases} x^2 = 1_{\mathbb{K}} \\ x \in \mathbb{K} \end{cases}$$

$$\begin{aligned} x^2 = 1_{\mathbb{K}} &\iff x^2 - 1_{\mathbb{K}} = 0_{\mathbb{K}} \\ &\iff (x - 1_{\mathbb{K}})(x + 1_{\mathbb{K}}) = 0_{\mathbb{K}} \\ &\iff x - 1_{\mathbb{K}} = 0_{\mathbb{K}} \text{ ou } x + 1_{\mathbb{K}} = 0_{\mathbb{K}} \\ &\iff x = 1_{\mathbb{K}} \text{ ou } x = -1_{\mathbb{K}} \end{aligned}$$

Il y a au plus 2 solutions.

Proposition: Soit $(\mathbb{K}, +, \times)$ un corps et P un polynôme à coefficients dans \mathbb{K} de degré n . Alors, l'équation $P(x) = 0_{\mathbb{K}}$ a au plus n solutions dans \mathbb{K} □

Corollaire ((Théorème de Wilson)): voir exercice 16 du TD 12

Définition: Soit $(\mathbb{K}, +, \times)$ un corps et $L \subset \mathbb{K}$.

On dit que L est un sous corps de \mathbb{K} si

1. L est un anneau de $(\mathbb{K}, +, \times)$ non nul
2. $\forall x \in L \setminus \{0_{\mathbb{K}}\}, x^{-1} \in L$

en d'autres termes si

1. $\forall (x, y) \in L^2, x - y \in L$
2. $\forall (x, y) \in L^2, x \times y^{-1} \in L$

On dit aussi que \mathbb{K} est une extension de L .

Proposition: Tout sous corps est un corps. □

Définition: Soient $(\mathbb{K}_1, +, \times)$ et $(\mathbb{K}_2, +, \times)$ deux corps et $f : \mathbb{K}_1 \rightarrow \mathbb{K}_2$. On dit que f est un morphisme de corps si f est un morphisme d'anneaux.

i.e. si

$$\begin{cases} \forall (x, y) \in \mathbb{K}_1^2, & f(x+y) = f(x) + f(y) \\ \forall (x, y) \in \mathbb{K}_1^2, & f(x \times y) = f(x) \times f(y) \end{cases}$$

Proposition: Tout morphisme de corps est injectif.

Preuve:

Soit $f : \mathbb{K}_1 \rightarrow \mathbb{K}_2$ un morphisme de corps.

- $\text{Ker}(f)$ est un sous groupe de $(\mathbb{K}_1, +)$
- Soit $x \in \text{Ker}(f)$ et $y \in \mathbb{K}_1$

$$f(x \times y) = f(x) \times f(y) = 0_{\mathbb{K}_2} \times f(y) = 0_{\mathbb{K}_2}$$

- Soit $x \in \text{Ker}(f) \setminus \{0_{\mathbb{K}_1}\}$.
Alors, x est inversible.

$$\left. \begin{array}{l} x \in \text{Ker}(f) \\ x^{-1} \in \mathbb{K}_1 \end{array} \right\} \text{donc } x \times x^{-1} \in \text{Ker}(f) \\ \text{donc } 1_{\mathbb{K}_1} \in \text{Ker}(f) \\ \text{donc } f(1_{\mathbb{K}_1}) = 0_{\mathbb{K}_2}$$

Or, $f(1_{\mathbb{K}_1}) = 1_{\mathbb{K}_2} \neq 0_{\mathbb{K}_2}$
Donc, $\text{Ker}(f) = \{0_{\mathbb{K}_1}\}$ donc f est injective. \square

EXEMPLE:

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \bar{z} \end{array} \text{ est un morphisme de corps}$$

4 Actions de groupes

Définition: Soit (G, \cdot) un groupe et X un ensemble non vide. Une action de G sur X est une application

$$\begin{aligned} \varphi : G \times X &\longrightarrow X \\ (g, x) &\longmapsto \underbrace{g \cdot x}_{\text{ce n'est pas la loi de } G} \end{aligned}$$

qui vérifie

1. $\forall x \in X, \varphi(e, x) = e \cdot x = x$
2. $\forall x \in X, \forall g, h \in G, g \cdot (h \cdot x) = (g \cdot h) \cdot x$

Dans ce cas, $\begin{array}{ccc} G & \longrightarrow & S(X) \\ g & \longmapsto & \varphi(g, \cdot) \end{array} : \begin{array}{ccc} X & \longrightarrow & X \\ x & \longmapsto & g \cdot x \end{array}$ est un morphisme de groupes.

Preuve:
 $\forall g \in G (x \mapsto g \cdot x)^{-1} =$ \square

5 Bilan

Groupe	Sous-groupe engendré
<p>On dit que (G, \diamond) est un groupe si</p> <ul style="list-style-type: none"> — \diamond est associative; — \diamond a un neutre $e \in G$; — tout élément $x \in E$ a un inverse $y \in E$: $x \diamond y = y \diamond x = e.$	<p>Le sous-groupe engendré par A, $\langle A \rangle$, est le plus petit sous groupe de G contenant A.</p> <p>S'il existe $a \in G$ tel que $G = \langle a \rangle$, on dit que G est monogène et a est un générateur de G.</p> <p>Soit $a \in G$. L'ordre de a est $\#\langle a \rangle$ i.e. $a^n = e$.</p>
<p>On dit que $H \subset G$ est un sous-groupe de G si</p> <ul style="list-style-type: none"> — $e \in H$; — $\forall x, y \in H, x \diamond y \in H$; — $\forall x \in H, x^{-1} \in H$. 	
<p>Si \diamond est commutative, on dit que (G, \diamond) est un groupe commutatif ou abélien.</p>	
<p>Pour montrer que H est un sous-groupe de G, on montre</p> <ul style="list-style-type: none"> — $H \neq \emptyset$; — $\forall x, y \in H, x \diamond y^{-1} \in H$. 	<p>Soit $f : G_1 \rightarrow G_2$ où (G_1, \cdot) et (G_2, \times) sont des groupes. f est un morphisme de groupes si</p> $\forall x, y \in G_1, f(x \cdot y) = f(x) \times f(y).$ <p>L'image directe d'un sous-groupe de G_1 est un sous-groupe de G_2. L'image réciproque d'un sous-groupe de G_2 est un sous-groupe de G_1.</p> $\forall u \in G_1; f(u^{-1}) = f(u)^{-1}.$
<p>L'intersection de sous-groupes est un sous-groupe. Attention, l'union de sous-groupes n'est pas forcément un sous-groupe.</p>	<p>f injective $\iff \text{Ker } f = \{e_1\}$.</p>

CHAPITRE

13

SYSTÈMES LINÉAIRES ET CALCULS MATRICIELS

EXEMPLE:

$$(S_1) : \left\{ \begin{array}{rcl} \text{pivot} \\ \boxed{x} & +y & +z & -t & = 1 \\ x & +2y & +3z & +t & = 0 \\ x & & +z & = 2 \end{array} \right.$$

$$\xrightarrow{\quad L_2 \leftarrow L_2 - L_1 \quad} \left\{ \begin{array}{rcl} \boxed{x} & +y & +z & -t & = 1 \\ y & +2z & +3z & +t & = -1 \\ & & & & \end{array} \right.$$

$$\xrightarrow{\quad L_3 \leftarrow L_3 - L_1 \quad} \left\{ \begin{array}{rcl} \boxed{x} & -z & -3t & = 2 \\ \boxed{y} & +2z & +2t & = -1 \\ 2z & +3z & +3t & = 0 \end{array} \right.$$

$$\xrightarrow{\quad L_1 \leftarrow L_1 - L_2 \quad} \left\{ \begin{array}{rcl} \boxed{x} + z & = 2 \\ \boxed{y} + \frac{2}{3}z & = -1 \\ 3t + 2z & = 0 \end{array} \right. \qquad \xrightarrow{\quad \begin{array}{l} x = 2 - z \\ y = -1 - \frac{2}{3}z \\ t = -\frac{2}{3}z \end{array} \quad}$$

L'ensemble des solutions est

$$\left\{ \left(2 - z, -1 - \frac{2}{3}z, z, -\frac{2}{3}z \right) \mid z \in \mathbb{K} \right\}$$

$$\begin{aligned}
 & \left\{ \begin{array}{l} x + y + z - t = 1 \\ x + 2y + 3z + t = 0 \\ x + \boxed{z} = 2 \end{array} \right. \\
 \iff & \begin{array}{l} L_1 \leftarrow L_1 - L_3 \\ L_2 \leftarrow L_2 - 3L_3 \end{array} \quad \left\{ \begin{array}{l} \boxed{y} - t = -1 \\ -2x + 2y + t = -6 \\ x + \boxed{z} = 2 \end{array} \right. \\
 \iff & L_2 \leftarrow \frac{L_2 - 2L_1}{-2} \quad \left\{ \begin{array}{l} \boxed{y} - t = -1 \\ \boxed{x} - \frac{3}{2}t = 2 \\ x + \boxed{z} = 2 \end{array} \right. \\
 \iff & L_3 \leftarrow L_3 - L_2 \quad \left\{ \begin{array}{l} \boxed{y} - t = -1 \\ \boxed{x} - \frac{3}{2}t = 2 \\ \boxed{z} + \frac{3}{2}t = 0 \end{array} \right. \\
 \iff & \left\{ \begin{array}{l} y = -1 + t \\ x = 2 + \frac{3}{2}t \\ z = -\frac{3}{2}t \end{array} \right.
 \end{aligned}$$

$$\begin{aligned}
 \mathcal{S} &= \left\{ \left(2 + \frac{3}{2}t, -1 + t, -\frac{3}{2}t, t \mid t \in \mathbb{K} \right) \right\} \\
 &= \left\{ \underbrace{(2, -1, 0, 0)}_A + t \underbrace{\left(\frac{3}{2}, 1, -\frac{3}{2}, 1 \right)}_u \mid t \in \mathbb{K} \right\}
 \end{aligned}$$

EXAMPLE:

$$\begin{aligned}
 & \left\{ \begin{array}{l} x + y + z = 0 \\ x - y + z = 1 \\ 2x - y + z = 2 \\ x - y - z = 3 \\ y + 3z = 1 \end{array} \right. \\
 \iff & L_2 \leftarrow \frac{L_2 - L_1}{-2} \quad \left\{ \begin{array}{l} \boxed{x} + y + z = 0 \\ \boxed{y} = \frac{1}{2} \\ -3y - z = 2 \\ -2y - 2z = 3 \\ y + 3z = 1 \end{array} \right. \\
 & L_3 \leftarrow L_3 - 2L_1 \quad \left. \begin{array}{l} \boxed{x} + z = \frac{1}{2} \\ \boxed{y} = -\frac{1}{2} \\ \boxed{z} = -\frac{1}{2} \\ -2z = 2 \\ 3z = \frac{3}{2} \end{array} \right. \\
 & L_4 \leftarrow L_4 - L_1 \quad \left. \begin{array}{l} \boxed{x} = 1 \\ \boxed{y} = -\frac{1}{2} \\ \boxed{z} = -\frac{1}{2} \\ 0 = 1 \\ 0 = 3 \end{array} \right. \text{ incompatibilité} \\
 \iff & L_1 \leftarrow L_1 - L_2 \quad \left. \begin{array}{l} \boxed{x} = 1 \\ \boxed{y} = -\frac{1}{2} \\ \boxed{z} = -\frac{1}{2} \\ 0 = 1 \\ 0 = 3 \end{array} \right. \text{ incompatibilité} \\
 & L_3 \leftarrow (L_3 - 3L_2) \\
 & L_4 \leftarrow L_4 + 3L_2 \\
 & L_5 \leftarrow L_5 - L_2
 \end{aligned}$$

Il n'y a pas de solution !

EXEMPLE:

$$\begin{aligned}
 (S_2) : & \left\{ \begin{array}{l} \boxed{x} + y - z = 1 \\ y + z = 0 \\ x + 2y = 0 \end{array} \right. \\
 \iff & L_3 \leftarrow L_3 - L_1 \quad (S'_2) : \left\{ \begin{array}{l} \boxed{x} + y - z = 1 \\ \boxed{y} + z = 0 \\ y + z = -1 \end{array} \right. \\
 \iff & L_1 \leftarrow L_1 - L_2 \quad \left. \begin{array}{l} \boxed{x} - 2z = 1 \\ \boxed{y} + z = 0 \\ 0 = -1 \end{array} \right.
 \end{aligned}$$

EXEMPLE:

$$\begin{aligned}
 (S_1) \iff & \underbrace{\begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 2 & -1 & 1 \\ 1 & -1 & -1 \\ 0 & 1 & 3 \end{pmatrix}}_A \underbrace{\begin{pmatrix} x \\ y \\ z \end{pmatrix}}_X = \underbrace{\begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 1 \end{pmatrix}}_B \\
 \iff & AX = B
 \end{aligned}$$

$$(S_2) \iff \underbrace{\begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & 1 \\ 1 & 2 & 0 \end{pmatrix}}_A \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

$$(S'_2) \iff \underbrace{\begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}}_{A'} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & 1 \\ 1 & 2 & 0 \end{pmatrix}}_A = \underbrace{\begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}}_{A'}$$

$$\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}}_{\in \mathrm{GL}_3(\mathbb{K})} \underbrace{\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix}}_{\in \mathrm{GL}_3(\mathbb{K})} A = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

$$A \in \mathrm{GL}_3(\mathbb{K}) \iff \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{K})$$

EXEMPLE:

$$A = \begin{pmatrix} \boxed{1} & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

$$\begin{aligned} A &\xrightarrow{\sim} C_3 \leftarrow C_3 - C_1 \quad \begin{pmatrix} \boxed{1} & 0 & 0 \\ 0 & 1 & 1 \\ 0 & \boxed{1} & -1 \end{pmatrix} \\ &\xrightarrow{\sim} C_1 \leftarrow C_1 - C_2 \quad \begin{pmatrix} \boxed{1} & 0 & 0 \\ -1 & 1 & \boxed{1} \\ 0 & \boxed{1} & 0 \end{pmatrix} \\ &\quad C_3 \leftarrow \frac{C_3 - C_2}{2} \\ &\xrightarrow{\sim} C_1 \leftarrow C_1 + C_3 \quad \begin{pmatrix} \boxed{1} & 0 & 0 \\ 0 & 0 & \boxed{1} \\ 0 & \boxed{1} & 0 \end{pmatrix} \\ &\quad C_2 \leftarrow C_2 - C_3 \\ &\xrightarrow{\sim} C_2 \leftrightarrow C_3 \quad I_3 \end{aligned}$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & -1 \end{pmatrix}$$

$$I_3 = A \underbrace{\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & -1 & 1 \end{pmatrix}}_{B} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

$A \in \mathrm{GL}_3(\mathbb{K})$ et $A^{-1} = I_3 \times B$

$$\begin{aligned} C_3 &\xleftarrow{\sim} C_3 - C_1 \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ C_1 &\xleftarrow{\sim} C_1 - C_2 \quad \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ C_3 &\xleftarrow{\sim} \frac{C_3 + C_2}{2} \quad \begin{pmatrix} 1 & 0 & -\frac{1}{2} \\ -1 & 1 & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} \end{pmatrix} \\ C_1 &\xleftarrow{\sim} C_1 + C_3 \quad \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix} \\ C_2 &\xleftarrow{\sim} C_2 - C_3 \quad \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{pmatrix} \\ C_2 &\xleftarrow{\sim} C_3 \quad \underbrace{\begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{pmatrix}}_{A^{-1}} \end{aligned}$$

REMARQUE (Résumé): — Méthode du pivot : opérations sur les lignes :

1. $L_i \leftarrow L_i + \lambda L_j$ ($\lambda \in \mathbb{K}$)
2. $L_i \leftarrow \mu L_i$ ($\mu \in \mathbb{K} \setminus \{0\}$)
3. $L_i \leftrightarrow L_j$

En appliquant la méthode du pivot on obtient

$$(S) \iff \begin{cases} x_{i_1} &= \ell_1(x_{j_1}, \dots, x_{j_{n-r}}) \\ x_{i_2} &= \ell_2(x_{j_1}, \dots, x_{j_{n-r}}) \\ \vdots &\vdots \\ x_{i_r} &= \ell_r(x_{j_1}, \dots, x_{j_{n-r}}) \\ 0 &= * \end{cases}$$

Les inconnues x_{i_1}, \dots, x_{i_r} sont les inconnues principales, les autres sont appelées paramètre.

On peut supprimer les équations $0 = 0$. S'il y a une équation $0 = \lambda$ avec $\lambda \neq 0$, il n'y a pas de solution : le système est incompatible.

Les inconnues principales dépendent des choix de pivots !

— Représentation matricielle

$$(S) \iff AX = B$$

où A est la matrice du système, $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$ et B est le second membre

(S) a n équations et p inconnues donc A a n lignes et p colonnes.

La matrice $(A | B)$ est la matrice augmentée du système.

- Faire un opération L sur les lignes d'une matrice M revient à multiplier M à gauche par une matrice R où R est obtenue en appliquant L sur I_n .
- La méthode du pivot matriciel par lignes :

EXEMPLE:

$$A = \begin{pmatrix} 5 & 1 & 4 & 4 \\ 2 & 1 & 0 & 0 \\ 7 & 2 & 3 & 4 \end{pmatrix}$$

$$\begin{array}{l} \left(\begin{array}{cccc} 5 & 1 & 3 & 4 \\ 2 & 1 & 0 & 0 \\ 7 & 2 & 3 & 4 \end{array} \right) \quad L_2 \leftarrow L_2 - L_1 \quad \sim \quad \left(\begin{array}{cccc} 5 & 1 & 3 & 4 \\ -3 & 0 & -3 & -4 \\ -3 & 0 & -3 & -4 \end{array} \right) \\ L_3 \leftarrow L_3 - 2L_1 \\ \\ L_2 \leftarrow -\frac{1}{3}L_2 \quad \sim \quad \left(\begin{array}{cccc} 5 & 1 & 3 & 4 \\ 1 & 0 & 1 & \frac{4}{3} \\ -3 & 0 & -3 & -4 \end{array} \right) \\ \\ L_1 \leftarrow L_1 - 5L_2 \quad \sim \quad \left(\begin{array}{cccc} 0 & 1 & -2 & -\frac{8}{3} \\ 1 & 0 & 1 & \frac{4}{3} \\ 0 & 0 & 0 & 0 \end{array} \right) \\ L_3 \leftarrow L_3 + 3L_2 \\ \\ L_1 \leftrightarrow L_2 \quad \sim \quad \left(\begin{array}{cccc} 1 & 0 & 1 & \frac{4}{3} \\ 0 & 1 & -2 & -\frac{8}{3} \\ 0 & 0 & 0 & 0 \end{array} \right) \end{array}$$

matrice échelonnée réduite par lignes

Définition (Rang d'une matrice): Soit M une matrice et R la matrice échelonnée réduite par lignes associée à M . Le nombre de lignes non nulles de R (le nombre de pivots) est appelée rang de M .

Soit S un système de matrice augmentée $(A | B)$. Le rang de S est le rang de la matrice A .

Le rang est noté rg.

Proposition (Interprétation):

- Soit S un système de n équations, p inconnues de rang r .
- r est le nombre d'inconnues principales, il y a $p - r$ paramètres.
- Soit $M \in \mathcal{M}_{n,p}(\mathbb{K})$ de rang r .
- r est le nombre de lignes indépendantes : il y a $n - r$ lignes combinaisons linéaires des r lignes indépendantes.

Corollaire: Soit S un système de n équations, p inconnues de rang n . Alors S a au moins une solution.

Si $n = p$ alors S a exactement une solution.

Si $p > n$, il y a une infinité de solutions.

□

Définition: Soit S un système à n équations, n inconnues et de rang n . On dit que S est un système de Cramer (il a une unique solution)

Proposition: Soit S un système de n équations, p inconnues de rang r .

- Si $r < n$ alors le système peut-être incompatible : il y a $n - r$ équations de la forme $0 = *$ après la méthode du pivot.
- Si $r < p$ alors il y a $p - r$ paramètres : si le système n'est pas incompatible, il y aura une infinité de solutions.

□

EXEMPLE:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\begin{array}{l} \left(\begin{array}{ccc} 1 & 2 & 3 \\ 5 & 1 & 2 \\ 1 & 1 & 1 \end{array} \right) \quad L_1 \xrightarrow{\sim} L_1 - 2L_2 \quad \left(\begin{array}{ccc} -9 & 0 & -1 \\ 5 & 1 & 2 \\ 4 & 0 & 1 \end{array} \right) \\ \qquad \qquad \qquad L_3 \xrightarrow{\sim} L_3 + L_2 \quad \left(\begin{array}{ccc} -9 & 0 & -1 \\ 5 & 1 & 2 \\ 4 & 0 & 1 \end{array} \right) \\ \qquad \qquad \qquad L_1 \xrightarrow{\sim} L_1 + L_3 \quad \left(\begin{array}{ccc} -5 & 0 & 0 \\ 5 & 1 & 2 \\ 4 & 0 & 1 \end{array} \right) \\ \qquad \qquad \qquad L_1 \xrightarrow{\sim} -L_1/5 \quad \left(\begin{array}{ccc} 1 & 0 & 0 \\ 5 & 1 & 2 \\ 4 & 0 & 1 \end{array} \right) \\ \qquad \qquad \qquad L_2 \xrightarrow{\sim} L_2 - 5L_1 \quad \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right) \\ \qquad \qquad \qquad L_3 \xrightarrow{\sim} L_3 - 4L_1 \\ \qquad \qquad \qquad L_2 \xrightarrow{\sim} L_2 + 2L_3 \end{array}$$

EXEMPLE:

$$(S) : \begin{cases} x + y + z + t = 1 \\ x - y + z + 2t = 0 \\ 2y - t = 1 \\ 2x + 2z + 3t = 1 \end{cases}$$

$$\begin{array}{ll} \left\{ \begin{array}{l} \boxed{x} + y + z + t = 1 \\ x - y + z + 2t = 0 \\ 2y - t = 1 \\ 2x + 2z + 3t = 1 \end{array} \right. & \iff \left\{ \begin{array}{l} \boxed{x} + y + z + t = 1 \\ -2y + \boxed{t} = -1 \\ 2y - t = 1 \\ -2y + t = -1 \end{array} \right. \\ & \iff \left\{ \begin{array}{l} \boxed{x} + y + z + t = 1 \\ -2y + \boxed{t} = -1 \\ 0 = 0 \\ 0 = 0 \end{array} \right. \quad \text{Système triangulaire} \\ & \iff \left\{ \begin{array}{l} t = -1 + 2y \\ x = 2 - 3y - z \end{array} \right. \end{array}$$

La matrice du système triangulaire est

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & -2 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Elle n'est pas échelonnée réduite par lignes !

Proposition: Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et C une opération élémentaire sur les colonnes de A . On pose A' la matrice obtenue en appliquant C sur les colonnes de A .

$$\text{rg}(A) = \text{rg}(A')$$

□

EXEMPLE:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\begin{array}{l} \left(\begin{array}{ccc} 1 & 2 & 3 \\ 5 & 1 & 2 \\ 1 & 1 & 1 \end{array} \right) \xrightarrow{\sim} C_2 \leftarrow C_2 - C_1 \quad \left(\begin{array}{ccc} 1 & 1 & 2 \\ 5 & -4 & -3 \\ 1 & 0 & 0 \end{array} \right) \\ \qquad \qquad \qquad C_3 \leftarrow C_3 - C_1 \\ \qquad \qquad \qquad \left(\begin{array}{ccc} 1 & 1 & 0 \\ 5 & -4 & 5 \\ 1 & 0 & 0 \end{array} \right) \xrightarrow{\sim} C_3 \leftarrow C_3 - 2C_2 \quad \left(\begin{array}{ccc} 1 & 1 & 0 \\ 5 & -4 & 0 \\ 1 & 0 & 0 \end{array} \right) \end{array}$$

Donc $\text{rg}(A) = 3$

EXEMPLE:

$$\text{rg} \left(\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \right) = 1$$

Proposition: Le rang d'une matrice est aussi le nombre de colonnes indépendantes.

□

Définition: Une matrice triangulaire supérieure est une matrice carrée avec des coefficients nuls sous sa diagonale :

$$T = \begin{pmatrix} * & & & \\ 0 & * & & \\ 0 & 0 & * & \\ \vdots & \vdots & \ddots & * \end{pmatrix}$$

et triangulaire inférieure si les coefficients au-dessus de la diagonale sont nuls :

$$T = \begin{pmatrix} * & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ * & \dots & \dots & 0 \end{pmatrix}$$

Un système triangulaire est de la forme

$$\left\{ \begin{array}{ccccccc} a_{11}x_1 & +a_{12}x_2 & +\dots & +a_{1p}x_p & = & b_1 & +\dots \\ & +a_{22}x_2 & +\dots & +a_{2p}x_p & = & b_2 & +\dots \\ & & \ddots & & & \vdots & \\ & & & a_{pp}x_p & = & b_p & +\dots \\ & & & 0 & = & \dots & \end{array} \right.$$

REMARQUE:

$$(S) \iff \begin{cases} AX = B \\ X \in \mathcal{M}_{p,1}(\mathbb{K}), B \in \mathcal{M}_{n,1}(\mathbb{K}), A \in \mathcal{M}_{n,p}(\mathbb{K}) \end{cases}$$

On pose

$$\begin{aligned} \varphi : \mathcal{M}_{p,1}(\mathbb{K}) &\longrightarrow \mathcal{M}_{n,1}(\mathbb{K}) \\ X &\longmapsto AX \end{aligned}$$

On cherche $\varphi^{-1}(\{B\})$

On sait que

— $(\mathcal{M}_{p,1}(\mathbb{K}), +)$ est un groupe

— $(\mathcal{M}_{n,1}(\mathbb{K}), +)$ aussi

Soient $X, Y \in \mathcal{M}_{p,1}(\mathbb{K})$

$$\varphi(X + Y) = A(X + Y) = AX + AY = \varphi(X) + \varphi(Y)$$

Donc φ est un morphisme de groupes.

On peut résoudre (S) de la façon suivante :

- On cherche $X_0 \in \mathcal{M}_{p,1}(\mathbb{K})$ tel que $\varphi(X_0) = B$
- On résout $\varphi(X) = 0$ ($X \in \text{Ker}(\varphi)$)

C'est le système homogène associé :

$$\varphi(X) = B \iff \exists H \in \text{Ker}(\varphi), X = X_0 + H$$

Proposition:

$$A = (a_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} \in \mathcal{M}_{n,p}(\mathbb{K})$$

$$B = (b_{k,\ell})_{\substack{1 \leq k \leq p \\ 1 \leq \ell \leq q}} \in \mathcal{M}_{p,q}(\mathbb{K})$$

$$AB = (c_{i,\ell})_{\substack{1 \leq i \leq n \\ 1 \leq \ell \leq q}} \in \mathcal{M}_{n,q}(\mathbb{K})$$

$$c_{i,\ell} = \sum_{j=1}^n a_{i,j} b_{j,\ell}$$

CHAPITRE

14

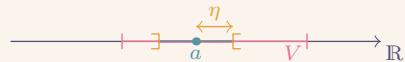
CONTINUITÉ

1 Définition d'une limite de fonctions

Définition: Soit $a \in \overline{\mathbb{R}} = \mathbb{R} \cup \{+\infty, -\infty\}$ et $V \in \mathcal{P}(\mathbb{R})$.

- Si $a \in \mathbb{R}$, on dit que V est un voisinage si

$$\exists \eta > 0,]a - \eta, a + \eta[\subset V.$$



- Si $a = +\infty$, on dit que V est un voisinage de a si

$$\exists M \in \mathbb{R},]M, +\infty[\subset V.$$

- Si $a = -\infty$, on dit que V est un voisinage de a si

$$\exists m \in \mathbb{R},]-\infty, m[\subset V.$$

On note \mathcal{V}_a l'ensemble des voisinages de a .

L'utilisation des voisinages permet d'exprimer une limite finie ou infinie plus simplement, sans disjonction de cas.

EXEMPLE:

Soit $u \in \mathbb{R}^{\mathbb{N}}$ de limite $a \in \overline{\mathbb{R}}$.

- Si $a \in \mathbb{R}$,

$$\begin{aligned} \forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, |u_n - a| \leq \varepsilon \\ \text{i.e. } \forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, a - \varepsilon \leq u_n \leq a + \varepsilon \\ \text{i.e. } \forall V \in \mathcal{V}_a, \exists N \in \mathbb{N}, \forall n \geq N, u_n \in V. \end{aligned}$$

— Si $a = +\infty$,

$$\begin{aligned} & \forall M \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \geq N, u_n \geq M \\ & \text{i.e. } \forall M \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \geq N, u_n \in [M, +\infty[\\ & \text{i.e. } \forall V \in \mathcal{V}_a, \exists N \in \mathbb{N}, \forall n \geq N, u_n \in V. \end{aligned}$$

— Si $a = -\infty$,

$$\begin{aligned} & \forall m \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \geq N, u_n \leq m \\ & \text{i.e. } \forall m \in \mathbb{R}, \exists N \in \mathbb{N}, \forall n \geq N, u_n \in]-\infty, m] \\ & \text{i.e. } \forall V \in \mathcal{V}_a, \exists N \in \mathbb{N}, \forall n \geq N, u_n \in V. \end{aligned}$$

Même si, dans chacun des cas, la définition de limite de la suite u est différente, en utilisant les voisinages, la notation est identique :

$$\forall V \in \mathcal{V}_a, \exists N \in \mathbb{N}, \forall n \geq N, u_n \in V.$$

En utilisant cette nouvelle notation, on peut redéfinir la limite plus simplement.

Définition: Soit f une fonction définie sur $D \subset \mathbb{R}$ à valeurs réelles. Soit $a \in \overline{D} = \{x \in \overline{\mathbb{R}} \mid \forall V \in \mathcal{V}_x, V \cap D \neq \emptyset\}$ (on “rajoute” chacune des bornes exclues des intervalles composant D) :

On dit que $f(x)$ tends vers ℓ si

$$\forall V \in \mathcal{V}_\ell, \exists W \in \mathcal{V}_a, \forall x \in W \cap D, f(x) \in V.$$

EXEMPLE:

Soit $f : \mathbb{R} \rightarrow \mathbb{R}$ telle que $f(x) \xrightarrow{x \rightarrow -1} 1$.

$$\forall V \in \mathcal{V}_1, \exists W \in \mathcal{V}_{-1}, \forall x \in W \cap D, f(x) \in V$$

donc

$$\forall \varepsilon > 0, \exists \eta > 0, \forall x \in]-1 - \eta, -1 + \eta[, f(x) \in [1 - \varepsilon, 1 + \varepsilon[$$

i.e.

$$\forall \varepsilon > 0, \exists \eta > 0, \forall x \in \mathbb{R}, (|x - (-1)| < \eta \implies |f(x) - 1| \leq \varepsilon).$$

Si $f(x) \xrightarrow{x \rightarrow -\infty} +\infty$,

$$\forall V \in \mathcal{V}_{+\infty}, \exists W \in \mathcal{V}_{-\infty}, \forall x \in W, f(x) \in V$$

i.e.

$$\forall M \in \mathbb{R}, \exists m \in \mathbb{R}, \forall x \in]-\infty, m], f(x) \in [M, +\infty[$$

i.e.

$$\forall M \in \mathbb{R}, \exists m \in \mathbb{R}, \forall x \in \mathbb{R}, (x \leq m \implies f(x) \geq M).$$

Définition: Soit $a \in \mathbb{R}$.

Un voisinage à gauche de a est une partie de \mathbb{R} qui contient un intervalle $]a - \eta, a]$ avec $\eta > 0$.

Un voisinage à droite de a est une partie de \mathbb{R} qui contient un intervalle $[a, a + \eta[$ avec $\eta > 0$.

EXEMPLE:

$$\text{Soit } f : x \mapsto \begin{cases} \frac{1}{x} & \text{si } x \neq 0, \\ 0 & \text{si } x = 0. \end{cases}$$

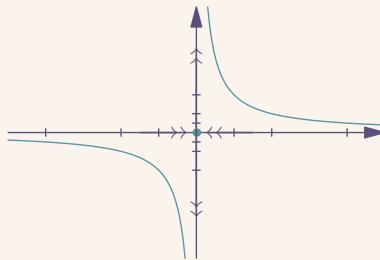
1. $\lim_{x \rightarrow 0} f(x)$ existe ? Si oui, que vaut elle ?
2. $\lim_{\substack{x \rightarrow 0 \\ \leqslant}} f(x)$ existe ? Si oui, que vaut elle ?

Réponse : $\lim_{x \rightarrow 0} f(x)$ n'existe pas. Pour le prouver, on raisonne par l'absurde.

$$\ell = \bigcap_{V \in \mathcal{V}_\ell} V$$

Si ℓ existe, alors $\ell = f(0)$.

Or, $0 \neq \lim_{x \rightarrow 0} f(x)$



Proposition: Si f admet une limite finie en $a \in I$, alors cette limite vaut $f(a)$.

Preuve:

Soit $\ell = \lim_{x \rightarrow a} f(x)$ et $a \in I$.

On sait que

$$\forall V \in \mathcal{V}_\ell, \exists W \in \mathcal{V}_a, \forall x \in W \cap I, f(x) \in V.$$

Soit $V \in \mathcal{V}_\ell$. Alors, $f(a) \in V$.

$$f(a) \in \bigcap_{V \in \mathcal{V}_\ell} V = \begin{cases} \{\ell\} & \text{si } \ell \in \mathbb{R}, \\ \emptyset & \text{si } \ell = \pm\infty. \end{cases}$$

Donc $\ell \in \mathbb{R}$ et $\ell = f(a)$. □

REMARQUE:

De même si $a \in I$ et si $\lim_{x \rightarrow a} f(x)$ existe (resp. $\liminf_{x \rightarrow a} f(x)$ et $\limsup_{x \rightarrow a} f(x)$) alors $f(a) = \lim_{x \rightarrow a} f(x)$ (resp $f(a) = \liminf_{x \rightarrow a} f(x)$ et $f(a) = \limsup_{x \rightarrow a} f(x)$)



EXEMPLE:

$\lim_{x \rightarrow 0} \delta(x)$ n'existe pas

$\lim_{x \rightarrow 0^+} \delta(x)$ et $\lim_{x \rightarrow 0^-} \delta(x)$ n'existent pas non plus.

$$\lim_{\substack{x \rightarrow 0 \\ \neq}} \delta(x)$$

$$\lim_{\substack{x \rightarrow 0 \\ <}} \delta(x) = 0, \lim_{\substack{x \rightarrow 0 \\ >}} \delta(x) = 0$$

$$\lim_{\substack{x \rightarrow a \\ <}} \frac{f(x) - f(a)}{x - a} = \lim_{\substack{x \rightarrow a \\ \neq}} \frac{f(x) - f(a)}{x - a}$$

Définition: Soit f définie sur D et $a \in D$. On dit que f est continue en a si $\lim_{x \rightarrow a} f(x)$ existe ou si $\lim_{\substack{x \rightarrow a \\ \neq}} f(x) = f(a)$.

EXEMPLE:

$$\text{Soit } f : x \mapsto \begin{cases} \frac{\sin(x)}{x} & \text{si } x \neq 0 \\ 1 & \text{si } x = 0 \end{cases}$$

$$\lim_{\substack{x \rightarrow 0 \\ \neq}} f(x) = \lim_{x \rightarrow 0} \frac{\sin(x)}{x} = 1 = f(0)$$

Donc f est continue en 0.

Proposition: f est continue en a si et seulement si

$$\lim_{\substack{x \rightarrow a \\ <}} f(x) = \lim_{\substack{x \rightarrow a \\ >}} f(x) = f(a)$$

Preuve (unicité de la limite):

On suppose que $f(x) \xrightarrow{x \rightarrow u} a$, $f(x) \xrightarrow{x \rightarrow u} b$ avec $a \neq b$.

Soient V et W comme dans le lemme (suivant),

$$\begin{cases} \exists W_1 \in \mathcal{V}_u, \forall x \in W_1 \cap \mathcal{D}, f(x) \in V \\ \exists W_2 \in \mathcal{V}_u, \forall x \in W_2 \cap \mathcal{D}, f(x) \in W \end{cases}$$

Donc

$$\forall x \in \underbrace{W_1 \cap W_2 \cap \mathcal{D}}_{\neq \emptyset \text{ car } W_1 \cap W_2 \in \mathcal{V}_u} \quad f(x) \in V \cap W = \emptyset$$

□

Lemme: Soient $a \neq b$ deux éléments de $\overline{\mathbb{R}}$

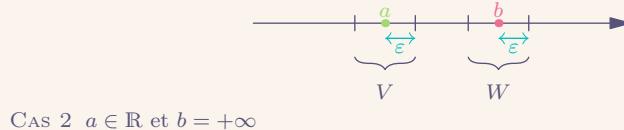
Alors $\exists V \in \mathcal{V}_a, \exists W \in \mathcal{V}_b, V \cap W = \emptyset$

Preuve: Cas 1 $(a, b) \in \mathbb{R}^2$. On suppose que $a < b$.

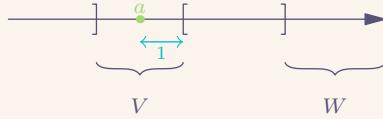
$$\text{On pose } \varepsilon = \frac{b-a}{2},$$

$$\begin{cases} V =]a - \varepsilon; a + \varepsilon[\\ W =]b - \varepsilon; b + \varepsilon[\end{cases}$$

On vérifie que $V \cap W = \emptyset$

CAS 2 $a \in \mathbb{R}$ et $b = +\infty$

$$\begin{cases} V =]a-1; a+1[\\ W =]a+2; +\infty[\end{cases}$$

CAS 3 $a = -\infty, b = +\infty$

$$\begin{cases} V =]-\infty; 0[\\ W =]0; +\infty[\end{cases}$$

□

Théorème: Soit f définie sur \mathcal{D} et $a \in \overline{\mathcal{D}}, \ell \in \overline{\mathbb{R}}$

$$f(x) \xrightarrow[x \rightarrow a]{} \ell \iff \forall (x_n) \in \mathcal{D}^{\mathbb{N}} \left(x_n \xrightarrow[n \rightarrow +\infty]{} a \implies f(x_n) \xrightarrow[n \rightarrow +\infty]{} \ell \right)$$

Preuve: “ \implies ” On suppose que $f(x) \xrightarrow[x \rightarrow a]{} \ell$.

Soit $(x_n) \in \mathcal{D}^{\mathbb{N}}$ telle que $x_n \xrightarrow[n \rightarrow +\infty]{} \ell$

Soit $V \in \mathcal{V}_\ell$. Soit $W \in \mathcal{V}_a$ tel que

$$\forall x \in W \cap \mathcal{D}, f(x) \in V$$

$x_n \xrightarrow[n \rightarrow +\infty]{} a$ donc il existe $N \in \mathbb{N}$ tel que

$$\forall n \geq N, x_n \in W \cap \mathcal{D}$$

Donc

$$\forall n \geq N, f(x_n) \in V$$

D'où, $f(x_n) \xrightarrow[n \rightarrow +\infty]{} \ell$

“ \impliedby ” On suppose que $f(x) \not\xrightarrow[x \rightarrow a]{} \ell$

$$\exists V \in \mathcal{V}_\ell, \forall W \in \mathcal{V}_a, \exists x \in W \cap \mathcal{D}, f(x) \notin V$$

Soit V comme ci dessus. Soit $W_1 \in \mathcal{V}_a$.

CAS 1 $a \in \mathcal{D}$ et $\forall x \in W \cap \mathcal{D} \setminus \{a\}, f(x) \in V$.

On le prouve par la contraposée. On suppose $f(x) \not\xrightarrow[x \rightarrow a]{} \ell \in \mathbb{R}$

Donc,

$$\exists \varepsilon > 0, \forall \eta > 0, \exists x \in]a-\eta, a+\eta[, |f(x) - \ell| > \varepsilon$$

On considère un tel ε donc

$$\forall n \in \mathbb{N}_*, \exists x_n \in \left[a - \frac{1}{n}, a + \frac{1}{n} \right], |f(x_n) - \ell| > \varepsilon$$

Par encadrement, $x_n \xrightarrow{n \rightarrow +\infty} a$ et $f(x_n) \xrightarrow{n \rightarrow +\infty} \ell$

Cas 2 Soit $x_1 \in W_1 \cap \mathcal{D}$ tel que $f(x_1) \notin V$

$$\begin{cases} x_1 \in \mathcal{D} \\ a \notin \mathcal{D} \end{cases} \quad \text{donc } x_1 \neq a$$

Cas 3 $\exists x \in W_1 \cap \mathcal{D} \setminus \{a\}, f(x) \notin V$

Soit x_1 un tel élément :

$$\begin{aligned} x_1 &\in W_1 \cap \mathcal{D} \\ x_1 &\neq a \\ f(x_1) &\notin V \end{aligned}$$

Dans les cas 2 et 3, on pose $W_2 \in \mathcal{V}_a$ tel que

$$W_2 \subset W_1 \setminus \{x_1\}$$

En itérant ce procédé, on construit une suite (x_n) qui tend vers a et telle que

$$\forall n \in \mathbb{N}, f(x_n) \notin V$$

$$\text{et donc } f(x_n) \xrightarrow{n \rightarrow +\infty} \ell$$

□

Proposition: Si $f(x) \xrightarrow{x \rightarrow a} \ell$ et $g(x) \xrightarrow{x \rightarrow a} \ell_2$ alors

1. $f(x) + g(x) \xrightarrow{x \rightarrow a} \ell_1 + \ell_2$
2. $f(x) \times g(x) \xrightarrow{x \rightarrow a} \ell_1 \times \ell_2$
3. Si $\ell_2 \neq 0$, $\frac{f(x)}{g(x)} \xrightarrow{x \rightarrow a} \frac{\ell_1}{\ell_2}$

Preuve: 1. Soit (x_n) une suite qui tends vers a alors $f(x_n) \xrightarrow{n \rightarrow +\infty} \ell_1$ et $g(x_n) \xrightarrow{n \rightarrow +\infty} \ell_2$
 Donc, $f(x_n) + g(x_n) \xrightarrow{n \rightarrow +\infty} \ell_1 + \ell_2$
 Donc $f(x) + g(x) \xrightarrow{n \rightarrow +\infty} \ell_1 + \ell_2$

□

Proposition: Si $f(x) \xrightarrow{x \rightarrow a} \ell_1$ et $g(x) \xrightarrow{x \rightarrow \ell_1} \ell_2$ alors $g(f(x)) \xrightarrow{x \rightarrow a} \ell_2$

Preuve:
 Soit (x_n) une suite qui tend vers a . Alors, $f(x_n) \xrightarrow{n \rightarrow +\infty} \ell_1$ donc $g(f(x_n)) \xrightarrow{n \rightarrow +\infty} \ell_2$
 donc $g(f(x)) \xrightarrow{x \rightarrow a} \ell_2$ □

Corollaire: Une somme, un produit, une composée de fonctions continues sont continues. □

REMARQUE:

Pour démontrer que $f(x)$ n'a pas de limite quand x tend vers a . On cherche deux suites (x_n) et (y_n) de limite a avec

$$\begin{cases} f(x_n) \rightarrow \ell_1 \\ f(y_n) \rightarrow \ell_2 \\ \ell_1 \neq \ell_2 \end{cases}$$

EXEMPLE:

$$\begin{aligned} \forall n \in \mathbb{N}, \sin(2\pi n) = 0 &\xrightarrow[n \rightarrow +\infty]{} 0 \\ \sin\left(\frac{\pi}{2} + 2\pi n\right) = 1 &\xrightarrow[n \rightarrow +\infty]{} 1 \end{aligned}$$

Or,

$$\begin{aligned} 2\pi n &\xrightarrow[n \rightarrow +\infty]{} +\infty \\ \frac{\pi}{2} + 2\pi n &\xrightarrow[n \rightarrow +\infty]{} +\infty \end{aligned}$$

Donc, sin n'a pas de limite en $+\infty$

Théorème (Limite monotone): Soit f une fonction croissante sur $]a, b[$ avec $a \neq b \in \overline{\mathbb{R}}$.

- Si f est majorée,

$$\exists M \in \mathbb{R}, \forall x \in]a, b[, f(x) \leq M$$

$$\text{alors } \lim_{\substack{x \rightarrow b \\ <}} f(x) = \sup_{x \in]a, b[} f(x) \in \mathbb{R}$$

- Si f n'est pas majorée,

$$\lim_{\substack{x \rightarrow b \\ <}} f(x) = +\infty$$

- Si f est minorée,

$$\exists m \in \mathbb{R}, \forall x \in]a, b[, f(x) \geq m$$

$$\text{alors } \lim_{\substack{x \rightarrow a \\ >}} f(x) = \inf_{]a, b[} f(x) \in \mathbb{R}$$

- Si f n'est pas minorée, $\lim_{\substack{x \rightarrow a \\ >}} f(x) = -\infty$

Preuve: 1. $\sup_{]a, b[} f$ existe

$$\forall \varepsilon > 0, \exists x \in]a, b[, f(x) > \sup_{]a, b[} f - \varepsilon$$

donc

$$\forall \varepsilon > 0, \exists x \in]a, b[, \forall y \in [x, b[, \sup_{]a, b[} f - \varepsilon < f(y) \leq \sup_{]a, b[} f < \sup_{]a, b[} f + \varepsilon$$

$$\text{donc } f(x) \xrightarrow[\substack{x \rightarrow b \\ <}]{} \sup_{]a, b[} f$$

- f n'est pas majorée

$$\forall M \in \mathbb{R}, \exists x \in]a, b[, f(x) > M$$

donc

$$\forall M \in \mathbb{R}, \exists x \in]a, b[, \forall y \in [x, b[, f(y) \in [M, +\infty[$$

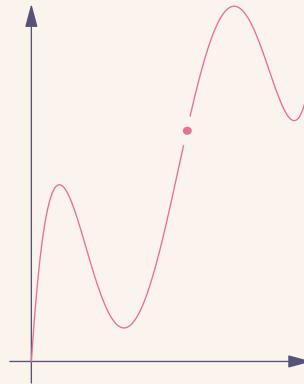
□

REMARQUE:

Avec les hypothèses ci-dessus, pour tout $x \in]a, b[$,
 f est croissante sur $]a, x[$, et majorée par $f(x)$ donc $\lim_{t \rightarrow x^-} f(t) \in \mathbb{R}$

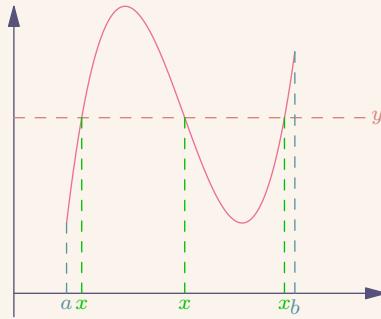
f est croissante sur $]x, b[$ et minorée par $f(x)$ donc $\lim_{t \rightarrow x^+} f(t) \in \mathbb{R}$

$\lim_{t \rightarrow x^-} f(t) \leq f(x) \leq \lim_{t \rightarrow x^+} f(t)$



Théorème (Théorème des valeurs intermédiaires): Soit f une fonction continue sur un intervalle I , $a < b$ deux éléments de I .

$$\forall y \in [f(a), f(b)] \cup [f(b), f(a)], \exists x \in [a, b], y = f(x)$$



Lemme: Soit f une fonction continue sur un intervalle I , $a < b$ deux éléments de I tels que $f(a) \leq 0 \leq f(b)$. Alors,

$$\exists x \in [a, b], f(x) = 0$$

Preuve (du lemme):

On pose $A = \{x \in [a, b] \mid f(x) \leq 0\}$

$A \neq \emptyset$ car $a \in A$ et A est majorée par b .
On pose $u = \sup(A)$. Soit $(x_n) \in A^{\mathbb{N}}$ qui converge vers u .

$$\forall n \in \mathbb{N}, x_n \in A \text{ donc } \forall n \in \mathbb{N}, \begin{cases} a \leq x_n \leq b \\ f(x_n) \leq 0 \end{cases}$$

On sait que $x_n \rightarrow u$ et $f(x_n) \rightarrow f(u)$ par continuité de f .

$$\text{Donc, } \begin{cases} a \leq u \leq b \\ f(u) \leq 0 \end{cases} \quad (\text{donc } u = \max(A))$$

De plus,

$$\forall x \in]u, b], f(x) > 0$$

donc

$$\begin{cases} \lim_{\substack{x \rightarrow u \\ >}} f(x) = f(u) \\ \lim_{\substack{x \rightarrow u \\ <}} f(x) \geq 0 \end{cases}$$

Donc, $f(u) \geq 0$ donc $f(u) = 0$

□

Preuve (du théorème):

On pose $g : x \mapsto f(x) - y$. g est continue sur I .

$$\underline{\text{Si }} f(a) < f(b) \text{ alors } \begin{cases} g(a) \leq 0 \\ g(b) \geq 0 \end{cases}$$

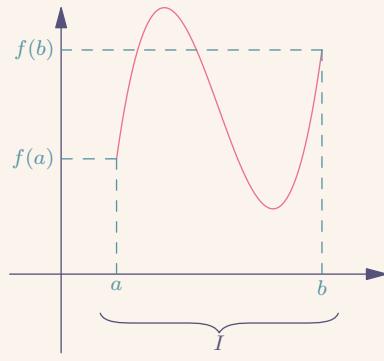
D'après le lemme, il existe $x \in [a, b]$ tel que $g(x) = 0$ et donc $f(x) = y$

$$\underline{\text{Si }} f(a) < f(b) \text{ alors } \begin{cases} h(a) \leq 0 \\ h(b) \geq 0 \end{cases} \quad \text{où } h : x \mapsto -g(x) = y - f(x) \text{ est continue}$$

D'après le lemme, il existe $x \in [a, b]$ tel que $h(x) = 0$ et donc $f(x) = y$

□

Corollaire: Soit f continue sur un intervalle I . Alors, $f(I)$ est un intervalle.



Preuve:

Montrons que $f(I)$ est convexe

Soit $\alpha \in f(I), \beta \in f(I)$ avec $\alpha < \beta$. Montrons que

$$\forall \gamma \in [\alpha, \beta], f(\gamma) \in f(I)$$

Or, $\begin{cases} \alpha \in f(I) & \exists a \in I, \alpha = f(a) \\ \beta \in f(I) & \exists b \in I, \beta = f(b) \end{cases}$

D'après le théorème des valeurs intermédiaires, il existe $x \in [a, b]$ tel que $\gamma = f(x)$ donc, $f(\gamma) \in f(I)$ \square

Corollaire: On peut généraliser le théorème des valeurs intermédiaires au cas où
 $\begin{cases} a \in \overline{\mathbb{R}} \\ b \in \overline{\mathbb{R}} \end{cases}$ en remplaçant $f(a)$ par $\lim_{x \rightarrow a^+} f(x)$ et $f(b)$ par $\lim_{x \rightarrow b^-} f(x)$

\square

Théorème (Théorème de la bijection): Soit f continue, strictement monotone sur un intervalle I . Alors, $J = f(I)$ est un intervalle de même nature (ouvert, semi-ouvert ou fermé) et f établit une bijection de I sur J .

Preuve:

D'après le théorème des valeurs intermédiaires, J est un intervalle. f est strictement monotone donc f injective. Donc f établit une bijection de I sur J .

CAS 1 $I = [a, b]$ et f croissante

$$\forall x \in I, a \leq x \leq b$$

$$\text{donc } \forall x \in I, f(a) \leq f(x) \leq f(b)$$

$$\text{donc } J \subset [f(a), f(b)]$$

Or, $[f(a), f(b)] \subset J$ d'après le théorème des valeurs intermédiaires

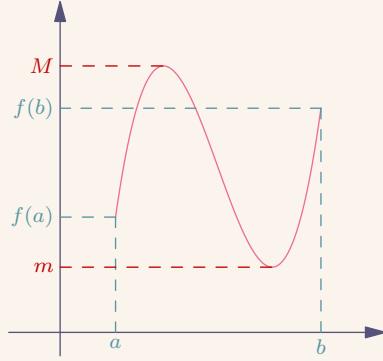
$$\text{Donc } J = [f(a), f(b)]$$

Les autres cas se démontrent de la même façon. \square

Théorème: Soit f continue sur un segment $[a, b]$. Alors, f est bornée et atteint ses bornes, i.e.

$$\exists (m, M) \in \mathbb{R}^2, f([a, b]) = [m, M]$$

▲ On peut avoir $m \neq f(a)$ et $M \neq f(b)$



Preuve:

On suppose que f n'est pas majorée :

$$\forall M \in \mathbb{R}, \exists x \in [a, b], f(x) \geq M$$

En particulier,

$$\forall n \in \mathbb{N}, \exists x_n \in [a, b], f(x_n) \geq n$$

$$\text{Donc, } f(x_n) \xrightarrow{n \rightarrow +\infty} +\infty$$

La suite $(x_n)_{n \in \mathbb{N}}$ est minorée par a et majorée par b donc bornée.

D'après le théorème de Bolzano-Weierstrass, il existe $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ strictement croissante

telle que $(x_{\varphi(n)})_{n \in \mathbb{N}}$ converge. On pose $\ell = \lim_{n \rightarrow +\infty} x_{\varphi(n)}$. On a bien $\ell \in [a, b]$ et $f(\ell) =$

$$\lim_{n \rightarrow +\infty} f(x_{\varphi(n)}) \text{ par continuité de } f.$$

Or, $(f(x_{\varphi(n)}))_{n \in \mathbb{N}}$ est une sous-suite de $(f(x_n))$ donc $f(x_{\varphi(n)}) \xrightarrow{n \rightarrow +\infty} +\infty$: une contradiction

Donc f est majorée et on pose

$$M = \sup_{a \leq x \leq b} f(x)$$

On prouve de même que f est minorée. On pose donc

$$m = \inf_{a \leq x \leq b} f(x)$$

Soit $(y_n) \in [a, b]^{\mathbb{N}}$ telle que $f(y_n) \xrightarrow{n \rightarrow +\infty} M$.

(y_n) est bornée donc il existe une sous-suite $(y_{\psi(n)})$ de (y_n) convergente. On pose $y = \lim_{n \rightarrow +\infty} y_{\psi(n)} \in [a, b]$

Comme f continue sur y ,

$$f(y) = \lim_{n \rightarrow +\infty} f(y_{\psi(n)})$$

Or, $(f(y_{\psi(n)}))$ est une sous-suite de $(f(y_n))$ donc

$$M = \lim_{n \rightarrow +\infty} f(y_{\psi(n)})$$

Par unicité de la limite, $M = f(y)$

Donc, $M = \max_{a \leq x \leq b} f(x)$. De même, $m \in f([a, b])$

Enfin, en posant $\begin{cases} M = f(y) & \text{avec } y \in [a, b] \\ m = f(z) & \text{avec } z \in [a, b] \end{cases}$, on obtient

$$\begin{aligned} [m, M] &= [f(z), f(y)] \underset{\substack{\text{théorème des valeurs intermédiaires}}} {\subset} f([a, b]) \underset{\substack{m \text{ minimum} \\ M \text{ maximum}}} {\subset} [m, M] \end{aligned}$$

donc $f([a, b]) = [m, M]$

□

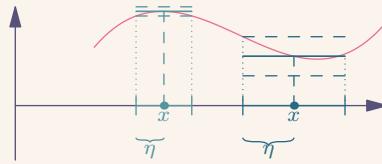
2 Continuité uniforme

REMARQUE:

$f : \mathbb{R} \rightarrow \mathbb{R}$ continue,

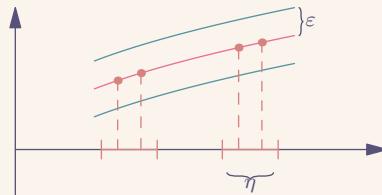
$$\forall x \in \mathbb{R}, \forall \varepsilon > 0, \exists \eta > 0, \forall y \in]x - \eta, x + \eta[, |f(x) - f(y)| \leq \varepsilon$$

Ici, η dépend de ε et de x



Dans certaines situations, il serait préférable d'avoir

$$\forall \varepsilon > 0, \exists \eta > 0, \forall (x, y) \in \mathbb{R}^2, |x - y| \leq \eta \implies |f(x) - f(y)| \leq \varepsilon$$

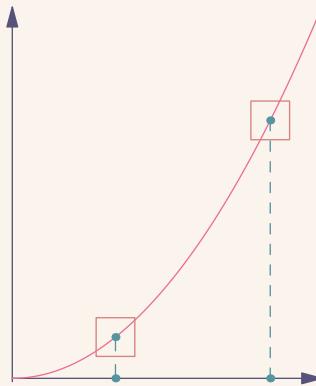


Lemme: Soit f uniformément continue sur un intervalle I . Soient $(x_n)_{n \in \mathbb{N}}, (y_n)_{n \in \mathbb{N}}$ deux suites d'éléments dans I telles que $x_n - y_n \xrightarrow{n \rightarrow +\infty} 0$.
Alors, $\lim_{n \rightarrow +\infty} (f(x_n) - f(y_n)) = 0$

□

EXEMPLE:

$$\begin{aligned} f : \mathbb{R}^+ &\longrightarrow \mathbb{R} \\ x &\longmapsto x^2 \end{aligned}$$



On pose $\forall n \in \mathbb{N}_*$, $\begin{cases} x_n = n \\ y_n = n + \frac{1}{n} \end{cases}$. On a bien $\forall n \in \mathbb{N}_*, x_n - y_n = \frac{1}{n} \xrightarrow{n \rightarrow +\infty} 0$.
 $\forall n \in \mathbb{N}_*, x_n^2 - y_n^2 = n^2 - (n + \frac{1}{n})^2 = n^2 - n^2 - \frac{1}{n^2} - 2 \xrightarrow{n \rightarrow +\infty} -2 \neq 0$

Donc, f n'est pas uniformément continue.

Théorème (Théorème de Heine): Soit f une fonction continue sur $[a, b]$. Alors, f est uniformément continue sur $[a, b]$.

Preuve:

On suppose f continue sur $[a, b]$ mais pas uniformément continue.

$$\exists \varepsilon > 0, \forall \eta > 0, \exists (x, y) \in [a, b]^2 \text{ avec } |x - y| \leq \eta \text{ et } |f(x) - f(y)| > \varepsilon$$

Soit $\varepsilon > 0$ comme ci-dessus. Alors,

$$\forall n \in \mathbb{N}, \exists (x_n, y_n) \in [a, b]^2 \text{ avec } \left| x_n - y_n \right| \leq \frac{1}{n+1} \text{ et } |f(x_n) - f(y_n)| > \varepsilon$$

(x_n) est bornée donc il existe une sous-suite $(x_{\varphi(n)})$ de (x_n) convergente. On note $\ell = \lim_{n \rightarrow +\infty} x_{\varphi(n)} \in [a, b]$ ($y_{\varphi(n)}$) est bornée, $(y_{\varphi(n)})$ a une sous-suite $(y_{\varphi(\psi(n))})$ convergente.

On pose $\ell' = \lim_{n \rightarrow +\infty} y_{\varphi(\psi(n))}$. $(x_{\varphi(\psi(n))})_{n \in \mathbb{N}}$ est une autre sous-suite de $(x_{\varphi(n)})$ donc $x_{\varphi(\psi(n))} \xrightarrow{n \rightarrow +\infty} \ell$.

De plus,

$$\forall n \in \mathbb{N}, |x_{\varphi(\psi(n))} - y_{\varphi(\psi(n))}| \leq \frac{1}{\varphi(\psi(n)) + 1}$$

On a vu que

$$\forall n \in \mathbb{N}, \varphi(\psi(n)) \geq n$$

car $\varphi \circ \psi$ est strictement croissante à valeurs dans \mathbb{N} .

Donc, $x_{\varphi(\psi(n))} - y_{\varphi(\psi(n))} \xrightarrow{n \rightarrow +\infty} 0$.

On en déduit que $\ell - \ell' = 0$. De plus

$$\forall n \in \mathbb{N}, |f(x_{\varphi(\psi(n))}) - f(x_{\varphi(\psi(n))})| > \varepsilon$$

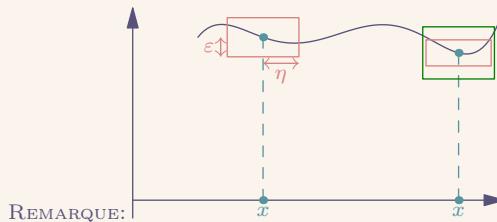
En passant à la limite,

$$0 = |f(\ell) - f(\ell)| > \varepsilon > 0$$

car f continue en ℓ

On a obtenu une contradiction. \square

\square



$$\begin{cases} \eta > 0 \\ \varepsilon > 0 \\ |x - y| \leq \eta \\ |f(x) - f(y)| \leq \varepsilon \end{cases}$$

Définition: Soit $f : I \rightarrow \mathbb{R}$ où I est un intervalle et $k \in \mathbb{R}$. On dit que f est k -lipschitzienne si

$$\forall (x, y) \in I^2, |f(x) - f(y)| \leq k|x - y|$$

On dit que f est lipschitzienne s'il existe $k \in \mathbb{R}$ tel que f soit k -lipschitzienne.

Proposition: Soit f une fonction lipschitzienne sur I . Alors, f est uniformément continue sur I donc continue sur I .

Preuve:

Soit $k \in \mathbb{R}$ tel que

$$\forall (x, y) \in I^2, |f(x) - f(y)| \leq k|x - y|$$

Soit $\varepsilon > 0$.

Si $k = 0$ alors f est constante donc uniformément continue.

On suppose $k \neq 0$. Soit $\varepsilon > 0$. On pose $\eta = \frac{\varepsilon}{k} > 0$ car $k > 0$.
 $\underbrace{k}_{\text{ne dépend pas de } x}$

Soit $(x, y) \in I^2$. On suppose $|x - y| \leq \eta$. Alors,

$$|f(x) - f(y)| \leq k|x - y| \leq k\eta = \varepsilon$$

□

EXEMPLE:

$x \mapsto |x|$ est 1-lipschitzienne sur \mathbb{R} .

$$\forall (x, y) \in \mathbb{R}^2, ||x| - |y|| \leq |x - y|$$

(inégalité triangulaire)

Théorème: Soit $f : I \rightarrow \mathbb{R}$ dérivable sur I telle qu'il existe $M \in \mathbb{R}$ vérifiant

$$\forall x \in I, |f'(x)| \leq M$$

Alors

$$\forall (a, b) \in I^2, |f(a) - f(b)| \leq M|a - b|$$

donc f est M -lipschitzienne.

Corollaire: Soit f de classe \mathcal{C}^1 sur $[a, b]$. Alors f est lipschitzienne.

Preuve:

f' est continue sur un segment donc bornée.

□

EXEMPLE:

$$\begin{aligned} f : \mathbb{R}^+ &\longrightarrow \mathbb{R}^+ \\ x &\longmapsto \sqrt{x} \end{aligned}$$

$$\forall x > 0, |f'(x)| = \frac{1}{2\sqrt{x}} \xrightarrow[x \rightarrow 0^+]{=} +\infty$$

Par contre,

$$\forall x \geq 1, |f'(x)| \leq \frac{1}{2}$$

Donc f est $\frac{1}{2}$ -lipschitzienne sur $[1, +\infty[$ donc uniformément continue sur $[1, +\infty[$.

f est continue sur $[0, 1]$ donc uniformément continue sur $[0, 1]$ (théorème de Heine).

Soit $\varepsilon > 0$. Soient $\eta_1, \eta_2 \in \mathbb{R}_*^+$ tels que

$$\begin{cases} \forall (x, y) \in [0, 1]^2, |x - y| \leq \eta_1 \implies |\sqrt{x} - \sqrt{y}| \leq \frac{\varepsilon}{2} \\ \forall (x, y) \in [1, +\infty[^2, |x - y| \leq \eta_2 \implies |\sqrt{x} - \sqrt{y}| \leq \frac{\varepsilon}{2} \end{cases}$$

On pose $\eta = \min(\eta_1, \eta_2)$. Soient $(x, y) \in (\mathbb{R}^+)^2$. On suppose $|x - y| \leq \eta$

CAS 1 $\begin{cases} x \leq 1 \\ y \leq 1 \end{cases}$

Alors, $|x - y| \leq \eta \leq \eta_1$ donc $|\sqrt{x} - \sqrt{y}| \leq \varepsilon_2 \leq \varepsilon$

CAS 2 $\begin{cases} x \geq 1 \\ y \geq 1 \end{cases}$

Alors, $|x - y| \leq \eta \leq \eta_2$ donc $|\sqrt{x} - \sqrt{y}| \leq \frac{\varepsilon}{2} \leq \varepsilon$

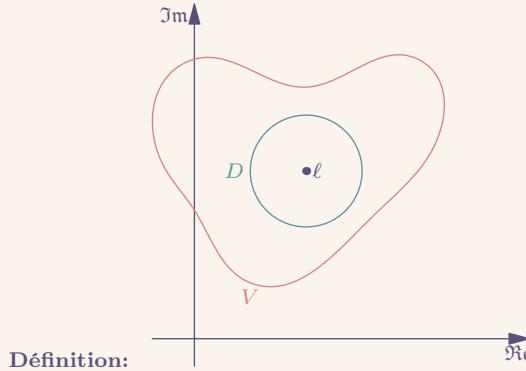
CAS 3 $x \leq 1 \leq y$

$$\begin{aligned} |\sqrt{x} - \sqrt{y}| &= \left| \sqrt{x} - \sqrt{1 + \sqrt{1 - y}} \right| \\ &\leq \left| \sqrt{x} - \sqrt{1} \right| + \left| \sqrt{1 - y} - \sqrt{1} \right| \end{aligned}$$

$$\begin{aligned} |x - 1| \leq |x - y| \leq \eta \leq \eta_1 \text{ donc } |\sqrt{x} - \sqrt{1}| \leq \frac{\varepsilon}{2} \\ |y - 1| \leq |x - y| \leq \eta \leq \eta_2 \text{ donc } |\sqrt{1 - y} - \sqrt{1}| \leq \frac{\varepsilon}{2} \end{aligned}$$

Donc $|\sqrt{x} - \sqrt{y}| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$

3 Fonctions à valeurs dans \mathbb{C}



V est un voisinage de ℓ s'il existe $r > 0$ tel que $V \supset D(\ell, r)$
où $D(\ell, r) = \{z \in \mathbb{C} \mid |z - \ell| < r\}$

Proposition: Soit $f : I \rightarrow \mathbb{C}$ et $a \in I$, $\ell \in \mathbb{C}$.

$$f(x) \xrightarrow{x \rightarrow a} \ell \iff \begin{cases} \Re(f(x)) \xrightarrow{x \rightarrow a} \Re(\ell) \\ \Im(f(x)) \xrightarrow{x \rightarrow a} \Im(\ell) \end{cases}$$

□

REMARQUE (Rappel):

On dit que $I \rightarrow \mathbb{C}$ est bornée s'il existe $M \in \mathbb{R}$ tel que

$$\forall x \in I, |f(x)| \leq M$$

4 Annexe

Théorème: *Théorème 2.11*
 $f : I \rightarrow J$ bijective monotone avec I et J deux intervalles.
Alors, f^{-1} est continue (et f aussi)

Preuve:

f monotone donc $f(I) = J$
donc f continue (d'après 2.10).
 f^{-1} monotone, $f^{-1}(J) = I$
donc f^{-1} est continue □

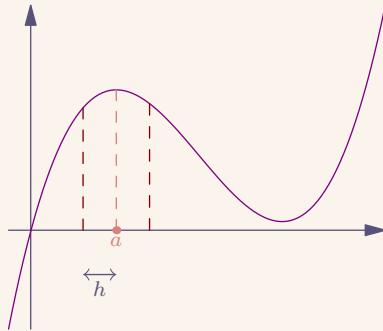
Définition: Un homéomorphisme est une application bijective, continue dont la réci-proque est continue.

REMARQUE:

Preuve du programme de colle

Preuve:

$$\exists \eta > 0, \forall h \in]-\eta, +\eta[, f(a) \geq f(a+h)$$



$$\begin{aligned} f'(a) &= \lim_{h \rightarrow 0} \frac{f(a+h) - f(a)}{h} = \lim_{\substack{h \rightarrow 0 \\ >}} \frac{f(a+h) - f(a)}{h} \leq 0 \\ &= \lim_{\substack{h \rightarrow 0 \\ <}} \frac{f(a+h) - f(a)}{h} \geq 0 \end{aligned}$$

Donc, $f'(a) = 0$ □

CHAPITRE

15

ESPACES VECTORIELS

1 Définition et premières propriétés

Définition: Soit E un ensemble muni d'une loi interne $+$ et d'une loi \cdot définie sur $\mathbb{K} \times E$ à valeurs dans E où \mathbb{K} est un corps.

On dit que $(E, +, \cdot)$ est un \mathbb{K} -espace vectoriel (ou un espace vectoriel sur \mathbb{K}) si

1. $(E, +)$ est un groupe abélien
2. (a)

$$\forall u \in E, \forall (\lambda, \mu) \in \mathbb{K}^2, \\ \mu \cdot (\lambda \cdot u) = (\underbrace{\mu \times \lambda}_{\times \text{ de } \mathbb{K}}) \cdot u$$

- (b) $\forall u \in E, 1_{\mathbb{K}} \cdot u = u$
3. (a)

$$\forall u \in E, \forall (\lambda, \mu) \in \mathbb{K}^2 \\ (\lambda \cdot u) \underbrace{+}_{+ \text{ de } E} (\mu \cdot u) = (\underbrace{\lambda + \mu}_{+ \text{ de } \mathbb{K}}) \cdot u$$

- (b)

$$\forall \lambda \in \mathbb{K}, \forall (u, v) \in E^2, \\ \lambda \cdot (u + v) = (\lambda \cdot u) + (\lambda \cdot v)$$

Les éléments de E sont alors appelés vecteurs et les éléments de \mathbb{K} sont dits scalaires.
Par convention, \cdot est prioritaire sur $+$.

EXEMPLE:

Soit \mathbb{K} corps, \mathbb{K} est un \mathbb{K} -espace vectoriel

EXEMPLE:

Soit \mathcal{P} l'ensemble des vecteurs du plan. \mathcal{P} est un \mathbb{R} -espace vectoriel.

EXEMPLE:

\mathbb{C} est un \mathbb{R} -espace vectoriel.

En généralisant, tout corps \mathbb{K} est un \mathbb{L} -espace vectoriel pour \mathbb{L} un sous-corps de \mathbb{K}

EXEMPLE:

$(\mathbb{K}^n, +, \cdot)$ avec

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$$

$$\lambda \cdot (y_1, \dots, y_n) = (\lambda \cdot y_1, \dots, \lambda \cdot y_n)$$

est un espace vectoriel.

EXEMPLE:

Soient $(E, +, \cdot)$ un \mathbb{K} -espace vectoriel et \mathcal{D} un ensemble non vide.
 $(E^\mathcal{D}, +, \cdot)$ est un \mathbb{K} -espace vectoriel où pour $f, g \in E^\mathcal{D}$ et $\lambda \in \mathbb{K}$

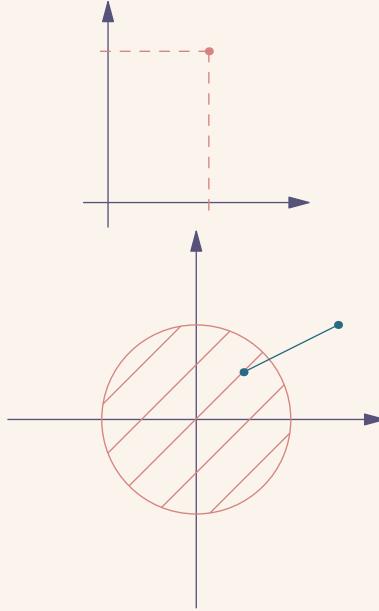
$$\begin{aligned} f + g : \mathcal{D} &\longrightarrow E \\ x &\longmapsto f(x) + g(x) \end{aligned}$$

$$\begin{aligned} \lambda f : \mathcal{D} &\longrightarrow \mathbb{K} \\ x &\longmapsto \lambda \cdot f(x) \end{aligned}$$

Par exemple, $\mathbb{C}^{\mathbb{N}}$ est un \mathbb{R} -espace vectoriel
 $\mathcal{C}^0(\mathcal{D}, \mathbb{R})$ est un \mathbb{R} -espace vectoriel

EXEMPLE: — \mathbb{R}^+ n'est pas un \mathbb{R} -espace vectoriel

— $\{(x, 0) \mid x \in \mathbb{R}\} \cup \{(0, y) \mid y \in \mathbb{R}\}$ n'est pas un \mathbb{R} -espace vectoriel pour les lois usuelles



Proposition: Soit $(E, +, \cdot)$ un \mathbb{K} -espace vectoriel.

1. $\forall u \in E, 0_{\mathbb{K}} \cdot u = 0_E$
2. $\forall \lambda \in \mathbb{K}, \lambda \cdot 0_E = 0_E$
3. $\forall \lambda \in \mathbb{K}, \forall u \in E, \lambda \cdot u = 0_E \implies \lambda = 0_{\mathbb{K}} \text{ ou } u = 0_E$

Preuve: 1. Soit $u \in E$.

$$\begin{aligned} 0_{\mathbb{K}} \cdot u &= (0_{\mathbb{K}} + 0_{\mathbb{K}}) \cdot u \\ &= 0_{\mathbb{K}} \cdot u + 0_{\mathbb{K}} \cdot u \end{aligned}$$

$(E, +)$ est un groupe donc $0_E = 0_{\mathbb{K}} \cdot u$

2. Soit $\lambda \in \mathbb{K}$.

$$\lambda \cdot 0_E = \lambda \cdot (0_E + 0_E) = \lambda \cdot 0_E + \lambda \cdot 0_E$$

$\lambda \cdot 0_E$ est régulier pour $+$:

$$0_E = \lambda \cdot 0_E$$

3. Soit $\lambda \in \mathbb{K}$ et $u \in E$ tel que $\lambda \cdot u = 0_E$

CAS 1 $\lambda = 0_{\mathbb{K}}$

CAS 2 $\lambda \neq 0_{\mathbb{K}}$ Alors, $\lambda^{-1} \in \mathbb{K}$ et donc

$$\begin{aligned} \lambda \cdot u = 0_E &\implies \lambda^{-1}(\lambda \cdot u) = \lambda^{-1} \\ &\implies (\lambda^{-1} \times \lambda) \cdot u = 0_E \text{ d'après 2.} \\ &\implies 1_{\mathbb{K}} \cdot u = 0_E \\ &\implies u = 0_E \end{aligned}$$

□

Proposition: Soit $(E, +, \cdot)$ un \mathbb{K} -espace vectoriel et $u \in E$. Alors, $-u = (-1_{\mathbb{K}}) \cdot u$

Preuve:

$$\begin{aligned} u + (-1_{\mathbb{K}}) \cdot u &= (1_{\mathbb{K}} \cdot u) + (-1_{\mathbb{K}}) \cdot u \\ &= (1_{\mathbb{K}} + (-1_{\mathbb{K}})) \cdot u \\ &= 0_{\mathbb{K}} u \\ &= 0_E \end{aligned}$$

Donc $-u = (-1_{\mathbb{K}}) \cdot u$

□

2 Sous-espaces vectoriels

Définition: Soit $(E, +, \cdot)$ un \mathbb{K} -espace vectoriel. Soit $F \subset E$. On dit que F est un sous- \mathbb{K} -espace vectoriel de E si

1. $F \neq \emptyset$
2. $\forall (u, v) \in F^2, u + v \in F$
3. $\forall \lambda \in \mathbb{K}, \forall u \in F, \lambda u \in F$

Proposition: Avec les notations précédentes, $(F, +, \cdot)$ est un \mathbb{K} -espace vectoriel

Preuve: — D'après 2., $+$ est interne dans F

- $(E, +)$ est un groupe abélien donc $+$ est associative et commutative dans E donc dans F
- $F \neq \emptyset$. Soit $u \in F$. D'après 3.,

$$0_{\mathbb{K}} \cdot u \in F$$

Comme $u \in E$ et $(E, +, \cdot)$ est un \mathbb{K} -espace vectoriel,

$$0_{\mathbb{K}} \cdot u = 0_E$$

Donc, $0_E \in F$

- Soit $u \in F$. Comme $u \in E$,

$$-u = -(1_{\mathbb{K}}) \cdot u \in F \text{ d'après 3.}$$

- Les autres axiomes sont aisément vérifiés.

□

Proposition: Soit $(E, +, \cdot)$ un \mathbb{K} -espace vectoriel et $F \subset E$. F est un sous-espace vectoriel de $(E, +, \cdot)$ si et seulement si

1. $F \neq \emptyset$
2. $\forall (\lambda, \mu) \in \mathbb{K}^2, \forall (u, v) \in F^2, \lambda \cdot u + \mu \cdot v \in F$

Preuve: “ \implies ” On sait déjà que F est non vide.

$$\left. \begin{array}{l} \forall u, v \in F, \forall \lambda, \mu \in \mathbb{K}, \\ \quad \lambda u \in F \\ \quad \mu v \in F \end{array} \right\} \text{ donc } \lambda u + \mu v \in F$$

“ \impliedby ” — On sait déjà que F est non-vide

- Soient $u, v \in F$

$$u + v = 1_{\mathbb{K}} \cdot u + 1_{\mathbb{K}} \cdot v \in F$$

- Soit $u \in F, \lambda \in \mathbb{K}$.

$$\lambda \cdot u = \lambda \cdot u + 0_{\mathbb{K}} \cdot u \in F$$

□

Définition: Soient $(E, +, \cdot)$ un \mathbb{K} -espace vectoriel et $(u_1, \dots, u_n) \in E^n$. Une combinaison linéaire de (u_1, \dots, u_n) est un vecteur de E de la forme $\sum_{i=1}^n \lambda_i u_i$ où $(\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n$

REMARQUE:

On peut aussi démontrer que F est un sous-espace vectoriel de E si et seulement si

$$F \neq \emptyset \text{ et } \forall u, v \in F, \forall \lambda \in \mathbb{K}, \lambda u + v \in F$$

EXEMPLE: 1. $F = \{z \in \mathbb{C} \mid \Re(z) + \Im(z) = 1\} \subset \mathbb{C}$

F est un sous- \mathbb{R} -espace vectoriel de \mathbb{C} ?

Non car $0 \notin F$

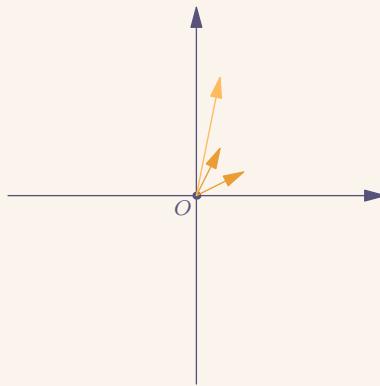
2. $F = \{z \in \mathbb{C} \mid \Re(z) + \Im(z) = 0\}$ est un sous- \mathbb{R} -espace vectoriel de \mathbb{C} mais pas un sous- \mathbb{C} -espace vectoriel.

En effet, $1 - i \in F$ $i(1 - i) = i + 1 \notin F$

3. $E = \mathbb{R}^{\mathbb{N}}$ est un \mathbb{R} -espace vectoriel.
 $F = \{u \in \mathbb{R}^{\mathbb{N}} \mid \forall n \in \mathbb{N}, u_{n+1} = 3u_n\}$ est un sous-espace vectoriel de E .
 $G = \{u \in \mathbb{R}^{\mathbb{N}} \mid \forall n \in \mathbb{N}, u_{n+1} = 3u_n + 2\}$ n'est pas un sous-espace vectoriel de E puisque $0_E \notin G$.
4. $E = \mathbb{R}^D$ est un \mathbb{R} -espace vectoriel
 $F = \mathcal{C}^0(D, \mathbb{R})$ est un sous-espace vectoriel de E (fonctions continues)
 $G = \mathcal{D}(D, \mathbb{R})$ est un sous-espace vectoriel de E (fonctions dérivables)
Si $D =]-a, a[$ avec $a \in \mathbb{R}$, $H = \{f \in E \mid f \text{ impaire}\}$ est un sous-espace vectoriel de E
Si $D = \mathbb{R}$, $L = \{f \in E \mid f \text{ 1-périodique}\}$ est un sous-espace vectoriel de E
 $M = \{f \in E \mid f \text{ périodique}\}$ n'est pas un sous-ensemble vectoriel de E
5. L'ensemble des solutions sur un intervalle I d'une équation différentielle linéaire est un sous-espace vectoriel de \mathbb{R}^I

EXERCICE (Exercice):

Trouver tous les sous- \mathbb{R} -espaces vectoriels de \mathbb{R}^2



- $\{(0, 0)\}$ est un sous-espace vectoriel de \mathbb{R}^2
- Les droites passant par O sont des sous-espaces vectoriels de \mathbb{R}^2
- \mathbb{R}^2 est un sous-espace vectoriel de \mathbb{R}^2

et rien d'autre!

Proposition: Soit $(E, +, \cdot)$ un \mathbb{K} -espace vectoriel et \mathcal{F} une famille non vide de sous-espaces vectoriels de E . Alors $\bigcap_{F \in \mathcal{F}} F$ est un sous-espace vectoriel de E .

Preuve:

On pose $G = \bigcap_{F \in \mathcal{F}} F$.

- $\forall F \in \mathcal{F}, 0_E \in F$ car F est un sous espace vectoriel de E donc $0_E \in G$.
- Soient $u, v \in G$ et $\lambda, \mu \in \mathbb{K}$. On pose $w = \lambda u + \mu v$.

$$\left. \begin{array}{l} \forall F \in \mathcal{F}, u \in F \\ v \in F \end{array} \right\} \text{ donc } w \in F$$

donc $w \in G$

□

REMARQUE (Attention Δ):

Une réunion de sous-espaces vectoriels n'est pas un sous-espace vectoriel en général.

EXERCICE:

$F \cup G$ est un sous-espace vectoriel de $E \iff F \subset G$ ou $G \subset F$

Définition: Soient F et G deux sous-espaces vectoriels de E . On définit leur somme $F + G$ par

$$F + G = \{x + y \mid x \in F, y \in G\}$$

Proposition: Avec les notations précédentes, $F + G$ est le plus petit sous-espace vectoriel de E contenant $F \cup G$.

Preuve: — — $0_E = \underbrace{0_E}_{\in F} + \underbrace{0_E}_{\in G} \in F + G$

— Soient $u \in F + G, v \in F + G, \lambda, \mu \in \mathbb{K}$
On pose

$$\begin{cases} u = x + y \text{ avec } \begin{cases} x \in F \\ y \in G \end{cases} \\ v = a + b \text{ avec } \begin{cases} a \in F \\ b \in G \end{cases} \end{cases}$$

Donc,

$$\begin{aligned} \lambda u + \mu v &= \lambda(x + y) + \mu(a + b) \\ &= \lambda x + \lambda y + \mu a + \mu b \\ &= (\underbrace{\lambda x + \mu a}_{\in F}) + (\underbrace{\lambda y + \mu b}_{\in G}) \in F + G \end{aligned}$$

Ainsi $F + G$ est un sous-espace vectoriel de E .

— Soit $x \in F \cup G$.

Si $x \in F$ alors $x = \underbrace{x}_{\in F} + \underbrace{0_E}_{\in G} \in F + G$

Si $x \in G$ alors $x = \underbrace{0_E}_{\in F} + \underbrace{x}_{\in G} \in F + G$

Donc, $F \cup G \subset F + G$

— Soit H un sous-espace vectoriel de E tel que $F \cup G \subset H$

Soit $u \in F + G$. On pose $u = x + y$ avec $\begin{cases} x \in F \\ y \in G \end{cases}$

$$\begin{cases} x \in F \subset F \cup G \subset H \\ y \in G \subset F \cup G \subset H \end{cases}$$

H est un sous-espace vectoriel de E donc $x + y \in H$.
On a montré que $F + G \subset H$

□

Définition: Soit $(E, +, \cdot)$ un \mathbb{K} -espace vectoriel et $(F_i)_{i \in I}$ une famille quelconque non

vide de sous-espaces vectoriels de E . On définit $\sum_{i \in I} F_i$ par

$$\begin{aligned}\sum_{i \in I} F_i &= \left\{ \sum_{i \in I} x_i \mid (x_i)_{i \in I} \in \prod_{i \in I} F_i; (x_i) \text{ presque nulle} \right\} \\ &= \left\{ \sum_{i \in I} x_i \mid (x_i) \in \prod_{i \in I} F_i; \{i \in I \mid x_i \neq 0_E\} \text{ est fini} \right\}\end{aligned}$$

$\sum_{i \in I} F_i$ est l'ensemble de sommes finies obtenues à partir d'éléments de $\prod_{i \in I} F_i$

EXEMPLE:

$$E = \mathbb{R}^{\mathbb{R}}$$

$$\forall i \in \mathbb{N}, F_i = \{x \mapsto ax^i \mid a \in \mathbb{R}\}$$

$\sum_{i \in \mathbb{N}} F_i$ est l'ensemble des fonctions polynomiales

Proposition: Une somme quelconque de sous-espaces vectoriels est le plus petit sous-espace vectoriel contenant leur réunion. \square

Définition: Soient F et G deux sous-espaces vectoriels de E . On dit qu'ils sont en somme directe si

$$\forall u \in F + G, \exists! (x, y) \in F \times G, u = x + y$$

Dans ce cas, l'espace $F + G$ est noté $F \oplus G$

EXEMPLE:

$$E = \mathbb{R}^3$$

$$F = \{(x, 0, x) \mid x \in \mathbb{R}\}$$

$$G = \left\{ (x, y, z) \mid (S) : \begin{cases} x + y + z = 0 \\ y - z = 0 \end{cases} \right\}$$

$F \oplus G$?

— $(0, 0, 0) \in F$ car $0 \in \mathbb{R}$

$$\text{Soient } x, y \in \mathbb{R}, \begin{cases} u = (x, 0, x) \\ v = (y, 0, y) \end{cases}$$

Soient $\lambda, \mu \in \mathbb{R}$

$$\begin{aligned}\lambda u + \mu v &= \lambda(x, 0, x) + \mu(y, 0, y) \\ &= (\lambda x, 0, \lambda x) + (\mu y, 0, \mu y) \\ &= (\lambda x + \mu y, 0, \lambda x + \mu y) \in F\end{aligned}$$

Donc F est un sous-espace vectoriel de E

— $(0, 0, 0) \in G$ car (S) est homogène

$$\begin{cases} u = (x, y, z) \in G \\ v = (a, b, c) \in G \end{cases}$$

Soient $\lambda, \mu \in \mathbb{R}$

$$\begin{aligned}
\lambda u + \mu v \in G &\iff \lambda(x, y, z) + \mu(a, b, c) \in G \\
&\iff (\lambda x + \mu a, \lambda y + \mu b, \lambda z + \mu c) \in G \\
&\iff \begin{cases} (\lambda x + \mu a) + (\lambda y + \mu b) + (\lambda z + \mu c) = 0 \\ (\lambda y + \mu b) - (\lambda z + \mu c) = 0 \end{cases} \\
&\iff \begin{cases} \lambda \underbrace{(x+y+z)}_{=0} + \mu \underbrace{(a+b+c)}_{=0} = 0 \\ \lambda \underbrace{(y-z)}_{=0} + \mu \underbrace{(b-c)}_{=0} = 0 \end{cases} \\
&\iff \begin{cases} 0 = 0 \\ 0 = 0 \end{cases}
\end{aligned}$$

— Soit $w \in E$. On pose $w = (x, y, z)$

$$\begin{aligned}
w \in F + G &\iff \exists(u, v) \in F \times G, w = u + v \\
&\iff \exists x' \in \mathbb{R}, \exists(a, b, c) \in \mathbb{R}^3, \begin{cases} w = (x', 0, x') + (a, b, c) \\ a + b + c = 0 \\ b - c = 0 \end{cases} \\
&\iff \exists(x', a, b, c) \in \mathbb{R}^4, \begin{cases} (x, y, z) = (a + x', b, c + x') \\ a + b + c = 0 \\ b - c = 0 \end{cases} \\
&\iff \exists(x', a, b, c) \in \mathbb{R}^4, (S'): \begin{cases} a + x' = x \\ b = y \\ c + x' = z \\ a + b + c = 0 \\ b - c = 0 \end{cases}
\end{aligned}$$

(S') est un système linéaire à 4 inconnues (x', a, b, c) , 5 équations, 3 paramètres (x, y, z)

$$(S') \iff \begin{cases} b = y \\ c = y \\ x' = z - y \\ a = x - z + y \\ x + 3y - z = 0 \end{cases}$$

Si $x + 3y - z \neq 0$ alors (S') n'a pas de solutions et donc $w \notin F + G$
Si $x + 3y - z = 0$ alors (S') a une unique solution alors

$$\exists!(u, v) \in F \times G, w = u + v$$

On a montré que

$$F \oplus G = \{(x, y, z) \in \mathbb{R}^3 \mid x + 3y - z = 0\}$$

Proposition: Soient $(E, +, \cdot)$ un \mathbb{K} -espace vectoriel, F et G deux sous-espaces vectoriels de E
 F et G sont en somme directe si et seulement si $F \cap G = \{0_E\}$

Preuve: “ \implies ” On suppose la somme directe.

Soit $x \in F \cap G$.

$$\text{D'une part, } 0_E = \underbrace{0_E}_{\in F} + \underbrace{0_E}_{\in G}$$

D'autre part, $0_E = \underbrace{x}_{\in F} + \underbrace{(-x)}_{\in G}$

Par unicité, $x = 0_E$
 “ \iff ” On suppose $F \cap G = \{0_E\}$
 Soit $x \in F + G$ et on suppose que x a deux décompositions :

$$\begin{cases} x = u + v, & u \in F, v \in G \\ x = u' + v', & u' \in F, v' \in G \end{cases}$$

D'où, $u - u' = v' - v$

$$\text{Or, } \begin{cases} u - u' \in F \\ v - v' \in G \end{cases}$$

Donc, $u - u' \in F \cap G = \{0_E\}$
 donc $u - u' = 0_E$ donc $u = u'$ donc $v' = v$

□

REMARQUE:

Ce résultat est inutile pour l'instant (en l'absence d'arguments dimensionnels) pour prouver un résultat de la forme $E = F \oplus G$

EXEMPLE:

$$E = \mathbb{R}^{\mathbb{R}}$$

$$F = \{f \in E \mid f \text{ paire}\} \text{ et } G = \{f \in E \mid f \text{ impaire}\}$$

Prouvons que $E = F \oplus G$

Soit $f \in F \cap G$ donc

$$\forall x \in \mathbb{R}, f(-x) = f(x) = -f(x)$$

Donc

$$\forall x \in \mathbb{R}, f(x) = -f(x)$$

et donc

$$\forall x \in \mathbb{R}, f(x) = 0$$

donc $f = 0_E$

Ainsi, la somme de F est G est directe

$$F + G = F \oplus G$$

Montrons que $E = F + G$. Soit $f \in E$.

ANALYSE Soient $g \in G$ et $h \in F$ telles que

$$f = g + h$$

Donc

$$\forall x \in \mathbb{R}, \begin{cases} f(x) = g(x) + h(x) \\ f(-x) = -g(x) + h(x) \end{cases}$$

et donc

$$\begin{cases} h(x) = \frac{1}{2}(f(x) + f(-x)) \\ g(x) = \frac{1}{2}(f(x) - f(-x)) \end{cases}$$

Donc $F + G = F \oplus G$.

SYNTHÈSE On pose

$$\begin{cases} g : x \mapsto \frac{1}{2}(f(x) - f(-x)) \\ h : x \mapsto \frac{1}{2}(f(x) + f(-x)) \end{cases}$$

On vérifie que $\begin{cases} g \in F \\ h \in F \\ g + h = f \end{cases}$

On a prouvé que $E = F + G$

EXEMPLE:

$$E = \mathcal{M}_2(\mathbb{C})$$

$$F = S_2(\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ b & c \end{pmatrix} \mid a, b, c \in \mathbb{C} \right\}$$

$$\left(\begin{array}{c|c} & \overbrace{\quad \quad \quad (u) \quad \quad \quad} \\ \diagup & \diagup \\ & (u) \\ \diagdown & \diagdown \end{array} \right)$$

$$G = A_2(\mathbb{C}) = \left\{ \begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix} \mid a \in \mathbb{C} \right\}$$

$$\left(\begin{array}{c|c} 0 & \overbrace{\quad \quad \quad (u) \quad \quad \quad} \\ \diagup & \diagup \\ & (-u) \\ \diagdown & \diagdown \end{array} \right)$$

$$E = F \oplus G$$

Définition: Soit $(E, +, \cdot)$ un \mathbb{K} -espace vectoriel. On dit que F et G sont supplémentaires dans E si

$$E = F \oplus G$$

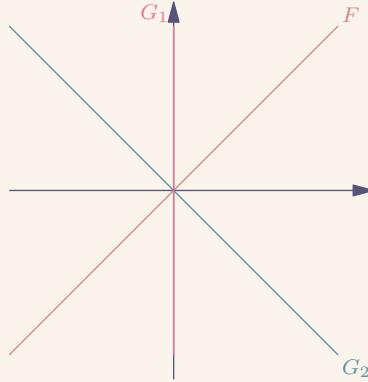
en d'autres termes,

$$\forall x \in E, \exists ! (y, z) \in F \times G, x = y + z$$

EXEMPLE:

$$E = \mathbb{R}^2$$

$$F = \{(x, y) \in \mathbb{R}^2, y = x\}$$



$$G_1 \oplus F = E \text{ et } G_2 \oplus F = E$$

Soit $(x, y) \in E$

$$\begin{aligned} (x, y) &= \underbrace{(x, x)}_{\in F} + \underbrace{(0, y - x)}_{\in G_1} \\ &= \underbrace{\left(\frac{x+y}{2}, \frac{x+y}{2} \right)}_{\in F} + \underbrace{\left(\frac{x+y}{2}, \frac{x+y}{2} \right)}_{\in G_2} \end{aligned}$$

Définition: Soit $(F_i)_{i \in I}$ une famille non vide de sous-espaces vectoriels de $(E, +, \cdot)$. On dit qu'ils sont en somme directe si

$$\forall x \in \sum_{i \in I} F_i, \exists! (x_i)_{i \in I} \in \prod_{i \in I} F_i \text{ presque nulle telle que } x = \sum_{i \in I} x_i$$

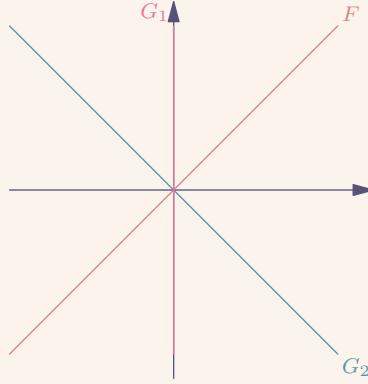
Dans ce cas, on écrit $\bigoplus_{i \in I} F_i$ à la place de $\sum_{i \in I} F_i$

EXEMPLE:
 E : l'espace des fonctions polynomiales

$$\forall i \in \mathbb{N}, F_i = \{x \mapsto ax^i \mid a \in \mathbb{K}\}$$

$$E = \bigoplus_{i \in \mathbb{N}} F_i$$

EXEMPLE:
 $E = \mathbb{R}^2$



$$\begin{cases} F = \{(x, x) \mid x \in \mathbb{R}\} \\ G = \{(0, x) \mid x \in \mathbb{R}\} \\ H = \{(x, -x) \mid x \in \mathbb{R}\} \end{cases}$$

On a $F \cap G \cap H = \{0_E\}$ mais leur somme n'est pas directe

$$\begin{aligned} (0, 0) &= \underbrace{(1, 1)}_{\in F} + \underbrace{(0, -2)}_{\in G} + \underbrace{(-1, 1)}_{\in H} \\ &= \underbrace{(2, 2)}_{\in F} + \underbrace{(0, -4)}_{\in G} + \underbrace{(-2, 2)}_{\in H} \end{aligned}$$

3 Familles de vecteurs

Définition: Soit $(E, +, \cdot)$ un \mathbb{K} -espace vectoriel et $A \in \mathcal{P}(E)$. Le sous-espace vectoriel engendré par A est le plus petit sous espace vectoriel V de E tel que $A \subset V$.
 On le note $\text{Vect}(A)$

EXEMPLE:
 E un \mathbb{K} -espace vectoriel.
 — $\text{Vect}(\{0_E\}) = \{0_E\}$

- $\text{Vect}(\emptyset) = \{0_E\}$
- $\text{Vect}(E) = E$
- Soit $u \in E \setminus \{0_E\}$
 $\text{Vect}(\{u\}) = \{\lambda u \mid \lambda \in \mathbb{K}\} = \mathbb{K}u$
- Soient $u, v \in E \setminus \{0_E\}$
 $\text{Vect}(\{u, v\}) = \{\lambda u + \mu v \mid (\lambda, \mu) \in \mathbb{K}^2\} = \mathbb{K}u + \mathbb{K}v$

Définition: Soit $(E, +, \cdot)$ un \mathbb{K} -espace vectoriel et $u \in E \setminus \{0_E\}$. La droite (vectorielle) engendrée par u est $\mathbb{K}u = \text{Vect}(u) = \text{Vect}(\{u\})$. Soit $v \in E$. On dit que u et v sont colinéaires si $v \in \mathbb{K}u$. Si v n'est pas colinéaire à u alors, $\text{Vect}(u, v) = \mathbb{K}u + \mathbb{K}v$ est appelé plan (vectoriel) engendré par u et v .

EXEMPLE:

L'ensemble des solutions d'une équation différentielle linéaire homogène d'ordre 1 est une droite vectorielle.

L'ensemble des solutions d'une équation différentielle linéaire homogène d'ordre 2 à coefficients constants est un plan vectoriel.

$$\{y \in \mathcal{C}^2(\mathbb{R}) \mid y'' + y = 0\} = \text{Vect}(\cos, \sin)$$

Proposition: Soit $(e_i)_{i \in I}$ un famille non vide de vecteurs d'un \mathbb{K} -espace vectoriel $(E, +, \cdot)$. Alors,

$$\begin{aligned} \text{Vect}((e_i)_{i \in I}) &= \left\{ \sum_{i \in I} \lambda_i e_i \mid (\lambda_i)_{i \in I} \in \mathbb{K}^I \text{ et } (\lambda_i) \text{ presque nulle} \right\} \\ &= \sum_{i \in I} \mathbb{K}e_i \end{aligned}$$

Preuve:

$$\text{On pose } F = \sum_{i \in I} \mathbb{K}e_i$$

F est un sous espace vectoriel de E .

$$\begin{aligned} \forall i \in I, e_i &= \underbrace{\sum_{j \in I} \lambda_j e_j}_{\in F} \text{ où } \lambda_j = \begin{cases} 0 & \text{si } i \neq j \\ 1 & \text{si } i = j \end{cases} \\ &= \delta_{i,j} \text{ (symbole de Kronecker)} \end{aligned}$$

Soit G un sous espace vectoriel de E tel que

$$\forall i \in I, e_i \in G$$

Soit $u \in F$. Soit $(\lambda_i)_{i \in I}$ une famille presque nulle de scalaires telle que $u = \sum_{i \in I} \lambda_i e_i$

Soit $\{i_1, \dots, i_k\} = \{i \in I \mid \lambda_i \neq 0_K\}$
 Donc,

$$u = \sum_{j=1}^k \underbrace{\lambda_{i_j} e_{i_j}}_{\in G} \in G$$

Donc $F \subset G$

□

Définition: On dit que $(e_i)_{i \in I}$ est une famille génératrice de E si

$$E = \text{Vect}((e_i)_{i \in I})$$

EXEMPLE:

$$E = \mathbb{R}^3$$

$$\begin{cases} e_1 = (1, 0, 1) \\ e_2 = (0, 1, 1) \\ e_3 = (1, 1, 1) \\ e_4 = (1, 0, 0) \\ e_5 = (0, 1, 2) \end{cases}$$

Soit $(x, y, z) \in \mathbb{R}^3$. On cherche $(\lambda_1, \dots, \lambda_5) \in \mathbb{R}^5$ tels que

$$(E) : (x, y, z) = \sum_{i=1}^5 \lambda_i e_i$$

$$\begin{aligned} (E) &\iff (x, y, z) = (\lambda_1 + \lambda_3 + \lambda_4, \lambda_2 + \lambda_3 + \lambda_5, \lambda_1 + \lambda_2 + \lambda_3 + 2\lambda_5) \\ &\iff \begin{cases} \lambda_1 + \lambda_3 + \boxed{\lambda_4} = x \\ \lambda_2 + \boxed{\lambda_3} + \lambda_5 = y \\ \boxed{\lambda_1} + \lambda_2 + \lambda_3 + 2\lambda_5 = z \end{cases} \\ &\iff \begin{cases} \lambda_4 = x - \lambda_1 - \lambda_3 \\ \lambda_3 = y - \lambda_2 - \lambda_5 \\ \lambda_1 = z - \lambda_2 - \lambda_3 - 2\lambda_5 \end{cases} \end{aligned}$$

Par exemple, $(\lambda_1 = z - y, \lambda_2 = 0, \lambda_3 = y, \lambda_4 = x - z, \lambda_5 = 0)$ est solution

Donc

$$\text{Vect}(e_1, e_2, e_3, e_4, e_5) = E$$

EXEMPLE:
 $E = \mathbb{R}^4$

$$\begin{cases} e_1 = (1, 0, 1, 0) \\ e_2 = (0, 1, 0, 1) \\ e_3 = (1, 1, 1, 1) \\ e_4 = (1, -1, 1, -1) \\ e_5 = (1, 1, 0, 0) \end{cases}$$

Soit $(x, y, z, t) \in \mathbb{R}^4$, $(\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5) \in \mathbb{R}^5$

$$(E) \quad (x, y, z, t) = \sum_{i=1}^5 \lambda_i e_i \iff \begin{cases} x = \lambda_1 + \lambda_3 + \lambda_4 + \lambda_5 \\ y = \lambda_2 + \lambda_3 - \lambda_4 + \lambda_5 \\ z = \lambda_1 + \lambda_3 + \lambda_4 \\ t = \lambda_2 + \lambda_3 - \lambda_4 \end{cases}$$

$$\stackrel{L_2 \leftarrow L_2 - L_4}{\iff} \begin{cases} \lambda_5 = x - z \\ \lambda_5 = y - t \\ \lambda_1 + \lambda_3 + \lambda_4 = z \\ \lambda_2 + \lambda_3 - \lambda_4 = t \end{cases}$$

$$\stackrel{L_2 \leftarrow L_2 - L_1}{\iff} \begin{cases} \lambda_5 = x - z \\ 0 = y - t - x + z \\ \lambda_1 + \lambda_3 + \lambda_4 = z \\ \lambda_1 + \lambda_3 - \lambda_4 = t \end{cases}$$

Par exemple ; $(1, 0, 0, 0) \notin \text{Vect}(e_1, e_2, e_3, e_4, e_5)$

Proposition: Soit $(e_i)_{i \in I}$ une famille génératrice de E et $(u_j)_{j \in J}$ une surfamille de $(e_i)_{i \in I}$ constituée de vecteurs de E :

$$\forall i \in I, \exists j \in J, e_i = u_j$$

Alors, $(u_j)_{j \in J}$ engendre E . □

Proposition: Soit $(e_i)_{i \in I}$ une famille génératrice de E et $i_0 \in I$

$$\begin{aligned} (e_i)_{i \in I \setminus \{i_0\}} \text{ engendre } E &\iff e_{i_0} \in \text{Vect}((e_i)_{i \in I \setminus \{i_0\}}) \\ &\iff e_{i_0} \text{ est une combinaison linéaire des } e_i \ (i \in I, i \neq i_0) \end{aligned}$$

Preuve: “ \implies ” $E = \text{Vect}((e_i)_{i \neq i_0})$ et $e_{i_0} \in E$
“ \impliedby ” Soit $u \in E$. Soit $(\lambda_i)_{i \in I}$ une famille presque nulle de scalaires telle que

$$u = \sum_{i \in I} \lambda_i e_i$$

Soit $(\mu_i)_{i \neq i_0}$ une famille de scalaires telle que

$$e_{i_0} = \sum_{i \in I \setminus \{i_0\}} \mu_i e_i$$

D'où,

$$\begin{aligned} u &= \lambda_{i_0} e_{i_0} + \sum_{i \in I \setminus \{i_0\}} \lambda_i e_i \\ &= \lambda_{i_0} \sum_{i \in I \setminus \{i_0\}} \mu_i e_i + \sum_{i \in I \setminus \{i_0\}} \lambda_i e_i \\ &= \sum_{i \in I \setminus \{i_0\}} (\lambda_{i_0} \mu_i + \lambda_i) e_i \\ &\in \text{Vect}((e_i)_{i \in I \setminus \{i_0\}}) \end{aligned}$$

□

Proposition: Soit $(e_i)_{i \in I}$ une famille génératrice de E , $i_0 \in I$.

1. On pose $u_i = \begin{cases} e_i & \text{si } i \neq i_0 \\ \lambda e_{i_0} & \text{sinon} \end{cases}$ où $\lambda \in \mathbb{K} \setminus \{0_{\mathbb{K}}\}$

Alors, $(u_i)_{i \in I}$ engendre E

2. Soit $v \in \text{Vect}((e_i)_{i \in I \setminus \{i_0\}})$.

$$\text{On pose } u_i = \begin{cases} e_i & \text{si } i \neq i_0 \\ e_{i_0} + v & \text{sinon} \end{cases} \text{ où } \lambda \in \mathbb{K} \setminus \{0_{\mathbb{K}}\}$$

Alors, $(u_i)_{i \in I}$ engendre E

Preuve: 1. Soit $u \in E$. On pose

$$u = \sum_{i \in I} \lambda_i e_i$$

où $(\lambda_i) \in \mathbb{K}^I$ presque nulle

$$\begin{aligned} u &= \lambda_{i_0} e_{i_0} + \sum_{i \in I \setminus \{i_0\}} \lambda_i e_i \\ &= \lambda_{i_0} \lambda^{-1} u_{i_0} + \sum_{i \in I \setminus \{i_0\}} \lambda_i u_i \\ &\in \text{Vect}((u_i)_{i \in I}) \end{aligned}$$

$$2. \text{ Soit } u = \sum_{i \in I} \lambda_i e_i \in E$$

$$\begin{aligned} u &= \lambda_{i_0} e_{i_0} + \sum_{i \in I \setminus \{i_0\}} \lambda_i e_i \\ &= \lambda_{i_0} (u_{i_0} - v) + \sum_{i \in I \setminus \{i_0\}} \lambda_i u_i \end{aligned}$$

Or, $v = \sum_{i \in I \setminus \{i_0\}} \mu_i e_i = \sum_{i \in I \setminus \{i_0\}} \mu_i u_i$ où $(\mu_i)_{i \in I}$ presque nulle

Donc, $u = \lambda_{i_0} + \sum_{i \in I \setminus \{i_0\}} (\lambda_i - \lambda_{i_0} \mu_i) u_i \in \text{Vect}((u_i)_{i \in I})$

□

Définition: Soit $(e_i)_{i \in I}$ une famille de vecteurs. On dit que $(e_i)_{i \in I}$ est libre si aucun vecteur de cette famille n'est une combinaison linéaire des autres vecteurs de cette famille :

$$\forall i \in I, e_i \notin \text{Vect}((e_j)_{j \in I \setminus \{i\}})$$

On dit aussi que les e_i sont linéairement indépendants

]

Proposition:

$$(e_i)_{i \in I} \text{ est libre} \iff \forall (\lambda_i) \in \mathbb{K}^I \text{ presque nulle}, \left(\sum_{i \in I} \lambda_i e_i = 0_E \implies \forall i \in I, \lambda_i = O_{\mathbb{K}} \right)$$

Preuve: “ \implies ” Soit $(\lambda_i) \in \mathbb{K}^I$ presque nulle. On suppose que

$$\sum_{i \in I} \lambda_i e_i = 0_E$$

On suppose aussi qu'il existe $i_0 \in I$ tel que $\lambda_{i_0} \neq 0_{\mathbb{K}}$
On a alors

$$\lambda_{i_0} e_{i_0} = - \sum_{i \in I \setminus \{i_0\}} \lambda_i e_i$$

$\lambda_{i_0} \neq 0_{\mathbb{K}}$ donc il a un inverse $\lambda_{i_0}^{-1}$ donc

$$e_{i_0} = \sum_{i \in I \setminus \{i_0\}} (-\lambda_i \lambda_{i_0}^{-1}) e_i \in \text{Vect}((e_i)_{i \in I \setminus \{i_0\}})$$

une contradiction \nparallel
“ \iff ” On suppose que $(e_i)_{i \in I}$ n'est pas libre. On considère $i_0 \in I$ tel que e_{i_0} soit une combinaison linéaire des $e_i, i \in I \setminus \{i_0\}$

$$e_{i_0} = \sum_{i \in I \setminus \{i_0\}} \mu_i e_i$$

avec $(\mu_i)_{i \in I \setminus \{i_0\}}$ famille presque nulle de scalaires.

Alors, $1_{\mathbb{K}} e_{i_0} - \sum_{i \in I \setminus \{i_0\}} \mu_i e_i = 0_E$ Par hypothèse

$$\begin{cases} 1_{\mathbb{K}} = 0_{\mathbb{K}} \\ \forall i \neq i_0, -\mu_i = 0_{\mathbb{K}} \end{cases}$$

une contradiction \nparallel

□

EXEMPLE:

$E = \mathbb{R}^3$ On pose $\begin{cases} e_1 = (1, 1, 0) \\ e_2 = (1, 0, 1) \end{cases}$
Soit $(\lambda_1, \lambda_2) \in \mathbb{R}^2$.

$$\lambda_1 e_1 + \lambda_2 e_2 = 0_E \iff (\lambda_1 + \lambda_2, \lambda_1, \lambda_2) = (0, 0, 0)$$

$$\iff \begin{cases} \lambda_1 + \lambda_2 = 0 \\ \lambda_1 = 0 \\ \lambda_2 = 0 \end{cases} \iff \lambda_1 = \lambda_2 = 0$$

Donc, (e_1, e_2) est libre.

EXEMPLE:

$E = \mathbb{R}^{\mathbb{R}}, e_1 = \cos, e_2 = \sin$

Soit $(\lambda_1, \lambda_2) \in \mathbb{R}^2$.

$$\begin{aligned}\lambda_1 e_1 + \lambda_2 e_2 = 0_E &\iff \forall x \in \mathbb{R}, \lambda_1 \cos(x) + \lambda_2 \sin(x) = 0 \\ &\implies \begin{cases} \lambda_1 = 0 & (x = 0) \\ \lambda_2 = 0 & (x = 0 \text{ dans la dérivée}) \end{cases}\end{aligned}$$

Donc (e_1, e_2) est libre.

Proposition: Soit $(e_i)_{i \in I}$ une famille libre de E . Alors

$$\sum_{i \in I} \mathbb{K}e_i = \bigoplus_{i \in I} \mathbb{K}e_i$$

i.e.

$$\forall u \in \sum_{i \in I} \mathbb{K}e_i, \exists! (\lambda_i) \in \mathbb{K}^I \text{ presque nulle telle que } u = \sum_{i \in I} \lambda_i e_i$$

En d'autres termes, tout vecteur de E a au plus une décomposition en combinaisons linéaires des $e_i, i \in I$

Preuve:

$$\text{Soit } u \in \sum_{i \in I} \mathbb{K}e_i$$

On suppose que u a au plus 2 décompositions

$$u = \sum_{i \in I} \lambda_i e_i = \sum_{i \in I} \mu_i e_i$$

avec (λ_i) et (μ_i) presque nulles.

Alors,

$$0_E = u - u = \sum_{i \in I} \lambda_i e_i - \sum_{i \in I} \mu_i e_i = \sum_{i \in I} (\lambda_i - \mu_i) e_i$$

Or, $(e_i)_{i \in I}$ est libre donc

$$\forall i \in I, \lambda_i \mu_i = 0_{\mathbb{K}}$$

□

Proposition: Soit $(e_i)_{i \in I}$ une famille libre de E .

1. Toute sous famille de (e_i) est encore libre
2. Soit $u \in E$, $\mathcal{F} = (e_i \mid i \in I) \cup \{u\}$.

$$\mathcal{F} \text{ est libre} \iff u \notin \text{Vect}(e_i \mid i \in I)$$

3. (a) Quand on remplace un vecteur e_i par λe_i avec $\lambda \neq 0_{\mathbb{K}}$, la famille obtenue est libre.
- (b) Quand on remplace un vecteur e_i par $v + e_i$ avec $v \in \text{Vect}(e_j \mid j \neq i)$, la famille obtenue est libre.

Définition: Soit $(e_i)_{i \in I}$ une famille de vecteurs de E . On dit que (e_i) est une base de E si c'est à la fois une famille libre et génératrice de E ; i.e. si

$$E = \bigoplus_{i \in I} \mathbb{K}e_i$$

i.e. si

$$\forall u \in E, \exists!(\lambda_i) \in \mathbb{K}^I \text{ presque nulle telle que } u = \sum_{i \in I} \lambda_i e_i$$

Dans ce cas, on dit que les λ_i sont les coordonnées de u dans la base $(e_i)_{i \in I}$ EXEMPLE: 1. $(1, i)$ est une base de \mathbb{C} en tant que \mathbb{R} -espace vectoriel2. (1) est une base de \mathbb{C} en tant que \mathbb{C} -espace vectoriel

3.

$$\begin{cases} u = 1 + i \\ v = 1 - i \end{cases}$$

 (u, v) est une \mathbb{R} -base de \mathbb{C} En effet, soit $z = a + ib \in \mathbb{C}$ avec $(a, b) \in \mathbb{R}^2$. Soient $\lambda, \mu \in \mathbb{R}$.

$$\begin{aligned} z = \lambda u + \mu v &\iff a + ib = \lambda + \mu + i(\lambda - \mu) \\ &\iff \begin{cases} a = \lambda + \mu \\ b = \lambda - \mu \end{cases} \\ &\iff \begin{cases} \lambda = \frac{a+b}{2} \\ \mu = \frac{a-b}{2} \end{cases} \end{aligned}$$

AUTRE MÉTHODE $(1, i)$ basedonc $(1, 1+i)$ basedonc $(1 - (1+i), 1+i)$ basedonc $(-2i, 1+i)$ basedonc $(1+i-2i, 1+i)$ basedonc $(1-i, 1+i)$ baseEXEMPLE (Bases canoniques): 1. La base canonique de \mathbb{K}^n est (e_1, \dots, e_n) où $\forall i, e_i = (0_{\mathbb{K}}, \dots, 0_{\mathbb{K}}, \underbrace{1_{\mathbb{K}}}_{\text{en } i\text{ème position}}, 0_{\mathbb{K}}, \dots, 0_{\mathbb{K}})$ car

$$\begin{aligned} \forall u \in \mathbb{K}^n, \exists! (x_1, \dots, x_n) \in \mathbb{K}^n, u &= (x_1, \dots, x_n) = x_1(1_{\mathbb{K}}, 0_{\mathbb{K}}, \dots, 0_{\mathbb{K}}) \\ &\quad + x_2(0_{\mathbb{K}}, 1_{\mathbb{K}}, \dots, 0_{\mathbb{K}}) \\ &\quad \vdots \quad \vdots \\ &\quad + x_n(0_{\mathbb{K}}, 0_{\mathbb{K}}, \dots, 1_{\mathbb{K}}) \\ &= \sum_{i=1}^n x_i e_i \end{aligned}$$

2. E l'ensemble des fonctions polynomiales de \mathbb{K} dans \mathbb{K} à coefficients dans \mathbb{K} où \mathbb{K} est infini.La base canonique de E est $(x \mapsto x^n)_{n \in \mathbb{N}}$ car

$$\forall P \in E, \exists! n \in \mathbb{N}, \exists! (a_0, \dots, a_n) \in \mathbb{K}^{n+1}, \forall x \in \mathbb{K}, P(x) = \sum_{i=0}^n a_i x^i$$

3. $E = \mathcal{M}_{n,p}(\mathbb{K})$ La base canonique de E est $(E_{i,j})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}}$ où

$$\forall i \in [\![1, n]\!], \forall j \in [\![1, p]\!], E_{i,j} = (\sigma_{i,j}^{k,\ell})_{\substack{1 \leqslant k \leqslant n \\ 1 \leqslant \ell \leqslant p}}$$

i.e.

$$E_{i,j} = \begin{pmatrix} 0_K & \cdots & 0_K \\ \vdots & 1_K & \vdots \\ 0_K & \cdots & 0_K \end{pmatrix} \xleftarrow{i} \downarrow^j$$

$$\forall A = (a_{i,j}) \in \mathcal{M}_{n,p}, A = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} a_{i,j} E_{i,j}$$

CHAPITRE

16

DÉRIVATION

1 Définition et premières propriétés

Dans ce paragraphe, f désigne une fonction définie sur un intervalle ouvert non vide I à valeurs réelles.

Définition: Soit $a \in I$. On dit que f est dérivable en a si $\frac{f(x) - f(a)}{x - a}$ a une limite qui est finie quand $x \rightarrow a$.

Dans ce cas, cette limite est notée $f'(a)$ et est appelée nombre dérivée de f en a .
On dit que f est dérivable sur I si f est dérivable en tout $a \in I$.

L'application $\begin{matrix} I \longrightarrow \mathbb{R} \\ a \mapsto f'(a) \end{matrix}$ est la dérivée de f et est notée f'

Proposition:

f est dérivable en $a \iff f$ a un développement limité d'ordre 1 au voisinage de a

Preuve: “ \implies ” $f'(a) = \lim_{x \rightarrow a} \frac{f(x) - f(a)}{x - a}$

$$\text{donc } \frac{f(x) - f(a)}{x - a} = f'(a) + \underset{x \rightarrow a}{\mathcal{o}}(1)$$

$$\text{donc } f(x) - f(a) = (x - a)f'(a) + \underset{x \rightarrow a}{\mathcal{o}}(x - a)$$

$$\text{donc } f(x) = f(a) + (x - a)f'(a) + \underset{x \rightarrow a}{\mathcal{o}}(x - a)$$

$$\text{“} \iff \text{” } f(x) = a_0 + a_1(x - a) + \underset{x \rightarrow a}{\mathcal{o}}(x - a)$$

Alors, avec $x = a$, $a_0 = f(a)$ et donc

$$\frac{f(x) - f(a)}{x - a} = \frac{a_1(x - a) + \mathcal{o}(x - a)}{x - a} = a_1 + \mathcal{o}(1) \xrightarrow{x \rightarrow a} a_1 \in \mathbb{R}$$

□

Proposition: Si f est dérivable en a alors f est continue en a .

Preuve:

$$\forall x, f(x) = f(a) + f'(a)(x - a) + \underset{x \rightarrow a}{\circ}(x - a)$$

donc

$$\lim_{\substack{x \rightarrow a \\ \neq}} f(x) = f(a) + f'(a) \times 0 + 0 = f(a)$$

□

Proposition: Soient f et g dérivables en a

1. $f + g$ est dérivable en a et $(f + g)'(a) = f'(a) + g'(a)$
2. $f \times g$ est dérivable en a et $(fg)'(a) = f'(a)g(a) + f(a)g'(a)$
3. Si $g(a) \neq 0$, alors $\frac{f}{g}$ est dérivable en a et

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

Preuve:

$$\begin{cases} f(x) = f(a) + f'(a)(x - a) + \circ(x - a) \\ g(x) = g(a) + g'(a)(x - a) + \circ(x - a) \end{cases}$$

$$f(x) + g(x) = f(a) + g(a) + (x - a) \underbrace{(f'(a) + g'(a))}_{(f+g)'(a)} + \circ(x - a)$$

2.

$$f(x) \times g(x) = f(a)g(a) + (x - a) \underbrace{(f(a)g'(a) + g(a)f'(a))}_{(fg)'(a)} + \circ(x - a)$$

3. On suppose $g(a) \neq 0$

$$\begin{aligned} \frac{1}{g(x)} &= \frac{1}{g(a) + (x - a)g'(a) + \circ(x - a)} \\ &= \frac{1}{g(a)} \times \frac{1}{1 + (x - a)\frac{g'(a)}{g(a)} + \circ(x - a)} \\ &= \frac{1}{g(a)} \times \left(1 - (x - a)\frac{g'(a)}{g(a)} + \circ(x - a)\right) \end{aligned}$$

D'où,

$$\begin{aligned}\frac{f(x)}{g(x)} &= \frac{1}{g(a)} \left(f(a) + (x-a) \left(-\frac{f(a)g'(a)}{g(a)} + f'(a) \right) \right) \circ(x-a) \\ &= \frac{f(a)}{g(a)} + (x-a) \frac{-f(a)g'(a) + f'(a)g(a)}{(g(a))^2} + \circ(x-a)\end{aligned}$$

□

Proposition: Soit f dérivable en a et g dérivable en $f(a)$. Alors, $f \circ g$ est dérivable en a et

$$(g \circ f)'(a) = g'(f(a))f'(a)$$

Preuve:

$$\begin{cases} \forall x, f(x) = f(a) + (x-a)f'(a) + \underset{x \rightarrow a}{\circ}(x-a) \\ \forall y, g(y) = g(f(a)) + (y-f(a))g'(f(a)) + \underset{y \rightarrow f(a)}{\circ}(y-f(a)) \end{cases}$$

Donc,

$$\begin{aligned}g(f(x)) &= g(f(a)) + (f(x)-f(a))g'(f(a)) + \underset{x \rightarrow a}{\circ}(f(x)-f(a)) \text{ car } f \text{ est continue en } a \\ &= g(f(a)) + (x-a)f'(a)g'(f(a)) + \underset{x \rightarrow a}{\circ}((x-a)f'(a) + \underset{x \rightarrow a}{\circ}(x-a)) \\ &= g(f(a)) + (x-a)f'(a)g'(f(a)) + \underset{x \rightarrow a}{\circ}(x-a)\end{aligned}$$

□

Proposition: On suppose que f est bijective dérivable en a et $f'(a) \neq 0$. Si f^{-1} est continue, alors f^{-1} est dérivable en $f(a)$ et

$$(f^{-1})'(f(a)) = \frac{1}{f'(a)}$$

Preuve:

$\forall y \neq f(a)$ on pose $x = f^{-1}(y)$.

$y \xrightarrow{x \rightarrow a} f(a)$ et $x \xrightarrow{y \rightarrow f(a)} a$

$$\frac{f^{-1}(y) - f^{-1}(f(a))}{y - f(a)} = \frac{x - a}{f(x) - f(a)} = \frac{1}{\frac{f(x) - f(a)}{x - a}} \xrightarrow{x \rightarrow a} \frac{1}{f'(a)}$$

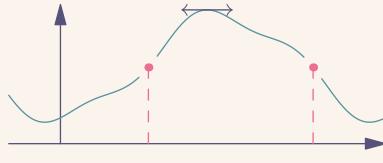
□

2 Théorème de Rolle et accroissements finis

Théorème (Théorème de Rolle): Soit $f : [a, b] \rightarrow \mathbb{R}$ continue sur $[a, b]$ et dérivable sur $]a, b[$. On suppose que $f(a) = f(b)$.

Alors,

$$\exists c \in]a, b[, f'(c) = 0$$



Preuve:

f est continue sur le segment $[a, b]$. On pose

$$\begin{cases} M = \max_{[a, b]}(f) \\ m = \min_{[a, b]}(f) \end{cases}$$

CAS 1

$$\exists c \in]a, b[, M = f(c)$$

$$\begin{aligned} f'(c) &= \lim_{\substack{x \rightarrow c \\ <}} \frac{f(x) - f(c)}{x - c} \geqslant 0 \text{ car } \forall x < c, \begin{cases} f(x) - f(c) \leqslant 0 \\ x - c < 0 \end{cases} \\ &= \lim_{\substack{x \rightarrow c \\ >}} \frac{f(x) - f(c)}{x - c} \leqslant 0 \text{ car } \forall x > c, \begin{cases} f(x) - f(c) \leqslant 0 \\ x - c > 0 \end{cases} \end{aligned}$$

Donc, $f'(c) = 0$

CAS 2

$$\exists c \in]a, b[, m = f(c)$$

$$\begin{aligned} f'(c) &= \lim_{\substack{x \rightarrow c \\ <}} \leqslant 0 \text{ car } \forall x < c, \begin{cases} f(x) - f(c) \geqslant 0 \\ x - c < 0 \end{cases} \\ &= \lim_{\substack{x \rightarrow c \\ >}} \frac{f(x) - f(c)}{x - c} \geqslant 0 \end{aligned}$$

Donc $f'(c) = 0$

CAS 3

$$\forall c \in]a, b[, f(c) \notin \{m, M\}$$

Alors

$$\begin{cases} M \in \{f(a), f(b)\} \\ m \in \{f(a), f(b)\} \end{cases}$$

Or, $f(a) = f(b)$ donc $M = m$ donc f est constante donc

$$\forall x \in [a, b], f'(x) = 0$$

□

Définition: On dit que f présente un maximum local en a s'il existe $\eta > 0$ tel que

$$\forall x \in]a - \eta, a + \eta[, f(x) \leqslant f(a)$$

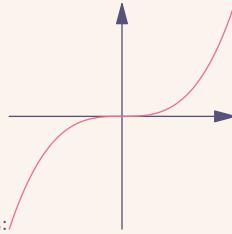
et un minimum local en a s'il existe $\eta > 0$ tel que

$$\forall x \in]a - \eta, a + \eta[, f(x) \geq f(a)$$

Un extremum local est un minimum local ou un maximum local.

Proposition: Soit $a \in I$ tel que $f(a)$ est un extremum local de f où f est dérivable en a . Alors, $f'(a) = 0$ \square

Définition: Soit f dérivable et $a \in I$. On dit que a est un point critique de f si $f'(a) = 0$. On dit que $f(a)$ est une valeur critique.



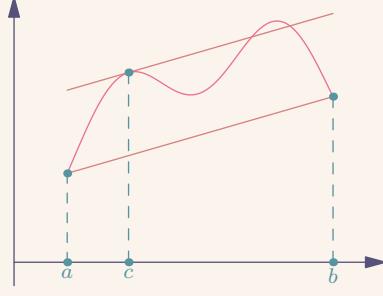
EXEMPLE:

$$x \mapsto x^3$$

$$f'(0) = 0 \text{ mais } 0 \text{ n'est pas un extremum local}$$

Théorème (Théorème des accroissements finis): Soit $f : [a, b] \rightarrow \mathbb{R}$ continue sur $[a, b]$ et dérivable sur $]a, b[$.
Alors, il existe $c \in]a, b[$ tel que

$$\frac{f(b) - f(a)}{b - a} = f'(c)$$



Preuve:

$$\text{On pose } \tau = \frac{f(b) - f(a)}{b - a}$$

$g : x \mapsto f(x) - \tau x$ continue sur $[a, b]$ et dérivable sur $]a, b[$.

$$g(a) - g(b) = f(a) - f(b) - \tau(a - b) = 0$$

D'après le théorème de Rolle, il existe $c \in]a, b[$ tel que $g'(c) = 0$.

$$\forall x, g'(x) = f'(x) - \tau$$

Donc, $f'(c) = \tau$

□

Proposition: Soit $f : I \rightarrow \mathbb{R}$ dérivable avec I un intervalle non vide.

1. f est croissante sur $I \iff \forall x \in I, f'(x) \geq 0$
2. f est décroissante sur $I \iff \forall x \in I, f'(x) \leq 0$
3. $\forall x \in I, f'(x) > 0 \implies f$ strictement croissante
4. $\forall x \in I, f'(x) < 0 \implies f$ strictement décroissante
5. f constante $\iff \forall x \in I, f'(x) = 0$

Preuve: 1. “ \implies ” On suppose f croissante.

Soit $x \in I$.

$$f'(x) = \lim_{y \rightarrow x} \frac{f(y) - f(x)}{y - x}$$

Or, $\forall y, f(y) - f(x)$ et $y - x$ sont de même signe donc $\frac{f(y) - f(x)}{y - x} \geq 0$.

Et donc $f'(x) \geq 0$.

“ \iff ” On suppose que

$$\forall x \in I, f'(x) \geq 0$$

Soit $(a, b) \in I^2$. On suppose que $a \leq b$.

f est continue sur $[a, b]$

f est dérivable sur $]a, b[$

donc, d'après le théorème des accroissements finis, il existe $c \in]a, b[$ tel que

$$f(a) - f(b) = \underbrace{f'(c)}_{\geq 0} \underbrace{(a - b)}_{\leq 0} \leq 0$$

donc $f(a) \leq f(b)$

Donc f est croissante.

On procède de la même manière pour les autres propositions

□

Théorème (Théorème de la limite de la dérivée): Soit $f : I \rightarrow \mathbb{R}$ continue (sur I), $a \in I$. On suppose f dérivable sur $I \setminus \{a\}$ et que $\lim_{\substack{x \rightarrow a \\ \neq}} f'(x)$ existe.

Alors,

$$\frac{f(x) - f(a)}{x - a} \xrightarrow[\substack{x \rightarrow a \\ \neq}]{} \lim_{\substack{x \rightarrow a \\ \neq}} f'(a)$$

Preuve:

On pose $\ell = \lim_{\substack{x \rightarrow a \\ \neq}} f'(x) \in \overline{\mathbb{R}}$.

Soit $x \in I \setminus \{a\}$.

f est continue sur I donc sur $[a, x]$ si $x \geq a$ et sur $[x, a]$ si $x < a$

f est dérivable sur $I \setminus \{a\}$ donc sur $]a, x[$ si $x > a$ et sur $]x, a[$ si $x < a$

D'après le théorème des accroissements finis, il existe $c_x \in]a, x[\cup]x, a[$ tel que

$$\frac{f(x) - f(a)}{x - a} = f'(c_x)$$

— $\forall x < a$, on a $x < c_x < a$

Par encadrement, $c_x \xrightarrow[x \rightarrow a]{<} a$
 — $\forall x > a$, on a $x > c_x > a$
 Par encadrement, $c_x \xrightarrow[x \rightarrow a]{>} a$

Donc,

$$\lim_{x \rightarrow a} c_x = a$$

donc

$$f'(c_x) \xrightarrow[x \rightarrow a]{\neq} \ell$$

(compositions des limites)

□

Proposition: Soit $f : I \rightarrow \mathbb{R}$ dérivable. On suppose qu'il existe $M \in \mathbb{R}$ tel que

$$\forall x \in I, |f'(x)| \leq M$$

Alors f est M -lipschitzienne sur I .

Preuve:

Soient $(a, b) \in I^2$.

D'après le théorème des accroissements finis, il existe $c \in I$ tel que

$$f(a) - f(b) = f'(c)(a - b)$$

donc

$$\begin{aligned} |f(a) - f(b)| &= |f'(c)| |a - b| \\ &\leq M |a - b| \end{aligned}$$

□

3 Dérivées n -ièmes

Définition: On dit que f est une fois dérivable si f est dérivable. Dans ce cas, on note $f^{(1)}$ la fonction f' .

Pour $n \in \mathbb{N}_*$, on dit que f est dérivable n fois si f est dérivable $n - 1$ fois et $f^{(n-1)}$ est dérivable une fois. Dans ce cas, $f^{(n)} = (f^{(n-1)})'$.

REMARQUE (Convention):

$$f^{(0)} = f$$

Définition: f est de classe \mathcal{C}^n si f est dérivables n fois et $f^{(n)}$ est continue.

Proposition: Soit f dérivable n fois et $k \leq n$.

Alors f est dérivables k fois et $f^{(n)} = (f^{(k)})^{(n-k)}$

□

Proposition: Soit f et g deux fonctions dérivables n fois en a . Alors, $f + g$ est dérivable n fois en a et

$$(f + g)^{(n)}(a) = f^{(n)}(a) + g^{(n)}(a)$$

Si f et g sont de classe \mathcal{C}^n , alors, $f + g$ est de classe \mathcal{C}^n

Preuve (Récurrence immédiate sur n): □

Proposition (Leibniz): Soient f et g dérivables n fois en a . Alors, $f \times g$ est dérivables n fois en a . et

$$(*) : (f \times g)^{(n)}(a) = \sum_{k=0}^n \binom{n}{k} f^{(n)}(a) g^{(n-k)}(a)$$

Si f et g sont de classe \mathcal{C}^n alors $f \times g$ est de classe \mathcal{C}^n .

Preuve (par récurrence sur n): — Soient f et g deux fonctions

$$(f \times g)^{(0)}(a) = (f \times g)(a) = f(a)g(a)$$

et

$$\sum_{k=0}^0 \binom{0}{k} f^{(k)}(a) g^{(n-k)}(a) = f^{(0)}(a) g^{(0)}(a) = f(a)g(a)$$

— Soit $n \in \mathbb{N}$. On suppose $(*)$ vraie quelles que soient les fonctions f et g dérivables n fois en a .

Soient f et g dérivables $n - 1$ fois en a . En particulier, elles sont dérivables n fois en a . Donc

$$(f \times g)^{(n)}(a) = \sum_{k=0}^n \binom{n}{k} f^{(k)}(a) g^{(n-k)}(a)$$

$$\forall k \in \llbracket 0, n \rrbracket, \begin{cases} f^{(k)} \text{ est dérivable en } a \\ g^{(n-k)} \text{ est dérivable en } a \end{cases}$$

Donc, $(f \times g)^{(n)}$ est dérivable en a donc $f \times g$ est dérivables $n + 1$ fois en a .

$$\begin{aligned} (f \times g)^{(n+1)}(a) &= \sum_{k=0}^n \binom{n}{k} \left(f^{(k+1)}(a) g^{(n-k)}(a) + f^{(k)}(a) g^{(n-k+1)}(a) \right) \\ &= \sum_{k=1}^n \binom{n}{k-1} f^{(k)}(a) \times g^{(n-k+1)}(a) + \sum_{k=0}^n \binom{n}{k} f^{(k)}(a) g^{(n-k+1)}(a) \\ &= \sum_{k=1}^n \binom{n+1}{k} f^{(k)}(a) g^{(n+1-k)} + f^{(n+1)}(a) g(a) + f(a) g^{(n+1)}(a) \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} f^{(k)}(a) g^{(n+1-k)}(a) \end{aligned}$$

□

Proposition: Soient f et g dérivables n fois (resp. de classe \mathcal{C}^n). On suppose $g(a) \neq 0$. Alors, $\frac{f}{g}$ est dérivables n fois (resp. \mathcal{C}^n) en a .

Preuve (par récurrence sur n):

Le résultat est vrai pour $n = 0$ et $n = 1$.

Soit $n \in \mathbb{N}$ tel que pour toutes fonctions f et g dérivables n fois en a avec $g(a) \neq 0$, $\frac{f}{g}$ est aussi dérivables n fois en a .

Soient f et g dérivables $n + 1$ fois en a telles que $g(a) \neq 0$. Alors, $\frac{f}{g}$ dérivable en a . et

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

- f' est dérivables n fois en a
- g est dérivables n fois en a
- f est dérivables n fois en a
- g' est dérivables n fois en a

Donc, $f' \times g - f \times g'$ et g^2 sont dérivables n fois en a et $g(a)^2 \neq 0$

D'après l'hypothèse de récurrence, $\frac{f' \times g - f \times g'}{g^2}$ est dérivable n fois en a donc $\frac{f}{g}$ dérivable $n + 1$ fois en a \square

Proposition: Soit f dérivable n fois en a et g dérivable n fois en $f(a)$ (resp. f et g de classe \mathcal{C}^n).

Alors, $g \circ f$ est dérivable n fois en a (resp. de classe \mathcal{C}^n).

Preuve (similaire à la précédente):

\square

Définition: On dit que f est de classe \mathcal{C}^∞ si f est de classe \mathcal{C}^n pour tout $n \in \mathbb{N}$, i.e. f est dérivable une infinité de fois.

Proposition (formule de Taylor avec reste intégral): Soit $f : I \rightarrow \mathbb{R}$ de classe \mathcal{C}^{n+1} et $a \in I$. Alors

$$(*) \quad \forall x \in I, f(x) = \sum_{k=0}^n \frac{f^{(k)}(a)}{k!} (x-a)^k + \int_a^x f^{(n+1)}(t) \frac{(x-t)^n}{n!} dt$$

Preuve (par récurrence sur n): — Soit $f : I \rightarrow \mathbb{R}$ de classe \mathcal{C}^1 et $a \in I$. Soit $x \in I$.

$$\begin{aligned} \sum_{k=0}^0 \frac{f^{(k)}(a)}{k!} (x-a)^k + \int_a^x f^{(1)}(t) \frac{(x-t)^0}{0!} dt &= f(a) + \int_a^x f'(t) dt \\ &= f(a) + f(x) - f(a) \\ &= f(x) \end{aligned}$$

— Soit $n \in \mathbb{N}$ tel que $(*)$ est vraie pour toute fonction f de classe \mathcal{C}^{n+1} sur $I \ni a$. Soit f de classe \mathcal{C}^{n+2} . Alors, f est de classe \mathcal{C}^{n+1} donc

$$\forall x \in I, f(x) = \sum_{k=0}^n \frac{f^{(k)}(a)}{k!} (x-a)^k + \int_a^x f^{(n+1)}(t) \frac{(x-t)^n}{n!} dt$$

Soit $x \in I$. On pose $\begin{cases} u : t \mapsto -\frac{(x-t)^{n+1}}{(n+1)!} \\ v = f^{(n+1)} \end{cases}$

Les fonctions u et v sont de classe \mathcal{C}^1 donc

$$\int_a^x u'(t)v(t) dt = [u(t)v(t)]_a^x - \int_a^x u(t)v'(t) dt$$

donc

$$\int_a^x f^{(n+1)}(t) dt = \left[-\frac{(x-t)^{n+1}}{(n+1)!} f^{(n+1)}(t) \right]_a^x + \int_a^x f^{(n+2)}(t) \frac{(x-t)^{n+1}}{(n+1)!} dt$$

D'où,

$$f(x) = \sum_{k=0}^n \frac{f^{(k)}(a)}{k!} (x-a)^k + \frac{(x-a)^{n+1}}{(n+1)!} f^{(n+1)}(a) + \int_a^x f^{(n+2)}(t) \frac{(x-t)^{n+1}}{(n+1)!} dt$$

□

Proposition (Inégalité de Taylor-Lagrange): Soit $f : I \rightarrow \mathbb{R}$ de classe \mathcal{C}^{n+1} et $M \in \mathbb{R}$ tel que

$$\forall x \in I, |f^{(n+1)}(x)| \leq M$$

Alors, pour tout $a \in I$,

$$\forall x \in I, \left| f(x) - \sum_{k=0}^n \frac{(x-a)^k}{k!} f^{(k)}(a) \right| \leq M \frac{|x-a|^{n+1}}{(n+1)!}$$

Preuve:

D'après la formule de Taylor avec reste intégral,

$$\begin{aligned} \forall x \in I, \left| f(x) - \sum_{k=0}^n \frac{f^{(k)}(a)(x-a)^k}{k!} \right| &= \left| \int_a^x f^{(n+1)}(t) \frac{(x-t)^n}{n!} dt \right| \\ &\leq \left| \int_a^x |f^{(n+1)}|(t) \frac{|x-t|^n}{n!} dt \right| \\ &\leq \left| \int_a^x M \frac{|x-t|^n}{n!} dt \right| \end{aligned}$$

On suppose $x \geq a$.

$$\begin{aligned} \left| f(x) - \sum_{k=0}^n \frac{f^{(k)}(a)}{k!} (x-a)^k \right| &\leq M \int_a^x \frac{(x-t)^n}{n!} dt = M \left[-\frac{(x-t)^{n+1}}{(n+1)!} \right]_a^x \\ &\leq M \frac{(x-a)^{n+1}}{(n+1)!} \end{aligned}$$

On suppose $x \leq a$.

$$\begin{aligned} \left| f(x) - \sum_{k=0}^n \frac{f^{(k)}(a)}{k!} (x-a)^k \right| &\leq M \int_x^a \frac{(t-x)^n}{n!} dt \\ &\leq M \left[\frac{(t-x)^{n+1}}{(n+1)!} \right]_x^a \\ &\leq M \frac{(a-x)^{n+1}}{(n+1)!} = M \frac{|x-a|^{n+1}}{(n+1)!} \end{aligned}$$

□

EXEMPLE:

$$\forall x \in \mathbb{R}, e^x = \lim_{n \rightarrow +\infty} \sum_{k=0}^n \frac{x^k}{k!}$$

On pose

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto e^x \end{aligned}$$

. Soit $n \in \mathbb{N}$ et $a = 0$.

f est de classe \mathcal{C}^1 sur \mathbb{R} . Soit $x \in \mathbb{R}^+$ et $I = [0, x]$

$$\begin{aligned} \forall t \in I, |f^{(n+1)}(t)| &= |e^t| = e^t \leq e^x \\ \forall t \in I, \left| e^t - \sum_{k=0}^n \frac{t^k}{k!} \right| &\leq e^x \frac{t^{n+1}}{(n+1)!} \xrightarrow[n \rightarrow +\infty]{} 0 \end{aligned}$$

donc

$$\forall t \in I, \lim_{n \rightarrow +\infty} \sum_{k=0}^n \frac{t^k}{k!} = e^t$$

donc

$$e^x = \lim_{n \rightarrow +\infty} \frac{x^n}{n!}$$

EXERCICE:

$$\text{Montrer que } \ln 2 = \lim_{n \rightarrow +\infty} \sum_{k=1}^n \frac{(-1)^{k+1}}{k}$$

4 Fonctions à valeurs complexes

Définition: Soient $f : I \rightarrow \mathbb{C}$, (I intervalle de \mathbb{R}) et $a \in I$.

f est dérivable en a si $\lim_{x \rightarrow a} \frac{f(x) - f(a)}{x - a} \in \mathbb{C}$

Proposition:

f est dérivable en $a \iff \Re(f)$ et $\Im(f)$ sont dérivables en a

Dans ce cas, $f'(a) = \Re(f)'(a) + i\Im(f)'(a)$

□

Proposition: La somme, le produit, de fonctions dérivables sont dérivables ; le quotient également si le dénominateur ne s'annule pas.

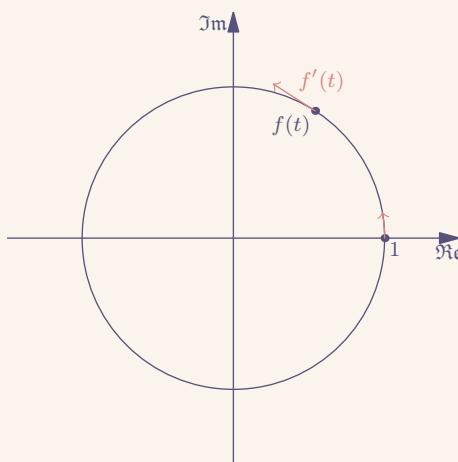
□

Proposition: idem avec les dérivées n -ièmes

□

REMARQUE (Attention Δ):

Le théorème de Rolle n'est plus vraie.



$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{C} \\ t &\longmapsto e^{it} \end{aligned}$$

$$f(0) = f(2\pi) = 1$$

f est continue sur $[0, 2\pi]$ et dérivable sur $]0, 2\pi[$

$$\forall t, f'(t) = ie^{it} \neq 0$$

Proposition: La formule de Taylor avec reste intégral et l'inégalité de Taylor-Lagrange sont aussi vrais dans \mathbb{C} .

□

CHAPITRE

17

DIMENSION FINIE

Définition: Soit E un \mathbb{K} -espace vectoriel. On dit que E est de dimension finie si E a au moins une famille génératrice finie. On dit que E est de dimension infinie sinon.

Théorème (Théorème de la base extraite): Soit E un \mathbb{K} -espace vectoriel non nul de dimension finie. Soit \mathcal{G} une famille génératrice finie de E . Alors, il existe une base \mathcal{B} de E telle que $\mathcal{B} \subset \mathcal{G}$.

Preuve (par récurrence sur $\#G = \text{Card}(G)$): — Soit E un \mathbb{K} -espace vectoriel non nul engendré par $\mathcal{G} = (u)$.

Si $u = 0_E$, alors $E = \{0_E\}$: une contradiction.

Donc $u \neq 0_E$ donc (u) est libre. En effet,

$$\forall \lambda \in \mathbb{K}, \lambda u = 0_E \implies \lambda = 0_{\mathbb{K}}$$

Donc \mathcal{G} est une base de E .

— Soit $n \in \mathbb{N}_*$. Soit E un \mathbb{K} -espace vectoriel. On suppose que si E a une famille génératrice constituée de n vecteurs, alors on peut extraire de cette famille une base de E .

Soit \mathcal{G} une famille génératrice de E avec $n + 1$ vecteurs.

Si \mathcal{G} est libre, alors \mathcal{G} est une base de E .

Si \mathcal{G} n'est pas libre, alors il existe $u \in \mathcal{G}$ tel que $u \in \text{Vect}(\mathcal{G} \setminus \{u\})$

Donc $\mathcal{G} \setminus \{u\}$ engendre E . Or, $\mathcal{G} \setminus \{u\}$ possède n vecteurs. D'après l'hypothèse de récurrence, il existe une base \mathcal{B} de E telle que

$$\mathcal{B} \subset \mathcal{G} \setminus \{u\} \subset \mathcal{G}$$

□

Corollaire: Tout espace de dimension finie a une base.

□

Théorème (Théorème de la base incomplète): Soit E un \mathbb{K} -espace vectoriel de dimension finie, \mathcal{G} une famille génératrice finie de E , \mathcal{L} une famille libre de E . Alors, il existe une base \mathcal{B} de E telle que

$$\mathcal{L} \subset \mathcal{B} \text{ et } \mathcal{B} \setminus \mathcal{L} \subset \mathcal{G}$$

Preuve (par récurrence sur $\#(\mathcal{G} \setminus \mathcal{L})$): — Avec les notations précédentes, on suppose que $\mathcal{G} \setminus \mathcal{L} \neq \emptyset$

$$\forall u \in \mathcal{G}, u \in \mathcal{L}$$

Donc $\mathcal{G} \subset \mathcal{L}$ donc \mathcal{L} est génératrice donc \mathcal{L} est une base de E . On pose $\mathcal{B} = \mathcal{L}$ et alors

$$\mathcal{L} \subset \mathcal{B} \text{ et } \mathcal{B} \setminus \mathcal{L} = \emptyset \subset \mathcal{G}$$

— Soit $n \in \mathbb{N}$. On suppose que si \mathcal{G} est génératrice et \mathcal{L} libre avec $\#(\mathcal{G} \setminus \mathcal{L}) = n$ alors il existe une base \mathcal{B} de E telle que

$$\mathcal{L} \subset \mathcal{B} \text{ et } \mathcal{B} \setminus \mathcal{L} \subset \mathcal{G}$$

Soient à présent \mathcal{G} une famille génératrice de E et \mathcal{L} une famille libre de E telles que $\#(\mathcal{G} \setminus \mathcal{L}) = n + 1 > 0$. Si \mathcal{L} engendre E , alors \mathcal{L} est une base de E . On pose $\mathcal{B} = \mathcal{L}$ et on a bien

$$\mathcal{L} \subset \mathcal{B} \text{ et } \mathcal{B} \setminus \mathcal{L} = \emptyset \subset \mathcal{G}$$

On suppose que \mathcal{L} n'engendre pas E . Il existe $u \in \mathcal{G}$ tel que $u \notin \overline{\mathcal{L}}$ (car sinon, $\mathcal{G} \subset \text{Vect}(\mathcal{L})$ et donc $\underbrace{\text{Vect}(\mathcal{G})}_{=E} \subset \underbrace{\text{Vect}(\mathcal{L})}_{\subset E}$)

Donc $\mathcal{L} \cup \{u\}$ est libre. On pose $\mathcal{L}' = \mathcal{L} \cup \{u\}$

$$\mathcal{G} \setminus \mathcal{L}' = \mathcal{G} \setminus (\mathcal{L} \cup \{u\}) = (\mathcal{G} \setminus \mathcal{L}) \setminus \{u\}$$

$$\text{donc } \#(\mathcal{G} \setminus \mathcal{L}') = n + 1 - 1 = n$$

D'après l'hypothèse de récurrence, il existe \mathcal{B} une base de E telle que

$$\mathcal{L} \subset \mathcal{L}' \subset \mathcal{B} \text{ et } \mathcal{B} \setminus \mathcal{L}' \subset \mathcal{G}$$

$$\mathcal{B} \setminus \mathcal{L} = \underbrace{\mathcal{B} \setminus \mathcal{L}'}_{\subset \mathcal{G}} \cup \underbrace{\{u\}}_{\subset \mathcal{G} \text{ car } u \in \mathcal{G}}$$

On a $\mathcal{B} \setminus \mathcal{L} \subset \mathcal{G}$

□

Théorème: Soit E un \mathbb{K} -espace vectoriel de dimension finie. Toutes les bases de E ont le même cardinal.

Preuve:

Soit \mathcal{G} une famille génératrice finie de E et $\mathcal{B} \subset \mathcal{G}$ une base de E . On note $n = \#\mathcal{B}$. Soit \mathcal{B}' une base de E . On pose $p = n - \#(\mathcal{B} \cap \mathcal{B}')$. Montrons par récurrence sur p que $\#\mathcal{B} = \#\mathcal{B}'$

- On suppose que $p = 0$. Alors, $\#(\mathcal{B} \cap \mathcal{B}') = n$
Or, $\mathcal{B}' \cap \mathcal{B} \subset \mathcal{B}$ donc $\mathcal{B} \cap \mathcal{B}' = \mathcal{B}$ donc $\mathcal{B} \subset \mathcal{B}'$ et donc $\mathcal{B} = \mathcal{B}'$
- Soit $p \in \mathbb{N}$. On suppose que si \mathcal{B}' est une base de E telle que $n - \#(\mathcal{B} \cap \mathcal{B}') = p$, alors $\#\mathcal{B}' = n$
Ainsi \mathcal{B}' une base de E telle que $n - \#(\mathcal{B} \cap \mathcal{B}') = p + 1 > 0$
Donc $\mathcal{B} \cap \mathcal{B}' \neq \mathcal{B}$. Soit $u \in \mathcal{B}' \setminus \mathcal{B}$. D'après le lemme d'échange, il existe

$v \in \mathcal{B} \setminus \mathcal{B}'$ tel que $\mathcal{B}' \setminus \{u\} \cup \{v\}$ est une base de E . On pose $\mathcal{B}'' = \mathcal{B}' \setminus \{u\} \cup \{v\}$

$$\begin{aligned}\mathcal{B}'' \cap \mathcal{B} &= ((\mathcal{B}' \setminus \{u\}) \cap \mathcal{B}) \cup \{v\} \\ &= (\mathcal{B}' \cap \mathcal{B}) \cup \{v\}\end{aligned}$$

donc,

$$\begin{aligned}n - \#(\mathcal{B}'' \cap \mathcal{B}) &= n - (\#(\mathcal{B}' \cap \mathcal{B}) + 1) \\ &= p + 1 - 1 \\ &= p\end{aligned}$$

D'après l'hypothèse de récurrence,

$$\#\mathcal{B}'' = n$$

Or, $\#\mathcal{B}'' = \#\mathcal{B}'$

□

Lemme: Soient \mathcal{B} et \mathcal{B}' deux bases de E telles que $\mathcal{B} \subset \mathcal{B}'$. Alors, $\mathcal{B} = \mathcal{B}'$.

Preuve:

On suppose $\mathcal{B}' \neq \mathcal{B}$. Soit $u \in \mathcal{B}' \setminus \mathcal{B}$ $u \in E = \text{Vect}(\mathcal{B})$ donc $\mathcal{B} \cup \{u\}$ n'est pas libre. Donc $\mathcal{B} \cup \{u\} \subset \mathcal{B}'$ et \mathcal{B}' est libre donc $\mathcal{B} \cup \{u\}$ est libre : une contradiction. □

Lemme (Lemme d'échange): Soient \mathcal{B}_1 et \mathcal{B}_2 deux bases de E et $u \in \mathcal{B}_1 \setminus \mathcal{B}_2$. Alors, il existe $v \in \mathcal{B}_2$ tel que $(\mathcal{B}_1 \setminus \{u\}) \cup \{v\}$ soit une base de E .

Preuve (1^{nde} méthode):

On suppose que pour tout $v \in \mathcal{B}_2$, $(\mathcal{B}_1 \setminus \{u\}) \cup \{v\}$ n'est pas une base de E . Soit $v \in \mathcal{B}_2$.

- Supposons $(\mathcal{B}_1 \setminus \{u\}) \cup \{v\}$ non libre. $\mathcal{B}_1 \setminus \{u\}$ est libre. Donc $v \in \text{Vect}(\mathcal{B}_1 \setminus \{u\})$
- Supposons $(\mathcal{B}_1 \setminus \{u\}) \cup \{v\}$ non génératrice. Comme \mathcal{B}_1 engendre E , $u \notin \text{Vect}(\mathcal{B}_1 \setminus \{v\})$. On suppose que $\mathcal{B}_1 \neq \mathcal{B}_2$. $\forall v \in \mathcal{B}_2 \setminus \mathcal{B}_1$, $\text{Vect}(\mathcal{B}_1 \setminus \{v\}) = \text{Vect}(\mathcal{B}_1) = E \ni u$ donc, $(\mathcal{B}_1 \setminus \{u\}) \cup \{v\}$ engendre E et donc

$$v \in \text{Vect}(\mathcal{B}_1 \setminus \{u\})$$

On a aussi

$$\forall v \in \mathcal{B}_1 \setminus \{u\}, v \in \text{Vect}(\mathcal{B}_1 \setminus \{u\})$$

Comme $u \notin \mathcal{B}_2$, on a

$$\forall v \in \mathcal{B}_2, v \in \text{Vect}(\mathcal{B}_1 \setminus \{u\})$$

donc

$$E = \text{Vect}(\mathcal{B}_2) \subset \text{Vect}(\mathcal{B}_1 \setminus \{u\})$$

donc $\mathcal{B}_1 \setminus \{u\}$ engendre E donc $\mathcal{B}_1 \setminus \{u\}$ est une base de E . Or, $\mathcal{B}_1 \setminus \{u\} \subset \mathcal{B}_1$, donc $\mathcal{B}_1 \setminus \{u\} = \mathcal{B}_1$

□

Preuve (2^{nde} méthode):

On suppose que pour tout $v \in \mathcal{B}_2$, $(\mathcal{B}_1 \setminus \{u\}) \cup \{v\}$ n'est pas une base de E

- Comme $u \in \mathcal{B}_1 \setminus \mathcal{B}_2$, nécessairement $\mathcal{B}_1 \neq \mathcal{B}_2$ donc $\mathcal{B}_2 \not\subset \mathcal{B}_1$, donc $\mathcal{B}_2 \setminus \mathcal{B}_1 \neq \emptyset$
- Soit $v \in \mathcal{B}_2 \setminus \mathcal{B}_1$. Il existe $(\lambda_w)_{w \in \mathcal{B}_1}$ une famille de scalaires presque nulle telle que

$$v = \sum_{w \in \mathcal{B}_1} \lambda_w w - \lambda_u u + \sum_{w \in \mathcal{B}_1 \setminus \{u\}} \lambda_w w$$

Si $\lambda_u \neq 0_E$, alors

$$\begin{aligned} u &= \lambda_u^{-1} \left(v - \sum_{w \in \mathcal{B}_1 \setminus \{u\}} \lambda_w w \right) \\ &\in \text{Vect}(\mathcal{B}_1 \setminus \{u\} \cup v) \end{aligned}$$

donc $\mathcal{B}_1 \subset \text{Vect}(\mathcal{B}_1 \setminus \{u\} \cup \{v\})$

et donc $E \subset \text{Vect}(\mathcal{B}_1 \setminus \{u\} \cup \{v\})$

et donc $\mathcal{B}_1 \setminus \{u\} \cup \{v\}$ engendre E

donc $\mathcal{B}_1 \setminus \{u\} \cup \{v\}$ n'est pas libre

donc $v \in \text{Vect}(\mathcal{B}_1 \setminus \{u\})$ (car $\mathcal{B}_1 \setminus \{u\}$ est libre)

donc $\lambda_u = 0_{\mathbb{K}}$

Donc, $\lambda_u = 0_{\mathbb{K}}$, donc $v \in \text{Vect}(\mathcal{B}_1 \setminus \{u\})$

On vient de prouver que

$$\begin{aligned} \mathcal{B}_2 \setminus \mathcal{B}_1 &\subset \text{Vect}(\mathcal{B}_1 \setminus \{u\}) \\ \mathcal{B}_1 \setminus \{u\} &\subset \text{Vect}(\mathcal{B}_1 \setminus \{u\}) \end{aligned}$$

Comme $u \notin \mathcal{B}_2$,

$$\mathcal{B}_2 \subset \text{Vect}(\mathcal{B}_1 \setminus \{u\})$$

donc

$$E = \text{Vect}(\mathcal{B}_2) \subset \text{Vect}(\mathcal{B}_1 \setminus \{u\})$$

donc $\mathcal{B}_1 \setminus \{u\}$ engendre E . Donc, $\mathcal{B}_1 \setminus \{u\}$ est une base de E .

Or, $\mathcal{B}_1 \setminus \{u\} \subset \mathcal{B}_1$, donc $\mathcal{B}_1 \setminus \{u\} = \mathcal{B}_1$

□

Définition: Soit E un \mathbb{K} -espace vectoriel de dimension finie. Le cardinal commun à toutes les bases de E est appelé dimension de E est notée $\dim(E)$ ou $\dim_{\mathbb{K}}(E)$. C'est donc aussi le nombre de coordonnées de n'importe quel vecteur dans n'importe quelle base.

EXEMPLE: 1. $\dim_{\mathbb{R}}(\mathbb{C}) = 2$ et $\dim_{\mathbb{C}}(\mathbb{C}) = 1$

2. $\dim_{\mathbb{K}}(\mathbb{K}^n) = n$

3. $\dim_{\mathbb{K}}(\mathcal{M}_{n,p}(\mathbb{K})) = np$

Corollaire: Soit E un \mathbb{K} -espace vectoriel de dimension finie, \mathcal{L} une famille libre de E , \mathcal{G} une famille génératrice de E . On note $n = \dim(E)$

1. $\#\mathcal{G} \geq n$ et $(\#\mathcal{G} = n \implies \mathcal{G} \text{ est une base de } E)$

2. $\#\mathcal{L} \leq n$ et $(\#\mathcal{L} = n \implies \mathcal{L} \text{ est une base de } E)$

Corollaire: $\mathbb{R}^{\mathbb{R}}$ est de dimension infinie. $\forall i \in \mathbb{N}, e_i : x \mapsto x^i$
 $(e_i)_{i \in \mathbb{N}}$ est libre dans $\mathbb{R}^{\mathbb{R}}$

Proposition: Soient E et F deux \mathbb{K} -espaces vectoriels de dimension finie. Alors $E \times F$ est de dimension finie et $\dim(E \times F) = \dim(E) + \dim(F)$

Preuve:

Soit (e_1, \dots, e_n) une base de E , (f_1, \dots, f_p) une base de F . On pose

$$\left\{ \begin{array}{rcl} u_1 & = & (e_1, 0_F) \\ u_2 & = & (e_2, 0_F) \\ \vdots & & \\ u_n & = & (e_n, 0_F) \\ u_{n+1} & = & (0_E, f_1) \\ u_{n+2} & = & (0_E, f_2) \\ \vdots & & \\ u_{n+p} & = & (0_E, f_p) \end{array} \right.$$

Soit $(x, y) \in E \times F$.

$$\left\{ \exists (x_1, \dots, x_n) \in \mathbb{K}^n, x = \sum_{i=1}^n x_i e_i \exists (y_1, \dots, y_p) \in \mathbb{K}^p, y = \sum_{j=1}^p y_j f_j \right.$$

$$\begin{aligned} (x, y) &= \left(\sum_{i=1}^n x_i e_i, \sum_{j=1}^p y_j f_j \right) \\ &= \sum_{i=1}^n x_i (e_i + 0_F) + \sum_{j=1}^p y_j (0_E, f_j) \\ &= \sum_{i=1}^n x_i u_i + \sum_{j=1}^p y_j u_{n+j} \end{aligned}$$

Donc, $E \times F = \text{Vect}(u_1, \dots, u_{n+p})$ donc $E \times F$ est de dimension finie.
 Soit $(\lambda_1, \dots, \lambda_{n+p}) \in \mathbb{K}^{n+p}$ tel que

$$(*) : \sum_{k=1}^{n+p} \lambda_k u_k = 0_{E \times F} = (0_E, 0_F)$$

$$\begin{aligned} (*) &\iff \sum_{k=1}^n \lambda_k (e_k, 0_F) + \sum_{k=n+1}^p \lambda_k (0_E, f_{k-n}) = (0_E, 0_F) \\ &\iff \begin{cases} \sum_{k=1}^n \lambda_k e_k = 0_E \\ \sum_{k=n+1}^p \lambda_k f_{k-n} = 0_F \end{cases} \\ &\iff \begin{cases} \forall k \in \llbracket 1, n \rrbracket, \lambda_k = 0_{\mathbb{K}} & (\text{car } (e_1, \dots, e_n) \text{ est libre}) \\ \forall k \in \llbracket n+1, n+p \rrbracket, \lambda_k = 0_{\mathbb{K}} & (\text{car } (f_1, \dots, f_n) \text{ est libre}) \end{cases} \end{aligned}$$

Donc (u_1, \dots, u_{n+p}) est une base de $E \times F$. Donc, $\dim(E \times F) = n + p = \dim(E) + \dim(F)$ \square

REMARQUE (Convention):

$$\dim(\{0_E\}) = 0$$

Théorème: Soit E un \mathbb{K} -espace vectoriel de dimension finie, F un sous-espace vectoriel de E . Alors, F est de dimension finie et $\dim(F) \leq \dim(E)$
Si $\dim(F) = \dim(E)$, alors $F = E$

Preuve:

On considère

$$A = \{k \in \mathbb{N} \mid \text{il existe une famille libre de } F \text{ à } k \text{ éléments}\}$$

On suppose $F \neq \{0_E\}$.

- Soit $u \in F \setminus \{0_E\}$. (u) est libre donc $1 \in A$ et donc $A \neq \emptyset$
- Soit \mathcal{L} une famille libre de F . Alors, \mathcal{L} est une famille libre de E donc $\#\mathcal{L} \leq \dim(E)$
Donc A est majorée par $\dim(E)$
On en déduit que A a un plus grand élément p .
- Soit \mathcal{L} une famille libre de F avec p éléments.
Si \mathcal{L} n'engendre pas F , alors il existe $u \in F$ tel que $u \notin \text{Vect}(\mathcal{L})$ et donc $\mathcal{L} \cup \{u\}$ est une famille libre de F , donc $p+1 \in A$ en contradiction avec la maximalité de p .
Donc \mathcal{L} est une base de F donc F est de dimension finie et $\dim(F) = p \leq \dim(E)$

Soit \mathcal{B} une base de F . Alors, \mathcal{B} est aussi une famille de libre de E . Donc $\#\mathcal{B} \leq \dim(E)$ donc $\dim(F) = \dim(E)$

Si $\dim(F) = \dim(E)$, alors \mathcal{B} est une base de E , et donc $F = \text{Vect}(\mathcal{B}) = E$ \square

Proposition (Formule de Grassmann): Soit E un \mathbb{K} -espace vectoriel de dimension finie, F et G deux sous-espace vectoriels de E . Alors,

$$\dim(F + G) = \dim(F) + \dim(G) - \dim(F \cap G)$$

Preuve:

Soit (e_1, \dots, e_p) une base de $F \cap G$. (e_1, \dots, e_p) est une famille libre de F .

On complète (e_1, \dots, e_p) en une base $(e_1, \dots, e_p, u_1, \dots, u_q)$ de F .

De même, on complète (e_1, \dots, e_p) en une base $(e_1, \dots, e_p, v_1, \dots, v_r)$ de G .

On pose $\mathcal{B} = (e_1, \dots, e_p, u_1, \dots, u_q, v_1, \dots, v_r)$. Montrons que \mathcal{B} est une base de $F + G$

- Soit $u \in F + G$

On pose $u = v + w$ avec $\begin{cases} v \in F \\ w \in G \end{cases}$.

On pose $v = \sum_{i=1}^p \lambda_i e_i + \sum_{i=1}^q \mu_i u_i$ avec $(\lambda_1, \dots, \lambda_p, \mu_1, \dots, \mu_q) \in \mathbb{K}^{p+q}$

On pose aussi $w = \sum_{i=1}^p \lambda'_i e_i + \sum_{j=1}^r \nu_j v_j$ avec $(\lambda'_1, \dots, \lambda'_p, \nu_1, \dots, \nu_r) \in \mathbb{K}^{p+r}$

D'où,

$$u = \sum_{i=1}^p (\lambda_i + \lambda'_i) e_i + \sum_{j=1}^q \mu_j u_j + \sum_{k=1}^r \nu_k v_k \in \text{Vect}(\mathcal{B})$$

— Soient $(\lambda_1, \dots, \lambda_p, \mu_1, \dots, \mu_q, \nu_1, \dots, \nu_r) \in \mathbb{K}^{p+q+r}$.

On suppose

$$(*) \quad \sum_{i=1}^p \lambda_i e_i + \sum_{j=1}^q \mu_j u_j + \sum_{k=1}^r \nu_k v_k = 0_E$$

D'où,

$$\underbrace{\sum_{i=1}^p \lambda_i e_i}_{\in F} + \underbrace{\sum_{j=1}^q \mu_j u_j}_{\in G} = - \underbrace{\sum_{k=1}^r \nu_k v_k}_{\in G}$$

Donc,

$$f = \sum_{i=1}^p \lambda_i e_i + \sum_{j=1}^q \mu_j u_j \in F \cap G$$

Comme (e_1, \dots, e_p) est une base de $F \cap G$, $\exists!(\lambda'_1, \dots, \lambda'_p) \in \mathbb{K}^p$ tel que

$$f = \sum_{i=1}^p \lambda'_i e_i = \sum_{i=1}^p \lambda'_i e_i + \sum_{j=1}^q 0_{\mathbb{K}} u_j$$

Comme $(e_1, \dots, e_p, u_1, \dots, u_q)$ est une base de F ,

$$\forall k \in \llbracket 1, q \rrbracket, \mu_j = 0_{\mathbb{K}}$$

De même,

$$\forall k \in \llbracket 1, r \rrbracket, \nu_k = 0_{\mathbb{K}}$$

On remplace dans $(*)$ pour trouver

$$\sum_{i=1}^p \lambda_i e_i = 0_E$$

Comme (e_1, \dots, e_p) est libre,

$$\forall i \in \llbracket 1, p \rrbracket, \lambda_i = 0_{\mathbb{K}}$$

Donc \mathcal{B} est libre.

Donc,

$$\begin{aligned} \dim(F + G) &= p + q + r \\ &= (p + q) + (p + r) - p \\ &= \dim(F) + \dim(G) - \dim(F \cap G) \end{aligned}$$

□

Corollaire: Avec les hypothèses précédentes,

$$E = F \oplus G \iff \begin{cases} F \cap G = \{0_E\} \\ \dim(E) = \dim(F) + \dim(G) \end{cases}$$

Preuve: “ \implies ” On suppose $E = F \oplus G$

Comme la somme est directe, $F \cap G = \{0_E\}$

$$\begin{aligned}\dim(E) &= \dim(F) \\ &= \dim(F) + \dim(G) - \dim(F \cap G) \\ &= \dim(F) + \dim(G)\end{aligned}$$

“ \Leftarrow ” On suppose $F \cap G = \{0_E\}$ et $\dim(E) = \dim(F) + \dim(G)$.
On sait déjà que $F + G = F \oplus G$

$$\dim(F + G) = \dim(F) + \dim(G) - \dim(F \cap G) = \dim(E)$$

Donc $F + G = E$

□

Proposition: Soit F un \mathbb{K} -espace vectoriel de dimension finie n . Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de F . L'application

$$\begin{aligned}f : \mathbb{K}^n &\longrightarrow F \\ (\lambda_1, \dots, \lambda_n) &\longmapsto \sum_{i=1}^n \lambda_i e_i\end{aligned}$$

est bijective.

Si \mathbb{K} est infini, \mathbb{K}^n aussi et donc F aussi.

Si $\#\mathbb{K} = p \in \mathbb{N}_*$,

$$\#\mathbb{K}^n = p^n$$

$$\begin{array}{c} \| \\ \#F \end{array}$$

CHAPITRE

18

POLYNÔMES FORMELS

Dans ce chapitre, \mathbb{K} désigne un corps

1 Définition

- Définition:**
- Un polynôme à coefficients dans \mathbb{K} est une suite presque nulle de $\mathbb{K}^{\mathbb{N}}$
 - Le polynôme nul, noté 0 est la suite nulle.
 - Soit $P = (a_n)_{n \in \mathbb{N}}$ un polynôme non nul.
 $\{n \in \mathbb{N} \mid a_n \neq 0_{\mathbb{K}}\}$ est non-vide et majoré. Le degré de P est $\max\{n \in \mathbb{N} \mid a_n \neq 0_{\mathbb{K}}\}$, et on le note $\deg(P)$ et $a_{\deg(P)}$ est le coefficients dominante de P , il est noté $\text{dom}(P)$.
 - Le degré du polynôme nul est $-\infty$

Proposition – Définition: Soient $P = (a_n)_{n \in \mathbb{N}}$ et $Q = (b_n)_{n \in \mathbb{N}}$ deux polynômes à coefficients dans \mathbb{K} . Alors, $P + Q = (a_n + b_n)_{n \in \mathbb{N}}$ est un polynôme appelé somme de P et Q .

Preuve:

$$\begin{aligned}\exists N_1 \in \mathbb{N}, \forall n \geq N_1, a_n &= 0 \\ \exists N_2 \in \mathbb{N}, \forall n \geq N_2, b_n &= 0\end{aligned}$$

On pose $N = \max(N_1, N_2)$ donc

$$\forall n \geq N, a_n + b_n = 0 + 0 = 0$$

donc $P + Q$ est une suite presque nulle. \square

Proposition – Définition: Soient $P = (a_n)_{n \in \mathbb{N}}$ et $Q = (b_n)_{n \in \mathbb{N}}$ deux polynômes à coefficients dans \mathbb{K} . On pose

$$\forall n \in \mathbb{N}, c_n = \sum_{k=0}^n a_k b_{n-k}$$

La suite $(c_n)_{n \in \mathbb{N}}$ est presque nulle. Ce polynôme est appelé produit de P et Q et noté PQ .

Preuve:

$$\exists N_1 \in \mathbb{N}, \forall n \geq N_1, a_n = 0$$

$$\exists N_2 \in \mathbb{N}, \forall n \geq N_2, b_n = 0$$

On pose $N = N_1 + N_2$

$$\forall n \geq N, c_n = \sum_{k=0}^n a_k b_{n-k} = \sum_{k=0}^{N_1} a_k b_{n-k} + \sum_{k=N_1+1}^n a_k b_{n-k}$$

$$\forall k \geq N_1 + 1, a_k = 0 \text{ donc } \sum_{k=N_1+1}^n a_k b_{n-k} = 0$$

$\forall k \leq N_1, b - k \geq n - N_1 \geq N_1 + N_2 - N_1 \geq N_2$ donc $\forall k \leq N_1, b_{n-k} = 0$ et donc

$$\sum_{k=0}^{N_1} a_k b_{n-k} = 0$$

Donc

$$\forall n \geq N, c_n = 0$$

\square

REMARQUE (Notation):

Soit $P = (a_n)_{n \in \mathbb{N}}$, un polynôme à coefficients dans \mathbb{K} et $\lambda \in \mathbb{K}$. Le polynôme $(\lambda a_n)_{n \in \mathbb{N}}$ est noté λP

REMARQUE (Notation):

On pose $X = (0_{\mathbb{K}}, 1_{\mathbb{K}}, 0_{\mathbb{K}}, \dots) = (\delta_{1,n})_{n \in \mathbb{N}}$

EXEMPLE:

$$\begin{aligned} X^2 &= XX \\ &= (0 \times 0, 0 \times 1 + 1 \times 0, 0 \times 0 + 1 \times 1 + 0 \times 0, 0, \dots) \\ &= (0, 0, 1, 0, \dots) \end{aligned}$$

Théorème: Soit $P = (a_n)_{n \in \mathbb{N}}$ un polynôme non nul à coefficients dans \mathbb{K} . Alors

$$P = \sum_{k=0}^n a_k X^k \quad \text{où } n = \deg(P) \text{ et } X^0 = (1, 0, \dots)$$

Preuve:

Pour $k \in \mathbb{N}$, $\mathcal{P}(n)$: “ $X^k = (\delta_{k,n})_{n \in \mathbb{N}}$ ” où $\delta_{k,n} = \begin{cases} 1 & \text{si } n = k \\ 0 & \text{si } n \neq k \end{cases}$

- $\delta_{0,n} = (1, 0, \dots) = X^0$ donc $\mathcal{P}(0)$ est vrai
- Soit $k \in \mathbb{N}$. On suppose $\mathcal{P}(k)$ vraie.

$$X^{k+1} = X^k X = (c_n)_{n \in \mathbb{N}}$$

où

$$\forall n \in \mathbb{N}, c_n = \sum_{j=0}^n \delta_{k,j} \delta_{1,n-j}$$

Donc, pour tout $n \in \mathbb{N}$ et pour tout $j \in \llbracket 0, n \rrbracket$

$$\begin{aligned} \delta_{k,j} \delta_{1,n-j} \neq 0 &\iff \begin{cases} k = j \\ 1 = n - j \end{cases} \\ &\iff \begin{cases} k = j \\ n = k + 1 \end{cases} \end{aligned}$$

Donc, si $n \neq k + 1$, alors

$$\forall j \in \llbracket 0, n \rrbracket, \delta_{k,j} \delta_{1,n-j} = 0$$

et donc $c_n = 0$

$$c_{k+1} = \sum_{j=0}^{k+1} \delta_{k,j} \delta_{1,j+1-k} = \delta_{k,k} \delta_{1,1} = 1$$

Donc

$$\forall n \in \mathbb{N}, c_n = \delta_{k+1,n}$$

donc $\mathcal{P}(k+1)$ est vraie

Ainsi, $\mathcal{P}(k)$ est vraie pour tout $k \in \mathbb{N}$. Soit $P = (a_0, \dots, a_n, 0, \dots)$ un polynôme de degré n .

$$\begin{aligned} \sum_{k=0}^n a_k X^k &= a_0(1, 0, 0, 0, \dots) \\ &\quad + a_1(0, 1, 0, 0, \dots) \\ &\quad + a_2(0, 0, 1, 0, \dots) \\ &\quad \vdots \\ &\quad + a_n(0, \dots, 0, 1, 0, \dots) \\ &= (a_0, a_1, \dots, a_n, 0, \dots) \\ &= P \end{aligned}$$

□

REMARQUE (Notation):

On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans \mathbb{K} dont l'indéterminée $(0, 1, 0, \dots)$

est notée X .

Proposition: $(\mathbb{K}[X], +, \times, \cdot)$ est une \mathbb{K} -algèbre commutative i.e.

1. $(\mathbb{K}[X], +, \times)$ est un anneau commutatif
2. $(\mathbb{K}[X], +, \cdot)$ est un \mathbb{K} -espace vectoriel
3. $\forall \lambda \in \mathbb{K}, \forall (P, Q) \in (\mathbb{K}[X])^2, \lambda \cdot (P \times Q) = (\lambda \cdot P) \times Q = P \times (\lambda \cdot Q)$

Preuve: 1. $(\mathbb{K}[X], +)$ est un groupe abélien car $(\mathbb{K}[X], +, \cdot)$ est un \mathbb{K} -espace vectoriel

— $X^0 = (1, 0, \dots)$ est le neutre de \times

En effet, $\forall P = (a_n)_{n \in \mathbb{N}} \in \mathbb{K}[X]$, en posant $(c_n)_{n \in \mathbb{N}} = PX^0$ on a

$$\forall n \in \mathbb{N}, c_n = \sum_{k=0}^n a_k \delta_{k,n-k} = a,$$

donc $PX^0 = P$

— \times est commutative : $\forall P = (a_n)_{n \in \mathbb{N}} \in \mathbb{K}[X], \forall Q = (b_n)_{n \in \mathbb{N}} \in \mathbb{K}[X]$, on pose $R = (c_n)_{n \in \mathbb{N}} = PQ, S = (d_n)_{n \in \mathbb{N}} = QP$ alors

$$\begin{aligned} \forall n \in \mathbb{N}, c_n &= \sum_{k=0}^n a_k b_{n-k} \\ &= \sum_{j=0}^n a_{n-j} b_j \quad (j = n - k) \\ &= \sum_{j=0}^n b_j a_{n-j} \\ &= d_n \end{aligned}$$

donc $PQ = QP$

— Soient

$$\begin{cases} P = (a_n)_{n \in \mathbb{N}} \in \mathbb{K}[X] \\ Q = (b_n)_{n \in \mathbb{N}} \in \mathbb{K}[X] \\ R = (c_n)_{n \in \mathbb{N}} \in \mathbb{K}[X] \end{cases}$$

On pose

$$\begin{cases} S = (d_n)_{n \in \mathbb{N}} = PQ \\ T = (e_n)_{n \in \mathbb{N}} = SR = (PQ)R \\ U = (f_n)_{n \in \mathbb{N}} = QR \\ V = (g_n)_{n \in \mathbb{N}} = PU = P(QR) \end{cases}$$

Donc,

$$\begin{aligned}
\forall n \in \mathbb{N}, e_n &= \sum_{k=0}^n d_k c_{n-k} \\
&= \sum_{k=0}^n \left(\sum_{j=0}^k a_j b_{k-j} \right) c_{n-k} \\
&= \sum_{j=0}^n \sum_{k=j}^n a_j b_{k-j} c_{n-k} \\
&= \sum_{j=0}^n a_j \sum_{k=j}^n b_{k-j} c_{n-k} \\
&= \sum_{j=0}^n a_j \sum_{\ell=0}^{n-j} b_{\ell} c_{n-j-\ell} \quad (\ell = k - j) \\
&= \sum_{j=0}^n a_j f_{n-j} \\
&= g_n
\end{aligned}$$

- Donc $T = V$
- Soient $P = (a_n)_{n \in \mathbb{N}}, Q = (b_n)_{n \in \mathbb{N}}, R = (C_n)_{n \in \mathbb{N}}$ trois polynômes et $P(Q + R) = (d_n)_{n \in \mathbb{N}}$ et $PQ + PR = (e_n)_{n \in \mathbb{N}}$.

$$\begin{aligned}
\forall n \in \mathbb{N}, d_n &= \sum_{k=0}^n a_k (b_{n-k} + c_{n-k}) \\
&= \sum_{k=0}^n a_k b_{n-k} + \sum_{k=0}^n a_k c_{n-k} \\
&= e_n
\end{aligned}$$

Donc, $(\mathbb{K}[X], +, \times)$ est un anneau commutatif

2. $\mathbb{K}[X] \subset \mathbb{K}^{\mathbb{N}}$
 $(\mathbb{K}^{\mathbb{N}}, +, \cdot)$ est un \mathbb{K} -espace vectoriel. D'après la propriété précédente,

$$\mathbb{K}[X] = \text{Vect}((X^n \mid n \in \mathbb{N}))$$

donc $\mathbb{K}[X]$ est un sous-espace vectoriel de $\mathbb{K}^{\mathbb{N}}$

3. Soit $\lambda \in \mathbb{K}, P = (a_n)_{n \in \mathbb{N}}, Q = (b_n)_{n \in \mathbb{N}}$ deux polynômes. On pose $(c_n)_{n \in \mathbb{N}} = PQ, R = (d_n)_{n \in \mathbb{N}} = \lambda(PQ), S = (e_n)_{n \in \mathbb{N}} = (\lambda P)Q, T = (f_n)_{n \in \mathbb{N}} = P(\lambda Q)$.

$$\begin{aligned}
\forall n \in \mathbb{N}, d_n &= \lambda c_n = \lambda \sum_{k=0}^n a_k b_{n-k} \\
&= \sum_{k=0}^n (\lambda a_k) b_{n-k} = e_n \\
&= \sum_{k=0}^n a_k (\lambda b_{n-k}) = f_n
\end{aligned}$$

□

REMARQUE:

$(\mathcal{M}_n(\mathbb{K}), +, \times, \cdot)$ est une \mathbb{K} -algèbre non commutative (si $n > 1$)

Proposition: $i : \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K}[X] \\ \lambda & \longmapsto & \lambda X^0 \end{array}$ est un morphisme d'algèbre injectif, i.e.

$$\forall \lambda, \mu \in \mathbb{K}, \begin{cases} i(\lambda + \mu) = i(\lambda) + i(\mu) \\ i(\lambda \cdot \mu) = i(\lambda) \times i(\mu) \end{cases}$$

et i est injective.

REMARQUE (Notation):

On identifie $\lambda \in \mathbb{K}$ avec $\lambda X^0 \in \mathbb{K}[X]$. Ainsi, on peut écrire $X^0 = 1$, on peut écrire $2 + X + 3X^2$ au lieu de $2X^0 + X + 3X^2$

Proposition: Soient $P, Q \in \mathbb{K}[X]$

- $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$
- Si $\deg(P) \neq \deg(Q)$, alors
 - $\deg(P + Q) = \max(\deg(P), \deg(Q))$
 - $\text{dom}(P + Q) = \begin{cases} \text{dom}(P) & \text{si } \deg(P) > \deg(Q) \\ \text{dom}(Q) & \text{si } \deg(P) < \deg(Q) \end{cases}$
- Si $\deg(P) = \deg(Q)$ et $\text{dom}(P) + \text{dom}(Q) \neq 0$,
 - alors $\begin{cases} \deg(P + Q) = \deg(P) = \deg(Q) \\ \text{dom}(P + Q) = \text{dom}(P) + \text{dom}(Q) \end{cases}$
- Si $\deg(P) = \deg(Q)$ et $\deg(P) + \deg(Q) = 0$, alors $\deg(P + Q) < \deg(P)$

Preuve: — Si $P = 0$, alors $\deg(P + Q) = \deg(Q)$ et donc $\max(\deg(P), \deg(Q)) = \max(-\infty, \deg(Q))$

On a bien $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$

— De même avec $Q = 0$

— On suppose $P \neq 0$ et $Q \neq 0$

On pose $\begin{cases} P = \sum_{k=0}^p a_k X^k & p = \deg(P) \\ Q = \sum_{k=0}^q b_k X^k & q = \deg(Q) \end{cases}$

On peut supposer $p \geq q$. On pose $b_{q+1} = \dots = b_p = 0$ si $p > q$

Ainsi, $Q = \sum_{k=0}^q b_k X^k$

$$P + Q = \sum_{k=0}^p (a_k + b_k) X^k \text{ donc } \deg(P + Q) \leq p \text{ et } p = \max(\deg(P), \deg(Q))$$

De plus, $a_p + b_p = \begin{cases} \text{dom}(P) & \text{si } p > q \\ \neq 0 & \\ \text{dom}(P) + \text{dom}(Q) & \text{si } p = q \end{cases}$

□

Proposition: Soient $P, Q \in \mathbb{K}[X]$. Alors

$$\deg(PQ) = \deg(P) + \deg(Q)$$

Preuve:

Si P ou Q est nul, alors la formule est vraie car

$$\begin{cases} \deg(PQ) = -\infty \\ \deg(P) + \deg(Q) = \begin{cases} \text{cste} - \infty = -\infty \\ -\infty + \text{cste} = -\infty \\ -\infty - \infty = -\infty \end{cases} \end{cases}$$

On suppose $P \neq 0$ et $Q \neq 0$. On pose $P = \sum_{k=0}^p a_k X^k$ avec $a_p \neq 0$ et $Q = \sum_{k=0}^q b_k X^k$ avec $b_q \neq 0$

$$\begin{aligned} PQ &= \left(\sum_{k=0}^p a_k X^k \right) \left(\sum_{\ell=0}^q b_\ell X^\ell \right) \\ &= \sum_{k=0}^p \sum_{\ell=0}^q a_k b_\ell X^{k+\ell} \end{aligned}$$

donc $\deg(PQ) \leq p+q$ et le coefficient devant X^{p+q} est $a_p b_q \neq 0$ (car \mathbb{K} est intègre)

donc $\deg(PQ) = p+q$

□

2 Évaluation

Définition: Soit A une \mathbb{K} -algèbre et $P \in \mathbb{K}[X]$. On pose $P = \sum_{k=0}^n e_k X^k$. Soit $a \in A$.

On pose

$$\begin{aligned} P(a) &= \sum_{k=0}^n e_k a^k \\ &= e_0 1_A + e_1 a + e_2 a^2 + \cdots + e_n a^n \in A \end{aligned}$$

On dit qu'on a évalué P en a , ou spécialisé X avec la valeur de a , ou remplacé X par a , substitué a à X .

Définition: Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.
On dit que a est une racine de P si $P(a) = 0_{\mathbb{K}}$.

Définition: Soit $P \in \mathbb{K}[X] \in \mathcal{M}_n(\mathbb{K})$. On dit que c'est un polynôme de matrices.

EXEMPLE:

$$\begin{aligned}
P &= 1 + 2X - 3X^2, \quad A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \\
P(A) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 2 \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} - 3 \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^2 \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix} - 3 \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 0 & 0 \\ -4 & 0 \end{pmatrix}
\end{aligned}$$

Définition: Soient $P, Q \in \mathbb{K}[X]$, $P = \sum_{k=0}^n a_k X^k$.
Alors $P(Q) = \sum_{k=0}^n a_k Q^k \in \mathbb{K}[X]$
C'est la composée de P et Q .

REMARQUE (\triangleleft Attention):
Ne pas confondre $\underbrace{P(X+1)}_{\text{composée}}$ et $\underbrace{P(X+1)}_{\text{produit}}$.
On a $\underbrace{P(X+1)}_{\text{produit}} = (X+1)P = P(X)(X+1) = P \times (X+1)$

Proposition: Soient $P, Q \in \mathbb{K}[X]$ avec $\begin{cases} Q \neq 0 \\ P \neq 0 \end{cases}$. On a

$$\deg(P(Q)) = \deg(P) \times \deg(Q)$$

□

EXEMPLE:
 $\mathbb{K} = \mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$

$P = X^2 + X + 1 \in \mathbb{K}[X]$ et $Q = 1 \in \mathbb{K}[X]$
 $P \neq Q$

$$\begin{aligned}
f_P : \mathbb{Z}/2\mathbb{Z} &\longrightarrow \mathbb{Z}/2\mathbb{Z} \\
x &\longmapsto P(x)
\end{aligned}$$

$$\begin{aligned}
f_Q : \mathbb{Z}/2\mathbb{Z} &\longrightarrow \mathbb{Z}/2\mathbb{Z} \\
x &\longmapsto Q(x)
\end{aligned}$$

$$\begin{aligned}
f_P(\bar{0}) &= \bar{1} = f_Q(\bar{0}) \\
f_P(\bar{1}) &= \bar{1} + \bar{1} + \bar{1} = \bar{1} = f_Q(\bar{1}) \\
\text{donc } f_P &= f_Q \text{ alors que } P \neq Q
\end{aligned}$$

Théorème: Soit A une \mathbb{K} -algèbre. L'application

$$\begin{aligned}\varphi : \mathbb{K}[X] &\longrightarrow A^A \\ P &\longmapsto f_P : \begin{array}{ccc} A & \longrightarrow & A \\ a & \longmapsto & P(a) \end{array}\end{aligned}$$

vérifie

1. $\forall P, Q \in \mathbb{K}[X], \varphi(P + Q) = \varphi(P) + \varphi(Q)$
2. $\forall P, Q \in \mathbb{K}[X], \varphi(PQ) = \varphi(P) \times \varphi(Q)$
3. $\forall \lambda \in \mathbb{K}, \forall P \in \mathbb{K}[X], \varphi(\lambda P) = \lambda \varphi(P)$

□

EXEMPLE:

$\mathbb{K} = \mathbb{R}$

$$X^2 - 1 = (X - 1)(X + 1)$$

— \mathbb{C} est une \mathbb{R} -algèbre donc

$$\forall z \in \mathbb{C}, z^2 - 1 = (z - 1)(z + 1)$$

— $\mathcal{M}_2(\mathbb{R})$ est une \mathbb{R} -algèbre

$$\forall A \in \mathcal{M}_2(\mathbb{R}), A^2 - I_2 = (A - I_2)(A + I_2)$$

Définition: Soit $P \in \mathbb{K}[X]$,

$$P = \sum_{k=0}^n a_k X^k$$

Le polynôme dérivé de P est

$$P' = \sum_{k=0}^n k a_k X^{k-1} = \sum_{k=1}^n k a_k X^{k-1}$$

où

$$\begin{aligned}\forall k \in [\![1, n]\!], k a_k &= \underbrace{a_k + \cdots + a_k}_{k \text{ fois}} \\ 0_{\mathbb{N}} a_k &= 0_{\mathbb{K}}\end{aligned}$$

REMARQUE:

$$\text{Si } P \in \mathbb{R}[X], f_p : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & P(x) \end{array}$$

$$f_{P'} : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & P'(x) \end{array} \text{ alors } f_{P'} = f'_P$$

Proposition:

$$\forall P \in \mathbb{K}[X], \deg(P') = \begin{cases} \deg(P) - 1 & \text{si } \deg(P) > 0 \\ -\infty & \text{sinon} \end{cases}$$

Proposition: Soient $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.

1. $(P + Q)' = P' + Q'$

- | | |
|--|--|
| | 2. $(PQ)' = P'Q + PQ'$
3. $(\lambda P)' = \lambda P'$ |
|--|--|

Preuve:

On pose

$$P = \sum_{k=0}^p a_k X^k \quad Q = \sum_{k=0}^q b_k X^k$$

1. On peut supposer $p \geq q$
 Si $p > q$, on pose $b_{q+1} = \dots = b_p = 0$

$$P + Q = \sum_{k=0}^p (a_k + b_k) X^k$$

donc

$$\begin{aligned} (P + Q)' &= \sum_{k=0}^p k(a_k + b_k) X^{k-1} \\ &= \sum_{k=0}^p k a_k X^{k-1} + \sum_{k=0}^p k b_k X^{k-1} \\ &= P' + Q' \end{aligned}$$

2.

$$PQ = \sum_{k=0}^p \sum_{\ell=0}^q a_k b_\ell X^{k+\ell}$$

D'après 1.,

$$\begin{aligned} (PQ)' &= \sum_{k=0}^p \sum_{\ell=0}^q (a_k b_\ell X^{k+\ell})' \\ &= \sum_{k=0}^p \sum_{\ell=0}^q a_k b_\ell (k + \ell) X^{k+\ell-1} \\ &= \sum_{k=0}^p \sum_{\ell=0}^q k a_k b_\ell X^{k-1+\ell} + \sum_{k=0}^p \sum_{\ell=0}^q \ell a_k b_\ell X^{k+\ell-1} \\ &= \sum_{k=0}^p k a_k X^{l-1} \sum_{\ell=0}^q b_\ell X^\ell + \sum_{k=0}^p a_k X^k \sum_{\ell=0}^q \ell b_\ell X^{\ell-1} \\ &= P'Q + PQ' \end{aligned}$$

3.

$$\lambda P = \sum_{k=0}^p \lambda a_k X^k$$

donc

$$(\lambda P)' = \sum_{k=0}^p \lambda a_k k X^{k-1} = \lambda \sum_{k=0}^p k a_k X^{k-1} = \lambda P'$$

□

Définition: Pour $k \in \mathbb{N}$, on définit la dérivée k -ième d'un polynôme $P \in \mathbb{K}[X]$ par

- si $k = 0$, $P^{(k)} = P$
- si $k = 1$, $P^{(1)} = P'$
- si $k > 1$, $P^{(k)} = (P^{(k-1)})'$

Proposition:

$$\forall k, j \in \mathbb{N}^2, (X^k)^{(j)} = \begin{cases} 0 & \text{si } j > k \\ k(k-1)\cdots(k-j+1)X^{k-j} = \frac{k!}{(k-j)!} X^k & \text{si } j \leq k \end{cases}$$

Preuve (par récurrence sur j à k fixé): □

Proposition: Soient $P, Q \in \mathbb{K}[X]$, $\lambda \in \mathbb{K}$

1. $\forall k \in \mathbb{N}, (P + Q)^{(k)} = P^{(k)} + Q^{(k)}$
2. $\forall k \in \mathbb{N}, (PQ)^{(k)} = \sum_{i=0}^k \binom{k}{i} P^{(i)} Q^{(k-i)}$
3. $\forall k \in \mathbb{N}, (\lambda P)^{(k)} = \lambda P^{(k)}$

Preuve (par récurrence sur k): □

3 Arithmétique dans $\mathbb{K}[X]$

Définition: Soient $A, B \in \mathbb{K}[X]$. On dit que A divide B (dans $\mathbb{K}[X]$) s'il existe $C \in \mathbb{K}[X]$ tel que

$$AC = B$$

On dit dans ce cas que A est un diviseur de B ou que B est un multiple de A . On le note alors $A | B$

On dit que A et B sont associés s'il existe $\lambda \in \mathbb{K} \setminus \{0\}$ tel que $A = \lambda B$. Il s'agit d'une relation d'équivalence.

Proposition: Soient $A, B \in \mathbb{K}[X]$.

$$\left. \begin{array}{l} A | B \\ B | A \end{array} \right\} \iff A \text{ et } B \text{ sont associés}$$

Preuve: “ \implies ” Soit $C \in \mathbb{K}[X]$ tel que $AC = B$ et $D \in \mathbb{K}[X]$ tel que $BD = A$.
D'où,

$$A = BD = ACD$$

Or, $\mathbb{K}[X]$ est un anneau intègre.

D'où

$$A(1 - CD) = 0$$

donc $A = 0$ ou $CD = 1$

Si $A = 0$, alors $B = 0 \times C = 0 = 1 \times A$ donc A et B sont associés

Si $CD = 1$, on sait que $\mathbb{K}[X]^\times = \mathbb{K} \setminus \{0\}$

Alors, A et B sont associés.

“ \Leftarrow ” évident

□

Lemme: $\mathbb{K}[X]$ est un anneau intègre.

Preuve:

Soient $P, Q \in \mathbb{K}[X]$ tels que $PQ = 0$. On suppose que $P \neq 0$ et $Q \neq 0$

Alors $\deg(PQ) = \deg(P) + \deg(Q) \geq 0$

Or, $PQ = 0$ et $\deg(0) = -\infty$: une contradiction

□

Lemme:

$$\mathbb{K}[X]^\times = \mathbb{K} \setminus \{0\}$$

Preuve:

Soient $P, Q \in \mathbb{K}[X]$ tels que $PQ = 1$.

Alors, $0 = \deg(1) = \deg(PQ) = \deg(P) + \deg(Q)$

Comme $P \neq 0$, $\deg(P) \geq 0$. De même, $\deg(Q) \geq 0$

Donc $\deg(P) = \deg(Q) = 0$ Donc, il existe $\lambda, \mu \in \mathbb{K}$ tels que $\lambda\mu = 1$

Donc $\lambda \in \mathbb{K}^\times = \mathbb{K} \setminus \{0\}$

□

Proposition: $|$ est une relation réflexive et transitive.

□

Proposition: Soient $A, B, C \in \mathbb{K}[X]$ tels que $A | B$ et $A | C$. Alors

$$\forall (P, Q) \in \mathbb{K}[X]^2, A | BQ + CP$$

□

Proposition – Définition: Soit $A \in \mathbb{K}[X], B \in \mathbb{K}[X] \setminus \{0\}$.

$$\exists! (P, Q) \in \mathbb{K}[X]^2, \begin{cases} A = PQ + R \\ \deg(R) < \deg(B) \end{cases}$$

On dit que Q est le quotient et R le reste de la division (euclidienne) de A par B .

Preuve: — On prouve l'existence par récurrence sur le degré de A . On fixe $B \in \mathbb{K}[X] \setminus \{0\}$

$\forall n \in \mathbb{N}, \mathcal{P}(n) : \text{``} \forall A \in \mathbb{K}[X] \text{ tel que } \deg(A) = n,$

$$\exists(Q, R) \in \mathbb{K}[X]^2, \begin{cases} A = BQ + R \\ \deg(R) < \deg(B) \end{cases} \text{''}$$

— Soit $A \in \mathbb{K}[X]$. On suppose $\deg(A) = 0$

Si $\deg(B) > 0$ alors on pose $Q = 0$ et $R = A$. Ainsi $\begin{cases} BQ + R = A \\ \deg(R) = 0 < \deg(B) \end{cases}$

Si $\deg(B) = 0$, alors $A = \lambda$ et $B = \mu$ avec $(\lambda, \mu) \in (\mathbb{K} \setminus \{0\})^2$.

On pose $\begin{cases} Q = \mu^{-1}\lambda \\ R = 0 \end{cases}$. Alors, $\begin{cases} BQ + R = \mu\mu^{-1}\lambda = \lambda = A \\ \deg(R) = -\infty < 0 = \deg(B) \end{cases}$

Donc $\mathcal{P}(0)$ est vraie.

— Soit $n \in \mathbb{N}$. On suppose $\mathcal{P}(k)$ pour tout $k \leq n$. Soit $A \in \mathbb{K}[X]$ tel que $\deg(A) = n+1$. On pose $p = \deg(B)$

Si $p > n+1$, on pose $\begin{cases} Q = 0 \\ R = A \end{cases}$ et on a

$$\begin{cases} BQ + R = A \\ \deg(R) = n+1 < p = \deg(B) \end{cases}$$

Si $p \leq n+1$. On pose $\begin{cases} Q = a_{n+1}b_b^{-1}X^{n+1-p} \\ R = A - BQ \end{cases}$ où $\begin{cases} a_{n+1} = \text{dom}(A) \\ a_p = \text{dom}(b) \end{cases}$ On

a $A = BQ + R$

Or, $\begin{cases} \deg(BQ) = p + n + 1 - p = n + 1 = \deg(A) \\ \text{dom}(BQ) = b_p b_p^{-1} a_{n+1} = a_{n+1} = \text{dom}(A) \end{cases}$

donc $\deg(R) < \deg(A)$ donc $\deg(R) \leq n$

D'après $\mathcal{P}(n)$,

$$\exists(Q_1, R_1) \in \mathbb{K}[X]^2, \begin{cases} R = BQ_1 + R_1 \\ \deg(R_1) < \deg(B) \end{cases}$$

D'où,

$$\begin{aligned} A &= BQ + R \\ &= BQ + BQ_1 + R_1 \\ &= B(Q + Q_1) + R_1 \end{aligned}$$

et $\deg(R_1) < \deg(B)$ donc $\mathcal{P}(n+1)$ est vraie.

Donc, $\mathcal{P}(n)$ est vraie pour tout $n \in \mathbb{N}$ par récurrence forte. Si $A = 0$, on pose $Q = R = 0$ et on a bien $BQ + R = 0 = A$ et $\deg(R) = -\infty < \deg(B)$

— Unicité

Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. On suppose que $A = BQ_1 + R_1 = BQ_2 + R_2$ avec

$Q_1, Q_2, R_1, R_2 \in \mathbb{K}[X]$ et $\begin{cases} \deg(R_1) < \deg(B) \\ \deg(R_2) < \deg(B) \end{cases}$

D'où,

$$B(Q_1 - Q_2) = R_2 - R_1$$

Or,

$$\deg(R_2 - R_1) \leq \max(\deg(R_2), \deg(R_1)) < \deg(B)$$

Or,

$$\begin{aligned}\deg(B(Q_1 - Q_2)) &= \deg(B) + \deg(Q_1 - Q_2) \\ &\geq \deg(B) \text{ si } Q_1 - Q_2 \neq 0\end{aligned}$$

Donc,

$$\begin{cases} Q_1 - Q_2 = 0 \\ R_2 - R_1 = B(Q_2 - Q_1) = 0 \end{cases}$$

et donc

$$\begin{cases} Q_1 = Q_2 \\ R_2 = R_1 \end{cases}$$

□

EXEMPLE:

Division euclidienne de $A = X^5 + X^3 - X^2 + 1$ par $B = X^2 + \frac{1}{2}X - 1$ dans $\mathbb{R}[X]$

$\begin{array}{r} X^5 + X^3 - X^2 + 1 \\ - X^5 + \frac{1}{2}X^4 - X^3 \\ \hline - \frac{1}{2}X^4 + 2X^3 - X^2 + 1 \\ - \frac{1}{2}X^4 - \frac{1}{4}X^3 + \frac{1}{2}X^2 \\ \hline \frac{9}{4}X^3 - \frac{3}{2}X^2 + 1 \\ - \frac{9}{4}X^3 + \frac{9}{8}X^2 - \frac{9}{4}X \\ \hline - \frac{21}{8}X^2 + \frac{9}{4}X + 1 \\ - \frac{21}{8}X^2 - \frac{21}{16}X + \frac{21}{8} \\ \hline \frac{57}{16}X - \frac{13}{8} \end{array}$	$\begin{array}{r} X^2 + \frac{1}{2}X - 1 \\ \hline X^3 - \frac{1}{2}X^2 + \frac{9}{4}X - \frac{21}{8} \\ \text{quotient} \\ \hline \text{reste} \\ \left[\frac{57}{16}X - \frac{13}{8} \right] \end{array}$
--	--

Théorème: Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.

$$P(a) = 0 \iff X - a \mid P$$

Preuve: “ \Leftarrow ” On suppose $P = (X - A) \times Q$ avec $Q \in \mathbb{K}[X]$. On substitue a à X

$$P(a) = (a - a) \times Q(a) = 0_{\mathbb{K}} \times Q(a) = 0_{\mathbb{K}}$$

“ \Rightarrow ” On suppose que $P(a) = 0$. On réalise la division euclidienne de P par $X - a$:

$$\begin{cases} P = (X - a) \times Q + R \\ \deg(R) < \deg(X - a) = 1 \end{cases}$$

donc $R = \lambda$ avec $\lambda \in \mathbb{K}$
D'où,

$$0 = P(a) = (a - a) \times Q(a) + R(a) = \lambda$$

donc

$$P = (X - a) \times Q$$

et donc

$$X - a \mid P$$

□

Corollaire: Soit $P \in \mathbb{K}[X]$ non nul de degré n . Alors, P a au plus n racines distinctes dans \mathbb{K}

Preuve (par récurrence sur n): — C'est évident pour $n = 0$

- Soit $n \in \mathbb{N}$. On suppose la proposition vraie pour les polynômes de degré n .
- Soit $P \in \mathbb{K}[X]$ de degré $n + 1$
- Si P n'a pas de racine alors le résultat est trivialement vrai pour P
- Si P a une racine a , alors il existe $Q \in \mathbb{K}[X]$ non nul tel que $P = (X - a) \times Q$
- $n + 1 = \deg(P) = 1 + \deg(Q)$ donc $\deg(Q) = n$
- D'après l'hypothèse de récurrence, Q a au plus n racines distinctes
- Soit b une racine de P différente de a . Alors,

$$0 = P(b) = \underbrace{(b - a)}_{\neq 0} \times Q(b)$$

$$\text{donc } Q(b) = 0$$

Donc P a bien au plus $n + 1$ racines.

□

Définition: Soient A et B deux polynômes dont l'un au moins est non nul, $D \in \mathbb{K}[X]$. On dit que D est un PGCD de A et B si D est un diviseur commun de A et B et de degré maximal.

Proposition: Avec les hypothèses précédentes, deux PGCD quelconques de A et B sont nécessairement associés

Preuve:

On forme

$$E = \{AU + BV \mid (U, V) \in \mathbb{K}[X]^2\}$$

— E est un sous-groupe de $(\mathbb{K}[X], +)$

— $\forall P \in E, \forall Q \in \mathbb{K}[X], PQ \in E$

On dit que E est un *idéal* de $\mathbb{K}[X]$

Soit $D \in E$ un polynôme non nul de degré minimal. Soit $P \in E$ On divise P par D :

$$\begin{cases} P = DQ + R \\ \deg(R) < \deg(D) \end{cases}$$

D'où

$$R = \underbrace{P}_{\in E} - \underbrace{DQ}_{\in E} \in E$$

$\deg(R) < \deg(D)$ donc $R = 0$

Donc,

$$\forall P \in E, D \mid P$$

$A \in E$ donc $D \mid A$

$B \in E$ donc $D \mid B$

Soit Δ un diviseur commun quelconque de A et B . On pose $D = AU + BV$

$$\left. \begin{array}{l} \Delta \mid A \\ \Delta \mid B \end{array} \right\} \text{donc } \Delta \mid AU + BV \text{ donc } \Delta \mid D$$

donc $\deg(\Delta) \leq \deg(D)$

Ainsi, D est un PGCD de A et B . De plus, Δ est un PGCD de A et B alors

$$\left\{ \begin{array}{l} \Delta \mid D \\ \deg(\Delta) = \deg(D) \end{array} \right.$$

Donc $D = \Delta Q$ avec $\left\{ \begin{array}{l} Q \in \mathbb{K}[X] \\ \deg(Q) = 0 \end{array} \right.$

donc D et Δ sont associés. \square

REMARQUE:

Dans la preuve précédente, on a aussi montré les deux propositions suivantes.

Théorème (Théorème de Bézout): Soient $A, B \in \mathbb{K}[X]$ tels que $A \neq 0$ ou $B \neq 0$
Soit D un PGCD de A et B . Alors

$$\exists (U, V) \in \mathbb{K}[X]^2, AU + BV = D$$

Proposition: Avec les hypothèses précédentes,

$$\forall \Delta \in \mathbb{K}[X], \quad \left. \begin{array}{l} \Delta \mid A \\ \Delta \mid B \end{array} \right\} \iff \Delta \mid D$$

Définition: On dit qu'un polynôme est unitaire si son coefficient dominant vaut 1.

Proposition – Définition: Soient A et B deux polynômes dont l'un au moins est non nul. Parmi tous les PGCD de A et B , un seul est unitaire. On le note $A \wedge B$.

Preuve:

Soit D un PGCD de A et B . Alors $\text{dom}(D)^{-1}D$ est associé à D , donc c'est un PGCD de A et B et il est unitaire. Soient D et Δ deux PGCD unitaires de A et B . Ils sont associés

$$\Delta = \lambda D \text{ avec } \lambda \in \mathbb{K} \setminus \{0\}$$

D'où,

$$1 = \text{dom}(\Delta) = \lambda \text{dom}(D) = \lambda$$

Donc $\Delta = D$

□

Proposition: Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Soit R le reste de la division de A par B . Alors,

$$A \wedge B = B \wedge R$$

Preuve (idem que dans \mathbb{Z}):

□

EXEMPLE:

$$D = (5X^2 + 3X - 1) \wedge (X + 3)$$

$$\begin{array}{r|rr} & X^2 + 3X - 1 & X + 3 \\ \hline - & 5X^2 + 15X & 5X - 12 \\ \hline & -12X - 1 & \\ - & -12X - 36 & \\ \hline & 35 & \end{array} \quad \begin{array}{r|rr} & X + 3 & 35 \\ \hline - & X & \frac{1}{35}X + \frac{3}{35} \\ \hline & 3 & \\ - & 3 & \\ \hline & 0 & \end{array}$$

$$D = (X + 3) \wedge 35 = 1$$

Théorème (Théorème de Gauß): Soient A, B, C trois polynômes non nuls tels que

$$\left\{ \begin{array}{l} A \mid BC \\ A \wedge B = 1 \end{array} \right.$$

Alors, $A \mid C$

Preuve (idem que dans \mathbb{Z}):

□

Corollaire: Avec les notations précédentes,

$$\left. \begin{array}{l} A \mid B \\ B \mid C \\ A \wedge B = 1 \end{array} \right\} \implies AB \mid C$$

Proposition: Soient A et B deux polynômes non nuls et D un PGCD de A et B . Soit $x \in \mathbb{K}$.

$$\boxed{A(x) = B(x) = 0 \iff D(X) = 0}$$

Preuve: “ \implies ” On suppose $A(x) = B(x) = 0$
D'après le théorème de Bézout,

$$D = AU + BV \text{ avec } (U, V) \in \mathbb{K}[X]^2$$

Donc,

$$D(x) = A(x)U(x) + B(x)V(x) = 0 + 0 = 0$$

“ \impliedby ” On suppose $D(x) = 0$. On pose $\begin{cases} A = DA_1 \\ B = DB_1 \end{cases}$ avec $(A_1, B_1) \in \mathbb{K}[X]^2$

D'où,

$$\begin{cases} A(x) = D(x)A_1(x) = 0 \\ B(x) = D(x)B_1(x) = 0 \end{cases}$$

□

Définition: Soit $P \in \mathbb{K}[X]$.

On dit que P n'est pas irréductible si il existe $(Q, R) \in \mathbb{K}[X]^2$ non constants tels que $P = QR$ ou si P est constant.

Sinon, on dit que P est irréductible.

EXEMPLE: 1. $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$

On suppose que

$$X^2 + 1 = QR \text{ avec } (Q, R) \in \mathbb{R}[X]^2$$

$$\begin{cases} \deg(Q) > 0 \\ \deg(R) > 0 \end{cases}$$

Donc, P et Q sont de degré 1, donc ont chacun une racine réelle donc $X^2 + 1$ a au moins une racine réelle : \nexists une contradiction.

2. $X^2 + 1$ n'est pas irréductible dans $\mathbb{C}[X]$:

$$X^2 + 1 = (X - i)(X + i)$$

3. $X^4 + 1$ n'est pas irréductible dans $\mathbb{R}[X]$ et pourtant il n'a aucune racine réelle.

$$\begin{aligned} X^2 + 1 &= X^4 + 2X^2 + 1 - 2X^2 \\ &= (X^2 + 1)^2 - 2X^2 \\ &= \underbrace{(X^2 + 1 - \sqrt{2}X)}_{\in \mathbb{R}[X]} \underbrace{(X^2 + 1 + \sqrt{2}X)}_{\in \mathbb{R}[X]} \end{aligned}$$

Théorème (Théorème de D'Alembert - Gauß):

$$\forall P \in \mathbb{C}[X] \text{ non constant}, \exists a \in \mathbb{C}, P(a) = 0$$

□

Corollaire: Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.

Preuve:

Les polynômes de degré 1 sont évidemment irréductibles.

Soit $P \in \mathbb{K}[X]$ tel que $\deg(P) \geq 2$. Soit $a \in \mathbb{C}$ une racine de P .
Donc $X - a \mid P$.

$$\begin{cases} P = (X - a) \times Q \\ Q \in \mathbb{C}[X] \\ \deg(Q) \geq 1 \\ \deg(X - a) = 1 \end{cases} \text{ donc } P \text{ n'est pas irréductible.} \quad \square$$

EXEMPLE:

Factoriser $X^4 + 1$ dans \mathbb{C}

Les racines complexes de $X^4 + 1$ sont $\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$ et $-\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$
Donc,

$$\begin{aligned} X^4 - 1 &= \left(X - \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2} \right) \left(X + \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2} \right) \\ &\quad \times \left(X + \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} \right) \left(X - \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} \right) \end{aligned}$$

Définition: Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$, $\mu \in \mathbb{N}$.
On dit que a est une racine de P de multiplicité μ si

$$\begin{cases} (X - a)^\mu \mid P \\ (X - a)^{\mu+1} \nmid P \end{cases}$$

Si $\mu = 1$, on dit que a est une racine simple.

Si $\mu = 2$, on dit que a est une racine double.

REMARQUE:

a est une racine de multiplicité 0 si et seulement si $P(a) \neq 0$

Lemme: Soient $(A, B) \in \mathbb{R}[X]^2$ non nuls. On suppose que A divise B dans $\mathbb{C}[X]$
Alors, A divise B dans $\mathbb{R}[X]$

Preuve:

On suppose que

$$(*) \quad B = AQ \text{ avec } Q \in \mathbb{C}[X]$$

On divise B par A dans $\mathbb{R}[X]$:

$$(**) \quad B = AQ_1 + R_1 \text{ avec } \begin{cases} (Q_1, Q_2) \in \mathbb{R}[X]^2 \\ \deg(R_1) < \deg(A) \end{cases}$$

Comme $\mathbb{R}[X] \subset \mathbb{C}[X]$, $(**)$ est aussi le résultat de la division euclidienne de B par A

dans $\mathbb{C}[X]$.

(*) correspond aussi à une division euclidienne dans $\mathbb{C}[X]$

Par unicité, $\begin{cases} Q = Q_1 \in \mathbb{R}[X] \\ R_1 = 0 \end{cases}$

Donc A divise B dans $\mathbb{R}[X]$

□

Proposition: Soit $P \in \mathbb{R}[X]$ et $a \in \mathbb{C} \setminus \mathbb{R}$, $\mu \in \mathbb{N}$.

Si a est une racine de P de multiplicité μ alors \bar{a} est une racine de P de multiplicité μ .

Preuve (par récurrence sur μ):

On pose

$$\forall n \in \mathbb{N}, \mathcal{P}(n) : \text{"}\forall P \in \mathbb{R}[X] \text{ et } a \in \mathbb{C} \setminus \mathbb{R} \text{ racine de } P \text{ de multiplicité } \mu, \text{ alors } \bar{a} \text{ est aussi une racine de } P \text{ de multiplicité } \mu\text{"}$$

— Soit $P \in \mathbb{R}[X]$ et $a \in \mathbb{C} \setminus \mathbb{R}$ tel que $P(a) \neq 0$.

On pose $P = \sum_{i=0}^p \alpha_i X^i$ avec $\alpha_0, \dots, \alpha_p \in \mathbb{R}$

$$\begin{aligned} P(\bar{a}) &= \sum_{i=0}^p \alpha_i \bar{a}^i \\ &= \sum_{i=0}^p \overline{\alpha_i a^i} \\ &= \sum_{i=0}^p \overline{\alpha_i a^i} \\ &= \overline{\left(\sum_{i=0}^p \alpha_i a^i \right)} \\ &= \overline{P(a)} \\ &\neq 0 \end{aligned}$$

Donc $\mathcal{P}(0)$ est vraie

— Soit $\mu \in \mathbb{N}$. On suppose $\mathcal{P}(\mu)$ vraie.

Soit $P \in \mathbb{R}[X]$ et $a \in \mathbb{C} \setminus \mathbb{R}$ une racine de P de multiplicité $\mu + 1$. On pose

$$\begin{cases} P = (X - a)^{\mu+1} Q \\ Q \in \mathbb{C}[X] \\ Q(a) \neq 0 \end{cases}$$

On pose aussi $P = \sum_{i=0}^p \alpha_i a^i$ avec $\alpha_0, \dots, \alpha_p \in \mathbb{R}$

$\mu + 1 \geq 1$ donc $P(a) = 0$. D'où, $P(\bar{a}) = \overline{P(a)} = \bar{0} = 0$
donc $\underbrace{(\bar{a} - a)^{\mu+1}}_{\neq 0} Q(\bar{a}) = 0$

Donc, $Q = (X - \bar{a})Q_1$ avec $Q_1 \in \mathbb{C}[X]$
D'où

$$\begin{aligned} P &= (X - a)^{\mu+1} (X - \bar{a}) Q_1 \\ &= (X - a)(X - \bar{a})(X - a)^{\mu} Q_1 \end{aligned}$$

Or,

$$\begin{aligned}(X - a)(X - \bar{a}) &= X^2 - (a + \bar{a})X + a\bar{a} \\ &= X^2 - 2\Re(a)X + |a|^2 \in \mathbb{R}[X]\end{aligned}$$

D'après le lemme précédent, $(X - a)^\mu Q_1 \in \mathbb{R}[X]$
De plus,

$$0 \neq Q(a) = (\bar{a} - a)Q_1(a)$$

Donc $Q_1(a) \neq 0$

Donc a est une racine de $(X - a)^\mu Q_1 \in \mathbb{R}[X]$ de multiplicité μ .

D'après $\mathcal{P}(\mu)$, \bar{a} est aussi une racine de $(X - a)^\mu Q_1$ de multiplicité μ .

Donc, on peut écrire

$$(X - a)^\mu Q_1 = (X - \bar{a})^\mu Q_2 \text{ avec } \begin{cases} Q_2 \in \mathbb{C}[X] \\ Q_2(\bar{a}) \neq 0 \end{cases}$$

Donc,

$$P = (X - a)(X - \bar{a})^{\mu+1} Q_2$$

Donc \bar{a} est une racine de P de multiplicité $\mu + 1$

□

Corollaire: Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatifs.

Preuve:

- Les polynômes de degré 1 sont évidemment irréductibles
- Les polynômes constants ne sont pas irréductibles par définition
- Les polynômes de degré 2 ayant au moins une racine réelle peuvent s'écrire comme produit de deux polynômes réels de degré 1 à coefficients réels
- Réciproquement, si un polynôme de degré 2 n'est pas irréductible, c'est forcément un produit de 2 polynômes de degré 1 à coefficients réels et donc ce polynôme a au moins une racine réelle
- Soit $P \in \mathbb{R}[X]$ tel que $\deg(P) \geq 3$
On note a_1, \dots, a_r les racines réelles distinctes de P ,

$$a_{r+1}, \overline{a_{r+1}}, a_{r+2}, \overline{a_{r+2}}, \dots, a_s, \overline{a_s}$$

les racines non réelles distinctes de P . On note aussi

$$\forall k \in \llbracket 1, s \rrbracket, \mu_k \text{ la multiplicité de } a_k$$

Donc

$$\begin{aligned}P &= \text{dom}(P)(X - a_1)^{\mu_1} \cdots (X - a_r)^{\mu_r} (X - a_{r+1})^{\mu_{r+1}} (X - \overline{a_{r+1}})^{\mu_{r+1}} \\ &\quad \times \cdots \times (X - a_s)^{\mu_s} (X - \overline{a_s})^{\mu_s}\end{aligned}$$

Or,

$$\begin{aligned}\forall k \geq r+1, (X - a_k)^{\mu_k} (X - \overline{a_k})^{\mu_k} &= ((x - a)(x - \bar{a}))^{\mu_k} \\ &= (X^2 - 2\Re(a)X + |a|^2) \\ &\in \mathbb{R}[X]\end{aligned}$$

D'où,

$$P = \underbrace{\text{dom}(P)}_{\in \mathbb{R}} \prod_{k=1}^r (X - a_k)^{\mu_k} \prod_{k=r+1}^s \underbrace{(X^2 - 2\Re(a_k)X + |a_k|^2)^{\mu_k}}_{\in \mathbb{R}[X]}$$

$$P \text{ irréductible} \iff \begin{cases} \text{il y a une unique racine réelle simple} \\ \text{et aucune racine non réelle} \\ \text{OU} \\ \text{il n'y a aucune racine réelle et 2 racines} \\ \text{non réelles conjuguées simples} \end{cases}$$

□

Théorème: Soit $\mathbb{K} = \mathbb{R}$ ou \mathbb{C} .

Tout polynôme de \mathbb{K} se découpe en produit de facteurs irréductibles dans $\mathbb{K}[X]$ et cette décomposition est unique à multiplication par une constante non nulle près. □

Proposition: Soient $A, B \in \mathbb{C}[X]$ non nuls.

$$A \mid B \iff \forall a \in \mathbb{C}, \text{ si } a \text{ est une racine de } A \text{ de multiplicité } \mu \in \mathbb{N}, \text{ alors } a \text{ est racine de } B \text{ avec une multiplicité } \geq \mu$$

Preuve: “ \implies ” On suppose $A \mid B$

Soit $a \in \mathbb{C}$ une racine de A de multiplicité μ

Alors, $(X - a)^\mu \mid A$ donc $(X - a)^\mu \mid B$

Donc a est une racine de B de multiplicité $\geq \mu$

“ \impliedby ” On décompose A et B en produit de facteurs irréductibles sur $\mathbb{C}[X]$:

$$B = \text{dom}(B) \prod_{a \in \mathcal{R}} (X - a)^{\nu_a}$$

où \mathcal{R} est l'ensemble des racines de B ; et

$$A = \text{dom}(A) \prod_{a \in \mathcal{S}} (X - a)^{\mu_a}$$

où \mathcal{S} est l'ensemble des racines de A

On suppose que $\begin{cases} \mathcal{S} \subset \mathcal{R} \\ \forall a \in \mathcal{S}, \mu_a \leq \nu_a \end{cases}$

D'où,

$$B = \frac{\text{dom}(B)}{\text{dom}(A)} \underbrace{\text{dom}(A) \prod_{a \in \mathcal{S}} (X - a)^{\mu_a}}_A \times \underbrace{\prod_{a \in \mathcal{S}} (X - a)^{\nu_a - \mu_a}}_{\in \mathbb{C}[X]} \times \underbrace{\prod_{a \in \mathcal{R} \setminus \mathcal{S}} (X - a)^{\nu_a}}_{\in \mathbb{C}[X]}$$

Donc, $A \mid B$

□

EXERCICE:

Montrer que $1 + X + X^2 \mid X^{3n} - 1$
Les racines de $1 + X + X^2$ sont j et j^2

$$j^{3n} - 1 = (j^3)^n - 1 = 1 - 1 = 0$$

$$(j^2)^{3n} = (j^3)^{2n} - 1 = 1 - 1 = 0$$

Proposition: Soit $P \in \mathbb{C}[X]$ de degré $n > 0$
Alors P a exactement n racines comptées avec multiplicité.

Preuve:

$$P = \text{dom}(P) \times \prod_{a \in \mathcal{R}} (X - a)^{\mu_a}$$

où \mathcal{R} est l'ensemble des racines distinctes de P
 $n = \deg(P) = \sum_{a \in \mathcal{R}} \deg((X - a)^{\mu_a}) = \sum_{a \in \mathcal{R}} \mu_a$

□

4 L'espace vectoriel $\mathbb{K}[X]$

REMARQUE (Rappel):

$(\mathbb{K}[X], +, \cdot)$ est un \mathbb{K} -espace vectoriel engendré par $(1, X, X^2, \dots)$

Proposition: La famille $(X^n)_{n \in \mathbb{N}}$ est libre.

Preuve:

Soit $(\lambda_n)_{n \in \mathbb{N}}$ une famille presque nulle de scalaires telle que $\sum_{n \in \mathbb{N}} \lambda_n X^n = 0$

$(\lambda_n)_{n \in \mathbb{N}}$ est un polynôme de $\mathbb{K}[X]$: on le note P .

Or,

$$\sum_{n \in \mathbb{N}} \lambda_n X^n = (\lambda_0, \lambda_1, \dots, \lambda_n, \dots) = P$$

Donc $P = 0$ donc

$$\forall n \in \mathbb{N}, \lambda_n = 0$$

□

Corollaire:

$$\dim(\mathbb{K}[X]) = +\infty$$

□

Définition: Pour $n \in \mathbb{N}$, on note

$$\mathbb{K}_n[X] = \{P \in \mathbb{K}[X] \mid \deg(P) \leq n\}$$

Théorème: $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$ de dimension $n + 1$

Preuve:

$$\mathbb{K}_n[X] = \text{Vect}(1, X, \dots, X^n)$$

□

Proposition: Soit $(P_i)_{i \in I}$ une famille de polynômes non nuls telle que

$$\forall i \neq j, \deg(P_i) \neq \deg(P_j)$$

Alors $(P_i)_{i \in I}$ est libre.

Preuve:

Soit $n \in \mathbb{N}$ et i_1, \dots, i_n des éléments distincts de I

Soient $\lambda_1, \dots, \lambda_n \in \mathbb{K}$. On suppose

$$\lambda_1 P_{i_1} + \dots + \lambda_n P_{i_n} = 0$$

Quitte à renommer les polynômes, on peut supposer que

$$\forall k \in \llbracket 1, n \rrbracket, \deg(P_{i_k}) > \deg(P_{i_{k+1}})$$

Si $\lambda_n \neq 0$,

$$\deg(\lambda_1 P_{i_1} + \dots + \lambda_n P_{i_n}) = \deg(P_{i_n}) \neq -\infty$$

Donc $\lambda_n = 0$

$$\text{Donc } \lambda_1 P_{i_1} + \dots + \lambda_{n-1} P_{i_{n-1}} = 0$$

On conclut par récurrence sur n .

□

Théorème (Formule de Taylor): Soit $P \in \mathbb{K}_n[X]$ et $a \in \mathbb{K}$.

$$P(X) = \sum_{k=0}^n \frac{P^{(k)}(a)}{k!} (X-a)^k$$

Preuve:

$(1, X-a, \dots, (X-a)^n)$ est libre.

Comme $\dim(\mathbb{K}_n[X]) = n+1$, c'est une base de $\mathbb{K}_n[X]$.

Donc, il existe $(\lambda_0, \dots, \lambda_n) \in \mathbb{K}^{n+1}$ tel que

$$P = \sum_{k=0}^n \lambda_k (X-a)^k$$

On remarque que

$$P(a) = \lambda_0$$

$$\begin{aligned} \forall i \in \llbracket 1, n \rrbracket, P^{(i)}(a) &= \sum_{k=0}^n \lambda_k \underbrace{\left((X-a)^k \right)^{(i)}}_{\substack{0 \\ i!}}(a) \\ &= \begin{cases} 0 & \text{si } k < i \\ \frac{k!}{(k-i)!} (X-a)^{k+1} & \text{si } k = i \\ \lambda_i i! & \text{si } k > i \end{cases} \end{aligned}$$

$$\text{Donc } \lambda_i = \frac{P^{(i)}(a)}{i!}$$

□

Proposition: Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.

$$\left. \begin{array}{l} a \text{ est une racine de } P \\ \text{de multiplicité } \mu \end{array} \right\} \iff \left\{ \begin{array}{l} \forall k \leq \mu - 1, P^{(k)}(a) = 0 \\ P^{(\mu)}(a) \neq 0 \end{array} \right.$$

Preuve:

On pose $n = \deg(P)$

“ \iff ”

$$\begin{aligned} P &= \sum_{k=0}^n \frac{P^{(k)}(a)}{k!} (X-a)^k \\ &= \sum_{k=\mu}^n \frac{P^{(k)}(a)}{k!} (X-a)^k \\ &= (X-a)^\mu \underbrace{\sum_{k=\mu}^n \frac{P^{(k)}(a)}{k!} (X-a)^{k-\mu}}_{Q \in \mathbb{K}[X]} \end{aligned}$$

$$\begin{aligned} \text{Donc } \left\{ \begin{array}{l} (X-a)^\mu \mid P \\ Q(a) = \frac{P^{(\mu)}(a)}{\mu!} \neq 0 \end{array} \right. \\ \text{“ } \implies \text{”} \\ \left\{ \begin{array}{l} P = (X-a)^\mu Q \\ Q(a) \neq 0 \end{array} \right. \end{aligned}$$

$$\begin{aligned} \forall k \leq \mu - 1, P^{(k)}(a) &= \sum_{j=0}^k \binom{k}{j} ((X-a)^\mu)^{(j)}(a) Q^{(k-j)}(a) \\ &= \sum_{j=0}^k \binom{k}{j} \frac{\mu!}{(\mu-j)!} \underbrace{(a-a)^{\mu-j}}_{=0} Q^{(k-j)}(a) \\ &= 0 \end{aligned}$$

$$\begin{aligned} P^{(\mu)}(a) &= \binom{\mu}{\mu} \times \mu! \times 1 \times Q^{(0)}(a) \\ &= Q(a) \\ &\neq 0 \end{aligned}$$

□

Corollaire: Avec les notations précédentes, si a est une racine de P de multiplicité μ , alors a est une racine de P' de multiplicité $\mu - 1$

□

Définition: On dit qu'un polynôme P est scindé sur \mathbb{K} si P est un produit de polynômes de $\mathbb{K}[X]$ de degré 1, i.e. toutes les racines de P sont dans \mathbb{K}

- EXERCICE:**
1. Soit $P \in \mathbb{R}[X]$ scindé sur \mathbb{R} à racines simples avec $\deg(P) \geq 2$. Montrer que P' est scindé sur \mathbb{R} à racines simple.
 2. Soit $P \in \mathbb{R}[X]$ scindé avec $\deg(P) \geq 2$. Montrer que P' est scindé.

Solution

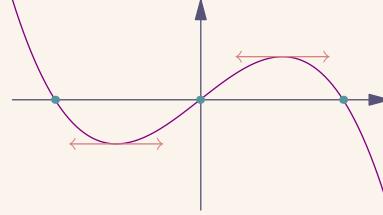
1. Soit $P \in \mathbb{R}[X]$ avec $\deg(P) = n$ scindé sur \mathbb{R} . On note $x_1 < x_2 < \dots < x_n$ les n racines de P . Soit $f_P : \mathbb{R} \rightarrow \mathbb{R}$ la fonction polynomiale. Aussi, f_P est \mathcal{C}^∞ sur \mathbb{R} .

D'après le théorème de Rolle,

$$\forall i \in \llbracket 1, n-1 \rrbracket, \exists y_i \in]x_i, x_{i+1}[, f'_P(y_i) = 0$$

Donc y_1, \dots, y_{n-1} sont racines de P' . De plus,

$$y_1 < x_2 < y_2 < x_3 < y_3 < \dots < y_{n-1}$$



On a donc trouvé $n-1$ racines distinctes de P' . Or, $\deg(P') = n-1$. Donc, on a trouvé TOUTES les racines complexes de P' . Donc P' est scindé à racines simples.

2. On note $x_1 < \dots < x_p$ les racines de P et $n = \deg(P)$. On note pour tout $i \in \llbracket 1, p \rrbracket$, μ_i la multiplicité de x_i . Donc,

$$\sum_{i=1}^p \mu_i = n$$

D'après le théorème de Rolle,

$$\forall i \in \llbracket 1, p-1 \rrbracket, \exists y_i \in]x_i, x_{i+1}[, P'(y_i) = 0$$

On a trouvé $p-1$ racines réelles de P' . $\forall i \in \llbracket 1, p \rrbracket, x_i$ est une racine de P' de multiplicité $\mu_i - 1$.

Ce qui fait, $\sum_{i=1}^p (\mu_i - 1) = n - p$ racines réelles de P' comptées avec multiplicité.

En tout, on a trouvé $n-1$ racines réelles de P' comptées avec multiplicité. Comme $\deg(P') = n-1$, P' n'a pas d'autres racines donc P' est scindé.

EXERCICE (Problème):

Soient $(x_1, \dots, x_n) \in \mathbb{K}^n$ tels que

$$\forall i \neq j, x_i \neq x_j$$

Soient $(y_1, \dots, y_n) \in \mathbb{K}^n$. On cherche $P \in \mathbb{K}[X]$ de degré minimal tel que

$$(*) \quad \forall i \in \llbracket 1, n \rrbracket, P(x_i) = y_i$$

$$\begin{aligned} \text{Soit } \varphi : \mathbb{K}[X] &\longrightarrow \mathbb{K}^n \\ P &\longmapsto (P(x_1), \dots, P(x_n)) \\ (*) &\iff \varphi(P) = (y_1, \dots, y_n) \end{aligned}$$

On cherche, parmi tous les antécédents de (y_1, \dots, y_n) celui de plus bas degré.
 φ est linéaire :

$$\begin{aligned} \forall P, Q \in \mathbb{K}[X], \forall \alpha, \beta \in \mathbb{K}, \\ \varphi(\alpha P + \beta Q) &= (\alpha P(x_1) + \beta Q(x_1), \dots, \alpha P(x_n) + \beta Q(x_n)) \\ &= (\alpha P(x_1), \dots, \alpha P(x_n)) + (\beta Q(x_1), \dots, \beta Q(x_n)) \\ &= \alpha \varphi(P) + \beta \varphi(Q) \end{aligned}$$

— Donc φ est un morphisme de groupes additifs.

$$— (y_1, \dots, y_n) = \sum_{i=0}^n y_i e_i \text{ où } (e_1, \dots, e_n) \text{ est la base canonique de } \mathbb{K}^n$$

Si on trouve $L_1, \dots, L_n \in \mathbb{K}[X]$ tels que $\varphi(L_i) = e_i, \dots, \varphi(L_n) = e_n$, alors

$$\begin{aligned} \varphi \left(\sum_{i=1}^n y_i L_i \right) &= \sum_{i=0}^n y_i \varphi(L_i) \\ &= \sum_{i=1}^n y_i e_i \\ &= (y_1, \dots, y_n) \end{aligned}$$

$$\begin{aligned} P \in \text{Ker}(\varphi) &\iff \varphi(P) = (0, \dots, 0) \\ &\iff \forall i \in \llbracket 1, n \rrbracket, P(x_i) = 0 \\ &\iff \exists Q \in \mathbb{K}[X], P = (X - x_1) \cdots (X - x_n)Q \end{aligned}$$

Soit $i \in \llbracket 1, n \rrbracket$ et $L_i \in \mathbb{K}[X]$.

$$\begin{aligned} \varphi(L_i) = e_i &\iff (L_i(x_1), L_i(x_2), \dots, L_i(x_n)) = (0, \dots, 0, \underbrace{1}_i, 0, \dots, 0) \\ &\iff \begin{cases} L_i(x_i) = 1 \\ \forall j \neq i, L_i(x_j) = 0 \end{cases} \\ &\iff \begin{cases} \exists Q \in \mathbb{K}[X], L_i = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (X - x_j)Q \\ 1 = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (x_i - x_j)Q(x_i) \end{cases} \\ &\iff L_i = \prod_{j \neq i} \frac{X - x_j}{x_i - x_j} \end{aligned}$$

D'où,

$$\begin{aligned} \varphi(P) = (y_1, \dots, y_n) &\iff \exists Q \in \mathbb{K}[X], P = \underbrace{\sum_{i=1}^n y_i L_i}_{\substack{\text{solution particulière} \\ \deg(\cdot) \leq n-1}} + \underbrace{\prod_{k=1}^n (X - x_k)Q}_{\substack{\text{solutions de l'équation} \\ \text{homogène associée} \\ \deg(\cdot) \geq n}} \end{aligned}$$

Le polynôme de plus bas degré solution du problème d'interpolation est

$$\sum_{i=1}^n y_i \prod_{j \neq i} \frac{X - x_j}{x_i - x_j}$$

Définition: Soit $(x_1, \dots, x_n) \in \mathbb{K}^n$ avec

$$\forall i \neq j, x_i \neq x_j$$

On pose

$$\forall i \in \llbracket 1, n \rrbracket, L_i = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} \frac{X - x_j}{x_i - x_j}$$

L_i est le i -ème polynôme interpolateur de Lagrange associé à (x_1, \dots, x_n) :

$$\forall j \in \llbracket 1, n \rrbracket, L_i(x_j) = \delta_{i,j}$$

Proposition: Avec les notations précédentes, (L_1, \dots, L_n) est une base de $\mathbb{K}_{n-1}[X]$.

Preuve: — $\forall i \in \llbracket 1, n \rrbracket, \deg(L_i) = n - 1$

— Soit $P \in \mathbb{K}_{n-1}[X]$. On pose

$$\forall i \in \llbracket 1, n \rrbracket, y_i = P(x_i)$$

On pose $Q = \sum_{i=1}^{n-1} y_i L_i$. Q est le seul polynôme de degré $\leq n-1$ tel que $Q(x_i) = y_i$

pour tout i .

Donc, $P = Q \in \text{Vect}(l_1, \dots, l_n)$. Donc (L_1, \dots, L_n) est une famille génératrice de $\mathbb{K}_{n-1}[X]$. Or, $\dim(\mathbb{K}_{n-1}[X]) = n$. Donc (L_1, \dots, L_n) est une base de $\mathbb{K}_{n-1}[X]$

□

EXEMPLE:

$\mathbb{K} = \mathbb{Z}/5\mathbb{Z}$ et $n = 3$

$$\begin{aligned} x_1 &= \bar{2} \\ x_2 &= \bar{0} \\ x_3 &= \bar{-1} \end{aligned}$$

$$\begin{aligned} y_1 &= \bar{1} \\ y_2 &= \bar{1} \\ y_3 &= \bar{2} \end{aligned}$$

Le seul polynôme de degré ≤ 2 tel que $P(x_i) = y_i$ pour tout $i \in \llbracket 1, 2 \rrbracket$ est $\sum_{i=1}^3 y_i \prod_{\substack{1 \leq j \leq 3 \\ j \neq i}} \frac{X - x_j}{x_i - x_j}$

$$\begin{aligned} L_1 &= (x_1 - x_2)^{-1}(x_1 - x_3)^{-1}(X - x_2)(X - x_3) \\ &= \bar{3} \times \bar{2} \times X(X + \bar{1}) = X(X + \bar{1}) = X^2 + X \end{aligned}$$

$$\begin{aligned} L_2 &= (x_2 - x_1)^{-1}(x_2 - x_3)^{-1}(X - x_1)(X - x_3) \\ &= \bar{2} \times \bar{1}(X - \bar{2}) \times (X - \bar{1}) \\ &= \bar{2}X^2 + \bar{3}X + \bar{1} \end{aligned}$$

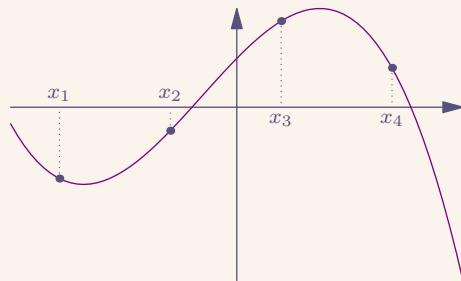
$$\begin{aligned} L_3 &= (x_3 - x_1)^{-1}(x_3 - x_2)^{-1}(X - x_1)(X - x_2) \\ &= \bar{3} \times \bar{4} \times (X - \bar{2}) \times X \\ &= \bar{2}X(X - \bar{2}) \\ &= \bar{2}X^2 + X \end{aligned}$$

Donc,

$$\begin{aligned} P &= X^2 + X + \bar{2}X + \bar{3}X + \bar{1} + \bar{4}X^2 + \bar{2} \\ &= \bar{2}X^2 + X + \bar{1} \end{aligned}$$

Vérification :

$$\begin{aligned} P(\bar{2}) &= \bar{3} + \bar{2} + \bar{1} = \bar{1} = y_1 \\ P(\bar{0}) &= \bar{1} = y_2 \\ P(\bar{-1}) &= \bar{2} - \bar{1} + \bar{1} = \bar{2} = y_3 \end{aligned}$$



CHAPITRE

19

APPLICATIONS LINÉAIRES

1 Premières propriétés

Définition: Soient E et F deux \mathbb{K} -espaces vectoriels et $f : E \rightarrow F$. On dit que f est linéaire si

$$\forall (x, y) \in E^2, \forall (\alpha, \beta) \in \mathbb{K}^2, f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$$

EXEMPLE: 1. $E = \mathcal{C}^0([a, b], \mathbb{C})$

$$\begin{aligned}\varphi : E &\longrightarrow \mathbb{C} \\ f &\longmapsto \int_a^b f(t) dt\end{aligned}$$

φ est linéaire

2. $E = \mathcal{D}(I, \mathbb{C})$ et $F = \mathbb{C}^I$

$$\begin{aligned}\varphi : E &\longrightarrow F \\ f &\longmapsto f'\end{aligned}$$

φ est linéaire

3. $f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & ax \end{array}$ est linéaire.

$$f(\alpha x + \beta y) = \alpha ax + \beta ay = \alpha f(x) + \beta f(y)$$

4. $E = \mathcal{C}^1(I, \mathbb{C})$ et $F = \mathcal{C}^0(I, \mathbb{C})$. $a \in F$

$$\varphi : \begin{array}{ccc} E & \longrightarrow & F \\ y & \longmapsto & y' + ay \end{array}$$

$$y' + a(x)y = b(x) \iff \varphi(y) = b$$

5. $E = \mathbb{C}^{\mathbb{N}} = F$

$$\varphi : \begin{array}{ccc} (u_n) & \longmapsto & (u_{n+2} - u_{n+1} - u_n) \end{array}$$

$$\forall n, u_{n+2} = u_{n+1} + u_n \iff \varphi(u) = 0$$

6. $E = \mathcal{M}_{p,1}(\mathbb{K})$, $F = \mathcal{M}_{n,1}(\mathbb{K})$, $A \in \mathcal{M}_{n,p}(\mathbb{K})$

$$\begin{aligned}\varphi : E &\longrightarrow F \\ X &\longmapsto AX\end{aligned}$$

$$AX = B \iff \varphi(X) = B$$

Définition: On dit qu'un problème est linéaire s'il se présente sous la forme :

$$\text{Résoudre } \varphi(x) = y$$

où l'inconnue est $x \in E$, y est un paramètre de F avec $\varphi : E \rightarrow F$ linéaire.

EXEMPLE:

Trouver toutes les fonctions $f : \mathbb{R} \rightarrow \mathbb{R}$ telles que

$$\forall x \in \mathbb{R}, f(x+1) - f(x-1) = \lambda$$

où $\lambda \in \mathbb{R}$ est fixé.

On pose $E = \mathbb{R}^{\mathbb{R}}$,

$$\begin{aligned}\varphi : E &\longrightarrow E \\ f &\longmapsto \varphi(f) : \begin{array}{ccc}\mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & f(x+1) - f(x-1)\end{array}\end{aligned}$$

et

$$\begin{aligned}y : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \lambda\end{aligned}$$

Le problème est équivalent à

$$\begin{cases} \varphi(f) = y \\ f \in E \end{cases}$$

Soient $f, g \in E$, $\lambda, \mu \in \mathbb{R}$.

$$\begin{aligned}\forall x \in \mathbb{R}, \varphi(\lambda f + \mu g)(x) &= (\lambda f + \mu g)(x+1) - (\lambda f + \mu g)(x-1) \\ &= \lambda f(x+1) - \mu g(x+1) - \lambda f(x-1) - \mu g(x-1) \\ &= \lambda(f(x+1) - f(x-1)) + \mu(g(x+1) - g(x-1)) \\ &= \lambda\varphi(f)(x) + \mu\varphi(g)(x)\end{aligned}$$

Donc, $\varphi(\lambda f + \mu g) = \lambda\varphi(f) + \mu\varphi(g)$

REMARQUE (Notation):

Soient E et F deux \mathbb{K} -espaces vectoriels.

L'ensemble des applications linéaires de E dans F est $\mathcal{L}(E, F)$.

Si $F = E$, alors on note plus simplement $\mathcal{L}(E)$ à la place de $\mathcal{L}(E, E)$.

Les éléments de $\mathcal{L}(E)$ sont appelés endomorphismes (linéaires) de E .

Proposition: Soit $f \in \mathcal{L}(E, F)$, $g \in \mathcal{L}(F, G)$. Alors $g \circ f \in \mathcal{L}(E, G)$.

Preuve:

Soient $u, v \in E$ et $\alpha, \beta \in \mathbb{K}$.

$$\begin{aligned} (g \circ f)(\alpha u + \beta v) &= g(f(\alpha u + \beta v)) \\ &= g(\alpha f(u) + \beta f(v)) \\ &= \alpha g(f(u)) + \beta g(f(v)) \\ &= \alpha(g \circ f)(u) + \beta(g \circ f)(v) \end{aligned}$$

□

Proposition: $\mathcal{L}(E, F)$ est un sous-espace vectoriel de F^E .

Preuve:

Soient $f, g \in \mathcal{L}(E, F)$ et $\lambda, \mu \in \mathbb{K}$. Montrons que $\lambda f + \mu g \in \mathcal{L}(E, F)$. Soient $u, v \in E$, $\alpha, \beta \in \mathbb{K}$.

$$\begin{aligned} (\lambda f + \mu g)(\alpha u + \beta v) &= \lambda f(\alpha u + \beta v) + \mu g(\alpha u + \beta v) \\ &= \lambda(\alpha f(u) + \beta f(v)) + \mu(\alpha g(u) + \beta g(v)) \\ &= \alpha(\lambda f(u) + \mu g(u)) + \beta(\lambda f(v) + \mu g(v)) \\ &= \alpha((\lambda f + \mu g)(u)) + \beta((\lambda f + \mu g)(v)) \end{aligned}$$

De plus, $\tilde{0} : \begin{matrix} E & \longrightarrow & F \\ x & \longmapsto & 0_F \end{matrix}$ est linéaire donc $\mathcal{L}(E, F) \neq \emptyset$.

□

Proposition: $(\mathcal{L}(E), +, \circ, \cdot)$ est une \mathbb{K} -algèbre (non commutative en général).

Preuve: — $(\mathcal{L}(E), +, \cdot)$ est un \mathbb{K} -espace vectoriel d'après la proposition précédente.

- $(\mathcal{L}(E), +)$ est un groupe abélien.
- “ \circ ” est associative et interne sur $\mathcal{L}(E)$.
- $\text{id}_E \in \mathcal{L}(E)$.
- Soient $f, g, h \in \mathcal{L}(E)$.

$$\begin{aligned} \forall x \in E, f \circ (g + h)(x) &= f((g + h)(x)) \\ &= f(g(x) + h(x)) \\ &= f(g(x)) + f(h(x)) \text{ car } f \text{ est linéaire} \\ &= (f \circ g + f \circ h)(x) \end{aligned}$$

Donc,

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

$$\begin{aligned} \forall x \in E, (g + h) \circ f(x) &= (g + h)(f(x)) \\ &= g(f(x)) + h(f(x)) \\ &= (g \circ f + h \circ f)(x) \end{aligned}$$

Donc,

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

Donc, $(\mathcal{L}(E), +, \circ)$ est un anneau

— Soit $\lambda \in \mathbb{K}$, $f, g \in \mathcal{L}(E)$.

$$\begin{aligned} \forall x \in E, \lambda \cdot (f \circ g)(x) &= \lambda f(g(x)) \\ (\lambda \cdot f) \circ g(x) &= \lambda f(g(x)) \end{aligned}$$

$$\begin{aligned} f \circ (\lambda \cdot g)(x) &= f(\lambda g(x)) \\ &= \lambda f(g(x)) \text{ car } f \in \mathcal{L}(E) \end{aligned}$$

□

Corollaire: Soit $P \in \mathbb{K}[X]$ et $u \in \mathcal{L}(E)$. On peut former $P(u) \in \mathcal{L}(X)$: on dit que $P(u)$ est un polynôme d'endomorphismes.

Proposition: Soit $f \in \mathcal{L}(E, F)$ bijective. Alors $f^{-1} \in \mathcal{L}(F, E)$.

Preuve:

Soit $u, v \in F$, $\alpha, \beta \in \mathbb{K}$.

$$\begin{aligned} f^{-1}(\alpha u + \beta v) &= \alpha f^{-1}(u) + \beta f^{-1}(v) \\ \iff \alpha u + \beta v &= f(\alpha f^{-1}(u) + \beta f^{-1}(v)) \\ \iff \alpha u + \beta v &= \alpha f(f^{-1}(u)) + \beta f(f^{-1}(v)) \\ \iff \alpha u + \beta v &= \alpha u + \beta v \end{aligned}$$

Donc, $f^{-1} \in \mathcal{L}(F, E)$

□

REMARQUE (Notation):

On note $\mathrm{GL}(E)$ l'ensemble des endomorphismes de E bijectifs, $\mathrm{GL}(E, F)$ l'ensemble des applications linéaires de E dans F bijectives.

Les éléments de $\mathrm{GL}(E)$ sont appelés automorphismes (linéaires) de E .

Corollaire: $\mathrm{GL}(E)$ est un sous-groupe de $(S(E), \circ)$

Définition: $\mathrm{GL}(E)$ est dit “ le groupe linéaire de E ”.

2 Noyau et image

Proposition: Soit $f \in \mathcal{L}(E, F)$, U un sous-espace vectoriel de E et V un sous-espace vectoriel de F .

1. $f(U)$ est un sous-espace vectoriel de F .
2. $f^{-1}(V)$ est un sous-espace vectoriel de E .

Preuve: 1. $0_F = f(0_E)$ et $0_E \in U$ donc $0_F \in f(U)$ donc $f(U) \neq \emptyset$

Soient $(x, y) \in f(U)^2$, $(\lambda, \mu) \in \mathbb{K}^2$. Soient $a, b \in U$ tels que $\begin{cases} x = f(a) \\ y = f(b) \end{cases}$.

$$\lambda x + \mu y = \lambda f(a) + \mu f(b) = f(\lambda a + \mu b) \text{ car } f \in \mathcal{L}(E, F)$$

U est un sous-espace vectoriel de E .

Donc $\lambda a + \mu b \in U$

donc $f(\lambda a + \mu b) \in f(U)$

donc $\lambda x + \mu y \in f(U)$.

2. $f(0_E) = 0_F \in V$ donc $0_E \in f^{-1}(V)$. Donc $f^{-1}(V) \neq \emptyset$.
Soient $x, y \in f^{-1}(V)$, $\lambda, \mu \in \mathbb{K}$.

$$f(\lambda x + \mu y) = \lambda \underbrace{f(x)}_{\in V} + \mu \underbrace{f(y)}_{\in V} \in V$$

donc $\lambda x + \mu y \in f^{-1}(V)$.

□

Corollaire: Soit $f \in \mathcal{L}(E, F)$.

1. $\text{Ker}(f) = f^{-1}(\{0_F\}) = \{x \in E \mid f(x) = 0_E\}$ est un sous-espace vectoriel de E .
2. $\text{Im}(f) = f(E) = \{f(u) \mid u \in E\}$ est un sous-espace vectoriel de F .

□

REMARQUE (Rappel):

Soit $f \in \mathcal{L}(E, F)$

$$f \text{ injective} \iff \text{Ker}(f) = \{0_E\}$$

$$f \text{ surjective} \iff \text{Im}(f) = F$$

EXEMPLE: 1. Soit I un intervalle, $E = \mathcal{D}(I, \mathbb{R})$ et $F = \mathbb{R}^I$

$$\begin{aligned} \varphi : E &\longrightarrow F \\ f &\longmapsto f' \end{aligned}$$

$$\text{Ker}(\varphi) = \{f : I \rightarrow \mathbb{R} \mid f \text{ constante}\}$$

$$\text{Im}(\varphi) \supset \mathcal{C}^0(I, \mathbb{R})$$

$$\begin{array}{ccc} E & \longrightarrow & F \\ P & \longmapsto & \int_0^1 P(t) dt \end{array}$$

$$\begin{aligned} \text{Ker}(\varphi) &= \left\{ P = a + bX + cX^2 \mid (a, b, c) \in \mathbb{R}^3 \text{ et } \int_0^1 P(t) dt = 0 \right\} \\ &= \left\{ a + bX + cX^2 \mid a + \frac{b}{2} + \frac{c}{3} = 0 \right\} \\ &= \left\{ a + bX + cX^2 \mid a = -\frac{b}{2} - \frac{c}{3} \right\} \\ &= \left\{ -\frac{b}{2} - \frac{c}{3} + bX + cX^2 \mid b, c \in \mathbb{R} \right\} \\ &= \left\{ b \left(-\frac{1}{2} + X \right) + c \left(-\frac{1}{3} + X^2 \right) \mid b, c \in \mathbb{R} \right\} \\ &= \text{Vect} \left(-\frac{1}{2} + X, -\frac{1}{3} + X^2 \right) \end{aligned}$$

$$\text{Im}(\varphi) = \mathbb{R}.$$

3 Théorème du rang

Dans ce paragraphe, E est un \mathbb{K} -espace vectoriel de dimension finie.

Proposition: Soit $f : E \rightarrow F$ un isomorphisme (i.e. une application linéaire bijective). Alors, $\dim(E) = \dim(F)$

Preuve:

Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E . On pose

$$\forall i \in \llbracket 1, n \rrbracket, u_i = f(e_i) \in F$$

— Soit $(\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n$. On suppose que $\sum_{i=0}^n \lambda_i u_i = 0_F$. D'où,

$$\begin{aligned} & \sum_{i=1}^n \lambda_i f(e_i) \text{ donc } f\left(\sum_{i=1}^n \lambda_i e_i\right) = 0_F \\ & \text{donc } \sum_{i=1}^n \lambda_i e_i \in \text{Ker}(f) = \{0_E\} \\ & \text{donc } \sum_{i=1}^n \lambda_i e_i = 0_E \\ & \text{donc } \forall i \in \llbracket 1, n \rrbracket, \lambda_i = 0 \end{aligned}$$

Donc (u_1, \dots, u_n) est libre.

Soit $y \in F$. Comme f est surjective, il existe $x \in E$ tel que $f(x) = y$. Comme \mathcal{B} engendre E , il existe $\lambda_1, \dots, \lambda_n \in \mathbb{K}^n$ tel que $x = \sum_{i=1}^n \lambda_i e_i$. Comme f est linéaire,

$$y = f(x) = \sum_{i=1}^n \lambda_i f(e_i) = \sum_{i=1}^n \lambda_i u_i$$

Donc, $F = \text{Vect}(u_1, \dots, u_n)$

Donc (u_1, \dots, u_n) est une base de F donc

$$\dim(E) = n = \dim(F)$$

□

La première partie de la preuve précédente justifie le résultat suivant.

Proposition: Soit $f \in \mathcal{L}(E, F)$ injective. $\mathcal{L} = (e_1, \dots, e_p)$ une famille libre de E . Alors $(f(e_1), \dots, f(e_p))$ est une famille libre de F . En particulier, $\dim(F) \geq \dim(E)$.

□

La deuxième partie de la preuve prouve :

Proposition: Soit $f \in \mathcal{L}(E, F)$ surjective et $\mathcal{G} = (e_1, \dots, e_p)$ une famille génératrice

de E . Alors $(f(e_1), \dots, f(e_p))$ est une famille génératrice de F . En particulier,

$$\dim(F) \leq \dim(E)$$

□

Théorème (Théorème du rang): Soit $f \in \mathcal{L}(E, F)$.

$$\dim(E) = \dim(\text{Ker}(f)) + \dim(\text{Im}(f))$$

Preuve (À connaître):

On pose

$$\begin{aligned} u : U &\longrightarrow \text{Im}(f) \\ x &\longmapsto f(x) \end{aligned}$$

où U est un supplémentaire de $\text{Ker}(f)$ dans E .

(U existe : voir remarque qui suit)

— $u \in \mathcal{L}(U, \text{Im}(f))$, en effet, soient $x, y \in U, \lambda, \mu \in \mathbb{K}$

$$\begin{aligned} u(\lambda x + \mu y) &= f(\lambda x + \mu y) \\ &= \lambda f(x) + \mu f(y) \\ &= \lambda u(x) + \mu u(y) \end{aligned}$$

— Soit $y \in \text{Im}(f)$. Soit $x \in E$ tel que $y = f(x)$. Comme $E = U \oplus \text{Ker}(f)$. On peut écrire

$$\begin{cases} x = a + b \\ a \in U, b \in \text{Ker}(f) \end{cases}$$

D'où,

$$y = f(x) = f(a + b) = f(a) + f(b) = u(a) + 0_E = u(a)$$

Donc u est surjective.

Soit $x \in U$.

$$\begin{aligned} x \in \text{Ker}(u) &\iff u(x) = 0_F \\ &\iff f(x) = 0_F \\ &\iff x \in \text{Ker}(f) \\ &\iff x = 0_E \text{ car } U \cap \text{Ker}(f) = \{0_E\} \end{aligned}$$

Donc u est injective.

Ainsi, $\dim(U) = \dim(\text{Im}(f))$

Or,

$$\begin{aligned} \dim(E) &= \dim(U \oplus \text{Ker}(f)) \\ &= \dim(U) + \dim(\text{Ker}(f)) \end{aligned}$$

donc

$$\dim(U) = \dim(E) - \dim(\text{Ker}(f))$$

Donc,

$$\dim(E) = \dim(\text{Ker}(f)) + \dim(\text{Im}(f))$$

□

REMARQUE:

Soit E un \mathbb{K} -espace vectoriel de dimension finie, et F un sous-espace vectoriel de E .

Cas1 $F = \{0_E\}$, alors E est un supplémentaire de F .

Cas2 $F \neq \{0_E\}$. Soit $\mathcal{B} = (e_1, \dots, e_p)$ une base de F . Alors \mathcal{B} est une famille libre de E . On complète \mathcal{B} en une base $(e_1, \dots, e_p, e_{p+1}, \dots, e_n)$ de E . On pose $G = \text{Vect}(e_{p+1}, \dots, e_n)$. On démontre que

$$F \oplus G = E$$

Corollaire: Soient E et F deux \mathbb{K} -espaces vectoriels de même dimension finie et $f \in \mathcal{L}(E, F)$.

$$\begin{aligned} f \text{ injective} &\iff f \text{ surjective} \\ &\iff f \text{ bijective} \end{aligned}$$

Preuve:

D'après le théorème du rang,

$$\dim(E) = \dim(\text{Ker}(f)) + \dim(\text{Im}(f))$$

Si f est injective, alors $\text{Ker}(f) = \{0_E\}$
et donc $\dim(\text{Ker}(f)) = 0$

et donc $\dim(\text{Im}(f)) = \dim(F)$
et donc $\text{Im}(f) = F$
et donc f est surjective.

Si f est surjective, alors $\text{Im}(f) = F$
et donc $\dim(\text{Im}(f)) = \dim(F) = \dim(E)$
et donc $\dim(\text{Ker}(f)) = 0$
et donc $\text{Ker}(f) = \{0\}$
et donc f est injective

□

EXEMPLE:

Soit $(x_1, \dots, x_n) \in \mathbb{K}^n$ tel que

$$\forall i \neq j, x_i \neq x_j$$

Soit $(y_1, \dots, y_n) \in \mathbb{K}^n$. On pose $\varphi : \begin{array}{ccc} \mathbb{K}_{n-1}[X] & \longrightarrow & \mathbb{K}^n \\ P & \longmapsto & (P(x_1), \dots, P(x_n)) \end{array}$

$$\begin{aligned} P \in \text{Ker}(\varphi) &\iff \varphi(P) = 0 \\ &\iff \forall i \in \llbracket 1, n \rrbracket, P(x_i) = 0 \\ &\iff P = 0 \text{ car } \deg(P) \leq n-1 \end{aligned}$$

Donc φ est injective et donc φ est bijective.

Donc,

$$\exists! P \in \mathbb{K}_{n-1}[X], \forall i \in \llbracket 1, n \rrbracket, P(x_i) = y_i$$

De plus, $\varphi^{-1} : \mathbb{K}^n \rightarrow \mathbb{K}_{n-1}[X]$ est un isomorphisme.

Soit (e_1, \dots, e_n) la base canonique de \mathbb{K}^n . $(\varphi^{-1}(e_1), \dots, \varphi^{-1}(e_n))$ est une base de $\mathbb{K}_{n-1}[X]$.
 $\forall i \in \llbracket 1, n \rrbracket, \varphi^{-1}(e_i) = L_i$ est le i -ème polynôme interpolateur de Lagrange.

$$\begin{aligned}
P &= \varphi^{-1}(y_1, \dots, y_n) \\
&= \varphi^{-1}\left(\sum_{i=1}^n y_i e_i\right) \\
&= \sum_{i=1}^n y_i \varphi^{-1}(e_i) \\
&= \sum_{i=1}^n y_i L_i
\end{aligned}$$

EXERCICE (Interpolation de Hermite):

Soit $(x_1, \dots, x_n) \in \mathbb{K}^n$ avec

$$\forall i \neq j, x_i \neq x_j$$

Soit $(y_1, \dots, y_n) \in \mathbb{K}^n$ et $(z_1, \dots, z_n) \in \mathbb{K}^n$.

Trouver un polynôme de plus bas degré tel que

$$(*) \quad \forall i \in \llbracket 1, n \rrbracket, \begin{cases} P(x_i) = y_i \\ P'(x_i) = z_i \end{cases}$$

$$\begin{array}{rcl}
\text{Soit } \varphi : & \mathbb{K}_{2n-1}[X] & \longrightarrow \mathbb{K}^{2n} \\
& P & \mapsto (P(x_1), \dots, P(x_n), P'(x_1), \dots, P'(x_n))
\end{array}$$

$$(*) \iff \varphi(P) = (y_1, \dots, y_n, z_1, \dots, z_n)$$

$$\begin{aligned}
P \in \text{Ker}(\varphi) &\iff \forall i, \begin{cases} P(x_i) = 0 \\ P'(x_i) = 0 \end{cases} \\
&\iff P = 0 \text{ car } \deg(P) \leq 2n - 1
\end{aligned}$$

Donc φ est un isomorphisme.

Corollaire: Soit $f \in \mathcal{L}(E)$ avec E de dimension finie. Alors,

$$f \in \text{GL}(E) \iff f \text{ injective} \iff f \text{ surjective}$$

□

REMARQUE:

Soit $f \in \mathcal{L}(E, F)$, $\mathcal{B} = (e_1, \dots, e_n)$ une base de E . Alors

$$\boxed{\text{Im}(f) = \text{Vect}(f(e_1), \dots, f(e_n))}$$

$$\dim(\text{Im}(f)) = \text{rg}(f(e_1), \dots, f(e_n))$$

Définition: Soit $f \in \mathcal{L}(E, F)$. Le rang de f est

$$\text{rg}(f) = \dim(\text{Im}(f))$$

4 Formes linéaires

Définition: Soit E un \mathbb{K} -espace vectoriel. Une forme linéaire sur E est une application linéaire de E dans \mathbb{K} . L'ensemble des formes linéaires est noté $E^* = \mathcal{L}(E, \mathbb{K})$. E^* est appelé espace dual de E .

Proposition: Toute forme linéaire est soit nulle, soit surjective.

Preuve:

Soit $f \in E^*$.

$\text{Im}(f)$ est un sous-espace vectoriel de \mathbb{K} donc $\text{rg}(f) \leq \dim(\mathbb{K}) = 1$.

Si $\text{rg}(f) = 0$, alors $\text{Im}(f) = \{0\}$ et donc

$$\forall x \in E, f(x) = 0$$

Si $\text{rg}(f) = 1$, alors $\text{Im}(f) = \mathbb{K}$ et donc f est surjective. \square

Proposition: Soit E un \mathbb{K} -espace vectoriel de dimension finie n et $f \in E^* \setminus \{0\}$. Alors $\text{Ker}(f)$ est de dimension $n - 1$.

Preuve:

Comme $f \neq 0$, donc $\text{rg}(f) = 1$

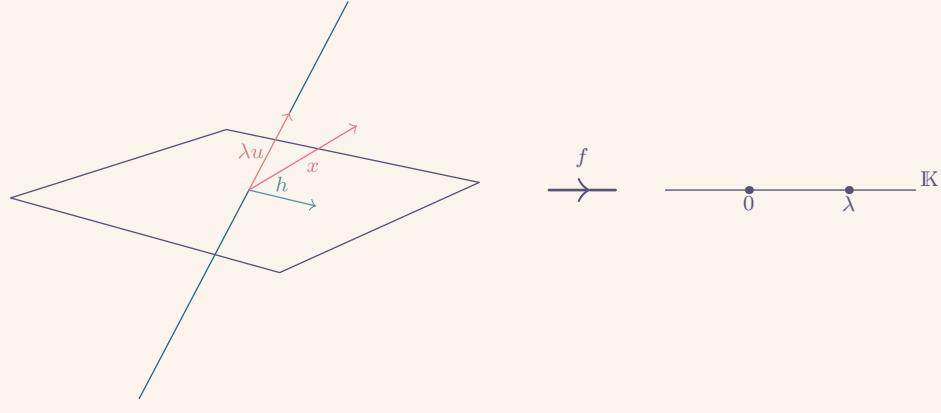
D'après le théorème du rang,

$$\dim(\text{Ker}(f)) = \dim(E) - \text{rg}(f) = n - 1$$

\square

Proposition: Soit E un \mathbb{K} -espace vectoriel de dimension finie n et H un sous-espace vectoriel de E de dimension $n - 1$. Alors,

$$\exists f \in E^*, \text{Ker}(f) = H$$



Preuve:

Soit D un supplémentaire de H dans E :

$$E = H \oplus D$$

Nécessairement,

$$\dim(D) = \dim(E) - \dim(H) = 1$$

Soit $u \in D \setminus \{0\}$. $D = \text{Vect}(u)$

$$E \longrightarrow \mathbb{K}$$

On pose $f : \begin{cases} x = h + \lambda u \\ (h \in H, \lambda \in \mathbb{K}) \end{cases} \mapsto \lambda$

Montrons que $f \in E^*$.

Soient $(x, y) \in E^2$, $(\alpha, \beta) \in \mathbb{K}^2$.

On pose

$$\begin{cases} x = h + \lambda u, & h \in H, \lambda \in \mathbb{K} \\ y = h' + \lambda' u, & h' \in H, \lambda' \in \mathbb{K} \end{cases}$$

D'où,

$$\begin{aligned} \alpha x + \beta y &= \alpha(h + \lambda u) + \beta(h' + \lambda' u) \\ &= \underbrace{(\alpha h + \beta h')}_{\in H} + \underbrace{(\alpha \lambda + \beta \lambda') u}_{\in \mathbb{K}} \end{aligned}$$

Donc,

$$\begin{aligned} f(\alpha x + \beta y) &= \alpha \lambda + \beta \lambda' \\ &= \alpha f(x) + \beta f(y) \end{aligned}$$

Soit $x \in E$. On pose $x = h + \lambda u$ avec $h \in H$ et $\lambda \in \mathbb{K}$

$$\begin{aligned} x \in \text{Ker}(f) &\iff f(x) = 0 \\ &\iff \lambda = 0 \\ &\iff x = y \\ &\iff x \in H \end{aligned}$$

Donc, $H = \text{Ker}(f)$.

□

EXEMPLE:

$E = \mathbb{R}^4$, $H = \text{Vect}((1, 0, 0, 1), (1, 1, 0, 0), (0, 1, 1, 0))$

Soit $u = (1, 2, 1, 1) \notin H$.

Soit $(x, y, z, t) \in E$. On cherche $(\alpha, \beta, \gamma, \lambda) \in \mathbb{R}^4$ tels que

$$(*) \quad (x, y, z, t) = \alpha(1, 0, 0, 1) + \beta(1, 1, 0, 0) + \gamma(0, 1, 1, 0) + \lambda(1, 2, 1, 1)$$

Plus précisément, on cherche à exprimer λ en fonction de x, y, z, t .

$$\begin{aligned}
 (*) &\iff \begin{cases} \alpha + \beta + \gamma = x \\ \beta + \gamma + 2\lambda = y \\ \gamma + \lambda = z \\ \alpha + \lambda = t \end{cases} \\
 &\iff \begin{cases} [\alpha] + \beta + \lambda = x \\ \beta + \gamma + 2\lambda = y \\ [\gamma] + \lambda = z \\ -\beta = t - x \end{cases} \\
 &\iff \begin{cases} [\alpha] + \beta + \lambda = x \\ \beta + \lambda = y - z \\ [\gamma] + \lambda = z \\ \beta = x - t \end{cases} \\
 &\iff \begin{cases} \lambda = y - z - x + t \\ \vdots \end{cases}
 \end{aligned}$$

Donc,

$$(x, y, z, t) \in H \iff y - z - x + t = 0$$

$$\text{Soit } f : \begin{matrix} \mathbb{R}^4 \\ (x, y, z, t) \end{matrix} \longrightarrow \begin{matrix} \mathbb{R} \\ x - y + z - t \end{matrix} \text{ et } H = \text{Ker}(f)$$

Proposition: Avec les notations précédentes, $\{f \in E^* \mid \text{Ker}(f) = H\}$ est une droite de E^* privée de l'application nulle. En d'autres termes, les équations de H sont 2 à 2 proportionnelles.

Preuve:

Soient $f, g \in E^*$ telles que

$$\text{Ker}(f) = \text{Ker}(g)$$

On pose $H = \text{Ker}(f)$. Soit $u \notin H$ de sorte que

$$H \oplus \text{Vect}(u) = E$$

$u \notin H$ donc $f(u) \neq 0$.

On pose $\alpha = \frac{g(u)}{f(u)}$. Montrons que $g = \alpha f$.

Soit $x \in E$. On pose $x = h + \lambda u$ avec $\begin{cases} h \in H \\ \lambda \in \mathbb{K} \end{cases}$

$$g(x) = g(h) + \lambda g(u) = 0 + \lambda \alpha f(u)$$

$$\begin{aligned}
 &\parallel \\
 \alpha f(x) &= \alpha(f(h) + \lambda f(u)) = \lambda \alpha f(u)
 \end{aligned}$$

□

Définition: Soit E un \mathbb{K} -espace vectoriel et H un sous-espace vectoriel de E . On dit

que H est un hyperplan de E s'il existe une droite D de E telle que

$$H \oplus D = E$$

En reprenant les démonstrations précédentes, on a encore les résultats suivants :

Proposition: Soit H un hyperplan de E . Alors, $\{f \in E^* \mid \text{Ker}(f) = H\}$ est une droite de E^* privée de l'application nulle. \square

Proposition: Soit $f \in E^*$ non nulle. Alors $\text{Ker}(f)$ est un hyperplan de E .

Preuve:

f non nulle. Soit $x \in E$ tel que

$$f(x) \neq 0$$

On pose $H = \text{Ker}(f)$ et $D = \text{Vect}(x)$. Montrons que $H \oplus D = E$.

ANALYSE Soit $y \in E$. On suppose $y = h + \lambda x$ avec $h \in H$ et $\lambda \in \mathbb{K}$. Alors,

$$f(y) = f(h) + \lambda f(x) = \lambda f(x) \text{ donc } \begin{cases} \lambda = f(y)f(x)^{-1} \\ h = y - f(y)f(x)^{-1}x \end{cases}$$

SYNTHÈSE Soit $y \in E$. On pose $\begin{cases} \lambda = f(y)f(x)^{-1} \\ h = y - f(y)f(x)^{-1}x \end{cases}$.

$$\text{Évidemment, } \begin{cases} h + \lambda x = y \\ \lambda \in \mathbb{K} \end{cases}$$

$$\begin{aligned} f(h) &= f(y - \lambda x) \\ &= f(y) - \lambda f(x) \\ &= f(y) - f(y)f(x)^{-1}f(x) \\ &= 0 \end{aligned}$$

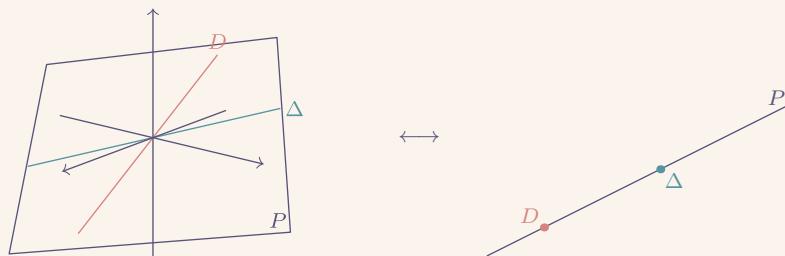
\square

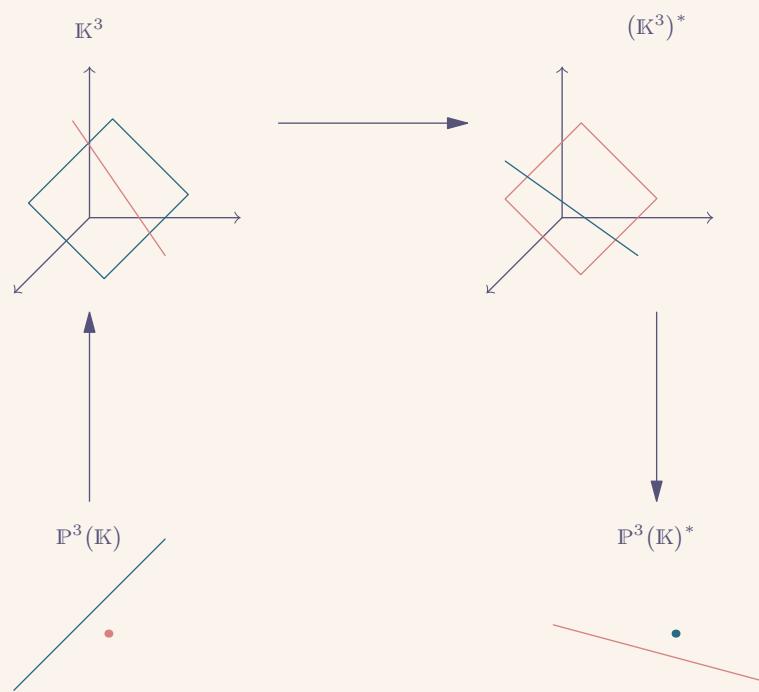
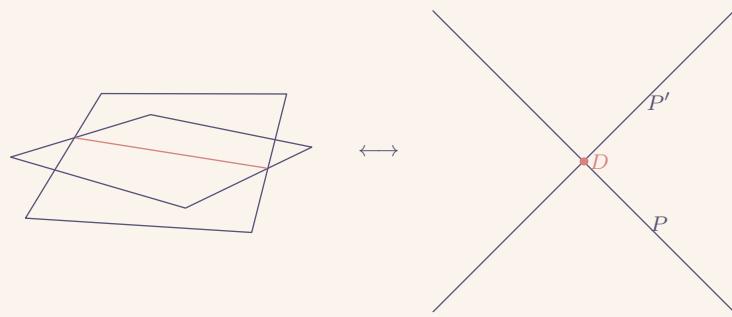
HORS-PROGRAMME

$$\mathbb{P}^3(\mathbb{K}) = \{D \setminus \{0\} \mid D \text{ droite vectorielle de } \mathbb{K}^3\}$$

Une droite projective de $\mathbb{P}^3(\mathbb{K})$ est un plan vectoriel de \mathbb{K}^3 privé de 0.

À faire : schéma A





À faire : schémas B et C

$$\begin{array}{ccc}
 & & h(D) \\
 \hline
 h(N) & \bullet & h(M) \\
 & & \bullet \\
 & & h(O) \longrightarrow \\
 \hline
 & & h(\Delta)
 \end{array}$$

5 Projections et symétries

Définition: Soit E un \mathbb{K} -espace vectoriel, F et G deux sous-espaces de E supplémentaires :

$$E = F \oplus G$$

Soit $x \in E$.

$$\exists! (a, b) \in F \times G, x = a + b$$

Le vecteur a est appelé projeté de x sur F parallèlement à G .

Le vecteur b est appelé projeté de x sur G parallèlement à F .

La projection sur F parallèlement à G est l'application qui à $x \in E$ associe son projeté sur F parallèlement à G .

EXEMPLE:

$E = \mathbb{R}^{\mathbb{R}}$, $F = \{f \in E \mid f$ paire $\}$ et $G = \{f \in E \mid f$ impaire $\}$

On a $E = F \oplus G$.

Soient p la projection sur F parallèlement à G et q la projection sur G parallèlement à F .

$$\forall x \in E, \begin{cases} p(f) : x \mapsto \frac{1}{2}(f(x) + f(-x)) \\ q(f) : x \mapsto \frac{1}{2}(f(x) - f(-x)) \end{cases}$$

Proposition: Soient F et G deux sous-espaces vectoriels de E supplémentaires et p la projection sur F parallèlement à G .

1. $p \in \mathcal{L}(E)$
2. $p|_F = \text{id}_F$ et $p|_G = 0$
3. $p \circ p = p$
4. $\text{id}_E - p$ est la projection sur G parallèlement à F .

Preuve: 1. $\forall x \in E, p(x) \in F \subset E$

Soit $(x, y) \in E^2$, $(\lambda, \mu) \in \mathbb{K}^2$.

On pose $x = a + b$ avec $\begin{cases} a \in F \\ b \in G \end{cases}$ et $y = c + d$ avec $\begin{cases} c \in F \\ d \in G \end{cases}$
donc,

$$\begin{aligned}
 \lambda x + \mu y &= \lambda(a + b) + \mu(c + d) \\
 &= \underbrace{(\lambda a + \mu c)}_{\in F} + \underbrace{(\lambda b + \mu d)}_{\in G}
 \end{aligned}$$

Donc,

$$p(\lambda x + \mu y) = \lambda a + \mu b = \lambda p(x) + \mu p(y)$$

2. $\forall x \in F, x = \underbrace{x}_{\in F} + \underbrace{0}_{\in G}$ donc $p(x) = x$
- $\forall x \in G, x = \underbrace{0}_{\in F} + \underbrace{x}_{\in G}$ donc $p(x) = 0$

3. $\forall x \in E, p(x) \in F$ donc $p(p(x)) = p(x)$
4. Soit $x \in E$. On pose $x = a + b$ avec $\begin{cases} a \in F \\ b \in G \end{cases}$. Donc $p(x) = a$. D'où, $x - p(x) = b$ est le projeté de x sur G parallèlement à F .

□

Définition: Soit $f \in \mathcal{L}(E)$. On dit que f est un projecteur si $f \circ f = f$

Proposition: Soit f un projecteur de E . Alors f est la projection sur $\text{Im}(f)$ parallèlement à $\text{Ker}(f)$. En particulier,

$$\text{Im}(f) \oplus \text{Ker}(f) = E$$

Preuve: ANALYSE Soit $x \in E$. On suppose que $x = a + b$ avec $\begin{cases} a \in \text{Ker}(f) \\ b \in \text{Im}(f) \end{cases}$. D'où,

$$\begin{aligned} f(x) &= f(a) + f(b) \\ &= 0 + f(b) \\ &= f(b) \end{aligned}$$

Soit $y \in E$ tel que $b = f(y)$. Donc,

$$f(b) = f(f(y)) = f(y) = b$$

Donc, $f(x) = b$ et donc $a = x - b = x - f(x)$

SYNTHÈSE Soit $x \in E$. On pose $\begin{cases} a = x - f(x) \\ b = f(x) \end{cases}$. Évidemment, $\begin{cases} a + b = x \\ b \in \text{Im}(f) \end{cases}$

$$\begin{aligned} f(a) &= f(x - f(x)) \\ &= f(x) - f(f(x)) \\ &= f(x) - f(x) \\ &= 0 \end{aligned}$$

Donc $a \in \text{Ker}(f)$. On a montré

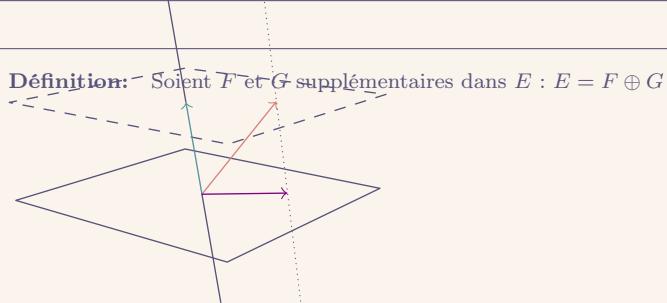
$$\text{Im}(f) \oplus \text{Ker}(f) = E$$

On considère la projection p sur $\text{Im}(f)$ parallèlement à $\text{Ker}(f)$. Soit $x \in E$. On a montré que

$$x = \underbrace{f(x)}_{\in \text{Im}(f)} + \underbrace{x - f(x)}_{\in \text{Ker}(f)}$$

donc $p(x) = f(x)$ et donc $p = f$

□



Soit $x \in E$. On décompose x :

$$x = a + b \text{ avec } \begin{cases} a \in F \\ b \in G \end{cases}$$

et on forme

$$y = a - b$$

On dit que y est le symétrique de x par rapport à F parallèlement à G

La symétrie par rapport à F parallèlement à G est l'application qui à tout $x \in E$ associe son symétrique parallèlement à G par rapport à F .

Proposition: Soient F et G supplémentaires dans E , δ la symétrie par rapport à F parallèlement à G .

1. $\delta \in \mathcal{L}(E)$
2. $\delta|_F = \text{id}_F$ et $\delta|_G = -\text{id}_G$
3. $\delta \circ \delta = \text{id}_E$

Preuve:

Soient p la projection sur F parallèlement à G et q la projection sur G parallèlement à F .

On remarque que $\delta = p - q$.

1. p et q sont des endomorphismes donc δ aussi
2. $\forall x \in E, \delta(x) = p(x) - q(x) = x - 0 = x$
 $\forall x \in G, \delta(x) = p(x) - q(x) = 0 - x = -x$
- 3.

$$\begin{aligned} \forall x \in E, \delta(\delta(x)) &= \delta(p(x) - q(x)) \\ &= \delta(\underbrace{p(x)}_{\in F} - \underbrace{q(x)}_{\in G}) \\ &= p(x) - (-q(x)) \\ &= x \end{aligned}$$

□

Définition: Soit $f \in \mathcal{L}(E)$. On dit que f est involutif si $f \circ f = \text{id}_E$.

Proposition: Soit $f \in \mathcal{L}(E)$ involutif. Alors f est la symétrie par rapport à $\text{Ker}(f -$

$\|$ id_E) parallèlement à Ker($f + \text{id}_E$). En particulier,

$$\text{Ker}(f - \text{id}_E) \oplus \text{Ker}(f + \text{id}_E) = E$$

Preuve: ANALYSE Soit $x \in E$. On suppose que $x = a + b$ avec $\begin{cases} a \in \text{Ker}(f - \text{id}_E) \\ b \in \text{Ker}(f + \text{id}_E) \end{cases}$

$$\begin{aligned} a \in \text{Ker}(f - \text{id}_E) &\iff (f - \text{id}_E)(a) = 0 \\ &\iff f(a) - a = 0 \\ &\iff a = f(a) \end{aligned}$$

$$\begin{aligned} b \in \text{Ker}(f + \text{id}_E) &\iff (f + \text{id}_E)(b) = 0 \\ &\iff f(b) + b = 0 \\ &\iff f(b) = -b \end{aligned}$$

On sait que $x = a + b$ et $f(x) = f(a) + f(b) = a - b$
D'où,

$$\begin{aligned} a &= \frac{1}{2}(x + f(x)) \\ b &= \frac{1}{2}(x - f(x)) \end{aligned}$$

SYNTHÈSE Soit $x \in E$. On pose

$$\begin{aligned} a &= \frac{1}{2}(x + f(x)) \\ b &= \frac{1}{2}(x - f(x)) \end{aligned}$$

Alors $a + b = x$

$$\begin{aligned} f(a) &= f\left(\frac{1}{2}(x + f(x))\right) \\ &= \frac{1}{2}(f(x) + f(f(x))) \\ &= \frac{1}{2}(f(x) + x) \\ &= a \end{aligned}$$

Donc $a \in \text{Ker}(f - \text{id}_E)$

$$\begin{aligned} f(b) &= f\left(\frac{1}{2}(x - f(x))\right) \\ &= \frac{1}{2}(f(x) - f(f(x))) \\ &= \frac{1}{2}(f(x) - x) \\ &= -b \end{aligned}$$

donc $b \in \text{Ker}(f + \text{id}_E)$
Ainsi,

$$\text{Ker}(f - \text{id}_E) \oplus \text{Ker}(f + \text{id}_E) = E$$

Soit s la symétrie par rapport à $\text{Ker}(f - \text{id}_E)$ parallèlement à $\text{Ker}(f + \text{id}_E)$.
Soit $x \in E$. On a vu que

$$x = \underbrace{\frac{1}{2}(x + f(x))}_{\in \text{Ker}(f - \text{id}_E)} + \underbrace{\frac{1}{2}(x - f(x))}_{\in \text{Ker}(f + \text{id}_E)}$$

Donc,

$$s(x) = \frac{1}{2}(x + f(x)) - \frac{1}{2}(x - f(x)) = f(x)$$

Donc $s = f$

□

EXEMPLE:
 $E = \mathbb{R}^n$ et

$$\begin{aligned} s : E &\longrightarrow E \\ f &\longmapsto s(f) : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & f(-x) \end{array} \end{aligned}$$

$s(f) = f \circ (-\text{id}_{\mathbb{R}})$
 $s \in \mathcal{L}(E)$, en effet :

$$\begin{aligned} \forall f, g \in \mathcal{L}(E), \forall \alpha, \beta \in \mathbb{R}, \\ s(\alpha f + \beta g) &= (\alpha f + \beta g) \circ (-\text{id}_{\mathbb{R}}) \\ &= \alpha(f \circ (-\text{id}_{\mathbb{R}})) + \beta(g \circ (-\text{id}_{\mathbb{R}})) \\ &= \alpha s(f) + \beta s(g) \end{aligned}$$

De plus, $s \circ s = \text{id}_E$. Donc s est une symétrie.

$$\begin{aligned} \text{Ker}(s - \text{id}_E) &= \{f \in E \mid f \text{ paire}\} = \mathcal{P} \\ \text{Ker}(s + \text{id}_E) &= \{f \in E \mid f \text{ impaire}\} = \mathcal{I} \end{aligned}$$

D'où,

$$\mathcal{P} \oplus \mathcal{I} = E$$

EXEMPLE:

$E = \mathcal{M}_n(\mathbb{K})$

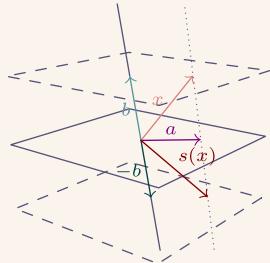
Pour $A \in E$, on note ${}^t A$ la transposée de A la matrice obtenue en écrivant en ligne les colonnes de A .

Soit

$$\begin{aligned} s : \mathcal{M}_n(\mathbb{K}) &\longrightarrow \mathcal{M}_n(\mathbb{K}) \\ A &\longmapsto {}^t A \end{aligned}$$

s est linéaire, $s \circ s = \text{id}_{\mathcal{M}_n(\mathbb{K})}$

$$\begin{aligned} \text{Ker}(s - \text{id}_E) &= S_n(\mathbb{K}) \\ \text{Ker}(s + \text{id}_E) &= A_n(\mathbb{K}) \end{aligned}$$



CHAPITRE

20

FRACTIONS RATIONNELLES

1 Construction de $\mathbb{K}(X)$

Proposition – Définition: On définit la relation \sim sur $\mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$ par

$$(P, Q) \sim (A, B) \iff PB = QA$$

Cette relation est une relation d'équivalence. On note $(\mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\}))/\sim$. Les éléments de $\mathbb{K}(X)$ sont appelés fractions rationnelles.

On note $\frac{P}{Q}$ la classe d'équivalence du couple (P, Q) .

Preuve:

On note $E = \mathbb{K}[X](\mathbb{K}[X] \setminus \{0\})$.

- Soit $(P, Q) \in E$. $PQ = QP$ car \times est commutative dans $\mathbb{K}[X]$. Donc $(P, Q) \sim (P, Q)$
- Soient $(P, Q) \in E$, $(A, B) \in E$. On suppose que $(P, Q) \sim (A, B)$. Donc $PB = QA$
Donc, $(A, B) \sim (P, Q)$
- Soit $((P, Q), (A, B), (C, D)) \in E^3$. On suppose

$$\begin{cases} (P, Q) \sim (A, B) \\ (A, B) \sim (C, D) \end{cases}$$

D'où,

$$\begin{cases} PB = QA \\ AD = BC \end{cases}$$

Donc

$$PBD = QAD = QBC$$

$$\text{donc } B(PD - QC) = 0$$

Comme $B \neq 0$ et comme $\mathbb{K}[X]$ est intègre,

$$PD - QC = 0$$

et donc $(P, Q) \sim (C, D)$

□

Proposition: Soient $(P, Q) \in \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$ et $R \in \mathbb{K}[X] \setminus \{0\}$. Alors

$$\frac{PR}{QR} = \frac{P}{Q}$$

Preuve:

$$\begin{aligned} \frac{PR}{QR} = \frac{P}{Q} &\iff (PQ, QR) \sim (P, Q) \\ &\iff PRQ = QRP \end{aligned}$$

□

Définition: Soit $(P, Q) \in \mathbb{K}[X] \setminus (\mathbb{K}[X] \setminus \{0\})$. On dit que la fraction $\frac{P}{Q}$ est sous forme irréductible si $P \wedge Q = 1$.

Proposition – Définition: Soient $(P, Q) \sim (A, B)$. Alors

$$\deg(P) - \deg(Q) = \deg(A) - \deg(B)$$

Le degré de $\frac{P}{Q}$ est $\deg(P) - \deg(Q)$. On note ce “nombre” $\deg\left(\frac{P}{Q}\right)$.

Preuve:

On sait que $PB = QA$ donc

$$\deg(P) + \deg(Q) = \deg(Q) + \deg(A)$$

et donc

$$\deg(P) - \deg(Q) = \deg(A) - \deg(B)$$

□

Proposition – Définition: Soient $(P, Q) \sim (A, B)$ et $(R, S) \sim (C, D)$. Alors, $(PR, QS) \sim (AC, BD)$.

Le produit de $\frac{P}{Q}$ avec $\frac{R}{S}$ est $\frac{PR}{QS}$

Preuve:

On sait que $\begin{cases} PB = QA \\ RD = SC \end{cases}$. D'où,

$$PBRD = QASC$$

et donc

$$(PR)(BD) = (QS)(AC)$$

donc

$$(PR, QS) \sim (AC, BD)$$

□

Proposition – Définition: Avec les notations précédentes,

$$(PS + RQ, QS) \sim (AD + BC, BD)$$

On définit la somme de $\frac{P}{Q}$ et $\frac{R}{S}$ par

$$\frac{P}{Q} + \frac{R}{S} = \frac{PS + RQ}{QS}$$

Preuve:

On sait que $\begin{cases} PB = QA \\ RD = SC \end{cases}$. Donc,

$$\begin{aligned} (PS + RQ)BD &= PSBD + RQBD \\ &= QASD + SCQB \\ &= QS(AD + BC) \end{aligned}$$

□

Théorème: $(\mathbb{K}(X), +, \times)$ est un corps.

Preuve (partielle): 1. “+” est associative : soient $\left(\frac{P}{Q}, \frac{R}{S}, \frac{A}{B}\right) \in \mathbb{K}(X)^3$.

$$\frac{P}{Q} + \left(\frac{R}{S} + \frac{A}{B}\right) = \frac{P}{Q} + \frac{RB + AS}{SB} = \frac{PSB + QRB + QAS}{QSB}$$

$$\left(\frac{P}{Q} + \frac{R}{S}\right) + \frac{A}{B} = \frac{PS + RQ}{QS} + \frac{A}{B} \stackrel{\parallel}{=} \frac{PSB + RQB + AQS}{QSB}$$

2. “+” est commutative

3. $\frac{0}{1}$ est neutre pour “+”

$$\frac{P}{Q} + \frac{0}{1} = \frac{P \times 1 + 0 \times Q}{Q \times 1} = \frac{P}{Q}$$

4. Soit $\frac{P}{Q} \in \mathbb{K}(X)$.

$$\frac{P}{Q} + \frac{-P}{Q} = \frac{PQ - QP}{Q^2} = \frac{0}{Q^2} = \frac{0}{1}$$

5. “ \times ” est associative

6. “ \times ” est commutative

7. $\frac{1}{1}$ est le neutre pour “ \times ”

8. Soient $\left(\frac{P}{Q}, \frac{R}{S}, \frac{A}{B}\right) \in \mathbb{K}(X)^3$

$$\frac{P}{Q} \left(\frac{R}{S} + \frac{A}{B} \right) = \frac{P}{Q} \times \frac{RB + AS}{SB} = \frac{PRB + PAS}{QSB}$$

et

$$\begin{aligned} \frac{P}{Q} \times \frac{R}{S} + \frac{P}{Q} \times \frac{A}{B} &= \frac{PR}{QS} + \frac{PA}{QB} \\ &= \frac{PRQB + QSPA}{Q^2 SB} \\ &= \frac{PRB + SPA}{QSB} \end{aligned}$$

9. Soit $\frac{P}{Q} \neq \frac{0}{1}$ donc $P \times 1 \neq Q \times 0$ donc $P \neq 0$.

$$\frac{P}{Q} \times \frac{Q}{P} = \frac{PQ}{PQ} = \frac{1}{1}$$

10. $\frac{1}{1} \neq \frac{0}{1}$ car $1 \times 1 \neq 0 \times 1$

□

Proposition:

$$\forall P, A \in \mathbb{K}[X], \forall Q \in \mathbb{K}[X] \setminus \{0\}, \quad \frac{P}{Q} + \frac{A}{Q} = \frac{P+A}{Q}$$

Proposition: $i : \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}(X) \\ P & \longmapsto & \frac{P}{1} \end{array}$ est un morphisme d'anneaux injectif.

Preuve:

Soient $P, Q \in \mathbb{K}[X]$.

$$i(P+Q) = \frac{P+Q}{1} = \frac{P}{1} + \frac{Q}{1} = i(P) + i(Q)$$

$$i(PQ) = \frac{PQ}{1} = \frac{PQ}{1 \times 1} = \frac{P}{1} \times \frac{Q}{1} = i(P) \times i(Q)$$

$$i(1) = \frac{1}{1}$$

Donc i est un morphisme d'anneaux.

$$\begin{aligned} P \in \text{Ker}(i) &\iff i(P) = \frac{0}{1} \\ &\iff \frac{P}{1} = \frac{0}{1} \\ &\iff P \times 1 = 0 \times 1 \\ &\iff P = 0 \end{aligned}$$

donc i est injective. \square

Définition: Soient $\lambda \in \mathbb{K}$ et $F = \frac{P}{Q} \in \mathbb{K}(X)$. On pose

$$\lambda F = \frac{\lambda P}{Q} = \frac{\lambda}{1} \times \frac{P}{Q}$$

Proposition: $(\mathbb{K}(X), +, \cdot)$ est un \mathbb{K} -espace vectoriel et $i : \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}(X) \\ P & \longmapsto & \frac{P}{1} \end{array}$ est linéaire. \square

REMARQUE:

On peut identifier $P \in \mathbb{K}[X]$ avec $\frac{P}{1} \in \mathbb{K}(X)$ i.e. écrire $P = \frac{P}{1}$ et alors $\begin{cases} \mathbb{K}[X] \text{ est un sous-anneau de } \mathbb{K}(X) \\ \mathbb{K}[X] \text{ est un sous-espace vectoriel de } \mathbb{K}(X) \end{cases}$ De plus, les deux définitions de degré coïncident.

Proposition: Soit $F, G \in \mathbb{K}(X)$.

1. $\deg(F + G) \leq \max(\deg F, \deg G)$
Si $\deg(F) \neq \deg(G)$ alors $\deg(F + G) = \max(\deg F, \deg G)$;
2. $\deg(FG) = \deg(F) + \deg(G)$;
3. Si $F \neq 0$, $\deg\left(\frac{1}{F}\right) = -\deg(F)$.

Preuve:

On pose $F = \frac{A}{B}$ et $G = \frac{P}{Q}$.

1. $F + G = \frac{AQ + PB}{BQ}$. On suppose que $\deg(F) \geq \deg(G)$ i.e. $\deg A - \deg B \geq \deg P - \deg Q$.

$$\deg(F + G) = \deg(QA + PB) - \deg(BQ)$$

On a

$$\deg(AQ) = \deg(A) + \deg(Q) \geq \deg(P) + \deg(B) = \deg(PB).$$

D'où

$$\deg(F + G) \leq \deg(AQ) - \deg(BQ) = \deg\left(\frac{AQ}{BQ}\right) = \deg(F).$$

Si $\deg(F) > \deg(G)$, alors $\deg(AQ) > \deg(BQ)$ et donc

$$\deg(F + G) = \deg(AQ) - \deg(BQ) = \deg(F).$$

2.

$$\begin{aligned}\deg(FG) &= \deg\left(\frac{AP}{BQ}\right) \\ &= \deg(AP) - \deg(BQ) \\ &= \deg(A) + \deg(P) - \deg(B) - \deg(Q) \\ &= \deg F + \deg G.\end{aligned}$$

$$3. \deg\left(\frac{1}{F}\right) = \deg(1) - \deg(F) = -\deg(F)$$

□

Définition

2 Décomposition en éléments simples

Lemme:

$$\forall F \in \mathbb{K}(X), \exists !(E, G) \in \mathbb{K}[X] \times \mathbb{K}(X), \begin{cases} F = E + G \\ \deg(G) < 0 \end{cases}$$

On dit que E est la partie entière de F .

Preuve:

On pose $F = \frac{P}{Q}$ avec $P \in \mathbb{K}[X], Q \in \mathbb{K}[X] \setminus \{0\}$.

ANALYSE Soit $E \in \mathbb{K}[X]$ et $G \in \mathbb{K}(X)$ tels que

$$F = E + G \quad \deg(G) < 0.$$

On pose $G = \frac{A}{Q}$ avec $A \in \mathbb{K}[X]$.

$$\begin{aligned}F = E + G &\iff \frac{P}{Q} = E + \frac{A}{Q} \\ &\iff P = EQ + A.\end{aligned}$$

$\deg G < 0, \deg A < \deg Q$.

Donc E est le quotient de la division euclidienne de P par Q et A est le reste.

SYNTHÈSE Soient E le quotient et A le reste de la division euclidienne de P par Q .

On a alors

$$\begin{cases} P = EQ + A \\ \deg(A) < \deg(Q) \end{cases}$$

et donc

$$F = E + \frac{A}{Q} \quad \deg\left(\frac{A}{Q}\right) < 0.$$

□

EXEMPLE:

$$F = \frac{X^3 + X - 1}{X^2 + 2}, \deg F = 1.$$

$$\begin{array}{r}
 X^3 + X - 1 \\
 - X^3 + 2X \\
 \hline
 -X - 1
 \end{array} \left| \begin{array}{c} X^2 + 2 \\ X \\ \hline \end{array} \right.$$

Donc,

$$F = \frac{X(X^2 + 2) - (X + 1)}{X^2 + 2} = X - \frac{X + 1}{X^2 + 2}.$$

Lemme: Soit $F = \frac{P}{AB}$ avec

$$\begin{cases} (P, A, B) \in \mathbb{K}[X]^3; \\ A \neq 0; B \neq 0; \\ A \wedge B = 1; \deg F < 0. \end{cases}$$

Alors,

$$\exists! (U, V) \in \mathbb{K}[X]^2, \begin{cases} F = \frac{U}{A} + \frac{V}{B} \\ \deg\left(\frac{U}{A}\right) < 0 \text{ et } \deg\left(\frac{V}{B}\right) \end{cases}.$$

Preuve: ANALYSE On suppose que

$$\begin{cases} F = \frac{U}{A} + \frac{V}{B} \\ U \in \mathbb{K}[X], \deg U < \deg A \\ V \in \mathbb{K}[X], \deg V < \deg B. \end{cases}$$

D'où

$$\frac{P}{AB} = \frac{UB + VA}{AB}$$

et donc $P = UB + VA$. D'après le théorème de Bézout, il existe $(R, S) \in \mathbb{K}[X]^2$ tel que

$$RB + SA = P.$$

On a alors

$$0 = B(R - U) + A(S - V)$$

donc

$$A(S - V) = B(U - R)$$

donc

$$A \mid B(U - R) \quad \text{dans } \mathbb{K}[X].$$

D'après le théorème de Gauß,

$$A \mid U - R$$

Donc $U - R = AT$ avec $T \in \mathbb{K}[X]$ donc

$$A(S - V) = BAT$$

donc

$$S - V = BT$$

donc

$$\begin{cases} R = -AT + U \\ S = BT + V \end{cases}.$$

On a

$$\begin{cases} S = BT + V \\ \deg V < \deg B \end{cases}$$

donc V est le reste de la division euclidienne de S par B et U est le reste de la division euclidienne de R par A .

SYNTHESE Soit $(R, S) \in \mathbb{K}[X]^2$ tel que

$$P = RB + SA.$$

Soit V le reste de la division euclidienne de S par B .

$$\begin{cases} S = BT + V, T \in \mathbb{K}[X] \\ \deg V < \deg B \end{cases}$$

D'où,

$$\frac{P}{AB} = \frac{R}{A} + T + \frac{V}{B} = \frac{R + AT}{A} + \frac{V}{B}$$

et

$$\deg\left(\frac{V}{B}\right) = \deg(V) - \deg(B) < 0.$$

Si $\deg\left(\frac{R + AT}{A}\right) \geq 0$, alors

$$\deg\left(\frac{R + AT}{A}\right) > \deg\left(\frac{V}{B}\right)$$

et alors

$$\deg\left(\frac{P}{AB}\right) = \deg\left(\frac{R + AT}{A}\right) \geq 0.$$

Or,

$$\deg\left(\frac{P}{AB}\right) < 0.$$

Donc

$$\deg\left(\frac{R + AT}{A}\right) < 0.$$

On pose $U = R + AT$. On a bien

$$\frac{P}{AB} = \frac{U}{A} + \frac{V}{B} \text{ avec } \deg\left(\frac{U}{V}\right) < 0 \text{ et } \deg\left(\frac{V}{R}\right) < 0.$$

□

Lemme: Soit $H \in \mathbb{K}[X]$ irréductible, $n \in \mathbb{N}_*$, $P \in \mathbb{K}[X]$, $F = \frac{P}{H^n}$ et $\deg F < 0$. Alors,

$$\begin{cases} \exists!(U, V) \in \mathbb{K}[X]^2, F = \frac{U}{H^n} + \frac{V}{H^{n+1}}; \\ \deg U < \deg H; \\ \deg\left(\frac{V}{H^{n+1}}\right) < 0. \end{cases}$$

Preuve: ANALYSE $F = \frac{U}{H^n} + \frac{V}{H^{n-1}}$ avec

$$\begin{cases} \deg U < \deg H, \\ U \in \mathbb{K}[X], V \in \mathbb{K}[X], \\ \deg\left(\frac{V}{H^{n-1}}\right) < 0. \end{cases}$$

D'où

$$P = U + VH, \deg U < \deg H.$$

Donc V est le quotient et U le reste de la division euclidienne de P par H .

SYNTHESE Soient V et U le quotient et le reste de la division euclidienne de P par H :

$$\begin{cases} P = U + VH \\ \deg U < \deg H. \end{cases}$$

D'où

$$F = \frac{U}{H^n} + \frac{V}{H^{n-1}}$$

$$\deg U < \deg H$$

Si $\deg\left(\frac{V}{H^{n-1}}\right) \geq 0$, alors $\deg F = \deg\left(\frac{V}{H^{n-1}}\right) \geq 0$: une contradiction. Donc
 $\deg\left(\frac{V}{H^{n-1}}\right) < 0$.

□

Théorème (Théorème de décomposition en éléments simples sur $\mathbb{C}(X)$): Soit $F \in \mathbb{K}(X)$, $F = \frac{P}{Q}$ la forme irréductible de F . On note (z_1, \dots, z_p) les racines complexes de Q et (μ_1, \dots, μ_p) leur multiplicité.

Alors,

$$\exists!(E, a_{1,1}, \dots, a_{1,\mu_1}, a_{2,1}, \dots, a_{2,\mu_2}, \dots, a_{p,1}, \dots, a_{p,\mu_p}) \in \mathbb{C}[X] \times \mathbb{C}^{\deg Q},$$

$$F = E + \sum_{i=1}^p \left(\sum_{j=1}^{\mu_i} \frac{a_{i,j}}{(X - z_i)^j} \right).$$

EXEMPLE:
 $F = \frac{X^7 - 1}{X^5 + 2X^3 + X} \in \mathbb{C}(X)$

$$\begin{array}{r} X^7 - 1 \\ - X^7 + 2X^5 + X^3 \\ \hline -2X^5 - X^3 - 1 \\ - 2X^5 - 4X^3 - 2X \\ \hline 3X^3 + 2X - 1 \end{array} \left| \begin{array}{r} X^5 + 2X^3 + X \\ \hline X^2 - 2 \end{array} \right.$$

$$F = (X^2 - 2) + \frac{3X^3 + 2X - 1}{X^5 + 2X^3 + X}$$

$$\begin{aligned} X^5 + 2X^3 + X &= X(X^4 + 2X^2 + 1) \\ &= X(X^2 + 1)^2 \\ &= X(X - i)^2(X + i)^2 \end{aligned}$$

D'après le 2^{ème} lemme,

$$\frac{3X^3 + 2X - 1}{X^5 + 2X^3 + X} = \frac{a}{X} + \frac{bX + c}{(X - i)^2}$$

D'après le 3^{ème} lemme,

$$\begin{aligned} \frac{bX + c}{(X - i)^2} &= \frac{f}{(X - i)^2} + \frac{g}{X - i} \\ \frac{dX + e}{(X + i)^2} &= \frac{h}{(X + i)^2} + \frac{h}{X + i} \\ F = (X^2 - 2) + \frac{a}{X} + \frac{f}{(X - i)^2} + \frac{g}{X - i} + \frac{h}{(X - i)^2} + \frac{k}{X + i}. \end{aligned}$$

On multiplie par X :

$$\frac{X^7 - 1}{X^4 + 2X^2 + 1} = a + X \left(X^2 - 2 + \frac{f}{(X - i)^2} + \frac{g}{X - i} + \frac{h}{(X - i)^2} + \frac{k}{X + 1} \right).$$

En remplaçant X par 0, on obtient

$$a = \frac{-1}{1} = -1.$$

On multiplie par $(X - i)^2$ et on remplace X par i :

$$\frac{3i^2 + 2i - 1}{i(2i)^2} = f.$$

Donc,

$$f = \frac{-i - 1}{-4i} = \frac{1}{4} - \frac{i}{4}$$

De même,

$$h = \frac{3(-i)^3 + 2(-i) - 1}{-i(-2i)^2} = \bar{f} = \frac{1}{4} + \frac{i}{4}$$

$$\frac{3X^2 + 2X - 1}{X^5 + 2X^3} + \frac{1}{X} - \left(\frac{1}{4} - \frac{i}{4}\right) \frac{1}{(X-i)^2} - \left(\frac{1}{4} + \frac{i}{4}\right) \frac{1}{(X+i)^2} = \frac{g}{X-i} + \frac{h}{X+i}$$

$$\begin{aligned} \frac{g}{X-i} + \frac{h}{X+i} &= \frac{3X^3 + 2X - 1 + X^4 + 2X^2 + 1 + X(X+i)^2(-\frac{1}{4} + \frac{i}{4}) - X(X-i)^2(\frac{1}{4} - \frac{i}{4})}{X^5 + 2X^3 + X} \\ &= \frac{12X^3 + 8X - 4 + 4X^4 + 8X^2 + 4 + X^3(-1+i) + (1-i)X - X^3(1+i) - 2X^2(1-i) + X(1+i)}{4(X^5 + 2X^3 + X)} \\ &= \frac{4X^4 + 10X^3 + 8X^2 + 10X}{4(X^5 + 2X^3 + X)} \\ &= \frac{2X^3 + 5X^2 + 2X + 5}{2(X^4 + 2X^2 + 1)} \\ &= \frac{(X-i)(X+i)(2X+5)}{2(X-i)^2(X+i)^2} \\ &= \frac{2X+5}{2(X-i)(X+i)} \end{aligned}$$

Donc,

$$\begin{cases} g = \frac{2i+5}{2 \times 2i} = \frac{(2i+5)i}{-4} = \frac{2-5i}{4} \\ h = \frac{2(-i)+5}{2(-2i)} = \frac{2+5i}{4} \end{cases}$$

Preuve:

On suppose $\frac{P}{Q} \notin \mathbb{C}[X]$. On peut supposer Q unitaire.

EXISTENCE D'après le lemme 1, il existe $E \in \mathbb{C}[X]$, $G \in \mathbb{C}(X)$ tels que

$$\begin{cases} \frac{P}{Q} = E + G \\ \deg(G) < 0 \end{cases}$$

Soit $\frac{A}{B}$ la forme irréductible de G avec B unitaire ($A \wedge B = 1$ et $A \neq 0$).

$$\frac{P}{Q} = E + \frac{A}{B}$$

donc

$$PB = EBQ + AQ \quad (*)$$

donc

$$AQ = PB - EBQ$$

donc

$$A \mid B(P - EQ)$$

D'après le théorème de Gauß,

$$A \mid P - EQ$$

Soit $R \in \mathbb{C}[X]$ tel que

$$AR = P - EQ$$

D'où

$$\frac{AR}{Q} = \frac{P}{Q} - E = \frac{A}{B}$$

D'où

$$\frac{R}{Q} = \frac{1}{B}$$

donc $B \mid Q$.

De (*), on a aussi

$$P \mid Q(EB + A)$$

Or, $P \wedge Q = 1$. Donc

$$P \mid EB + A$$

Soit $S \in \mathbb{C}[X]$ tel que

$$PS = EB + A$$

Donc

$$\frac{PS}{B} = E + \frac{A}{B} = \frac{P}{Q}$$

Donc

$$\frac{S}{B} = \frac{1}{Q}$$

et donc $Q \mid B$

Donc $Q = B$ (car ils sont unitaires).

Donc $G = \frac{A}{Q}$.

Or,

$$Q = \prod_{j=1}^p (X - z_j)^{\mu_j}$$

$$\forall j \neq k, (X - z_j)^{\mu_j} \wedge (X - z_k)^{\mu_k} = 1$$

D'après le lemme 2, il existe $(A_1, \dots, A_p) \in \mathbb{C}[X]^p$ tel que

$$\begin{cases} \frac{A}{Q} = \sum_{j=1}^p \frac{A_j}{(X - z_j)^{\mu_j}} \\ \forall j \in \llbracket 1, p \rrbracket, \deg(A_j) < \mu_j \end{cases}$$

Soit $j \in \llbracket 1, p \rrbracket$. D'après le lemme 3,

$$\frac{A_j}{(X - z_j)^{\mu_j}} = \frac{a_{j,\mu_j}}{(X - z_j)^{\mu_j}} + \frac{A_{j,1}}{(X - z_j)^{\mu_j-1}}$$

avec

$$\begin{cases} a_{j,\mu_j} \in \mathbb{C} \\ A_{j,1} \in \mathbb{C}_{\mu_j-2}[X] \end{cases}$$

En itérant ce procédé, on trouve $(a_{j,\mu_j}, \dots, a_{j,1}) \in \mathbb{C}^{\mu_j}$ tel que

$$\frac{A_j}{(X - z_j)^{\mu_j}} = \sum_{k=1}^{\mu_j} \frac{a_{j,k}}{(X - z_j)^k}$$

D'où

$$\frac{P}{Q} = E + \underbrace{\sum_{j=1}^p \sum_{k=1}^{\mu_j} \frac{a_{j,k}}{(X - z_j)^k}}_{\deg(\quad) < 0}$$

UNICITÉ Soit $E_1 \in \mathbb{C}[X]$ et $(b_{j,k})_{\substack{1 \leq j \leq p \\ 1 \leq k \leq \mu_j}} \in \mathbb{C}^{\sum_{j=1}^p \mu_j}$ tels que

$$\frac{P}{Q} = E_1 + \underbrace{\sum_{j=1}^p \sum_{k=1}^{\mu_j} \frac{b_{j,k}}{(X - z_j)^k}}_{\deg(\quad) < 0}$$

D'après le lemme 1,

$$E = E_1 \text{ et } \sum_{j=1}^p \sum_{k=1}^{\mu_j} \frac{a_{j,k}}{(X - z_j)^k} = \sum_{j=1}^p \sum_{k=1}^{\mu_j} \frac{b_{j,k}}{(X - z_j)^k}$$

$$\forall j \in \llbracket 1, p \rrbracket,$$

$$\sum_{k=0}^{\mu_j} \frac{b_{j,k}}{(X - z_j)^k} = \frac{\sum_{k=1}^{\mu_j} b_{j,k} (X - z_j)^{\mu_j - k}}{(X - z_j)^{\mu_j}}$$

||

$$\sum_{k=1}^{\mu_j} \frac{a_{j,k}}{(X - z_j)^k} = \frac{\sum_{k=1}^{\mu_j} a_{j,k} (X - z_j)^{\mu_j - k}}{(X - z_j)^{\mu_j}}$$

Donc,

$$\sum_{k=1}^{\mu_j} a_{j,k} (X - z_j)^k = \sum_{k=1}^{\mu_j} b_{j,k} (X - z_j)^k$$

Comme $(X - z_j, (X - z_j)^2, \dots, (X - z_j)^{\mu_j})$ est libre dans $\mathbb{C}[X]$,

$$\forall k \in \llbracket 1, \mu_j \rrbracket, b_{j,k} = a_{j,k}$$

□

Théorème (Théorème de décomposition en éléments simples sur $\mathbb{R}(X)$): Soit $(P, Q) \in \mathbb{R}[X]^2$, $P \wedge Q = 1$, Q unitaire, $Q \notin \{0, 1\}$. On pose

$$Q = \prod_{i=1}^p (X - a_i)^{\mu_i} \prod_{k=1}^q (X^2 + \alpha_k X + \beta_k)^{\nu_k}$$

avec

$$\begin{cases} p \in \mathbb{N}, q \in \mathbb{N}, \\ (a_1, \dots, a_p) \in \mathbb{R}^p \\ (\alpha_1, \dots, \alpha_q, \beta_1, \dots, \beta_q) \in \mathbb{R}^{2q} \\ (\mu_1, \dots, \mu_p, \nu_1, \dots, \nu_p) \in \mathbb{N}^{p+q} \\ \forall j \in \llbracket 1, q \rrbracket, \alpha_j^2 - 4\beta_j < 0 \end{cases}$$

Alors

$$\begin{aligned} \exists! (E, \gamma_{1,1}, \dots, \gamma_{1,\mu_1}, \gamma_{2,1}, \dots, \gamma_{2,\mu_2}, \dots, \gamma_{p,1}, \dots, \gamma_{p,\mu_p}, \\ \delta_{1,1}, \dots, \delta_{1,\nu_1}, \delta_{2,1}, \dots, \delta_{2,\nu_2}, \dots, \delta_{q,1}, \dots, \delta_{q,\nu_q}, \\ \varepsilon_{1,1}, \dots, \varepsilon_{1,\nu_1}, \varepsilon_{2,1}, \dots, \varepsilon_{2,\nu_2}, \dots, \varepsilon_{q,1}, \dots, \varepsilon_{q,\nu_q}) \\ \in \mathbb{R}[X] \times \mathbb{R}^{\mu_1 + \dots + \mu_p} \times \mathbb{R}^{2(\nu_1 + \dots + \nu_q)} \end{aligned}$$

$$\begin{aligned} \frac{P}{Q} = E + \sum_{i=1}^p \sum_{j=1}^{\mu_i} \frac{\gamma_{i,j}}{(X - a_i)^j} \\ + \sum_{k=1}^q \sum_{j=1}^{\nu_k} \frac{\delta_{k,j} X + \varepsilon_{k,j}}{(X^2 + \alpha_k X + \beta_k)^j} \end{aligned}$$

□

Définition: Soit $F \in \mathbb{C}(X)$. Soient $(P, Q) \in \mathbb{C}[X]^2$ tels que $\begin{cases} P \wedge Q = 1 \\ F = \frac{P}{Q} \end{cases}$.

Les racines de P sont appelées zéros de F

Les racines de Q sont appelées pôles de F

Proposition: Soit $F \in \mathbb{C}(X)$ et $z \in \mathbb{C}$ un pôle simple de F . Le coefficient devant $\frac{1}{X - z}$ dans la décomposition en éléments simples de F est $\frac{P(z)}{Q'(z)}$.

Preuve:

Soit $(P, Q) \in \mathbb{C}[X]^2$ tels que

$$\begin{cases} F = \frac{P}{Q} \\ P \wedge Q = 1 \\ Q \text{ unitaire} \end{cases}$$

On pose

$$Q = (X - z) \prod_{i=1}^q (X - z_i)^{\mu_i}$$

où z_1, \dots, z_q sont les racines distinctes de z du polynôme Q . Donc,

$$\frac{P}{Q} = F = \frac{a}{X - z} + \sum_{i=1}^q \sum_{k=1}^{\mu_i} \frac{b_{i,k}}{(X - z_i)^k}$$

avec $a, (b_{i,k})_{\substack{1 \leq i \leq q \\ 1 \leq k \leq \mu_i}}$ des nombres complexes.

On multiplie par $X - z$.

$$\frac{P}{\prod_{i=1}^q (X - z_i)^{\mu_i}} = a + (X - z) \sum_{i=1}^q \sum_{k=1}^{\mu_i} \frac{b_{i,k}}{(X - z_i)^k}$$

On remplace X par z .

$$\frac{P(z)}{\prod_{i=1}^q (z - z_i)^{\mu_i}} = a$$

Or,

$$Q = (X - z) \prod_{i=1}^q (X - z_i)^{\mu_i}$$

D'où

$$Q' = \prod_{i=1}^q (X - z_i)^{\mu_i} + (X - z) \left(\prod_{i=1}^q (X - z_i)^{\mu_i} \right)'$$

Don

$$Q'(z) = \prod_{i=1}^q (z - z_i)^{\mu_i}$$

Donc

$$a = \frac{P(z)}{Q'(z)}$$

□

Proposition: Soit $P \in \mathbb{C}[X]$ avec $\deg(P) \geq 1$, (z_1, \dots, z_p) les racines de P , μ_1, \dots, μ_p leur multiplicité. Alors

$$\frac{P'}{P} = \sum_{i=1}^p \frac{\mu_i}{X - z_i}$$

Preuve:

On pose

$$P = \alpha \prod_{i=1}^p (X - z_i)^{\mu_i}$$

Donc

$$P' = \alpha \sum_{i=1}^p \left(\prod_{j \neq i} (X - z_j)^{\mu_j} \right) \mu_i (X - z_i)^{\mu_i - 1}$$

D'où

$$\begin{aligned}\frac{P'}{P} &= \frac{\not{\alpha} \sum_{i=1}^p \mu_i (X - z_i)^{\mu_i - 1} \prod_{j \neq i} (X - z_j)^{\mu_j}}{\not{\alpha} \prod_{i=1}^p (X - z_i)^{\mu_i}} \\ &= \sum_{i=1}^p \mu_i \frac{(X - z_i)^{\mu_i - 1} \prod_{j \neq i} (X - z_j)^{\mu_j}}{\prod_{j=1}^p (X - z_j)^{\mu_j}} \\ &= \sum_{i=1}^p \mu_i \frac{1}{X - z_i}\end{aligned}$$

□

REMARQUE:

Il existe un "truc" pour retenir cette formule :

$$\frac{P'}{P} = \underbrace{\ln(P)'}_{\text{n'existe pas!}} = \left(\ln \left(\alpha \prod_{i=1}^p (X - z_i)^{\mu_i} \right) \right)' = \left(\sum_{i=1}^p \mu_i \ln(X - z_i) \right)' = \sum_{i=1}^p \mu_i \frac{1}{X - z_i}$$

CHAPITRE

21

MATRICES ET APPLICATIONS LINÉAIRES

1 Matrices d'un vecteur

Soit E un \mathbb{K} -espace vectoriel de dimension finie n . Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E .

Définition: Soit $x \in E$. On sait qu'il existe un unique n -uplet $(x_1, \dots, x_n) \in \mathbb{K}^n$ tel que

$$x = \sum_{i=1}^n x_i e_i$$

La matrice de x dans la base \mathcal{B} est la colonne

$$\text{Mat}_{\mathcal{B}}(x) = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

REMARQUE:

En général, si \mathcal{B} et \mathcal{B}' sont 2 bases différentes, alors $\text{Mat}_{\mathcal{B}}(x) \neq \text{Mat}_{\mathcal{B}'}(x)$.

EXEMPLE:

$E = \mathbb{R}_3[X]$, $\mathbb{K} = \mathbb{R}$, $\mathcal{B} = (1, X, X^2, X^3)$ et

$$\begin{aligned} \mathcal{C} &= \left(\frac{X(X-1)(X-2)}{6}, -\frac{X(X-1)(X-3)}{2}, \right. \\ &\quad \left. \frac{X(X-2)(X-3)}{2}, -\frac{(X-1)(X-2)(X-3)}{6} \right) \end{aligned}$$

$$P = X^2 - X + 1$$

$$\text{Mat}_{\mathcal{B}}(P) = \begin{pmatrix} 1 \\ -1 \\ 1 \\ 0 \end{pmatrix}$$

$$P = P(3) \frac{X(X-1)(X-2)}{6} + P(2) \frac{-X(X-1)(X-3)}{2} \\ + P(1) \frac{X(X-2)(X-3)}{2} + P(0) \frac{-(X-1)(X-2)(X-3)}{6}$$

$$\text{Mat}_{\mathcal{B}'}(P) = \begin{pmatrix} 7 \\ 3 \\ 1 \\ 1 \end{pmatrix}$$

2 Matrice d'une famille de vecteurs

Soient E est un \mathbb{K} -espace vectoriel de dimension finie n , $\mathcal{B} = (e_1, \dots, e_n)$ une base de E , $\mathcal{F} = (u_1, \dots, u_p)$ une famille de vecteurs de E .

Définition: La matrice de \mathcal{F} dans la base \mathcal{B} est la matrice M telle que, pour tout $j \in \llbracket 1, p \rrbracket$, la j -ème colonne de M est $\text{Mat}_{\mathcal{B}}(u_j)$.

EXEMPLE:

$$\text{Mat}_{\mathcal{C}}(\mathcal{B}) = \begin{pmatrix} 1 & 3 & 9 & 27 \\ 1 & 2 & 4 & 8 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Proposition: Soit \mathcal{F} une famille de vecteurs de E .

$$\text{rg}(\mathcal{F}) = \text{rg}(\text{Mat}_{\mathcal{B}}(\mathcal{F}))$$

Preuve:

Dans ce chapitre, on définit le rang d'une matrices comme le nombre maximale de colonnes linéairement indépendantes. \square

Corollaire: Soit $\mathcal{F} = (u_1, \dots, u_p) \in E^p$ et $\mathcal{B} = (e_1, \dots, e_n)$ une base de E , et $M = \text{Mat}_{\mathcal{B}}(\mathcal{F})$.

1. \mathcal{F} est libre $\iff \text{rg}(M) = p$
2. $E = \text{Vect}(\mathcal{F}) \iff \text{rg}(M) = n$
3. \mathcal{F} base de $E \iff n = p = \text{rg}(M) \iff M \in \text{GL}_n(\mathbb{K})$

Dans ce cas,

$$(\text{Mat}_{\mathcal{B}}(\mathcal{F}))^{-1} = \text{Mat}_{\mathcal{F}}(\mathcal{B})$$

EXEMPLE:

$$\text{Mat}_{\mathcal{C}}(\mathcal{B}) = \begin{pmatrix} 1 & 3 & 9 & 27 \\ 1 & 2 & 4 & 8 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} = M$$

On sait que \mathcal{B} est une base donc $M \in \text{GL}_4(\mathbb{R})$. Donc,

$$M^{-1} = \text{Mat}_{\mathcal{B}}(\mathcal{C}) = \begin{pmatrix} 0 & 0 & 0 & \frac{1}{6} \\ \frac{1}{3} & -\frac{3}{2} & 3 & -\frac{11}{6} \\ -\frac{1}{2} & 2 & -\frac{5}{2} & 1 \\ \frac{1}{6} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{6} \end{pmatrix}$$

Preuve:

1.

$$\begin{aligned} \mathcal{F} \text{ est libre} &\iff (u_1, \dots, u_p) \text{ base de } \text{Vect}(u_1, \dots, u_p) \\ &\iff \dim(\text{Vect}(u_1, \dots, u_p)) = p \\ &\iff \text{rg}((u_1, \dots, u_p)) = p \\ &\iff \text{rg}(M) = p \end{aligned}$$

2.

$$\begin{aligned} \mathcal{F} \text{ engendre } E &\iff E = \text{Vect}(u_1, \dots, u_p) \\ &\iff \dim(E) = \dim(\text{Vect}(u_1, \dots, u_p)) \\ &\iff n = \text{rg}(M) \end{aligned}$$

3.

$$\mathcal{F} \text{ base de } E \iff \begin{cases} \text{rg}(M) = p \\ \text{rg}(M) = n \end{cases}$$

On suppose que \mathcal{F} est une base de E .

$$M = \text{Mat}_{\mathcal{B}}(\mathcal{F}) = \begin{pmatrix} m_{11} & \dots & m_{1,n} \\ m_{21} & \dots & m_{2,n} \\ \vdots & \ddots & \vdots \\ m_{n,1} & \dots & m_{n,n} \end{pmatrix}$$

$$\text{Soit } A = \text{Mat}_{\mathcal{F}}(\mathcal{B}) = \begin{pmatrix} a_{11} & \dots & a_{1,n} \\ a_{21} & \dots & a_{2,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{pmatrix}. \text{ Montrons que } AM = I_n.$$

La première colonne de AM est

$$A \begin{pmatrix} m_{11} \\ \vdots \\ m_{n,1} \end{pmatrix} = m_{11} \begin{pmatrix} a_{11} \\ \vdots \\ a_{n,1} \end{pmatrix} + m_{21} \begin{pmatrix} a_{12} \\ \vdots \\ a_{n,2} \end{pmatrix} + \dots + m_{n,1} \begin{pmatrix} a_{1,n} \\ \vdots \\ a_{n,n} \end{pmatrix}$$

$$\text{Or, } \forall i \in \llbracket 1, n \rrbracket, \begin{pmatrix} a_{1,i} \\ \vdots \\ a_{n,i} \end{pmatrix} = \text{Mat}_{\mathcal{F}}(e_i).$$

Donc, la première colonne de AM est la colonne des coordonnées du vecteur

$m_{11}e_1 + m_{21}e_2 + \cdots + m_{n,1}e_n$ dans la base \mathcal{F} .
Or,

$$\text{Mat}_{\mathcal{B}}(u_1) = \begin{pmatrix} m_{11} \\ m_{21} \\ \vdots \\ m_{n,1} \end{pmatrix}$$

donc $u_1 = m_{11}e_1 + m_{21}e_2 + \cdots + m_{n,1}e_n$.
Comme $u_1 = 1 \cdot u_1 + 0 \cdot u_2 + \cdots + 0 \cdot u_n$,

$$\text{Mat}_{\mathcal{F}}(u_1) = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

La j -ème colonne de AM est

$$A \begin{pmatrix} m_{1,j} \\ \vdots \\ m_{n,j} \end{pmatrix} = m_{1,j} \begin{pmatrix} a_{11} \\ \vdots \\ a_{n,1} \end{pmatrix} + m_{2,j} \begin{pmatrix} a_{12} \\ \vdots \\ a_{n,2} \end{pmatrix} + \cdots + m_{n,j} \begin{pmatrix} a_{1,n} \\ \vdots \\ a_{n,n} \end{pmatrix}$$

$$\text{Or, } \forall i \in \llbracket 1, n \rrbracket, \begin{pmatrix} a_{1,i} \\ \vdots \\ a_{n,i} \end{pmatrix} = \text{Mat}_{\mathcal{F}}(e_i).$$

Donc, la j -ème colonne de AM est la colonne des coordonnées du vecteur $m_{1,j}e_1 + m_{2,j}e_2 + \cdots + m_{n,j}e_n$ dans la base \mathcal{F} .

Or,

$$\text{Mat}_{\mathcal{B}}(u_1) = \begin{pmatrix} m_{1,j} \\ m_{2,j} \\ \vdots \\ m_{n,j} \end{pmatrix}$$

donc $u_j = m_{1,j}e_1 + m_{2,j}e_2 + \cdots + m_{n,j}e_n$.
Comme $u_j = 0 \cdot u_1 + \cdots + 1 \cdot u_j + \cdots + 0 \cdot u_n$,

$$\text{Mat}_{\mathcal{F}}(u_1) = \begin{pmatrix} 0 \\ \vdots \\ 1 \leftarrow j \\ \vdots \\ 0 \end{pmatrix}$$

Donc,

$$AM = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} = I_n$$

En inversant les rôles de \mathcal{F} et \mathcal{B} , on prouve que $MA = I_n$.

On suppose maintenant que $M \in \text{GL}_n(\mathbb{K})$. Montrons que \mathcal{F} est une base de E .

On pose

$$M^{-1} = \begin{pmatrix} a_{11} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{pmatrix}$$

On sait que

$$MM^{-1} = I_n$$

Donc

$$\forall j \in \llbracket 1, n \rrbracket, a_{1,j} \begin{pmatrix} m_{11} \\ \vdots \\ m_{n,1} \end{pmatrix} + \dots + a_{n,j} \begin{pmatrix} m_{1,n} \\ \vdots \\ m_{n,n} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 1 \leftarrow j \\ \vdots \\ 0 \end{pmatrix}$$

donc

$$\forall j \in \llbracket 1, n \rrbracket, \text{Mat}_{\mathcal{B}} \left(\sum_{i=1}^n a_{i,j} u_i \right) = \text{Mat}_{\mathcal{B}}(e_j)$$

donc

$$\forall j \in \llbracket 1, n \rrbracket, e_j = \sum_{i=1}^n a_{i,j} u_i \in \text{Vect}(\mathcal{F})$$

Donc \mathcal{F} engendre E .

$$\text{Card}(\mathcal{F}) = n = \dim(E)$$

donc \mathcal{F} est une base de E .

□

3 Matrices d'une application linéaire

Soit $f \in \mathcal{L}(E, F)$, $\mathcal{B} = (e_1, \dots, e_n)$ une base de E et $\mathcal{C} = (f_1, \dots, f_p)$ une base de F .

Proposition – Définition: Soit $x \in E$ et $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \text{Mat}_{\mathcal{B}}(x)$. Soit $y \in F$ et $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_p \end{pmatrix} = \text{Mat}_{\mathcal{C}}(y)$. On pose $A = \begin{pmatrix} a_{11} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{p,1} & \dots & a_{p,n} \end{pmatrix} \in \mathcal{M}_{p,n}(\mathbb{K})$ telle que

$$\forall j \in \llbracket 1, n \rrbracket, \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{p,j} \end{pmatrix} = \text{Mat}_{\mathcal{C}}(f(e_j))$$

Alors

$$y = f(x) \iff Y = AX$$

On dit que A est la matrice de f dans les bases \mathcal{B} et \mathcal{C} . On la note $\text{Mat}_{\mathcal{B}, \mathcal{C}}(f)$.

Preuve:

$$x = \sum_{j=1}^n x_j e_j \quad y = \sum_{i=1}^p y_i f_i$$

$$\begin{aligned} y = f(x) &\iff \sum_{i=1}^p y_i f_i = f\left(\sum_{j=1}^n x_j e_j\right) \\ &\iff \sum_{i=1}^p y_i f_i = \sum_{j=1}^n x_j f(e_j) \end{aligned}$$

Or,

$$\forall j \in [\![1, n]\!], f(e_j) = \sum_{i=1}^p a_{i,j} f_i$$

D'où,

$$\begin{aligned} y = f(x) &\iff \sum_{i=1}^p y_i f_i = \sum_{j=1}^n x_j \sum_{i=1}^p a_{i,j} f_i \\ &= \sum_{i=1}^p \left(\sum_{j=1}^n a_{i,j} x_j \right) f_i \\ &\iff \forall i \in [\![1, p]\!], \sum_{j=1}^n a_{i,j} x_j = y_i \\ &\iff AX = Y \end{aligned}$$

□

EXEMPLE:

$E = \mathbb{R}^3$ et f la projection sur $R = \{(x, y, z) \mid x + y = 0\}$ parallèlement à $G = \text{Vect}((1, 1, 1))$.
— $\mathcal{B} = (e_1, e_2, e_3)$ base canonique.

$$\text{Mat}_{\mathcal{B}, \mathcal{B}}(f) = \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}$$

$$e_1 = (1, 0, 0) = \underbrace{\left(\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}\right)}_{\in F} + \underbrace{\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)}_{\in G}$$

$$f(e_1) = \left(\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}\right) = \frac{1}{2}e_1 - \frac{1}{2}e_2 - \frac{1}{2}e_3$$

$$e_2 = (0, 1, 0) = \left(-\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}\right) + \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$$

$$e_3 = (0, 0, 1) = (0, 0, 1) + (0, 0, 0)$$

Donc

$$\text{Mat}_{\mathcal{B}, \mathcal{B}}(f) = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 1 \end{pmatrix}$$

— $\mathcal{C} = (e_3, e_1 - e_2, e_1 + e_2 + e_3) = (u_1, u_2, u_3)$

$$\text{Mat}_{\mathcal{C}, \mathcal{C}}(f) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

car

$$f(u_1) = u_1 f(u_2) = u_2 f(u_3) = 0$$

$$\text{Mat}_{\mathcal{C}, \mathcal{B}} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\text{Mat}_{\mathcal{B}, \mathcal{C}}(f) = \begin{pmatrix} -\frac{1}{2} & -\frac{1}{2} & 1 \\ \frac{1}{2} & -\frac{1}{2} & 0 \\ \frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

— Soit $(x, y, z) \in \mathbb{R}^3$

$$\begin{aligned} \text{Mat}_{\mathcal{B}}(f((x, y, z))) &= \text{Mat}_{\mathcal{B}, \mathcal{B}}(f) \times \text{Mat}_{\mathcal{B}}((x, y, z)) \\ &= \begin{pmatrix} -\frac{1}{2} & -\frac{1}{2} & 1 \\ \frac{1}{2} & -\frac{1}{2} & 0 \\ \frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} \\ &= \begin{pmatrix} \frac{x-y}{2} \\ \frac{y-x}{2} \\ \frac{-x-y}{2} + z \end{pmatrix} \end{aligned}$$

Donc

$$f((x, y, z)) = \left(\frac{x-y}{2}, \frac{y-x}{2}, z - \frac{x+y}{2} \right)$$

$$\begin{aligned} \text{Mat}_{\mathcal{C}}(f(x, y, z)) &= \text{Mat}_{\mathcal{B}, \mathcal{C}}(f) \times \text{Mat}_{\mathcal{B}}((x, y, z)) \\ &= \begin{pmatrix} -\frac{1}{2} & -\frac{1}{2} & 1 \\ \frac{1}{2} & -\frac{1}{2} & 0 \\ \frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} \\ &= \begin{pmatrix} \frac{-x-y}{2} + z \\ \frac{x-y}{2} \\ \frac{2}{2} \end{pmatrix} \end{aligned}$$

Donc

$$f((x, y, z)) = \left(z - \frac{x+y}{2} \right) u_1 + \left(\frac{x-y}{2} \right) u_2$$

EXEMPLE:

Soient $E = \mathbb{C}$, $\mathcal{B} = (1, i)$, $\theta \in \mathbb{R}$ et f la rotation de centre O et d'angle θ .

$$\begin{aligned} f : \mathbb{C} &\longrightarrow \mathbb{C} \\ z &\longmapsto e^{i\theta} z \end{aligned}$$

f est linéaire :

$$\begin{aligned} \forall (\lambda, \mu) \in \mathbb{R}^2, \forall (z, w) \in \mathbb{C}^2 \quad &f(\lambda z + \mu w) = e^{i\theta}(\lambda z + \mu w) \\ &= \lambda e^{i\theta} z + \mu e^{i\theta} w \\ &= \lambda f(z) + \mu f(w) \end{aligned}$$

$$\text{Mat}_{\mathcal{B}}(f) = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

car

$$\begin{cases} f(1) = e^{i\theta} = \cos \theta + i \sin \theta \\ f(i) = ie^{i\theta} = -\sin \theta + i \cos \theta \end{cases}$$

$$z = x + iy \text{ avec } x, y \in \mathbb{R}$$

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \cos \theta & -y \sin \theta \\ x \sin \theta & y \cos \theta \end{pmatrix}$$

Théorème: Soient E et F deux \mathbb{K} -espaces vectoriels de dimension finie, $\mathcal{B} = (e_1, \dots, e_n)$ une base de E et $\mathcal{C} = (f_1, \dots, f_p)$ une base de F .

$$\begin{aligned} \Phi : \mathcal{L}(E, F) &\longrightarrow \mathcal{M}_{p,n}(\mathbb{K}) \\ f &\longmapsto \text{Mat}_{\mathcal{B}, \mathcal{C}}(f) \end{aligned}$$

Φ est un \mathbb{K} -isomorphisme linéaire.

Preuve: — Soient $(f, g) \in \mathcal{L}(E, F)^2$ et $(\lambda, \mu) \in \mathbb{K}^2$. On pose $A = \text{Mat}_{\mathcal{B}, \mathcal{C}}(f) = \Phi(f) = (a_{i,j})$ et $B = \text{Mat}_{\mathcal{B}, \mathcal{C}}(g) = \Phi(g) = (b_{i,j})$. On pose également $C = \text{Mat}_{\mathcal{B}, \mathcal{C}}(\lambda f + \mu g) = \Phi(\lambda f + \mu g) = (c_{i,j})$.

$$\forall j \in [\![1, n]\!], \begin{pmatrix} c_{1,j} \\ \vdots \\ c_{p,j} \end{pmatrix} = \text{Mat}_{\mathcal{C}}((\lambda f + \mu g)(e_j))$$

$$= \text{Mat}_{\mathcal{C}}(\lambda f(e_j) + \mu g(e_j))$$

Or,

$$\text{Mat}_{\mathcal{C}}(f(e_j)) = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{p,j} \end{pmatrix}$$

et

$$\text{Mat}_{\mathcal{C}}(g(e_j)) = \begin{pmatrix} b_{1,j} \\ \vdots \\ b_{p,j} \end{pmatrix}$$

Donc

$$\text{Mat}_{\mathcal{C}}(\lambda f(e_j) + \mu g(e_j)) = \lambda \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{p,j} \end{pmatrix} + \mu \begin{pmatrix} b_{1,j} \\ \vdots \\ b_{p,j} \end{pmatrix}$$

Donc $C = \lambda A + \mu B$ et donc Φ est linéaire.

— Soit $f \in \text{Ker } \Phi$:

$$\text{Mat}_{\mathcal{B}, \mathcal{C}}(f) = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$

Donc

$$\forall j \in [\![1, n]\!], f(e_j) = \sum_{i=1}^p 0 \cdot f_i = 0_F$$

Soit $x \in E$. On pose $x = \sum_{j=1}^n x_j e_j$.

$$f(x) = \sum_{j=1}^n x_j f(e_j) = 0_F$$

Donc $f = 0$. Donc Φ est injective.

Soit $A \in \mathcal{M}_{p,n}(\mathbb{K})$. On pose $A = (a_{i,j})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq n}}$.

On définit $F : E \rightarrow F$ de la façon suivante : pour tout $x \in E$, on décompose

$x = \sum_{j=1}^n x_j e_j$. On pose alors

$$\begin{aligned} f(x) &= \sum_{j=1}^n x_j \sum_{i=1}^p a_{i,j} f_i \\ &= \sum_{i=1}^p \sum_{j=1}^n a_{i,j} x_j f_i \end{aligned}$$

Montrons que $f \in \mathcal{L}(E, F)$ et $\Phi(f) = A$

— Soit $(x, y) \in E^2$ et $(\alpha, \beta) \in \mathbb{K}^2$. On pose

$$\begin{cases} x = \sum_{j=1}^n x_j e_j & \text{avec } (x_1, \dots, x_n) \in \mathbb{K}^n \\ y = \sum_{j=1}^n y_j e_j & \text{avec } (y_1, \dots, y_n) \in \mathbb{K}^n \end{cases}$$

Donc

$$\alpha x + \beta y = \sum_{j=1}^n (\alpha x_j + \beta y_j) (e_j)$$

D'où

$$\begin{aligned} f(\alpha x + \beta y) &= \sum_{i=1}^p \sum_{j=1}^n a_{i,j} (\alpha x_j + \beta y_j) f_i \\ &= \alpha \sum_{i=1}^p \sum_{j=1}^n a_{i,j} x_j f_i + \beta \sum_{i=1}^p \sum_{j=1}^n b_{i,j} y_j f_i \\ &= \alpha f(x) + \beta f(y) \end{aligned}$$

Soit $j \in \llbracket 1, p \rrbracket$.

$$f(e_j) = \sum_{i=1}^p a_{i,j} f_i$$

et

$$\text{Mat}_{\mathcal{C}}(f(e_j)) = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{p,j} \end{pmatrix}$$

donc

$$\text{Mat}_{\mathcal{B}, \mathcal{C}}(f) = A$$

□

Corollaire: Si E et F sont deux \mathbb{K} -espaces vectoriels de dimension finie, alors

$$\dim(\mathcal{L}(E, F)) = \dim(E) \times \dim(F)$$

□

EXEMPLE (*Trouver tous les endomorphismes de \mathbb{R}^2*):
Soit $\mathcal{B} = (e_1, e_2)$ la base canonique de \mathbb{R}^2 .

$$\begin{aligned} \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x, y) &\longmapsto (ax + cy, bx + dy) \end{aligned}$$

avec $(a, b, c, d) \in \mathbb{R}^4$.

Une base de $\mathcal{L}(\mathbb{R}^2)$ est (f_1, f_2, f_3, f_4) où

$$\begin{cases} f_1 : (x, y) \mapsto (x, 0) \\ f_2 : (x, y) \mapsto (0, x) \\ f_3 : (x, y) \mapsto (y, 0) \\ f_4 : (x, y) \mapsto (0, y) \end{cases}$$

Théorème: Soient $f \in \mathcal{L}(E, F)$ et $g \in \mathcal{L}(F, G)$, \mathcal{B} une base de E , \mathcal{C} une base de F et \mathcal{D} une base de G . Alors

$$\text{Mat}_{\mathcal{B}, \mathcal{D}}(g \circ f) = \text{Mat}_{\mathcal{C}, \mathcal{D}}(g) \times \text{Mat}_{\mathcal{B}, \mathcal{C}}(f)$$

Preuve:

On pose

$$\mathcal{B} = (e_1, \dots, e_n)$$

$$\mathcal{C} = (f_1, \dots, f_p)$$

$$\mathcal{D} = (g_1, \dots, g_q).$$

et

$$A = (a_{i,j})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq n}} = \text{Mat}_{\mathcal{B}, \mathcal{C}}(f)$$

$$B = (b_{k,i})_{\substack{1 \leq k \leq q \\ 1 \leq i \leq p}} = \text{Mat}_{\mathcal{C}, \mathcal{D}}(g)$$

$$C = (c_{k,j})_{\substack{1 \leq k \leq q \\ 1 \leq j \leq n}} = \text{Mat}_{\mathcal{B}, \mathcal{D}}(g \circ f)$$

Soit $j \in \llbracket 1, n \rrbracket$. La j -ième colonne de C est

$$\begin{aligned} \text{Mat}_{\mathcal{D}}(g \circ f(e_j)) &= \text{Mat}_{\mathcal{D}}(g(f(e_j))) \\ &= \text{Mat}_{\mathcal{C}, \mathcal{D}}(g) \times \text{Mat}_{\mathcal{C}}(f(e_j)) \\ &= BA_j \end{aligned}$$

où A_j est la j -ième colonne de A .

Or, la j -ième colonne de BA est aussi BA_j .

Donc, $C = BA$. □

4 Formules de changement de bases

Proposition: Soit E un \mathbb{K} -espace vectoriel de dimension finie n . Soient \mathcal{B}_1 et \mathcal{B}_2 deux bases de E et $x \in E$. Soit $P = P_{\mathcal{B}_1 \rightarrow \mathcal{B}_2} = \text{Mat}_{\mathcal{B}_1}(\mathcal{B}_2)$. Alors

$$\text{Mat}_{\mathcal{B}_2}(x) = P^{-1} \text{Mat}_{\mathcal{B}_1}(x)$$

Preuve:

$$P = \text{Mat}_{\mathcal{B}_2, \mathcal{B}_1}(\text{id}_E) = \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}$$

si $\begin{cases} \mathcal{B}_1 = (e_1, \dots, e_n) \\ \mathcal{B}_2 = (u_1, \dots, u_n) \end{cases}$

$$\begin{aligned} P \text{Mat}_{\mathcal{B}_2}(x) &= \text{Mat}_{\mathcal{B}_2, \mathcal{B}_1}(\text{id}_E) \times \text{Mat}_{\mathcal{B}_2}(x) \\ &= \text{Mat}_{\mathcal{B}_1}(\text{id}_E(x)) \\ &= \text{Mat}_{\mathcal{B}_1}(x) \end{aligned}$$

$$\begin{array}{ccc} E_{\mathcal{B}_2} & \xrightarrow[x]{\text{id}_E} & E_{\mathcal{B}_1} \\ X & \xrightarrow[P]{\quad} & PX \end{array}$$

□

Proposition: Soient E et F deux \mathbb{K} -espaces vectoriels de dimension finie \mathcal{B}_1 et \mathcal{B}_2 deux bases de E , et $\mathcal{C}_1, \mathcal{C}_2$ deux bases de F et $f \in \mathcal{L}(E, F)$.

Soient $\begin{cases} P = P_{\mathcal{B}_1 \rightarrow \mathcal{B}_2} = \text{Mat}_{\mathcal{B}_1}(\mathcal{B}_2) \\ Q = P_{\mathcal{C}_1 \rightarrow \mathcal{C}_2} = \text{Mat}_{\mathcal{C}_1}(\mathcal{C}_2) \\ A = \text{Mat}_{\mathcal{B}_1, \mathcal{C}_1}(f) \end{cases}$ Alors,

$$\text{Mat}_{\mathcal{B}_2, \mathcal{C}_2}(f) = Q^{-1}AP$$

Preuve:

$$\begin{array}{ccc} E_{\mathcal{B}_1} & \xrightarrow[A]{f} & F_{\mathcal{C}_1} \\ \text{id}_E \uparrow P & & \downarrow \text{id}_F Q^{-1} \\ E_{\mathcal{B}_2} & \xrightarrow[A']{f} & F_{\mathcal{C}_2} \end{array}$$

$f = \text{id}_F \circ f \circ \text{id}_E$ donc

$$\text{Mat}_{\mathcal{B}_2, \mathcal{C}_2}(f) = \text{Mat}_{\mathcal{C}_1, \mathcal{C}_2}(\text{id}_F) \text{Mat}_{\mathcal{B}_1, \mathcal{C}_1}(f) \text{Mat}_{\mathcal{B}_2, \mathcal{B}_1}(\text{id}_E)$$

□

EXEMPLE:

$E = \mathbb{R}^3$, $F = \{(x, y, z) \in \mathbb{R}^3 \mid x + y = 0\}$, $G = \text{Vect}((1, 1, 1))$ et f la projection sur F parallèlement à G .

Soient $\mathcal{B} = (e_1, e_2, e_3)$ base canonique de E et $\mathcal{C} = (u_1, u_2, u_3)$ avec $\begin{cases} u_1 = (0, 0, 1) \\ u_2 = (1, -1, 0) \\ u_3 = (1, 1, 1) \end{cases}$.

$$\text{Mat}_{\mathcal{C}}(f) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Donc

$$\text{Mat}_{\mathcal{B}}(f) = \begin{pmatrix} 0 & 1 & 1 \\ 0 & -1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 0 & -1 & 1 \\ 1 & 0 & 1 \end{pmatrix}^{-1}$$

Proposition – Définition: Soient $(A, B) \in \mathcal{M}_{p,n}(\mathbb{K})^2$.
On dit que A et B sont équivalentes si

$$\exists (P, Q) \in \text{GL}_n(\mathbb{K}) \times \text{GL}_p(\mathbb{K}), B = Q^{-1}AP$$

Cette relation est une relation d'équivalence. □

Théorème: Soit $f \in \mathcal{L}(E)$, \mathcal{B} et \mathcal{C} deux bases de E , $P = P_{\mathcal{B} \rightarrow \mathcal{C}} = \text{Mat}_{\mathcal{B}}(\mathcal{C})$, $A = \text{Mat}_{\mathcal{B}}(f)$ et $B = \text{Mat}_{\mathcal{C}}(f)$.

Alors

$$B = P^{-1}AP.$$

□

Définition: Soit $(A, B) \in \mathcal{M}_n(\mathbb{K})^2$. On dit que A et B sont semblables s'il existe $P \in \text{GL}_n(\mathbb{K})$ telle que

$$B = P^{-1}AP.$$

L'ensemble $\{P^{-1}AP \mid P \in \text{GL}_n(\mathbb{K})\}$ est la classe de similitude de A .**EXEMPLE:**

$$\begin{cases} \forall n \in \mathbb{N}, u_{n+2} = u_{n+1} + u_n \\ u_0 = 0 \\ u_1 = 1 \end{cases}$$

On pose

$$\forall n \in \mathbb{N}, X_n = \begin{pmatrix} u_n \\ u_{n+1} \end{pmatrix} \text{ et } X_0 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

On a

$$\begin{aligned}\forall n \in \mathbb{N}, X_{n+1} &= \begin{pmatrix} u_{n+1} \\ u_{n+2} \end{pmatrix} \\ &= \begin{pmatrix} u_{n+1} \\ u_n + u_{n+1} \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} u_n \\ u_{n+1} \end{pmatrix} \\ &= AX_n \text{ avec } A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.\end{aligned}$$

D'où

$$\forall n \in \mathbb{N}, X_n = A^n X_0$$

On aimerait trouver D diagonale et $P \in \mathrm{GL}_2(\mathbb{C})$ telles que

$$A = PDP^{-1}.$$

Soit $f : \begin{pmatrix} \mathbb{C}^2 \\ (z_1, z_2) \end{pmatrix} \mapsto \begin{pmatrix} \mathbb{C}^2 \\ (z_2, z_1 + z_2) \end{pmatrix}$ telle que $\mathrm{Mat}_{\mathcal{B}}(f) = A$ où $\mathcal{B} = (e_1, e_2)$ est la base canonique de \mathbb{C}^2 .

On cherche $\mathcal{C} = (u_1, u_2)$ une base de \mathbb{C}^2 telle que $\mathrm{Mat}_{\mathcal{C}}(f) = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = D$ avec $(\lambda_1, \lambda_2) \in \mathbb{C}^2$.

ANALYSE On suppose que \mathcal{C} existe. Dans ce cas,

$$\begin{cases} f(u_1) = \lambda_1 u_1, \\ f(u_2) = \lambda_2 u_2, \\ (\lambda_1, \lambda_2) \text{ libre.} \end{cases}$$

Soit $u = (x, y) \in \mathbb{C}^2$ et $\lambda \in \mathbb{C}$.

$$\begin{aligned}f(u) = \lambda u &\iff \begin{cases} y = \lambda x \\ x + y = \lambda y \end{cases} \\ &\iff \begin{cases} y = \lambda x \\ x + \lambda x - \lambda^2 x = 0 \end{cases} \\ &\iff \begin{cases} y = \lambda x \\ x(1 + \lambda - \lambda^2) = 0 \end{cases} \\ &\iff \begin{cases} x = 0 \\ y = 0 \end{cases} \text{ ou } \begin{cases} A + \lambda - \lambda^2 = 0 \\ y = \lambda x \end{cases} \\ &\iff u = (0, 0) \text{ ou } \begin{cases} \lambda = \frac{-1 + \sqrt{5}}{2} \\ y = \frac{-1 + \sqrt{5}}{2} x \end{cases} \text{ ou } \begin{cases} \lambda = \frac{-1 - \sqrt{5}}{2} \\ y = \frac{-1 - \sqrt{5}}{2} x \end{cases}\end{aligned}$$

SYNTHÈSE On pose $\begin{cases} \lambda_1 = \frac{-1 + \sqrt{5}}{2} = \varphi \\ u_1 = (1, \varphi) \end{cases}$ et $\begin{cases} \lambda_2 = \frac{-1 - \sqrt{5}}{2} = -\frac{1}{\varphi} \\ u_2 = \left(1, -\frac{1}{\varphi}\right) \end{cases}$.

Ainsi, $\begin{cases} f(u_1) = \lambda_1 u_1 \\ f(u_2) = \lambda_2 u_2. \end{cases}$

u_1 et u_2 ne sont pas colinéaires, ils forment une famille libre donc une base.

On pose $\mathcal{C} = (u_1, u_2)$ et $\mathrm{Mat}_{\mathcal{C}}(f) = \begin{pmatrix} \varphi & 0 \\ 0 & -\frac{1}{\varphi} \end{pmatrix} = D$.

$$A = PDP^{-1}$$

et

$$\begin{cases} P^{-1} = \text{Mat}_{\mathcal{B}, \mathcal{C}}(\text{id}_{\mathbb{C}^2}) = P_{\mathcal{C} \rightarrow \mathcal{B}} \\ P = \text{Mat}_{\mathcal{C}, \mathcal{B}}(\text{id}_{\mathbb{C}^2}) = P_{\mathcal{B} \rightarrow \mathcal{C}} \end{cases}$$

On a $P = \begin{pmatrix} 1 & \frac{1}{\varphi} \\ \varphi & -\frac{1}{\varphi} \end{pmatrix}$ donc

$$P^{-1} = -\frac{1}{\sqrt{5}} \begin{pmatrix} -\frac{1}{\varphi} & -1 \\ -\varphi & 1 \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} \frac{1}{\varphi} & 1 \\ \varphi & -1 \end{pmatrix}$$

Donc $A = PDP^{-1}$ et donc

$$\begin{aligned} \forall n \in \mathbb{N}, A^n &= PD^n P^{-1} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & \frac{1}{\varphi} \\ \varphi & -\frac{1}{\varphi} \end{pmatrix} \begin{pmatrix} \varphi^n & 0 \\ 0 & \left(-\frac{1}{\varphi}\right)^n \end{pmatrix} \begin{pmatrix} \frac{1}{\varphi} & 1 \\ \varphi & -1 \end{pmatrix} \\ &\quad \parallel \\ &\begin{pmatrix} * & u_n \\ * & * \end{pmatrix} \end{aligned}$$

EXEMPLE:

$$y'' + \omega^2 y = 0 \quad \omega \in \mathbb{R}_*$$

$$\forall t, Y(t) = \begin{pmatrix} y(t) \\ y'(t) \end{pmatrix}$$

$$\begin{aligned} \forall t, Y'(t) &= \begin{pmatrix} y'(t) \\ y''(t) \end{pmatrix} \\ &= \begin{pmatrix} y'(t) \\ -\omega^2 y(t) \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ -\omega^2 & 0 \end{pmatrix} \begin{pmatrix} y(t) \\ y'(t) \end{pmatrix} \\ &= AY(t) \end{aligned}$$

$$\text{Soit } f : \begin{matrix} \mathbb{C}^2 & \longrightarrow & \mathbb{C}^2 \\ (a, b) & \longmapsto & (b, -\omega^2 a) \end{matrix}.$$

$A = \text{Mat}_{\mathcal{B}}(f)$ où $\mathcal{B} = (e_1, e_2)$ base canonique de \mathbb{C}^2 . On cherche $\mathcal{C} = (u_1, u_2)$ une base de \mathbb{C}^2 telle que $\text{Mat}_{\mathcal{C}}(f) = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = D$.

ANALYSE Si \mathcal{C} existe,

$$\begin{cases} f(u_1) = \lambda_1 u_1 \\ f(u_2) = \lambda_2 u_2 \end{cases}$$

Soit $u = (a, b) \in \mathbb{C}^2$ et $\lambda \in C$.

$$\begin{aligned} f(u) = \lambda u &\iff \begin{cases} b = \lambda a \\ -\omega^2 a = \lambda b \end{cases} \\ &\iff \begin{cases} b = \lambda a \\ -\omega^2 a = \lambda^2 a \end{cases} \\ &\iff \begin{cases} a = 0 \\ b = 0 \end{cases} \text{ ou } \begin{cases} \lambda^2 = -\omega^2 \\ b = \lambda a \end{cases} \end{aligned}$$

$$\begin{array}{ccc}
 & \text{pose } \begin{cases} \lambda_1 = i\omega \\ u_1 = (1, i\omega) \end{cases} & \text{et } \begin{cases} \lambda_2 = -i\omega \\ u_2 = (1, -i\omega) \end{cases} . (u_1, u_2) \text{ est bien une base de} \\
 \text{id}_{\mathbb{C}^2} \downarrow \begin{matrix} \text{SYNTHÈSE} \\ P^{-1} \end{matrix} \text{id}_{\mathbb{C}^2} \uparrow P & & \\
 \mathbb{C}_{\mathcal{C}}^2 \xrightarrow[D]{f} \mathbb{C}_{\mathcal{C}}^2 & \text{et } \text{Mat}_{\mathcal{C}}(f) = \begin{pmatrix} i\omega & 0 \\ 0 & -i\omega \end{pmatrix} = D
 \end{array}$$

$$AP = PD \iff P^{-1}A = DP^{-1}$$

On a

$$P = P_{\mathcal{B} \rightarrow \mathcal{C}} = \begin{pmatrix} 1 & 1 \\ i\omega & -i\omega \end{pmatrix}$$

On pose

$$\forall t, X(t) = P^{-1} \times Y(t)$$

Donc

$$\begin{aligned}
 \forall t, X'(t) &= P^{-1}Y'(t) = P^{-1}AY(t) \\
 &= DP^{-1}Y(t) \\
 &= DX(t)
 \end{aligned}$$

On pose

$$\forall t, X(t) = \begin{pmatrix} a(t) \\ b(t) \end{pmatrix}$$

$$\begin{aligned}
 X'(t) = DX(t) &\iff \begin{cases} a'(t) = i\omega a(t) \\ b'(t) = -i\omega b(t) \end{cases} \\
 &\iff \begin{cases} a(t) = \lambda e^{i\omega t} \\ b(t) = \mu e^{-i\omega t} \end{cases} \quad (\lambda, \mu) \in \mathbb{C}^2.
 \end{aligned}$$

$$\begin{aligned}
 \forall t, Y(t) &= P \times X(t) \\
 &= \begin{pmatrix} 1 & 1 \\ i\omega & -i\omega \end{pmatrix} \begin{pmatrix} \lambda e^{i\omega t} \\ \mu e^{-i\omega t} \end{pmatrix} \\
 &= \begin{pmatrix} \lambda e^{i\omega t} + \mu e^{-i\omega t} \\ * \end{pmatrix}
 \end{aligned}$$

Donc,

$$\forall t, y(t) = \lambda e^{i\omega t} + \mu e^{-i\omega t}$$

Définition: Soit $A = (a_{i,j}) \in \mathcal{M}_n(\mathbb{K})$. La trace de A est

$$\text{tr}(A) = \sum_{i=1}^n a_{i,i}$$

Proposition:

1. $\text{tr} \in \mathcal{L}(\mathcal{M}_n(\mathbb{K}), \mathbb{K}) = \mathcal{M}_n(\mathbb{K})^*$
2. $\forall A, B \in \mathcal{M}_n(\mathbb{K}), \text{tr}(AB) = \text{tr}(BA)$

Preuve: 1. Soient $(A, B) \in \mathcal{M}_n(\mathbb{K})$ et $(\alpha, \beta) \in \mathbb{K}^2$. On pose $A = (a_{i,j})$ et $B = (b_{i,j})$.

$$\begin{aligned}\text{tr}(\alpha A + \beta B) &= \sum_{i=1}^n (\alpha a_{i,i} \beta b_{i,i}) \\ &= \alpha \sum_{i=1}^n a_{i,i} + \beta \sum_{i=1}^n b_{i,i} \\ &= \alpha \text{tr}(A) + \beta \text{tr}(B)\end{aligned}$$

2. Soit $(A, B) \in \mathcal{M}_n(\mathbb{K})^2$. On pose $A = (a_{i,j})$, $B = (b_{i,j})$, $AB = (c_{i,j})$ et $BA = (d_{i,j})$.

$$\begin{aligned}\text{tr}(AB) &= \sum_{i=1}^n c_{i,i} = \sum_{i=1}^n \sum_{j=1}^n a_{i,j} b_{j,i} \\ &= \sum_{j=1}^n \sum_{i=1}^n b_{j,i} a_{i,j} \\ &= \sum_{j=1}^n d_{j,j} \\ &= \text{tr}(BA)\end{aligned}$$

□

Proposition: Soit $(A, B) \in \mathcal{M}_n(\mathbb{K})^2$.

$$A \text{ et } B \text{ semblables} \implies \text{tr}(A) = \text{tr}(B)$$

Preuve:

On suppose A et B semblables. Soit $P \in \text{GL}_n(\mathbb{K})$ telle que $A = P^{-1}BP$. Donc

$$\text{tr}(A) = \text{tr}(P^{-1}(BP)) = \text{tr}((BP)P^{-1}) = \text{tr}(B)$$

□

REMARQUE (Δ Attention):

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ et } B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\text{tr}(A) = 2 = \text{tr}(B)$$

Or, A et B ne sont pas semblables, sinon

$$\begin{aligned}A &= P^{-1}BP \text{ avec } P \in \text{GL}_2(\mathbb{K}) &= P^{-1}I_2P \\ &= P^{-1}P \\ &= I_2 \neq A\end{aligned}$$

Définition

Corollaire: Soit $f \in \mathcal{L}(E)$ et \mathcal{B} une base de E . $A = \text{Mat}_{\mathcal{B}}(f)$. La trace de f est $\text{tr}(A)$.

Ce nombre ne dépend pas de la base \mathcal{B} choisie. On note ce nombre $\text{tr}(f)$. □

Proposition: Soit p un projecteur de E de dimension finie. Alors

$$\text{tr}(p) = \text{rg}(p)$$

Preuve:

On sait que

$$E = \text{Ker}(p) \oplus \text{Im}(p)$$

Soit $\mathcal{B}_1 = (e_1, \dots, e_k)$ une base $\text{Ker}(p)$ et $\mathcal{B}_2 = (e_{k+1}, \dots, e_n)$ une base de $\text{Im}(p)$.

On pose $\mathcal{B} = (e_1, \dots, e_k, e_{k+1}, \dots, e_n)$. \mathcal{B} est une base de E et

$$A = \text{Mat}_{\mathcal{B}}(p)$$

$$\text{tr}(p) = \text{tr}(A) = n - k = \#\mathcal{B}_2 = \dim(\text{Im } p) = \text{rg}(p)$$

□

EXEMPLE:

$$F = \{(x, y, z) \in \mathbb{R}^3 \mid x + y = 0\}$$

$$G = \text{Vect}((1, 1, 1))$$

f la projection sur F parallèlement à G .

$\mathcal{B} = (e_1, e_2, e_3)$ la base canonique de \mathbb{R}^3 .

$$\text{Mat}_{\mathcal{B}}(f) = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 1 \end{pmatrix} = A$$

$$\text{tr}(A) = 2 = \dim(F)$$

5 Conséquences

Proposition: La multiplication matricielle est associative.

Preuve:

$$\begin{cases} A \in \mathcal{M}_{n,p}(\mathbb{K}) \\ B \in \mathcal{M}_{p,q}(\mathbb{K}) \\ C \in \mathcal{M}_{q,r}(\mathbb{K}) \end{cases}$$

Soient $f \in \mathcal{L}(\mathbb{K}^p, \mathbb{K}^n)$, $g \in \mathcal{L}(\mathbb{K}^q, \mathbb{K}^p)$ et $h \in \mathcal{L}(\mathbb{K}^r, \mathbb{K}^q)$ telles que

$$\begin{cases} A = \text{Mat}_{\mathcal{B}, \mathcal{C}}(f) \\ B = \text{Mat}_{\mathcal{C}, \mathcal{D}}(g) \\ C = \text{Mat}_{\mathcal{D}, \mathcal{E}}(h) \end{cases}$$

où \mathcal{B} est la base canonique de \mathbb{K}^p , \mathcal{C} est la base canonique de \mathbb{K}^n , \mathcal{D} est la base canonique de \mathbb{K}^r , \mathcal{E} est la base canonique de \mathbb{K}^q .

$$\begin{aligned}
A(BC) &= \text{Mat}_{\mathcal{D}\mathcal{C}}(f \circ (g \circ h)) \\
&= \text{Mat}_{\mathcal{D},\mathcal{C}}((f \circ g) \circ h) \\
&= (AB)C
\end{aligned}$$

□

Proposition: Soit $(A, B) \in \mathcal{M}_n(\mathbb{K})^2$. On suppose que $AB = I_n$. Alors $(A, B) \in \text{GL}_n(\mathbb{K})^2$ et $A^{-1} = B$.

Preuve:

Soit \mathcal{B} la base canonique de \mathbb{K}^n , $f \in \mathcal{L}(\mathbb{K}^n)$ telle que $\text{Mat}_{\mathcal{B}}(f) = A$, $g \in \mathcal{L}(\mathbb{K}^n)$ telle que $\text{Mat}_{\mathcal{B}}(g) = B$.

$$\begin{aligned}
AB = I_n \text{ donc } \text{Mat}_{\mathcal{B}}(f \circ g) &= \text{Mat}_{\mathcal{B}}(\text{id}_{\mathbb{K}^n}) && \text{donc } f \circ g = \text{id}_{\mathbb{K}^n} \\
\text{donc } f \circ g \text{ est injective} \\
\text{donc } g \text{ est injective} \\
\text{donc } g \text{ est un isomorphisme}
\end{aligned}$$

Or, $f \circ g = \text{id}$ donc $f = f \circ g \circ g^{-1} = g^{-1}$

$$\begin{aligned}
BA &= \text{Mat}_{\mathcal{B}}(g) = \text{Mat}_{\mathcal{B}}(f) \\
&= \text{Mat}_{\mathcal{B}}(g \circ f) \\
&= \text{Mat}_{\mathcal{B}}(g \circ g^{-1}) \\
&= \text{Mat}_{\mathcal{B}}(\text{id}_{\mathbb{K}^n}) \\
&= I_n
\end{aligned}$$

Donc $A = B^{-1}$. □

REMARQUE:

Au passage, on a montré que

$$f \in \text{GL}(E) \iff \text{Mat}_{\mathcal{B}}(f) \in \text{GL}_n(\mathbb{K})$$

et, dans ce cas,

$$\text{Mat}_{\mathcal{B}}(f^{-1}) = \text{Mat}_{\mathcal{B}}(f)^{-1}$$

Proposition: Soit $A \in \mathcal{M}_{p,n}(\mathbb{K})$.

Le nombre maximal de lignes linéairement indépendantes de A est égal au rang de A .

Preuve:

On appelle rang par lignes le nombre exact de lignes linéairement indépendantes.

Ce rang par ligne est invariant quand on effectue une opération élémentaire sur les lignes.

En appliquant la méthode du pivot de Gauß, on obtient une matrice de la forme

$$\left(\begin{array}{ccc|cc|ccc} 0 & \dots & 0 & | & 1 & * & \dots & \dots & * \\ 0 & \dots & \dots & | & 0 & | & 1 & * & \dots \\ 0 & \dots & \dots & | & \dots & | & \dots & \dots & 0 \end{array} \right)$$

qui a le même rang par lignes que A .

On observe que ce rang r est égal au nombre de pivots.

Soit S le système homogène

$$AX = 0$$

où $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. D'après l'algorithme du pivot, la résolution de ce système fournit r inconnues principales et $n - r$ paramètres.

Sans perte de généralité, on peut supposer que x_1, \dots, x_{n-r} sont les paramètres et x_{n-r+1}, \dots, x_n les inconnues principales.

Soit $\mathcal{B} = (e_1, \dots, e_n)$ la base canonique de \mathbb{K}^n et $\mathcal{C} = (f_1, \dots, f_p)$ la base canonique de \mathbb{K}^p et $f \in \mathcal{L}(\mathbb{K}^n, \mathbb{K}^p)$ telle que

$$A = \text{Mat}_{\mathcal{B}, \mathcal{C}}(f).$$

Soit $x = (x_1, \dots, x_n) \in \mathbb{K}^n$ et $X = \text{Mat}_{\mathcal{B}}(x)$.

$$\begin{aligned} AX = 0 &\iff \text{Mat}_{\mathcal{B}, \mathcal{C}}(f) \text{Mat}_{\mathcal{B}}(x) = \text{Mat}_{\mathcal{C}}(0) \\ &\iff \text{Mat}_{\mathcal{C}}(f(x)) = \text{Mat}_{\mathcal{C}}(0) \\ &\iff f(x) = 0 \\ &\iff x \in \text{Ker } f \end{aligned}$$

Ainsi, l'ensemble E des solutions de (S) est un \mathbb{K} -espace vectoriel isomorphe à $\text{Ker}(f)$.

De plus,

$$g : E \longrightarrow \mathbb{K}^{n-r}$$

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \longmapsto (x_1, \dots, x_{n-r})$$

est un isomorphisme. Donc, $\dim(\text{Ker } f) = \dim(E) = n - r$.

D'après le théorème du rang,

$$\text{rg}(A) = \text{rg}(f) = \dim(\mathbb{K}^n) - \dim(\text{Ker } f) = n - (n - r) = r.$$

□

Définition: Soit $A = (a_{i,j})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq n}} \in \mathcal{M}_{p,n}(\mathbb{K})$.

La transposée de A , notée ${}^t A = (b_{j,i})_{\substack{1 \leq j \leq n \\ 1 \leq i \leq p}} \in \mathcal{M}_{n,p}(\mathbb{K})$ est définie par

$$\forall i \in [\![1, p]\!], \forall j \in [\![1, n]\!], b_{j,i} = a_{i,j}.$$

Les lignes de ${}^t A$ sont les colonnes de A . Les colonnes de ${}^t A$ sont les lignes de A .

EXEMPLE:
 $A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \\ 3 & -1 \end{pmatrix}$ donc ${}^t A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & -1 \end{pmatrix}$.

Corollaire:

$$\forall A \in \mathcal{M}_{n,p}(\mathbb{K}), \operatorname{rg}(A) = \operatorname{rg}({}^t A)$$

□

Proposition: $\begin{array}{ccc} \mathcal{M}_n(\mathbb{K}) & \longrightarrow & \mathcal{M}_n(\mathbb{K}) \\ A & \mapsto & {}^t A \end{array}$ est la symétrie par rapport à $S_n(\mathbb{K})$ parallèlement à $A_n(\mathbb{K})$ où

$$S_n(\mathbb{K}) = \{A \in \mathcal{M}_n(\mathbb{K}) \mid {}^t A = A\} = \left(\begin{array}{c|c} & \overbrace{\hspace{1cm}}^{(u)} \\ \diagdown & \diagup \\ \diagup & \diagdown \\ & \overbrace{\hspace{1cm}}^{(u)} \end{array} \right)$$

et

$$A_n(\mathbb{K}) = \{A \in \mathcal{M}_n(\mathbb{K}) \mid {}^t A = -A\} = \left(\begin{array}{c|c} 0 & \overbrace{\hspace{1cm}}^{(u)} \\ \dots & \dots \\ \diagup & \diagdown \\ \diagdown & \diagup \\ (-u) & \end{array} \right)$$

et donc

$$S_n(\mathbb{K}) \oplus A_n(\mathbb{K}) = \mathcal{M}_n(\mathbb{K}).$$

Preuve:

Soient $A = (a_{i,j})$, $B = (b_{i,j})$ et $(\alpha, \beta) \in \mathbb{K}^2$.

$$\begin{aligned} {}^t(\alpha A + \beta B) &= (\alpha a_{j,i} + \beta b_{j,i})_{1 \leq i, j \leq n} = \alpha(a_{j,i}) + \beta(b_{j,i}) \\ &= \alpha {}^t A + \beta {}^t B \end{aligned}$$

Clairement,

$$\forall A \in \mathcal{M}_n(\mathbb{K}), {}^t({}^t A) = A$$

donc $f : A \mapsto {}^t A$ est la symétrie par rapport à $\operatorname{Ker}(f - \operatorname{id}_{\mathcal{M}_n(\mathbb{K})})$ parallèlement à $\operatorname{Ker}(f + \operatorname{id}_{\mathcal{M}_n(\mathbb{K})})$.

Or,

$$\begin{aligned} \operatorname{Ker}(f - \operatorname{id}_{\mathcal{M}_n(\mathbb{K})}) &= \{A \in \mathcal{M}_n(\mathbb{K}) \mid f(A) - A = 0\} \\ &= \{A \in \mathcal{M}_n(\mathbb{K}) \mid {}^t A = A\} \\ &= S_n(\mathbb{K}) \end{aligned}$$

et

$$\begin{aligned} \operatorname{Ker}(f + \operatorname{id}_{\mathcal{M}_n(\mathbb{K})}) &= \{A \in \mathcal{M}_n(\mathbb{K}) \mid f(A) + A = 0\} \\ &= \{A \in \mathcal{M}_n(\mathbb{K}) \mid {}^t A = A\} \\ &= A_n(\mathbb{K}) \end{aligned}$$

□

Proposition: Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B \in \mathcal{M}_{p,q}(\mathbb{K})$.

$${}^t(AB) = {}^tB {}^tA$$

Preuve:

On pose

$$\begin{cases} A = (a_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} \\ B = (b_{j,k})_{\substack{1 \leq j \leq p \\ 1 \leq k \leq q}} \\ {}^tB {}^tA = (c_{k,i})_{\substack{1 \leq k \leq q \\ 1 \leq i \leq n}} \end{cases}$$

$$\begin{aligned} \forall k \in \llbracket 1, q \rrbracket, \forall i \in \llbracket 1, n \rrbracket, c_{k,i} &= \sum_{j=1}^p ({}^tB)_{k,j} ({}^tA)_{j,i} \\ &= \sum_{j=1}^p b_{j,k} a_{i,j} \\ &= \sum_{j=1}^p a_{i,j} b_{j,k} \\ &= (AB)_{i,k} \\ &= ({}^t(AB))_{k,i} \end{aligned}$$

Donc, ${}^t(AB) = {}^tB {}^tA$.

□

Corollaire: Si $A \in \mathrm{GL}_n(\mathbb{K})$ alors ${}^tA \in \mathrm{GL}_n(\mathbb{K})$ et

$$({}^tA)^{-1} = {}^t(A^{-1})$$

Preuve:

On suppose $A \in \mathrm{GL}_n(\mathbb{K})$.

$$AA^{-1} = I_n \text{ donc } {}^t(AA^{-1}) = {}^tI_n$$

$$\text{donc } {}^t(A^{-1}){}^tA = I_n$$

donc

$${}^tA \in \mathrm{GL}_n(\mathbb{K}) \quad {}^t(A^{-1}) = ({}^tA)^{-1}$$

□

6 Matrices par blocs

EXEMPLE:

Soit p un projecteur de E :

$$E = \mathrm{Ker} p \oplus \mathrm{Im} p$$

Soit $\mathcal{B} = (e_1, \dots, e_k, e_{k+1}, \dots, e_n)$ une base de E avec $\begin{cases} \text{Im}(p) = \text{Vect}(e_1, \dots, e_k) \\ \text{Ker}(p) = \text{Vect}(e_{k+1}, \dots, e_n) \end{cases}$

Alors,

$$\text{Mat}_{\mathcal{B}}(p) = \left(\begin{array}{c|cc} 1 & 0 & \dots & 0 \\ \dots & \vdots & \ddots & \vdots \\ & 0 & \dots & 0 \\ \hline 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{array} \right) = \left(\begin{array}{c|c} I_k & 0 \\ 0 & 0 \end{array} \right)$$

De même, si δ est une symétrie de E ,

$$E = \text{Ker}(\delta - \text{id}_E) \oplus \text{Ker}(\delta + \text{id}_E).$$

Soit $\mathcal{C} = (e'_1, \dots, e'_\ell, e'_{\ell+1}, \dots, e'_n)$ avec $\begin{cases} \text{Vect}(e'_1, \dots, e'_\ell) = \text{Ker}(\delta - \text{id}_E), \\ \text{Vect}(e'_{\ell+1}, \dots, e'_n) = \text{Ker}(\delta + \text{id}_E). \end{cases}$

Alors

$$\text{Mat}_{\mathcal{C}}(\delta) = \left(\begin{array}{c|c} I_\ell & 0 \\ 0 & -I_{n-\ell} \end{array} \right)$$

Proposition: Soient F et G supplémentaires dans E :

$$E = F \oplus G.$$

Soit $f \in \mathcal{L}(F)$ et $g \in \mathcal{L}(G)$. Alors

$$\exists ! h \in \mathcal{L}(E) \quad h|_F = f, \quad h|_G = g \quad \text{et} \quad h = f \circ p + g \circ q$$

où $\begin{cases} p \text{ est la projection sur } F \text{ parallèlement à } G \\ q \text{ est la projection sur } G \text{ parallèlement à } F \end{cases}$

On a aussi $q = \text{id}_E - p$.

Preuve: ANALYSE Soit $h \in \mathcal{L}(E)$ tel que $\begin{cases} h|_F = f \\ h|_G = g \end{cases}$.

Soit $x \in E$. Alors

$$x = \underbrace{p(x)}_{\in F} + \underbrace{q(x)}_{\in G}$$

Donc,

$$\begin{aligned} h(x) &= h(p(x)) + h(q(x)) \\ &= f(p(x)) + g(q(x)) \\ &= (f \circ p + g \circ q)(x) \end{aligned}$$

Si h existe, alors

$$h = f \circ p + g \circ q$$

SYNTHÈSE On pose $h = f \circ p + g \circ q$.

p, q, f et g sont linéaires donc h aussi.

Soit $x \in E$.

$$\begin{aligned} h(x) &= f(p(x)) + g(q(x)) \\ &= f(x) + g(0_E) \\ &= f(x) \end{aligned}$$

donc $h|_F = f$ et de même $h|_G = g$.

□

Proposition: On reprend les notations et hypothèses précédentes. Soit (e_1, \dots, e_p) une base de F , et (f_1, \dots, f_q) une base de G . Alors, $\mathcal{B} = (e_1, \dots, e_p, f_1, \dots, f_q)$ est une base de E et

$$\text{Mat}_{\mathcal{B}}(h) = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array} \right)$$

où $\begin{cases} A = \text{Mat}_{(e_1, \dots, e_p)}(f) \\ B = \text{Mat}_{(f_1, \dots, f_q)}(g) \end{cases}$

□

Proposition: Soient $(A, A') \in \mathcal{M}_n(\mathbb{K})^2$ et $(B, B') \in \mathcal{M}_p(\mathbb{K})^2$.

1.

$$\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array} \right) \left(\begin{array}{c|c} A' & 0 \\ \hline 0 & B' \end{array} \right) = \left(\begin{array}{c|c} AA' & 0 \\ \hline 0 & BB' \end{array} \right)$$

2.

$$\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array} \right) \in \text{GL}_{n+p}(\mathbb{K}) \iff \begin{cases} A \in \text{GL}_n(\mathbb{K}) \\ B \in \text{GL}_p(\mathbb{K}) \end{cases}$$

et dans ce cas,

$$\left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array} \right)^{-1} = \left(\begin{array}{c|c} A^{-1} & 0 \\ \hline 0 & B^{-1} \end{array} \right)$$

3.

$$\text{tr} \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array} \right) = \text{tr } A + \text{tr } B$$

Preuve: 1. Soit $\{f \in \mathcal{L}(F) \text{ tel que } \text{Mat}_{\mathcal{B}}(f) = A, f' \in \mathcal{L}(F) \text{ tel que } \text{Mat}_{\mathcal{B}}(f') = A', g \in \mathcal{L}(G) \text{ tel que } \text{Mat}_{\mathcal{C}}(g) = B, g'$

où $\begin{cases} F \oplus G = \mathbb{K}^{n+p}, \\ \dim(F) = n, \dim(G) = p, \\ \mathcal{B} \text{ base de } F, \\ \mathcal{C} \text{ base de } G. \end{cases}$ Soit $\begin{cases} h \in \mathcal{L}(\mathbb{K}^{n+p}) \text{ tel que } \begin{cases} h|_F = f \\ h|_G = g \end{cases} \\ h' \in \mathcal{L}(\mathbb{K}^{n+p}) \text{ tel que } \begin{cases} h'|_F = f' \\ h'|_G = g' \end{cases} \end{cases}$

Soit $\mathcal{D} = \mathcal{B} \cup \mathcal{C}$ une base de \mathbb{K}^{n+p} .

$$\begin{aligned} \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array} \right) \left(\begin{array}{c|c} A' & 0 \\ \hline 0 & B' \end{array} \right) &= \text{Mat}_{\mathcal{D}}(h) \text{Mat}_{\mathcal{D}}(h') \\ &= \text{Mat}_{\mathcal{D}}(h \circ h') \end{aligned}$$

Or, $(h \circ h')|_F = f \circ f'$ et $(h \circ h')|_G = g \circ g'$.

Donc,

$$\begin{aligned}\text{Mat}_{\mathcal{D}}(h \circ h') &= \left(\begin{array}{c|c} \text{Mat}_{\mathcal{B}}(f \circ f') & 0 \\ 0 & \text{Mat}_{\mathcal{C}}(g \circ g') \end{array} \right) \\ &= \left(\begin{array}{c|c} AA' & 0 \\ 0 & BB' \end{array} \right).\end{aligned}$$

□

Proposition: Soient $A, A' \in \mathcal{M}_n(\mathbb{K})$, $B, B' \in \mathcal{M}_{n,p}(\mathbb{K})$, $C, C' \in \mathcal{M}_{p,n}(\mathbb{K})$ et $D, D' \in \mathcal{M}_p(\mathbb{K})$.

$$\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array} \right) \left(\begin{array}{c|c} A' & B' \\ \hline C' & D' \end{array} \right) = \left(\begin{array}{c|c} AA' + BC' & AB' + BD' \\ \hline CA' + DC' & CB' + DD' \end{array} \right)$$

Cette formule se généralise à un nombre quelconque de blocs :

$$\left(\begin{array}{c|c|c|c} A_{11} & A_{12} & \cdots & A_{1,n} \\ \hline A_{21} & A_{22} & \cdots & A_{2,n} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline A_{p,1} & A_{p,2} & \cdots & A_{p,n} \end{array} \right) \left(\begin{array}{c|c|c|c} A'_{11} & A'_{12} & \cdots & A'_{1,n} \\ \hline A'_{21} & A'_{22} & \cdots & A'_{2,n} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline A'_{p,1} & A'_{p,2} & \cdots & A'_{p,n} \end{array} \right)$$

Cette matrice se calcyle comme on s'y attend si les dimensions des blocs autorisent les produits.

$$\begin{array}{ccc} \mathbb{C}_{\mathcal{B}}^2 & \xrightarrow[A]{f} & \mathbb{C}_{\mathcal{B}}^2 \\ \downarrow \text{id}_{\mathbb{C}^2} P & \nearrow \text{id}_{\mathbb{C}^2} P & \downarrow \text{id}_{\mathbb{C}^2} P \\ \mathbb{C}_{\mathcal{C}}^2 & \xrightarrow[D]{f} & \mathbb{C}_{\mathcal{C}}^2 \end{array}$$

Proposition: Le rang d'une matrice A , c'est la taille de la plus grande matrice carrée inversible que l'on peut extraire de A . □

CHAPITRE

22

FONCTIONS DE DEUX VARIABLES

1 Quelques généralités

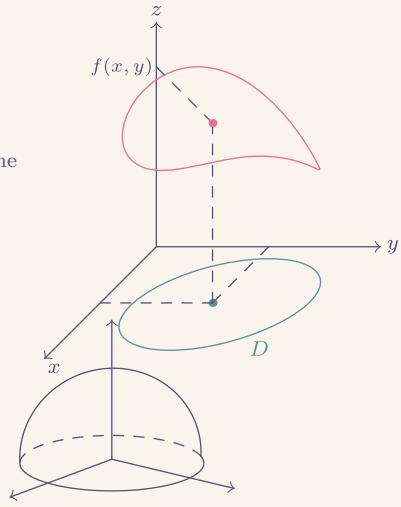
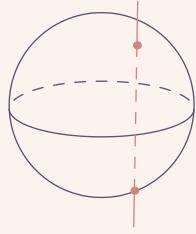
On s'intéresse dans ce chapitre à des fonctions définies sur une partie D de \mathbb{R}^2 à valeurs dans \mathbb{R} .

Par exemple,

$$f : (x, y) \mapsto 5xy + \sqrt{x^2 + y^2}$$

Une sphère n'est pas la surface représentative d'une fonction. Mais, une demi-sphère oui :

$$f : (x, y) \mapsto \sqrt{1 - x^2 - y^2}.$$



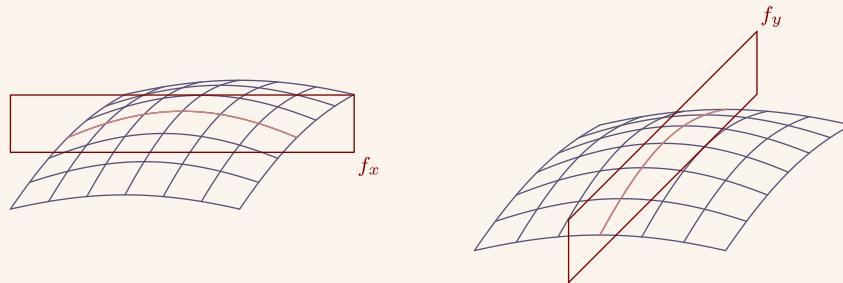
La surface de la demisphère est

$$S = \{(x, y, f(x, y)) \mid (x, y) \in D_O(1)\}.$$

où $D_O(1)$ est le disque unitaire à l'origine.

POINTDEVUENAÏF

Soit $f : D \subset \mathbb{R}^2 \rightarrow \mathbb{R}^2$. On fixe y et on étudie $f_y : x \mapsto f(x, y)$. Ou, on fixe x et on étudie $f_x : y \mapsto f(x, y)$.



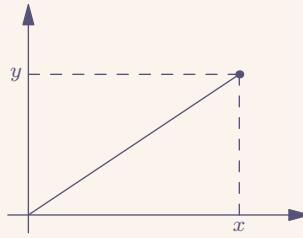
LEBONPOINTDEVUE

On reprend les notions d'une fonction d'une seule variable (limite, continuité, développement limité, ...) que l'on adapte aux fonctions à deux variables.

2 Topologie de \mathbb{R}^2

Définition: La norme (euclidienne) de \mathbb{R}^2 est l'application définie par

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



Proposition: La norme euclidienne vérifie :

1. (séparation)

$$\forall (x, y) \in \mathbb{R}^2, \|(x, y)\| = 0 \iff x = y = 0,$$

2. (homogénéité positive)

$$\forall \lambda \in \mathbb{R}, \forall (x, y) \in \mathbb{R}^2, \|\lambda(x, y)\| = |\lambda| \|(x, y)\|$$

3. (inégalité triangulaire)

$$\forall (x, y), (a, b) \in \mathbb{R}^2, \|(x, y) + (a, b)\| \leq \|(x, y)\| + \|(a, b)\|.$$

Preuve:

Déjà vue en remplaçant (x, y) par $x + iy \in \mathbb{C}$ et $\|(x, y)\|$ par $|x+iy|$

□

Définition: Soit $(a, b) \in \mathbb{R}^2$ et $r \in \mathbb{R}_+$.

La boule ouverte (ou disque ouvert) de centre (a, b) et de rayon r est

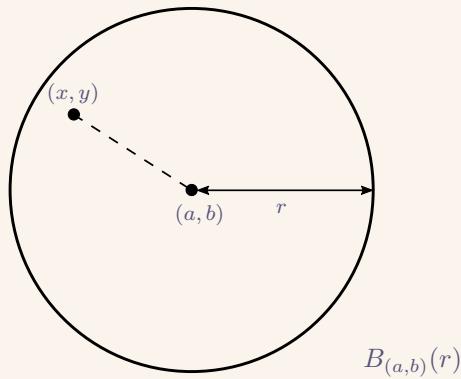
$$B_{(a,b)}(r) = \{(x, y) \in \mathbb{R}^2 \mid \|(x, y) - (a, b)\| < r\}.$$

La boule fermée (ou disque fermé) de centre (a, b) et de rayon r est

$$\overline{B_{(a,b)}}(r) = \{(x, y) \in \mathbb{R}^2 \mid \|(x, y) - (a, b)\| \leq r\}.$$

La sphère (ou boule) de centre (a, b) et de rayon r est

$$S_{(a,b)}(r) = \partial \overline{B_{(a,b)}}(r) = \{(x, y) \in \mathbb{R}^2 \mid \|(x, y) - (a, b)\| = r\}.$$



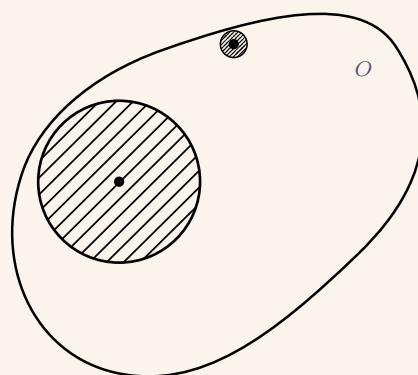
REMARQUE:

On parle de boule en dimension quelconque.

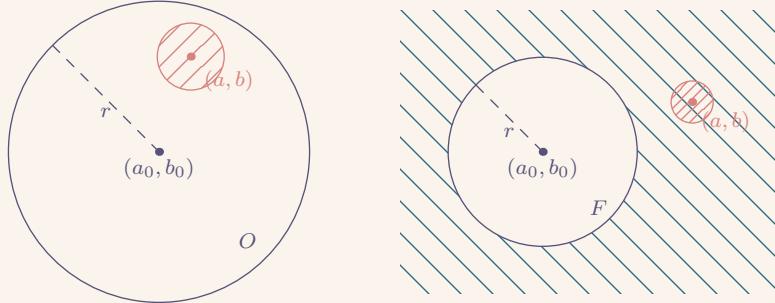
Définition: Une partie ouverte O de \mathbb{R}^2 (ou un ouvert) si

$$\forall (x, y) \in O, \exists r > 0, B_{(a,b)}(r) \subset O.$$

Une partie F est fermée si $\mathbb{R}^2 \setminus F$ est ouverte.



Proposition: Une boule ouverte est ouverte. Une boule fermée est fermée.



Preuve:

\emptyset est un ouvert.

Soit B la boule ouverte de centre $(a_0, b_0) \in \mathbb{R}^2$ et de rayon $r > 0$.

On pose $\rho = \frac{1}{2}(r - \|(a, b) - (a_0, b_0)\|)$. Montrons que

$$B_{(a,b)}(\rho) \subset B_{(a,b)}(r).$$

Soit $(x, y) \in B_{(a,b)}(\rho)$.

$$\begin{aligned} \|(x, y) - (a_0, b_0)\| &= \|(x, y) - (a, b) + (a, b) - (a_0, b_0)\| \\ &\leq \|(x, y) - (a, b)\| + \|(a, b) - (a_0, b_0)\| \\ &< \rho + \|(a, b) - (a_0, b_0)\| = \frac{1}{2}r + \frac{1}{2}\|(a, b) - (a_0, b_0)\| \\ &< r \end{aligned}$$

Soit F la boule fermée de centre (a_0, b_0) et de rayon $r \geq 0$.

Soit $(a, b) \notin F$. On pose

$$\rho = \frac{1}{2}(\|(a, b) - (a_0, b_0)\| - r) > 0.$$

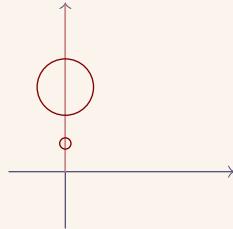
Montrons que $B_{(a,b)}(\rho) \subset \mathbb{R}^2 \setminus F$.

Soit $(x, y) \in B_{(a,b)}(\rho)$.

$$\begin{aligned} \|(x, y) - (a_0, b_0)\| &= \|(x, y) - (a, b) + (a, b) - (a_0, b_0)\| \\ &\geq \left| \underbrace{\|(x, y) - (a, b)\|}_{\leq \rho} - \underbrace{\|(a, b) - (a_0, b_0)\|}_{> r} \right| \\ &\geq \|(a, b) - (a_0, b_0)\| - \|(x, y) - (a, b)\| \\ &> \|(a, b) - (a_0, b_0)\| - \rho \\ &> \frac{1}{2}\|(a, b) - (a_0, b_0)\| + \frac{1}{2}r \\ &> r \end{aligned}$$

donc $(x, y) \notin F$. □

- EXEMPLE:**
1. \emptyset est ouvert.
 \mathbb{R}^2 est ouvert.
 2. \emptyset est fermé.
 \mathbb{R}^2 est fermé.
 3. $\{(x, 0) \mid x > 0\}$ n'est ni ouverte ni fermée.



Définition: Soit $(a, b) \in \mathbb{R}^2$ et $V \in \mathcal{P}(\mathbb{R}^2)$.

On dit que V est un voisinage de (a, b) s'il existe $r > 0$ tel que

$$B_{(a,b)}(r) \subset V.$$

Proposition: Un ouvert non vide est un voisinage en chacun de ces points. □

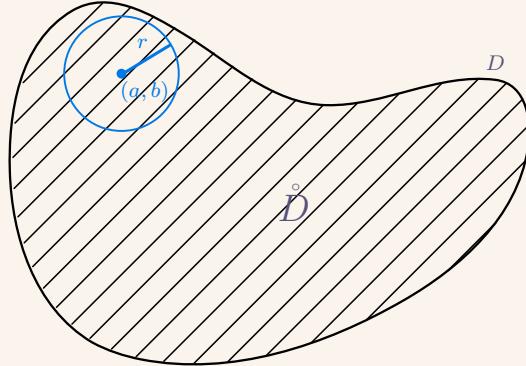
Définition: Soit $D \subset \mathbb{R}^2$. Un point intérieur de D est un couple $(a, b) \in D$ tel que

$$\exists r > 0, B_{(a,b)}(r) \subset D.$$

en d'autres termes, si D est un voisinage de (a, b) .

On note \mathring{D} l'ensemble des points intérieurs à D . C'est l'intérieur de D .

Proposition: \mathring{D} est le plus grand ouvert O de \mathbb{R}^2 tel que $O \subset D$.



Preuve:

Soit $(a, b) \in \overset{\circ}{D}$.

Par définition, il existe $r > 0$ tel que

$$B_{(a,b)}(r) \subset D.$$

Montrons que $B_{(a,b)}(r) \subset \overset{\circ}{D}$.

Soit $(x, y) \in B_{(a,b)}(r)$. Comme $B_{(a,b)}(r)$ est un ouvert de \mathbb{R}^2 , il existe $\rho > 0$ tel que

$$B_{(x,y)}(\rho) \subset B_{(a,b)}(r)$$

donc $(x, y) \in \overset{\circ}{D}$.

Donc $\overset{\circ}{D}$ est ouvert, $\overset{\circ}{D} \subset D$.

Soit O un ouvert de \mathbb{R}^2 tel que $O \subset D$. Montrons que $O \subset \overset{\circ}{D}$.

Soit $(x, y) \in O$. Soit $r > 0$ tel que

$$B_{(x,y)}(r) \subset O \subset D$$

donc $(x, y) \in \overset{\circ}{D}$. □

Définition: Soit $f : D \subset \mathbb{R}^2 \rightarrow \mathbb{R}$, $\ell \in \mathbb{R}$, $(a, b) \in \overset{\circ}{D}$.

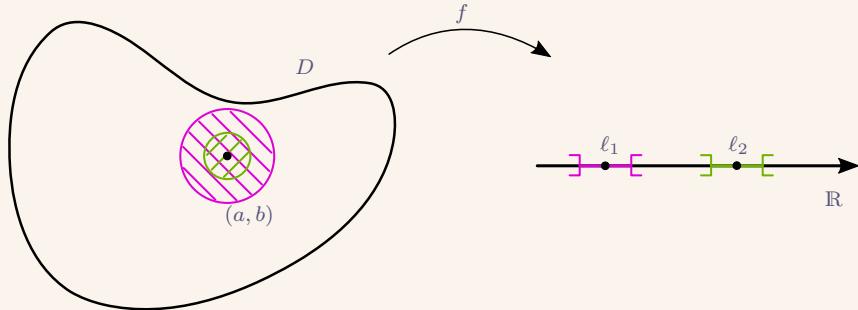
On dit que $f(x, y)$ tend vers ℓ quand (x, y) tend vers (a, b) ou que ℓ est une limite de f en (a, b) si

$$\forall \varepsilon > 0, \exists r > 0, \forall (x, y) \in D, \|(x, y) - (a, b)\| < r \implies |f(x, y) - \ell| < \varepsilon.$$

en d'autres termes si

$$\forall V \in \mathcal{V}_\ell, \exists W \in \mathcal{V}_{(a,b)}, \forall (x, y) \in W \cap D, f(x, y) \in V.$$

Proposition (unicité de la limite): Soit $f : D \rightarrow \mathbb{R}$, $(a, b) \in \overset{\circ}{D}$, $\ell_1, \ell_2 \in \mathbb{R}$ telles que ℓ_1 et ℓ_2 sont des limites de f en (a, b) .
Alors $\ell_1 = \ell_2$.



Preuve:

On suppose $\ell_1 < \ell_2$. On pose $\varepsilon = \frac{\ell_2 - \ell_1}{2} > 0$.

Soit $r_1 > 0$ tel que

$$f(B_{(a,b)}(r_1)) \subset]\ell_1 - \varepsilon, \ell_1 + \varepsilon[.$$

Soit $r_2 > 0$ tel que

$$f(B_{(a,b)}(r_2)) \subset]\ell_2 - \varepsilon, \ell_2 + \varepsilon[.$$

On pose $r = \min(r_1, r_2)$ donc

$$B_{(a,b)}(r_1) \cap B_{(a,b)}(r_2) = B_{(a,b)}(r) \neq \emptyset.$$

Soit $(x, y) \in B_{(a,b)}(r)$. Alors,

$$f(x, y) \in]\ell_1 - \varepsilon, \ell_1 + \varepsilon[\cap]\ell_2 - \varepsilon, \ell_2 + \varepsilon[= \emptyset.$$

□

Définition: Soit $f : D \rightarrow \mathbb{R}$, $(a, b) \in \overset{\circ}{D}$.

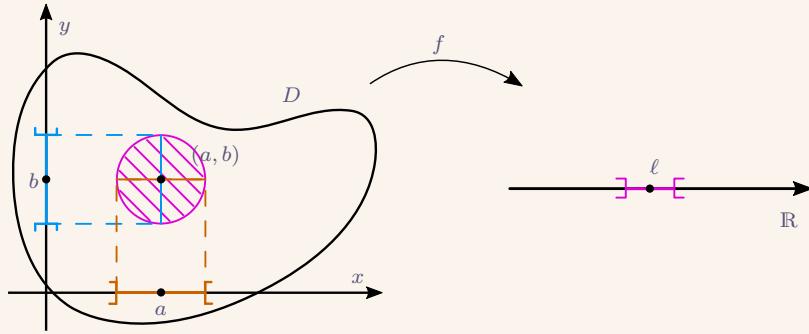
On dit que f est continue en (a, b) si

$$f(x, y) \xrightarrow{(x,y) \rightarrow (a,b)} f(a, b).$$

Proposition: Si $f(x, y) \xrightarrow{(x,y) \rightarrow (a,b)} \ell$

$$\left\| \text{alors} \begin{cases} f(x, b) \xrightarrow{x \rightarrow a} \ell \\ f(a, y) \xrightarrow{y \rightarrow b} \ell. \end{cases} \right.$$

Preuve:



□

Contre-exemple : exercice 3.

EXEMPLE: 1. $f : \begin{matrix} \mathbb{R}^2 \\ (x, y) \end{matrix} \longrightarrow \begin{matrix} \mathbb{R} \\ x \end{matrix}$ limite en $(0, 0)$?

Soit $\varepsilon > 0$. On pose $r = \varepsilon$.

$$\forall (x, y) \in B_{(0,0)}(r), |f(x, y)| = |x| \leq \| (x, y) \| < r = \varepsilon$$

Donc $f(x, y) \xrightarrow{(x,y) \rightarrow (a,b)} 0$.

2. limite $f : \begin{matrix} \mathbb{R}^2 \\ (x, y) \end{matrix} \longrightarrow \begin{matrix} \mathbb{R} \\ x^3 \end{matrix}$ en $(0, 0)$?

Soit $\varepsilon > 0$. On pose $r = \sqrt[3]{\varepsilon} > 0$.

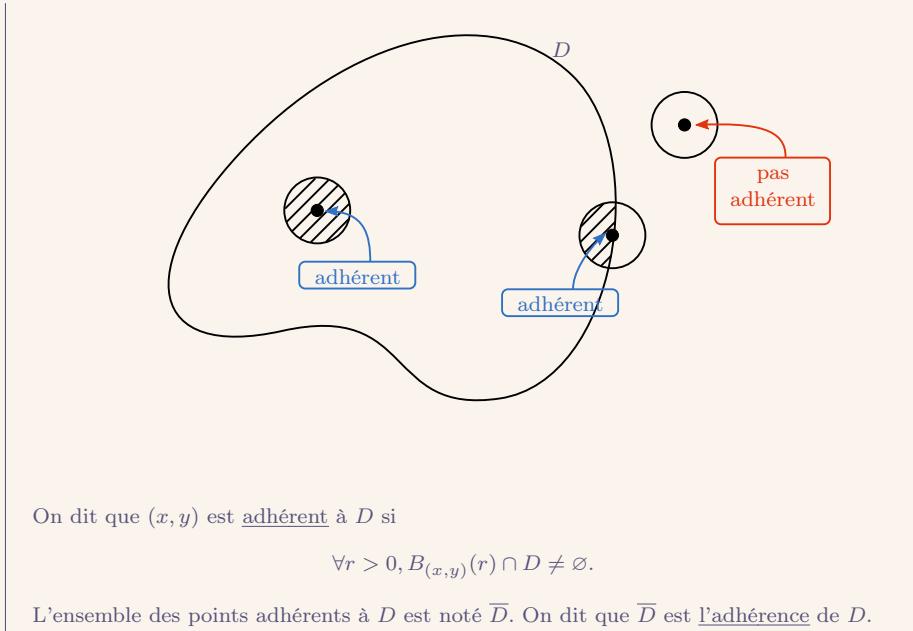
$$\forall (x, y) \in B_{(0,0)}(r), |f(x, y)| = |x^3| \leq \| (x, y) \|^3 < r^3 = \varepsilon$$

3. limite de $f : \begin{matrix} \mathbb{R}^2 \\ (x, y) \end{matrix} \longrightarrow \begin{matrix} \mathbb{R} \\ x^3 y^2 \end{matrix}$ en $(0, 0)$?

Soit $\varepsilon > 0$. On pose $r = \sqrt[5]{\varepsilon} > 0$.

$$\forall (x, y) \in B_{(0,0)}(r), |f(x, y)| = |x^3 y^2| \leq \| (x, y) \|^3 \| (x, y) \|^2 < r^5 = \varepsilon$$

Définition: Soient $D \subset \mathbb{R}^2$ et $(x, y) \in \mathbb{R}^2$.



Définition: Soit $f : D \subset \mathbb{R}^2 \rightarrow \mathbb{R}$ et $(a, b) \in \overline{D}$, $\ell \in \mathbb{R}$. On dit que f tend vers ℓ quand (x, y) tend vers (a, b) si

$$\forall \varepsilon > 0, \exists r > 0, \forall (x, y) \in B_{(a,b)}(r) \cap D, |f(x, y) - \ell| \leq \varepsilon.$$

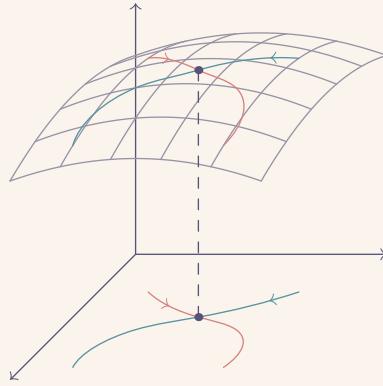
- Proposition:**
1. Dans ce contexte, il y a unicité de la limite
 2. La limite d'une somme, d'un produit, d'un quotient, d'une composée se comporte comme dans le cas d'une seule variable.
 3. Soit $f : D \rightarrow \mathbb{R}$ continue. Soient $g : I \rightarrow \mathbb{R}$ et $h : I \rightarrow \mathbb{R}$ continues telles que

$$\forall t \in I, (g(t), h(t)) \in D.$$

Alors

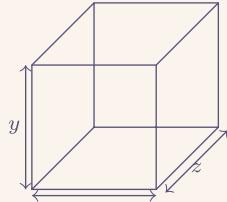
$$t \in I \mapsto f(g(t), h(t)) \in \mathbb{R}$$

est continue.



3 Dérivation

Motivation :



$$S(x, y, z) = 2(xy + xz + yz)$$

$$V(x, y, z) = xyz$$

On cherche à minimiser S avec la contrainte $V = 1$.

$$\text{Soit } f : \begin{array}{ccc} (\mathbb{R}_*)^2 & \longrightarrow & \mathbb{R} \\ (x, y) & \mapsto & S\left(x, y, \frac{1}{xy}\right) = 2\left(xy + \frac{1}{y} + \frac{1}{x}\right). \end{array}$$

On cherche $(a, b) \in (\mathbb{R}_*)^2$ tel que

$$\forall (x, y) \in (\mathbb{R}_*)^2, f(x, y) \geq f(a, b).$$

Définition: Soit $f : U \rightarrow \mathbb{R}$ où U est un ouvert de \mathbb{R}^2 . Soit $(a, b) \in U$.

Si $\lim_{x \rightarrow a} \frac{f(x, b) - f(a, b)}{x - a} \in \mathbb{R}$, alors on dit que f a une dérivée partielle suivant x en (a, b) et cette limite est notée

$$\partial f_1(a, b) = \frac{\partial f}{\partial x}(a, b).$$

Si $\lim_{y \rightarrow b} \frac{f(a, y) - f(a, b)}{y - b} \in \mathbb{R}$, alors on dit que f a une dérivée partielle suivant y en (a, b) et la limite est notée

$$\partial f_2(a, b) = \frac{\partial f}{\partial y}(a, b).$$

EXEMPLE: 1. $f : (x, y) \mapsto xy + x - y$.

$$\frac{\partial f}{\partial x} : (x, y) \mapsto y + 1,$$

$$\frac{\partial f}{\partial y} : (x, y) \mapsto x - 1.$$

2. $f : (x, y) \mapsto xy + \frac{1}{y} + \frac{1}{x}$.

$$\begin{aligned}\frac{\partial f}{\partial x} : (x, y) \mapsto y - \frac{1}{x^2}, \\ \frac{\partial f}{\partial y} : (x, y) \mapsto x - \frac{1}{y^2}.\end{aligned}$$

3. Trouver f telle que $\begin{cases} (1) : & \frac{\partial f}{\partial x} = y, \\ (2) : & \frac{\partial f}{\partial y} = x. \end{cases}$

D'après (1) :

$$\forall (x, y), \exists C(y) \in \mathbb{R}, f(x, y) = xy + C(y)$$

et donc

$$\frac{\partial f}{\partial y}(x, y) = x + C'(y)$$

donc $C'(y) = 0$ et donc C est constante.

4. Trouver f telle que $\begin{cases} \frac{\partial f}{\partial x} = -y, \\ \frac{\partial f}{\partial y} = x. \end{cases}$

Ce n'est pas possible !

Définition:

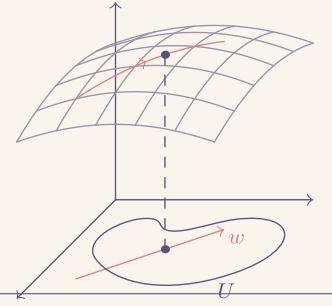
Soit $f : U \rightarrow \mathbb{R}$ où U est un ouvert. Soit $(a, b) \in U$. Soit $w = (w_1, w_2) \in \mathbb{R}^2$.

Si

$$\lim_{t \rightarrow 0} \frac{f(a + tw_1, b + tw_2) - f(a, b)}{t}$$

existe et est réelle, alors on dit que f a une dérivée dans la direction de w et la limite est notée

$$df(w)(a, b) = D_w(f)(a, b).$$



EXEMPLE:

$$\begin{aligned}f : (\mathbb{R}_*^+)^2 &\longrightarrow \mathbb{R} \\ (x, y) &\longmapsto xy + \frac{1}{x} + \frac{1}{y}.\end{aligned}$$

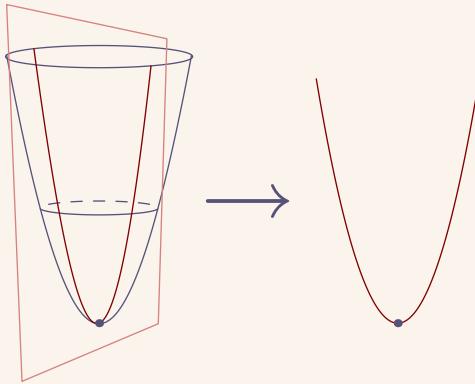
On pose $(a, b) = (1, 2)$, $w = (w_1, w_2) = (1, 1)$.

$$\begin{aligned}\frac{f(1+t, 2+t) - f(1, 2)}{t} &= \frac{1}{t} \left((1+t)(2+t) + \frac{1}{1+t} + \frac{1}{2+t} - 3 - \frac{1}{2} \right) \\ &= \frac{1}{t} \left(2 + 3t + o(t) + 1 - t + o(t) + \frac{1}{2} \left(1 - \frac{t}{2} + o(t) \right) - 3 - \frac{1}{2} \right) \\ &= \frac{1}{t} \left(\frac{7}{4}t + o(t) \right) \\ &= \frac{7}{4} + o(1) \xrightarrow[t \rightarrow 0]{} \frac{7}{4}.\end{aligned}$$

Donc,

$$df(1, 1)(1, 2) = \frac{7}{4}.$$

REMARQUE:



Théorème: Soit $f : U \rightarrow \mathbb{R}$, $(a, b) \in U$. On suppose que $\frac{\partial f}{\partial x}$ et $\frac{\partial f}{\partial y}$ existent en (a, b) et sont **continues** en (a, b) . Alors,

$$\forall (h, k) \in \mathbb{R}^2 \text{ tel que } (a+h, b+k) \in U, \\ f(a+h, b+k) = f(a, b) + h \frac{\partial f}{\partial x}(a, b) + k \frac{\partial f}{\partial y}(a, b) + \underset{(h, k) \rightarrow (0, 0)}{\mathcal{O}} (\|(h, k)\|).$$

On dit que f est de classe \mathcal{C}^1 si $\frac{\partial f}{\partial x}$ et $\frac{\partial f}{\partial y}$ existent et sont continues.

□

REMARQUE:

En physique, cette formule correspond à :

$$df = \frac{\partial f}{\partial x} dx + \frac{\partial f}{\partial y} dy.$$

En effet :

$$df = f(x + dx, y + dy) - f(x, y) \\ = \frac{\partial f}{\partial x} dx + \frac{\partial f}{\partial y} dy.$$

Proposition: Soit $f : U \rightarrow \mathbb{R}$ de classe \mathcal{C}^1 en $(a, b) \in U$. Alors,

$$\forall w = (w_1, w_2) \in \mathbb{R}^2, df(w)(a, b) = w_1 \frac{\partial f}{\partial x}(a, b) + w_2 \frac{\partial f}{\partial y}(a, b).$$

Preuve:

Soit $w = (w_1, w_2) \in \mathbb{R}^2$. Soit $t \in \mathbb{R}^*$.

$$\begin{aligned}\frac{1}{t}(f(a + tw_1, b + tw_2) - f(a, b)) &= \frac{1}{t} \left(tw_1 \frac{\partial f}{\partial x}(a, b) + tw_2 \frac{\partial f}{\partial y}(a, b) + \underset{t \rightarrow 0}{\mathcal{o}}(\|tw\|) \right) \\ &= w_1 \frac{\partial f}{\partial x}(a, b) + w_2 \frac{\partial f}{\partial y}(a, b) + \underset{t \rightarrow 0}{\mathcal{o}}(1) \\ &\xrightarrow[t \rightarrow 0]{} w_1 \frac{\partial f}{\partial x}(a, b) + w_2 \frac{\partial f}{\partial y}(a, b).\end{aligned}$$

□

Définition: Avec les hypothèses précédentes, en posant

$$\nabla f(a, b) = \left(\frac{\partial f}{\partial x}(a, b), \frac{\partial f}{\partial y}(a, b) \right)$$

on obtient

$$df(w)(a, b) = \langle w \mid \nabla f(a, b) \rangle$$

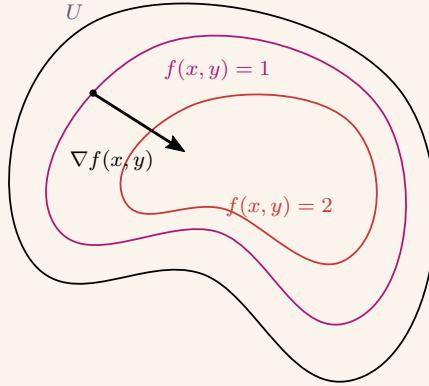
où $\langle \cdot, \cdot \rangle$ est le produit scalaire.

Le vecteur $\nabla f(a, b)$ est appelé gradient de f en (a, b) .

Le développement limité à l'ordre 1 de f devient

$$f((a, b) + w) = f(a, b) + \langle w \mid \nabla f(a, b) \rangle + \underset{w \rightarrow 0}{\mathcal{o}}(\|w\|)$$

Proposition: Soit $f : U \rightarrow \mathbb{R}$ de classe \mathcal{C}^1 .



∇f est orthogonal au lignes de niveaux de f , son orientation va dans le sens d'une augmentation de f .

Preuve:

Soit $\gamma : I \rightarrow U$ une courbe de niveau :

$$\forall t \in I, f(\gamma(t)) = \text{cste.}$$

D'après le lemme suivant :

$$\forall t \in I, 0 = (f \circ \gamma)'(t) = df(\gamma'(t))(\gamma(t)) = \langle \gamma'(t) | \nabla f(\gamma(t)) \rangle$$

Donc $\nabla f(\gamma(t))$ est orthogonal à $\gamma'(t)$.

Pour tout $t \in I$, on pose $w(t) = t \nabla f(\gamma(t))$. Donc

$$f(\gamma(t) + w(t)) = f(\gamma(t)) + t \|\nabla f(\gamma(t))\|^2 + \underset{t \rightarrow 0}{\circ}(t)$$

Pour t assez petit, $f(\gamma(t) + w(t)) - f(\gamma(t))$ est du même signe que t . \square

REMARQUE:

$$\begin{aligned} V : \mathbb{R}^3 &\longrightarrow \mathbb{R} \\ (x, y, z) &\longmapsto -mgz \end{aligned}$$

l'énergie potentielle de pesanteur

On a donc

$$\nabla V(x, y, z) = \left(\frac{\partial V}{\partial x}, \frac{\partial V}{\partial y}, \frac{\partial V}{\partial z} \right) = (0, 0, -mg) = \vec{P}.$$

Lemme: Soit $f : U \rightarrow \mathbb{R}$ de classe \mathcal{C}^1 , $\gamma : \begin{matrix} I \\ t \end{matrix} \xrightarrow{\quad} \begin{matrix} U \\ (x(t), y(t)) \end{matrix}$ où x et y sont dérivables.

On pose

$$\forall t \in I, \gamma'(t) = (x'(t), y'(t)).$$

Alors $f \circ \gamma : I \rightarrow \mathbb{R}$ est dérivable et

$$\begin{aligned} \forall t \in I, (f \circ \gamma)'(t) &= df(\gamma'(t))(\gamma(t)) \\ &= \langle \gamma'(t) | \nabla f(\gamma(t)) \rangle \\ &= x'(t) \frac{\partial f}{\partial x}(x(t), y(t)) + y'(t) \frac{\partial f}{\partial y}(x(t), y(t)). \end{aligned}$$

Preuve:

On fixe $t \in I$.

$$\begin{aligned} \forall h \neq 0, \frac{f \circ \gamma(t+h) - f \circ \gamma(t)}{h} &= \frac{1}{h} (f(\gamma(t)) + h\gamma'(t) + \underset{h \rightarrow 0}{\circ}(h) - f(\gamma(t))) \\ &= \frac{1}{h} \left(f(\gamma(t)) + \langle h\gamma'(t) | \nabla f(\gamma(t)) \rangle + \underset{h \rightarrow 0}{\circ} (\|h\gamma'(t)\|) - f(\gamma(t)) \right) \\ &= \langle \gamma'(t) | \nabla f(\gamma(t)) \rangle + \underset{h \rightarrow 0}{\circ}(1) \\ &\xrightarrow[h \rightarrow 0]{} \langle \gamma'(t) | \nabla f(\gamma(t)) \rangle \end{aligned}$$

\square

Définition: Soit $f : U \rightarrow \mathbb{R}$ de classe \mathcal{C}^1 et $(a, b) \in U$. On dit que (a, b) est un point critique de f si $\nabla f(a, b) = 0$ i.e. $\frac{\partial f}{\partial x}(a, b) = \frac{\partial f}{\partial y}(a, b) = 0$.

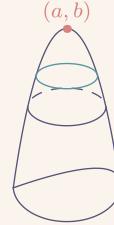
Dans ce cas, $f(a, b)$ est appelé valeur critique de f .

Proposition:

Soit $f : U \rightarrow \mathbb{R}$ de classe \mathcal{C}^1 et $(a, b) \in U$ tel que

$$\exists r > 0, \forall (x, y) \in B_{(a,b)}(r), f(x, y) \leq f(a, b)$$

Alors $\nabla f(a, b) = (0, 0)$.



Preuve:

Soit $g : x \mapsto f(x, b)$. $g(a)$ est un maximum local de g donc $g'(a) = 0$.

$$\text{Or, } g'(a) = \frac{\partial f}{\partial x}(a, b)$$

$$\text{donc } \frac{\partial f}{\partial x}(a, b) = 0.$$

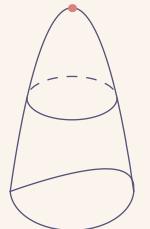
Soit $h : y \mapsto f(a, y)$. On a de même $h'(b) = 0$.

$$\text{Or, } h'(b) = \frac{\partial f}{\partial y}(a, b).$$

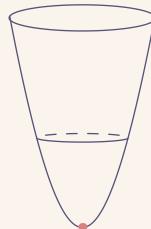
Donc, $\nabla f(a, b) = (0, 0)$. □

REMARQUE:

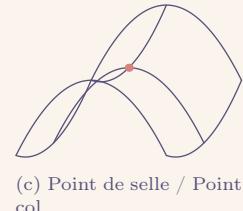
Un minimum local est aussi une valeur critique.



(a) Maximum local



(b) Minimum local



(c) Point de selle / Point col

EXEMPLE:

On revient à l'exemple donné en introduction :

$$\begin{aligned} f : (\mathbb{R}_+^*)^2 &\longrightarrow \mathbb{R} \\ (x, y) &\longmapsto 2 \left(xy + \frac{1}{x} + \frac{1}{y} \right). \end{aligned}$$

$(\mathbb{R}_+^*)^2$ est un ouvert de \mathbb{R}^2 . Soit $(x, y) \in (\mathbb{R}_+^*)^2$.

On a

$$\begin{cases} \frac{\partial f}{\partial x}(x, y) = 2 \left(y - \frac{1}{x^2} \right), \\ \frac{\partial f}{\partial y}(x, y) = 2 \left(x - \frac{1}{y^2} \right). \end{cases}$$

$$\begin{aligned}
& \frac{\partial f}{\partial x}(x, y) = \frac{\partial f}{\partial y}(x, y) = 0 \\
\iff & \begin{cases} y = \frac{1}{x^2} \\ x = \frac{1}{y^2} \end{cases} \\
\iff & \begin{cases} y = \frac{1}{x^2} \\ x = x^4 \end{cases} \\
\iff & \begin{cases} x = 1 \\ y = 1 \end{cases}
\end{aligned}$$

On vérifie que f présente en effet un minium local en $(1, 1)$.

$$f(1, 1) = 6$$

On fixe $y \in \mathbb{R}_*^+$ et

$$g : x \mapsto 2 \left(xy + \frac{1}{x} + \frac{1}{y} \right).$$

Donc

$$\forall x \in \mathbb{R}_*^+, g'(x) = 2 \left(y - \frac{1}{x^2} \right).$$

x	0	$\frac{1}{\sqrt{y}}$	$+\infty$
$g'(x)$	—	0	+
g		$2 \left(2\sqrt{y} + \frac{1}{y} \right)$	

Ainsi,

$$\forall x \in \mathbb{R}_*^+, \forall y \in \mathbb{R}_*^+, f(x, y) \geq 2 \left(2\sqrt{y} + \frac{1}{y} \right)$$

Soit $h : y \mapsto 2\sqrt{y} + \frac{1}{y}$. On a

$$\forall y > 0, h'(y) = \frac{1}{\sqrt{y}} - \frac{1}{y^2} = \frac{y\sqrt{y} - 1}{y^2} = \frac{y^{\frac{3}{2}} - 1}{y^2}$$

y	0	1	$+\infty$
$h'(y)$	—	0	+
h		3	

Donc,

$$\forall x, y > 0, f(x, y) \geq 2 \times 3 = 6 = f(1, 1).$$

Proposition (règle de la chaîne): Soit $f : \begin{matrix} U \\ (x, y) \end{matrix} \longrightarrow \begin{matrix} \mathbb{R}^2 \\ f(x, y) \end{matrix}$ de classe \mathcal{C}^1 et U, V deux ouverts de \mathbb{R}^2 .

$$\text{Soit } \varphi : \begin{matrix} V \\ (u, v) \end{matrix} \longrightarrow \begin{matrix} U \\ \varphi(u, v) = (x(u, v), y(u, v)) \end{matrix}.$$

On suppose que x et y sont de classe \mathcal{C}^1 sur V .

Alors, $f \circ \varphi : \begin{matrix} V \\ (u, v) \end{matrix} \longrightarrow \begin{matrix} \mathbb{R} \\ f(\varphi(u, v)) \end{matrix}$ est de classe \mathcal{C}^1 et

$$\begin{aligned} \forall (u_0, v_0) \in V, \frac{\partial(f \circ \varphi)}{\partial u}(u_0, v_0) &= \frac{\partial f}{\partial x}(\varphi(u_0, v_0)) \times \frac{\partial x}{\partial u}(u_0, v_0) \\ &\quad + \frac{\partial f}{\partial y}(\varphi(u_0, v_0)) \frac{\partial y}{\partial u}(u_0, v_0) \end{aligned}$$

$$\begin{aligned} \forall (u_0, v_0) \in V, \frac{\partial(f \circ \varphi)}{\partial v}(u_0, v_0) &= \frac{\partial f}{\partial x}(\varphi(u_0, v_0)) \times \frac{\partial x}{\partial v}(u_0, v_0) \\ &\quad + \frac{\partial f}{\partial y}(\varphi(u_0, v_0)) \frac{\partial y}{\partial v}(u_0, v_0) \end{aligned}$$

EXEMPLE (changement de coordonnées polaires):

On pose

$$\begin{aligned} \varphi : \mathbb{R}_*^+ \times]0, 2\pi[&\longrightarrow \mathbb{R}^2 \setminus (R_*^+ \times \{0\}) \\ (r, \theta) &\longmapsto (r \cos \theta, r \sin \theta), \end{aligned}$$

$$\begin{aligned} f : \mathbb{R}^2 \setminus (R_*^+ \times \{0\}) &\longrightarrow \mathbb{R} \\ (x, y) &\longmapsto f(x, y), \end{aligned}$$

$$\begin{aligned} g : \overbrace{\mathbb{R}_*^+ \times]0, 2\pi[}^{=V} &\longrightarrow \mathbb{R} \\ (r, \theta) &\longmapsto f(r \cos \theta, r \sin \theta). \end{aligned}$$

$$\forall (r_0, \theta_0) \in V,$$

$$\begin{aligned} \frac{\partial g}{\partial r}(r_0, \theta_0) &= \frac{\partial f}{\partial x}(r_0 \cos \theta_0, r_0 \sin \theta_0) \cos \theta_0 \\ &\quad + \frac{\partial f}{\partial y}(r_0 \cos \theta_0, r_0 \sin \theta_0) \sin \theta_0 \\ &= 2r_0 \cos^2 \theta_0 + 2r_0 \sin^2(\theta_0) \\ &= 2r_0 \end{aligned}$$

$$\begin{aligned} \frac{\partial g}{\partial \theta}(r_0, \theta_0) &= \frac{\partial f}{\partial x}(r_0 \cos \theta_0, r_0 \sin \theta_0) r_0 \sin \theta_0 \\ &\quad + \frac{\partial f}{\partial y}(r_0 \cos \theta_0, r_0 \sin \theta_0) r_0 \cos \theta_0 \\ &= -2r_0^2 \cos(\theta_0) \sin(\theta_0) + 2r_0^2 \sin(\theta_0) \cos(\theta_0) \\ &= 0 \end{aligned}$$

Donc,

$$g(r, \theta) = r^2.$$

EXEMPLE:
Résoudre

$$\begin{cases} \frac{\partial f}{\partial x} = \frac{x}{x^2 + y^2}, \\ \frac{\partial f}{\partial y} = \frac{y}{x^2 + y^2}. \end{cases}$$

On pose $g : (r, \theta) \mapsto f(r \cos \theta, r \sin \theta)$.

$$\begin{aligned} \frac{\partial g}{\partial r} &= \frac{1}{r} \cos^2 \theta + \frac{1}{r} \sin^2 \theta = \frac{1}{r}, \\ \frac{\partial g}{\partial \theta} &= -\cos(\theta) \sin(\theta) + \sin(\theta) \cos(\theta) = 0. \end{aligned}$$

Donc,

$$\exists C \in \mathbb{R}, g : (r, \theta) \mapsto \ln r + C$$

d'où,

$$\begin{aligned} \forall (x, y) \in \mathbb{R}^2 \setminus \{(0, 0)\}, f(x, y) &= \ln(\sqrt{x^2 + y^2}) + C \\ &= \frac{1}{2} \ln(x^2 + y^2) + C. \end{aligned}$$

REMARQUE:

Soit $\mathcal{B} = (e_1, e_2)$ la base canonique de \mathbb{R}^2 , $f : U \rightarrow \mathbb{R}$ de classe \mathcal{C}^1 avec U un ouvert de \mathbb{R}^2 .

Soit $(x, y) \in U$.

$$\text{Mat}_{\mathcal{B}}(\nabla f(x, y)) = \begin{pmatrix} \frac{\partial f}{\partial x}(x, y) \\ \frac{\partial f}{\partial y}(x, y) \end{pmatrix}$$

Soit

$$\begin{aligned} \varphi : V &\longrightarrow U \\ (u, v) &\longmapsto (x(u, v), y(u, v)) \end{aligned}$$

avec x, y de classe \mathcal{C}^1 . Soit $g = f \circ \varphi$.

$$\begin{aligned} \text{Mat}_{\mathcal{B}}(\nabla g(u, v)) &= \begin{pmatrix} \frac{\partial g}{\partial u}(u, v) \\ \frac{\partial g}{\partial v}(u, v) \end{pmatrix} \\ &= \begin{pmatrix} \frac{\partial x}{\partial u}(u, v) \frac{\partial f}{\partial x}(x, y) + \frac{\partial y}{\partial u}(u, v) \frac{\partial f}{\partial y}(x, y) \\ \frac{\partial x}{\partial v}(u, v) \frac{\partial f}{\partial x}(x, y) + \frac{\partial y}{\partial v}(u, v) \frac{\partial f}{\partial y}(x, y) \end{pmatrix} \\ &= \underbrace{\begin{pmatrix} \frac{\partial x}{\partial u}(u, v) & \frac{\partial y}{\partial u}(u, v) \\ \frac{\partial x}{\partial v}(u, v) & \frac{\partial y}{\partial v}(u, v) \end{pmatrix}}_{J(u, v)} \begin{pmatrix} \frac{\partial f}{\partial x}(x, y) \\ \frac{\partial f}{\partial y}(x, y) \end{pmatrix} \\ &= J(u, v) \text{Mat}_{\mathcal{B}}(\nabla f(x, y)) \end{aligned}$$

où $J(u, v) = (\text{Mat}_{\mathcal{B}}(\nabla x(u, v)) : \text{Mat}_{\mathcal{B}}(\nabla y(u, v)))$.

On dit que $J(u, v)$ est la jacobienne de φ en (u, v) . L'application linéaire canoniquement associée à $J(u, v)$ est la differentielle de φ en (u, v) noté $d\varphi(u, v)$.

On a $d\varphi(u, v) \in \mathcal{L}(R^2)$ et $\text{Mat}_{\mathcal{B}}(d\varphi(u, v)) = J(u, v)$.

Par exemple, la jacobienne du changement de coordonnées polaires est

$$J = \begin{pmatrix} \frac{\partial x}{\partial r} & \frac{\partial y}{\partial r} \\ \frac{\partial x}{\partial \theta} & \frac{\partial y}{\partial \theta} \end{pmatrix} = \begin{pmatrix} \cos \theta & \sin \theta \\ -r \sin \theta & r \cos \theta \end{pmatrix}.$$

$$\underbrace{\det(J)}_{\text{le jacobien}} = r \cos^2 \theta + r \sin^2 \theta = r$$

Dans une intégrale double, si $(x, y) = \varphi(u, v)$, alors $dx dy = \det(J) du dv$.

Ici,

$$dx dy = r dr d\theta.$$

Preuve:

On pose $(x_0, y_0) = \varphi(u_0, v_0)$. Pour tout $(h, k) \in R^2$ tels que $(u_0 + h, v_0 + k) \in V$, en posant $g = f \circ \varphi$.

$$\begin{aligned} g(u_0 + h, v_0 + k) &= f(x(u_0 + h, v_0 + k), y(u_0 + h, v_0 + k)) \\ &= f\left(x(u_0, v_0) + h \frac{\partial x}{\partial u}(u_0, v_0) + k \frac{\partial x}{\partial v}(u_0, v_0) + o(\|(h, k)\|),\right. \\ &\quad \left.y(u_0, v_0) + h \frac{\partial y}{\partial u}(u_0, v_0) + k \frac{\partial y}{\partial v}(u_0, v_0) + o(\|(h, k)\|)\right) \\ &= f(x_0, y_0) \\ &\quad + \left(h \frac{\partial x}{\partial u}(u_0, v_0) + k \frac{\partial x}{\partial v}(u_0, v_0) + o(\|(h, k)\|)\right) \frac{\partial f}{\partial x}(x_0, y_0) \\ &\quad + \left(h \frac{\partial y}{\partial u}(u_0, v_0) + k \frac{\partial y}{\partial v}(u_0, v_0) + o(\|(h, k)\|)\right) \frac{\partial f}{\partial y}(x_0, y_0) \\ &\quad + o(\|(h, k)\|) \\ &= f(x_0, y_0) \\ &\quad + h \left(\frac{\partial x}{\partial u}(u_0, v_0) \frac{\partial f}{\partial x}(x_0, y_0) + \frac{\partial y}{\partial u}(u_0, v_0) \frac{\partial f}{\partial y}(x_0, y_0)\right) \\ &\quad + k \left(\frac{\partial x}{\partial v}(u_0, v_0) \frac{\partial f}{\partial x}(x_0, y_0) + \frac{\partial y}{\partial v}(u_0, v_0) \frac{\partial f}{\partial y}(x_0, y_0)\right) + o(\|(h, k)\|) \\ &= g(u_0, v_0) + h \frac{\partial g}{\partial u}(u_0, v_0) + k \frac{\partial g}{\partial v}(u_0, v_0) + o(\|(h, k)\|) \end{aligned}$$

Par identification,

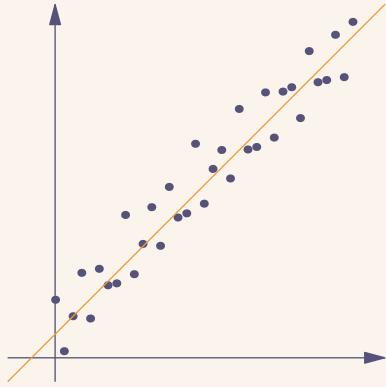
$$\frac{\partial g}{\partial u}(u_0, v_0) = \frac{\partial x}{\partial u}(u_0, v_0) \frac{\partial f}{\partial x}(x_0, y_0) + \frac{\partial y}{\partial u}(u_0, v_0) \frac{\partial f}{\partial y}(x_0, y_0)$$

et

$$\frac{\partial g}{\partial v}(u_0, v_0) = \frac{\partial x}{\partial v}(u_0, v_0) \frac{\partial f}{\partial x}(x_0, y_0) + \frac{\partial y}{\partial v}(u_0, v_0) \frac{\partial f}{\partial y}(x_0, y_0).$$

□

EXEMPLE (Régression linéaire):



$$y = ax + b$$

On fixe $(a, b) \in \mathbb{R}^2$.

$$\varepsilon(a, b) = \sum_{i=1}^n (y_i - (ax_i + b))^2$$

l'erreur totale.

On veut minimiser $\varepsilon(a, b)$. On a

$$\forall (a, b) \in \mathbb{R}^2, \begin{cases} \frac{\partial \varepsilon}{\partial a}(a, b) = -2 \sum_{i=1}^n (y_i - ax_i - b)x_i, \\ \frac{\partial \varepsilon}{\partial b}(a, b) = -2 \sum_{i=1}^n (y_i - ax_i - b). \end{cases}$$

Donc,

$$\begin{aligned} (a, b) \text{ point critique de } \varepsilon &\iff \begin{cases} a \sum_{i=1}^n x_i^2 + b \sum_{i=1}^n x_i = \sum_{i=1}^n y_i x_i \\ a \sum_{i=1}^n x_i + nb = \sum_{i=1}^n y_i \end{cases} \\ &\iff \begin{cases} a \left(\frac{1}{n} \sum_{i=1}^n x_i^2 - \bar{x}^2 \right) = \bar{y} - \bar{x}\bar{y} \\ b = \frac{1}{n} \sum_{i=1}^n y_i - \frac{a}{n} \sum_{i=1}^n x_i = \frac{1}{n} \sum_{i=1}^n x_i y_i - \bar{x}\bar{y} \end{cases} \\ &\quad \text{où } \bar{x} = \frac{1}{n} \sum_{i=1}^n x_i, \quad \bar{y} = \frac{1}{n} \sum_{i=1}^n y_i \\ &\iff \begin{cases} a = \frac{\text{Cov}(x, y)}{V(x)} \\ b = \bar{y} - a\bar{x} \end{cases} \end{aligned}$$

$$\text{Coefficient de corrélation : } \frac{\text{Cov}(x, y)}{\sigma_x \sigma_y} \in [-1, 1]$$

CHAPITRE

23

DÉNOMBREMENT

1 Cardinal d'un ensemble

Lemme: Soit $n \in \mathbb{N}^*$, $n \geq 2$, et $X \subsetneq [1, n]$ avec $X \neq \emptyset$ (\subsetneq signifie inclus et différent).

Alors

$$\exists 0 < p < n, \exists f : X \rightarrow [1, p] \text{ bijective}.$$

Preuve (par récurrence sur n):

On pose, pour $n \geq 2$,

$\mathcal{P}(n)$: “ $\forall X \subsetneq [1, n]$ tel que $X \neq \emptyset, \exists 0 < p < n, \exists f : X \rightarrow [1, p]$ bijective”

— Soit $X \subsetneq [1, 2]$ avec $X \neq \emptyset$. Par définition d'une inclusion,

$$X = \{1\} \text{ ou } X = \{2\}.$$

On pose $p = 1$.

Si $X = \{1\}$, alors on pose

$$\begin{aligned} f : X &\longrightarrow [1, 1] = \{1\} \\ 1 &\longmapsto 1 \end{aligned}$$

f est bien bijective.

Si $X = \{2\}$, alors on pose

$$\begin{aligned} f : X &\longrightarrow \{1\} \\ 2 &\longmapsto 1 \end{aligned}$$

De nouveau, f est bijective.

Ainsi, $\mathcal{P}(2)$ est vraie.

— Soit $n \geq 2$. On suppose $\mathcal{P}(n)$ vraie. Soit $X \subsetneq [1, n+1]$ avec $X \neq \emptyset$.

Cas1 On suppose que $n+1 \notin X$.

Alors $X \subset [1, n]$.

- Si $X = \llbracket 1, n \rrbracket$, alors on pose $p = n < n + 1$ et $f : \begin{array}{ccc} X & \longrightarrow & \llbracket 1, p \rrbracket = X \\ i & \longmapsto & i \end{array}$ est bijective.
 - Si $X \subsetneq \llbracket 1, n \rrbracket$, d'après $\mathcal{P}(n)$, il existe $p \in \llbracket 1, n - 1 \rrbracket$ et une bijection $f : X \rightarrow \llbracket 1, p \rrbracket$.
On a bien $p < n + 1$.
- Cas2 $n + 1 \in X$. On pose $Y = X \setminus \{n + 1\}$. Ainsi $Y \subset \llbracket 1, n + 1 \rrbracket$.
- Si $Y = \llbracket 1, n \rrbracket$, alors $X = \llbracket 1, n \rrbracket \cup \{n + 1\} : \not\exists$
 - Si $Y = \emptyset$, alors $X = \{n + 1\}$. On pose donc $p = 1 < n + 1$ et $f :$
$$\begin{array}{ccc} X & \longrightarrow & \llbracket 1, p \rrbracket = \{1\} \\ n + 1 & \longmapsto & 1 \end{array}$$
est bijective.
 - On suppose $Y \neq \emptyset$. D'après $\mathcal{P}(n)$, il existe $q \in \llbracket 1, n - 1 \rrbracket$ et $g : Y \rightarrow \llbracket 1, q \rrbracket$ bijective.
On pose $f :$
$$\begin{array}{ccc} X & \longrightarrow & \llbracket 1, q + 1 \rrbracket \\ x & \longmapsto & \begin{cases} g(x) & \text{si } x \neq n + 1, \\ q + 1 & \text{si } x = n + 1. \end{cases} \end{array}$$
On pose aussi $p = q + 1 \leq n < n + 1$. f est bijective.
On pose

$$h : \llbracket 1, q + 1 \rrbracket \longrightarrow X$$

$$i \longmapsto \begin{cases} g^{-1}(i) & \text{si } i \leq q, \\ n + 1 & \text{si } i = q + 1. \end{cases}$$

$$\begin{aligned} \forall i \in \llbracket 1, q + 1 \rrbracket, f(h(i)) &= \begin{cases} f(g^{-1}(i)) & \text{si } i \leq q \\ f(n + 1) & \text{si } i = q + 1 \end{cases} \\ &= \begin{cases} g(g^{-1}(i)) & \text{si } i \leq q \\ q + 1 & \text{si } i = q + 1 \end{cases} \\ &= i \end{aligned}$$

$$\begin{aligned} \forall x \in X, h(f(x)) &= \begin{cases} h(g(x)) & \text{si } x \neq n + 1 \\ h(q + 1) & \text{si } x = n + 1 \end{cases} \\ &= \begin{cases} g^{-1}(g(x)) & \text{si } x \neq n + 1 \\ n + 1 & \text{si } x = n + 1 \end{cases} \\ &= x \end{aligned}$$

□

Lemme: Soient n, p deux entiers non-nuls et $f : \llbracket 1, p \rrbracket \rightarrow \llbracket 1, n \rrbracket$ une surjection. Alors $p \geq n$.

Preuve (par récurrence sur n):
Pour $n \in \mathbb{N}^*$, on pose

$$\mathcal{P}(n) : " \forall p \in \mathbb{N}^*, \forall f : \llbracket 1, p \rrbracket \rightarrow \llbracket 1, n \rrbracket, f \text{ surjective} \implies p \geq n."$$

- Soit $p \in \mathbb{N}^*$ et $f : \llbracket 1, p \rrbracket \rightarrow \llbracket 1, 1 \rrbracket = \{1\}$. On suppose f surjective. Nécessairement, $p \geq 1$.
- Soit $n \in \mathbb{N}^*$. On suppose $\mathcal{P}(n)$ vraie. Soit $p \in \mathbb{N}^*$ et $f : \llbracket 1, p \rrbracket \rightarrow \llbracket 1, n + 1 \rrbracket$. On

suppose f surjective. On veut montrer que $p \geq n + 1$.

On pose

$$X = f^{-1}(\llbracket 1, n \rrbracket) = \{i \in \llbracket 1, p \rrbracket \mid f(i) \neq n + 1\}.$$

Comme f est surjective, $X \neq \emptyset$ et $X \neq \llbracket 1, p \rrbracket$. D'après le lemme précédent, il existe $0 < q < p$ et $g : X \rightarrow \llbracket 1, q \rrbracket$ bijective.

Ainsi $f \circ g^{-1} : \llbracket 1, q \rrbracket \rightarrow \llbracket 1, n \rrbracket$ est surjective.

D'après $\mathcal{P}(n)$, $q \geq n$.

Si $p \leq n$, alors $q < p \leq n$: $\frac{1}{2}$

Donc $p > n$ et donc $p \geq n + 1$.

□

Lemme: Soient $n \geq 1$ et $p \geq 1$, $f : \llbracket 1, p \rrbracket \rightarrow \llbracket 1, n \rrbracket$. Alors $p \leq n$.

Preuve:

On pose

$$\begin{aligned} g : \llbracket 1, n \rrbracket &\longrightarrow \llbracket 1, p \rrbracket \\ i &\longmapsto \begin{cases} 1 & \text{si } f^{-1}(\{i\}) = \emptyset, \\ j & \text{si } f^{-1}(\{i\}) = \{j\}. \end{cases} \end{aligned}$$

g est surjective. Soit $k \in \llbracket 1, p \rrbracket$, alors $g(f(k)) = k$ car k est un antécédant de $f(k)$ par f .

D'après le lemme précédent, $n \geq p$.

□

Corollaire: Soient $n, p \in \mathbb{N}^*$ et $f : \llbracket 1, n \rrbracket \rightarrow \llbracket 1, p \rrbracket$ bijective. Alors $n = p$

Définition: Soit X un ensemble. On dit que X est fini si $X = \emptyset$ ou s'il existe $n \in \mathbb{N}^*$ et une bijection $f : X \rightarrow \llbracket 1, n \rrbracket$.

Soit X un ensemble fini. Le cardinal de X est

- 0 si $X = \emptyset$
- sinon, c'est le seul entier $n \in \mathbb{N}^*$ pour lequel il existe une bijection de X dans $\llbracket 1, n \rrbracket$.

On le note $\text{Card}(X)$, $\#X$ ou $|X|$.

Proposition: Soit E un ensemble fini et $X \in \mathcal{P}(E)$.

Alors X est fini et $\#X \leq \#E$.

Si $\#X = \#E$, alors $X = E$.

Preuve: Cas1 Si $E = \emptyset$, alors $X = \emptyset$.

Cas2 $E \neq \emptyset$. On pose $n = \#E \in \mathbb{N}^*$. Soit $f : E \rightarrow \llbracket 1, n \rrbracket$ une bijection.

On suppose $X \neq \emptyset$. On pose $Y = f(X) \subset \llbracket 1, n \rrbracket$

- Si $Y = \llbracket 1, n \rrbracket$, alors $X = E$ et donc $\#X = n \leq \#E$.
- Si $Y \subsetneq \llbracket 1, n \rrbracket$, comme $Y \neq \emptyset$, il existe $p \in \llbracket 1, n - 1 \rrbracket$ et $g : Y \rightarrow \llbracket 1, p \rrbracket$: une bijection.

$$\begin{aligned} g : X &\longrightarrow \llbracket 1, p \rrbracket \\ x &\longmapsto g(f(x)) \end{aligned}$$

D'où

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ & \searrow h & \downarrow g \\ & & \llbracket 1, p \rrbracket \end{array}$$

Montrons que h est bijective. On pose

$$\begin{aligned} k : \llbracket 1, p \rrbracket &\longrightarrow X \\ i &\longmapsto f^{-1}(g^{-1}(i)). \end{aligned}$$

h et k sont réciproques l'une de l'autre, donc $\#X = p \leq n$.
On suppose $X = \emptyset$, alors $\#X = 0 < n$.

□

Proposition: Soit E un ensemble fini, $(A, B) \in \mathcal{P}(E)^2$ tel que $A \cap B = \emptyset$.

Alors

$$\#(A \cup B) = \#A + \#B.$$

Preuve:

Le résultat est évident si $A = \emptyset$ et $B = \emptyset$.

On suppose $A \neq \emptyset$ et $B \neq \emptyset$. On pose $a = \#A$ et $b = \#B$. Soient

$$\begin{cases} f : A \rightarrow \llbracket 1, a \rrbracket \text{ une bijection} \\ g : B \rightarrow \llbracket 1, b \rrbracket \text{ une bijection} \end{cases}$$

On pose

$$\begin{aligned} h : A \cup B &\longrightarrow \llbracket a+b \rrbracket \\ x &\longmapsto \begin{cases} f(x) & \text{si } x \in A, \\ a+g(x) & \text{si } x \in B. \end{cases} \end{aligned}$$

Comme $A \cap B = \emptyset$, h est bien définie.

Soit

$$\begin{aligned} k : \llbracket 1, a+b \rrbracket &\longrightarrow A \cup B \\ i &\longmapsto \begin{cases} f^{-1}(i) & \text{si } i \leq a \\ g^{-1}(i-a) & \text{si } i > a. \end{cases} \end{aligned}$$

On vérifie que h et k sont réciproques l'une de l'autre.

Donc $\#(A \cup B) = a+b$.

□

Proposition: Soient E un ensemble fini, $n \in \mathbb{N}^*$, $(A_1, \dots, A_n) \in \mathcal{P}(E)^n$ telles que

$$\forall i \neq j, A_i \cap A_j = \emptyset.$$

Alors

$$\# \left(\bigcup_{i=1}^n A_i \right) = \sum_{i=1}^n \# A_i$$

Preuve (par récurrence sur n):

On a traité le cas $n = 2$ précédemment.

Soit $n \geq 2$ pour lequel le résultat est vrai. Soit $(A_1, \dots, A_{n+1}) \in \mathcal{P}(E)^{n+1}$ telles que

$$\forall i \neq j, A_i \cap A_j = \emptyset.$$

On pose $A = \bigcup_{i=1}^n A_i$. Alors

$$\begin{aligned} A \cap A_{n+1} &= \left(\bigcup_{i=1}^n A_i \right) \cap A_{n+1} \\ &= \bigcup_{i=1}^n (A_i \cap A_{n+1}) \\ &= \bigcup_{i=1}^n \emptyset \\ &= \emptyset. \end{aligned}$$

Donc,

$$\begin{aligned} \# \left(\bigcup_{i=1}^{n+1} A_i \right) &= \#(A \cup A_{n+1}) \\ &= \#A = \#A_{n+1} \\ &= \sum_{i=1}^n \#A_i + \#A_{n+1} \\ &= \sum_{i=1}^{n+1} \#A. \end{aligned}$$

□

Proposition: Soient E un ensemble fini, $(A, B) \in \mathcal{P}(E)^2$. Alors

$$\#(A \cup B) = \#A + \#B - \#(A \cap B).$$

Preuve:

On pose $\begin{cases} C = A \cap B \\ A' = A \setminus C \\ B' = B \setminus C. \end{cases}$
Alors $\begin{cases} A' \cup B' \cup C = A \cup B, \\ A' \cap B' = A' \cap C = B' \cap C = \emptyset. \end{cases}$

D'où

$$\begin{aligned} \#(A \cup B) &= \#(A' \cup B' \cup C) \\ &= \#A' + \#B' + \#C. \end{aligned}$$

Or,

$$\begin{cases} A = A' \cup C \\ A' \cap C = \emptyset \end{cases}$$

donc

$$\#A = \#A' + \#C$$

donc

$$\#A' = \#A - \#C.$$

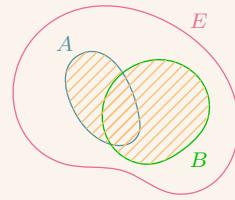
De même,

$$\#B' = \#B - \#C.$$

D'où

$$\begin{aligned} \#(A \cup B) &= \#A - \#C + \#B - \#C + \#C \\ &= \#A + \#B - \#C \end{aligned}$$

□



Au passage, on a prouvé la proposition suivante :

Proposition: Soient E un ensemble fini, $(A, B) \in \mathcal{P}(E)^2$ avec $B \subset A$. Alors

$$\#(A \setminus B) = \#A - \#B.$$

□

EXEMPLE:

Soit E un ensemble fini, $(A, B, C) \in \mathcal{P}(E)^3$.

$$\begin{aligned} \#(A \cup B \cup C) &= \#A + \#B + \#C \\ &\quad - \#(A \cap B) - \#(B \cap C) - \#(A \cap C) \\ &\quad + \#(A \cap B \cap C). \end{aligned}$$

Soit $(A, B, C, D) \in \mathcal{P}(E)^4$.

$$\begin{aligned} \#(A \cup B \cup C \cup D) &= \#A + \#B + \#C + \#D \\ &\quad - \#(A \cap B) - \#(A \cap C) - \#(A \cap D) - \#(B \cap C) - \#(B \cap D) - \#(C \cap D) \\ &\quad + \#(A \cap B \cap C) + \#(A \cap B \cap D) + \#(B \cap C \cap D) + \#(A \cap C \cap D) \\ &\quad - \#(A \cap B \cap C \cap D). \end{aligned}$$

En généralisant, on obtient la formule du criblé :

$$\# \left(\bigcup_{i=1}^n A_i \right) = \sum_{k=1}^n (-1)^{k+1} \sum_{1 \leq i_1 \leq \dots \leq i_k \leq n} \#(A_{i_1} \cap \dots \cap A_{i_k}).$$

Proposition: Soient E et F deux ensembles finis et $f : E \rightarrow F$.

1. Si f est injective, alors $\#E \leq \#F$,
2. Si f est surjective, alors $\#E \geq \#F$,
3. Si f est bijective, alors $\#E = \#F$,

Preuve:

1. $E \xrightarrow{f} F$
 $\begin{array}{ccc} E & \xrightarrow{f} & F \\ \text{bij} \uparrow & & \downarrow \text{bij} \\ \llbracket 1, n \rrbracket & \xrightarrow{\text{inj}} & \llbracket 1, p \rrbracket \end{array}$
2. $E \xrightarrow{\text{surj}} F$
 $\begin{array}{ccc} E & \xrightarrow{\text{surj}} & F \\ \text{bij} \uparrow & & \downarrow \text{bij} \\ \llbracket 1, n \rrbracket & \xrightarrow{\text{surj}} & \llbracket 1, p \rrbracket \end{array}$

□

Proposition (principe des tiroirs – pigeonhole principle): Soit $f : E \rightarrow F$ telle que $\#E > \#F$. Alors

$$\exists (x, y) \in E^2, \begin{cases} x \neq y, \\ f(x) = f(y) \end{cases}$$

Preuve:

C'est la contraposée du point 1. de la proposition précédente.

□

Proposition: Soit $E \rightarrow F$ où E et F sont finis et $\#E = \#F$.

$$f \text{ injective} \iff f \text{ surjective} \iff f \text{ bijective}.$$

Preuve: — On suppose f injective. Soit

$$\begin{aligned} g : E &\longrightarrow \text{Im}(f) \\ x &\longmapsto f(x) \end{aligned}$$

g est bijective donc $\#E = \#\text{Im}(f)$. Or, $\#E = \#F$ donc $\text{Im}(f) = F$ et donc f est surjective.

— On suppose f surjective. Alors

$$E = \bigcup_{y \in F} f^{-1}(\{y\})$$

donc

$$\#E = \sum_{y \in F} \#f^{-1}(\{y\}) \geq \sum_{y \in F} 1 = \#F$$

donc

$$\forall y \in F, \#f^{-1}(\{y\}) = 1$$

donc f est bijective.

□

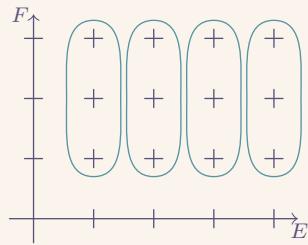
2 Dénombrément

Proposition: Soient E et F deux ensembles finis. Alors $E \times F$ est fini et

$$\#(E \times F) = \#E \times \#F.$$

Preuve:

$$E \times F = \bigcup_{x \in E} \underbrace{\{(x, y) \mid y \in F\}}_{F_x}.$$



Donc,

$$\#(E \times F) = \sum_{x \in E} (\#F_x)$$

Pour $x \in E$, soit

$$\begin{aligned} \varphi_x : F_x &\longrightarrow F \\ (x, y) &\longmapsto y. \end{aligned}$$

φ_x est bijective donc $\#F_x = \#F$. D'où

$$\#(E \times F) = \sum_{x \in E} (\#F) = \#(E) \times (\#F).$$

□

Proposition: Soit $n \in \mathbb{N}^*$ et E_1, \dots, E_n des ensembles finis. Alors $\prod_{i=1}^n E_i$ est fini et

$$\# \left(\prod_{i=1}^n E_i \right) = \prod_{i=1}^n (\#E_i).$$

Preuve:

par récurrence sur n .

□

Corollaire: Soit E un ensemble fini de cardinal n et $p \in \mathbb{N}^*$. Alors

$$\#(E^p) = n^p.$$

En d'autres termes, il y a n^p p-listes de E , où une p -lise de E est un (x_1, \dots, x_p) de E^p .

Définition: Soit E un ensemble fini et $p \in \mathbb{N}^*$. Un p -arrangement de E est une p -liste de E d'éléments deux à deux distincts :

$$(x_1, \dots, x_p) \in E^p \text{ est un } p\text{-arrangement} \iff \forall i \neq j, x_i \neq x_j.$$

Proposition: Soit E un ensemble fini de cardinal n et $p \in \mathbb{N}^*$. Il y a exactement $\frac{n!}{(n-p)!}$ p -arrangements si $p \leq n$ et 0 si $p > n$.

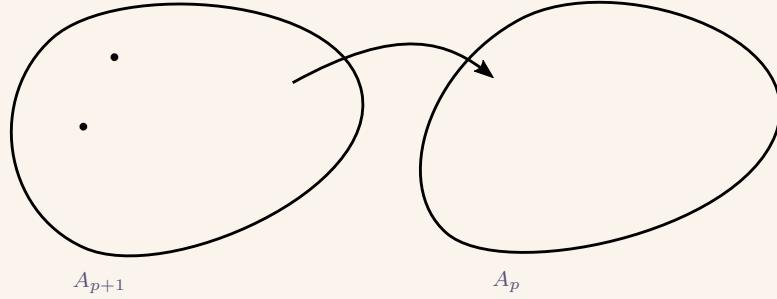
Preuve (par récurrence sur p): — Il y a $n-1$ -arrangements de E . Or, $\frac{n!}{(n-1)!} = n$.

— Soit $p \in \mathbb{N}^*$. On suppose qu'il y a $\frac{n!}{(n-p)!}$ p -arrangements.
Soit

$$\begin{aligned} f : \mathcal{A}_{p+1} &\longrightarrow \mathcal{A}_p \\ (x_1, \dots, x_{p+1}) &\longmapsto (x_1, \dots, x_p) \end{aligned}$$

où \mathcal{A}_{p+1} est l'ensemble des $(p+1)$ -arrangements et \mathcal{A}_p est l'ensemble des p -arrangements.

Soit $x = (x_1, \dots, x_p) \in \mathcal{A}_p$. x a exactement $n-p$ antécédents par f .



D'après le principe des bergers,

$$\begin{aligned}\#\mathcal{A}_{p+1} &= (n-p)\#\mathcal{A}_p \\ &= (n-p) \times \frac{n!}{(n-p)!} \\ &= \frac{n!}{(n-p-1)!} \\ &= \frac{n!}{(n-(p+1))!}\end{aligned}$$

□

Dans la preuve précédente, on a utilisé principe des bergers :

Lemme (principe des bergers): Soit $f : E \rightarrow F$ surjective telle que

$$\exists k, \forall y \in F, \#(f^{-1}(\{-y\})) = k$$

En d'autres termes, tous les éléments de F ont le même nombre d'antécédents.

Si F est fini, alors

$$\#E = k \#F.$$

Preuve:

On définit \sim sur E :

$$x \sim y \iff f(x) = f(y).$$

“ \sim ” est une relation d'équivalence sur E . Soit \mathcal{R} un système de représentants :

$$E = \bigcup_{x \in \mathcal{R}} \mathcal{C}(x).$$

On a donc

$$\forall x \in E, \exists ! u \in \mathcal{R}, x \sim u.$$

L'application $\begin{array}{ccc} \mathcal{R} & \longrightarrow & F \\ x & \longmapsto & f(x) \end{array}$ est bijective donc $\#\mathcal{R} = \#F$.

Soit $x \in \mathcal{R}$.

$$\begin{aligned}\forall y \in E, y \in \mathcal{C}(x) &\iff f(y) = f(x) \\ &\iff y \text{ est un antécédant de } f(x)\end{aligned}$$

donc $\#\mathcal{C}(x) = k$.

Finalement,

$$\begin{aligned}\#E &= \sum_{x \in \mathcal{R}} \#(\mathcal{C}(x)) \\ &= \sum_{x \in \mathcal{R}} k \\ &= k(\#\mathcal{R}) \\ &= k(\#F).\end{aligned}$$

□

Proposition: Soit E un ensemble fini de cardinal n . Il y a $n!$ permutations de E .

Preuve:

On note $S(E)$ l'ensemble des permutations de E , $\mathcal{A}_n(E)$ l'ensemble des n arrangements de E . On pose $E = \{a_1, \dots, a_n\}$ et

$$\begin{aligned} f : S(E) &\longrightarrow \mathcal{A}_n(E) \\ \sigma &\longmapsto (\sigma(a_1), \dots, \sigma(a_n)). \end{aligned}$$

et

$$\begin{aligned} g : \mathcal{A}_n(E) &\longrightarrow S(E) \\ (b_1, \dots, b_n) &\longmapsto \left(\sigma : \begin{array}{ccc} E & \longrightarrow & E \\ a_i & \longmapsto & b_i \end{array} \right). \end{aligned}$$

f et g sont réciproques l'une de l'autre donc

$$\#S(E) = \#\mathcal{A}_n(E) = \frac{n!}{0!} = n!.$$

□

EXEMPLE:

On pose $E = \{\pi, e, \sqrt{2}\}$. Alors,

$$S(E) = \left\{ \text{id}, \left(\begin{array}{c} \pi \mapsto e \\ e \mapsto \pi \\ \sqrt{2} \mapsto \sqrt{2} \end{array} \right), \dots \right\}$$

Donc,

$$f(\sigma) = (e, \pi, \sqrt{2}).$$

et alors

$$\begin{aligned} g(\sqrt{2}, \pi, e) : E &\longrightarrow E \\ \pi &\longmapsto \sqrt{2} \\ e &\longmapsto \pi \\ \sqrt{2} &\longmapsto e. \end{aligned}$$

Définition: Soit E un ensemble fini et $p \in \mathbb{N}^*$. Une p -combinaison de E est une partie de E de cardinal p .

Proposition: Soit E fini de cardinal n et $p \in \mathbb{N}^*$. Il y a exactement $\binom{n}{p}$ parties de E de cardinal p .

Preuve:

On note $\mathcal{A}_p(E)$ l'ensemble des p -arrangements et $\mathcal{C}_p(E)$ l'ensemble des p -combinaisons de E .

Soit

$$\begin{aligned} f : \mathcal{A}_p(E) &\longrightarrow \mathcal{C}_p(E) \\ (x_1, \dots, x_p) &\longmapsto \{x_1, \dots, x_p\}. \end{aligned}$$

f est surjective et

$$\forall X \in \mathcal{C}_p(E), \quad X \text{ a } p! \text{ antécédants.}$$

D'après le lemme des bergers :

$$\#\mathcal{A}_p(E) = p! \#\mathcal{C}_p(E)$$

et donc

$$\#\mathcal{C}_p(E) = \frac{n!}{(n-p)! p!} = \binom{n}{p}.$$

□

Corollaire:

$$\forall (n, p) \in \mathbb{N}^2, \quad \binom{n}{p} \in \mathbb{N}.$$

□

Proposition: Soit E et F deux ensembles finis. Alors F^E est fini et

$$\#(F^E) = (\#F)^{\#E}.$$

Preuve:

Soit

$$\begin{aligned} \varphi : F^E &\longrightarrow F^n \\ f &\longmapsto (f(x_1), \dots, f(x_n)) \end{aligned}$$

où $E = \{x_1, \dots, x_n\}$ et $n = \#E$.

Soit

$$\begin{aligned} \psi : F^n &\longrightarrow F^E \\ (y_1, \dots, y_n) &\longmapsto \begin{array}{ccc} E & \longrightarrow & F \\ x_i & \longmapsto & y_i. \end{array} \end{aligned}$$

On a $\varphi \circ \psi = \text{id}_{F^n}$ et $\psi \circ \varphi = \text{id}_{F^E}$.

Donc

$$\#(F^E) = (\#F)^n.$$

□

Proposition: Soit E fini de cardinal n . Alors $\#\mathcal{P}(E) = 2^n$.

Preuve: MÉTHODE1 Soit

$$\begin{aligned}\varphi : \mathcal{P}(E) &\longrightarrow \{0, 1\}^E \\ A &\longmapsto \mathbb{1}_A : \begin{aligned}[t] E &\longrightarrow \{0, 1\} \\ x &\longmapsto \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{sinon.} \end{cases} \end{aligned}\end{aligned}$$

φ est bijective :

$$\begin{aligned}\varphi^{-1} : \{0, 1\}^E &\longrightarrow \mathcal{P}(E) \\ f &\longmapsto \{x \in E \mid f(x) = 1\}.\end{aligned}$$

On a donc $\#\mathcal{P}(E) = 2^n$.

MÉTHODE2

$$\mathcal{P}(E) = \bigcup_{p=0}^n \mathcal{C}_p(E)$$

donc

$$\#\mathcal{P}(E) = \sum_{p=0}^n \binom{n}{p} = (1+1)^n = 2^n$$

MÉTHODE3 (par récurrence sur n).

- $n = 0$ donc $E = \emptyset$ et $\mathcal{P}(\emptyset) = \{\emptyset\}$. donc $\#\mathcal{P}(E) = 1 = 2^0$.
- Soit $n \in \mathbb{N}$. On suppose que

$$\forall E \text{ de cardinal } n, \quad \#\mathcal{P}(E) = 2^n$$

Soit E de cardinal $n+1 > 0$. Soit $a \in E$ et $F = E \setminus \{a\}$.

- Les parties de E qui ne contiennent pas a sont des parties de F et réciproquement : il y en a 2^n .
- A chaque partie de E contenant a , on peut faire correspondre une partie de F en supprimant a de la partie, et réciproquement : il y en a 2^n .

Donc,

$$\#\mathcal{P}(E) = 2^n + 2^n = 2 \times 2^n = 2^{n+1}.$$

□

3 Preuves combinatoires

Proposition:

$$\forall k \leq n \in \mathbb{N}, \quad \binom{n}{k} = \binom{n}{n-k}.$$

Preuve:

Il y a autant de façons de choisir k éléments parmi n que d'en choisir $n-k$ à exclure.

Formellement :
L'application

$$\begin{aligned}f : \mathcal{C}_k(\llbracket 1, n \rrbracket) &\longrightarrow \mathcal{C}_{n-k}(\llbracket 1, n \rrbracket) \\ X &\longmapsto \llbracket 1, n \rrbracket \setminus X\end{aligned}$$

est bijective. □

Proposition:

$$\forall k \leq n, \quad \binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}.$$

Preuve:

On pose

$$A_{n+1} = \{X \in \mathcal{C}_{k+1}(\llbracket 1, n+1 \rrbracket) \mid n+1 \in X\}, \quad B_{n+1} = \{X \in \mathcal{C}_{k+1}(\llbracket 1, n+1 \rrbracket) \mid n+1 \notin X\}.$$

donc

$$\mathcal{C}_{k+1}(\llbracket 1, n+1 \rrbracket) = A_{n+1} \cup B_{n+1}.$$

L'application $f : \begin{array}{ccc} A_{n+1} & \longrightarrow & \mathcal{C}_k(\llbracket 1, n \rrbracket) \\ X & \longmapsto & X \setminus \{n+1\} \end{array}$ est bijective

Donc

$$B_{n+1} = \mathcal{C}_{k+1}(\llbracket 1, n \rrbracket)$$

et donc

$$\begin{aligned} \binom{n+1}{k+1} &= \#A_{n+1} + \#B_{n+1} \\ &= \binom{n}{k} + \binom{n}{k+1}. \end{aligned}$$

□

Proposition: Soit $(A, +, \times)$ un anneau, $(a, b) \in A^2$ tel que $a \times b = b \times a$. Alors

$$\forall n \in \mathbb{N}^*, (a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}.$$

Preuve:

Soit $n \in \mathbb{N}^*$. On pose $a_1 = a$ et $a_2 = b$. Alors

$$\begin{aligned} (a+b)^n &= (a_1 + a_2)(a_1 + a_2) \cdots (a_1 + a_2) \\ &= \sum_{i_1=1}^2 a_{i_1} \sum_{i_2=1}^2 a_{i_2} \cdots \sum_{i_n=1}^2 a_{i_n} \\ &= \sum_{(i_1, \dots, i_n) \in \{1, 2\}^n} a_{i_1} a_{i_2} \cdots a_{i_n} \\ &= \sum_{k=0}^n \sum_{\substack{(i_1, \dots, i_n) \in \{1, 2\}^n \\ \#\{j \in \llbracket 1, n \rrbracket \mid i_j = 1\} = k}} a^k b^{n-k} \\ &= \sum_{k=0}^n \sum_{\substack{(i_1, \dots, i_n) \in \{1, 2\}^n \\ \#\{j \in \llbracket 1, n \rrbracket \mid i_j = 1\} = k}} a^k b^{n-k} \\ &= \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}. \end{aligned}$$

□

4 Bilan

Principe des tiroirs

Soit $f : E \rightarrow F$ avec $\#E > \#F$. Alors
 $\exists x \neq y \in E, f(x) = f(y)$.

Un p -arrangement est une p -liste d'éléments de E distincts. Il y en a, avec $n = \#E$,

$$\frac{n!}{(n-p)!}.$$

Soit $f : E \rightarrow F$ avec $\#E = \#F$. Alors
 f injective \iff f surjective
 \iff f bijective.

Principe des bergers

Soit $f : E \rightarrow F$ telle que chaque élément $y \in F$ ait exactement k antécédents dans F . Alors,

$$\#E = k\#F.$$

$$\# \left(\prod_{i=1}^n E_i \right) = \prod_{i=1}^n (\#E_i).$$

Une permutation est une bijection de E dans E . Il y en a $n!$ si $\#E = n$.

$$\#(E^n) = (\#E)^n.$$

Une p -liste est de la forme $(x_1, \dots, x_p) \in E^p$.

Une p -combinaison de E est une partie de E de cardinal p . Il y en a $\binom{n}{p}$ si $n = \#E$.

$$\#(F^E) = (\#F)^{\#E}.$$

$$\#\mathcal{P}(E) = 2^{\#E}.$$

CHAPITRE

24

GROUPE SYMÉTRIQUE

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

Le groupe symétrique est noté S_n : l'ensemble des permutations de $\llbracket 1, n \rrbracket$ muni de \circ .

$$\#S_n = n!$$

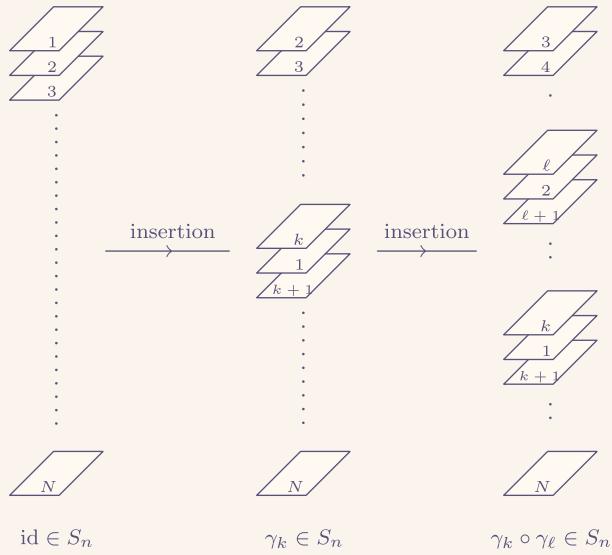
1 Mise en situation

BON MÉLANGE D'UN JEU DE CARTES :

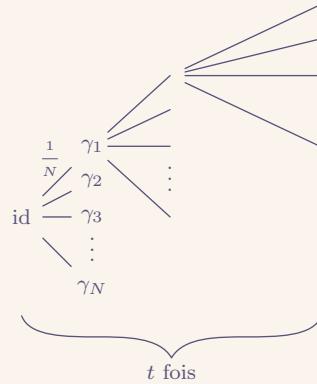
Soit un jeu neuf de N cartes. On procède à un mélange par insertion : on place la carte qui est au-dessus n'importe où dans le paquet, étape que l'on répète t fois.

Pour quelles valeurs de t obtient-on un jeu bien mélangé ?

Modélisation : On numérote les cartes de 1 à N dans l'ordre initial du jeu.



On peut modéliser par un arbre le mélange dont les nœuds sont des permutations des éléments de S_N .



On dit que le jeu est bien mélangé après t insertions si chaque élément de S_N est une feuille de cet arbre et la probabilité d'obtenir cette permutation est $\frac{1}{N!}$.

Avec $N = 4$, on a

$$\begin{array}{ll} \gamma_1 = \text{id} & \gamma_2 = \begin{matrix} 1 & 2 \\ 2 & 3 \rightarrow 1 \\ 3 & 4 \\ 4 & 4 \end{matrix} \\ \gamma_3 = \begin{matrix} 1 & 3 \\ 2 & 1 \\ 3 & 2 \\ 4 & 4 \end{matrix} \rightarrow & \gamma_4 = \begin{matrix} 1 & 4 \\ 2 & 3 \rightarrow 1 \\ 3 & 2 \\ 4 & 3 \end{matrix} . \end{array}$$

Avec $k = 2$ et $\ell = 1$,

$$\begin{matrix} 1 & 2 & 2 \\ 2 & \xrightarrow{\gamma_2 \circ} & 1 & \xrightarrow{\gamma_1 \circ} & 1 \\ 3 & & 3 & & 3 \\ 4 & & 4 & & 4 \end{matrix}$$

$\underbrace{}_{\gamma_2}$ $\underbrace{}_{\gamma_2}$

Avec $k = 2$ et $\ell = 2$, on a

$$\begin{array}{ccc} 1 & 2 & 1 \\ 2 & \rightarrow & 1 \\ 3 & \rightarrow & 2 \\ 4 & & 3 \end{array} .$$

Et avec $k = 2$ et $\ell = 3$, on a

$$\begin{array}{ccc} 1 & 2 & 1 \\ 2 & \rightarrow & 3 \\ 3 & \rightarrow & 2 \\ 4 & & 4 \end{array} .$$

$$\gamma_2 \circ \gamma_3 : \begin{array}{l} 1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 2 \\ 4 \mapsto 4 \end{array}$$

Est-ce que toute permutation peut s'écrire comme un produit des γ_k avec $k \in \llbracket 1, N \rrbracket$?

2 Cycles

REMARQUE (Notation):

Soit $\sigma \in S_n$.

$$\sigma : \llbracket 1, N \rrbracket \longrightarrow \llbracket 1, N \rrbracket$$

$$i \longmapsto \begin{cases} * & \text{si } i = 1 \\ * & \text{si } i = 2 \\ \vdots & \\ * & \text{si } i = N. \end{cases}$$

On écrit plutôt

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & N \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(N) \end{pmatrix}$$

EXEMPLE:

Avec $N = 4$, on a donc

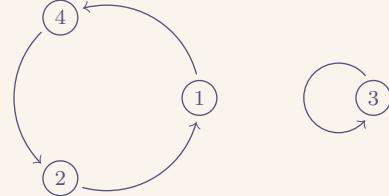
$$\gamma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad \gamma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

$$\gamma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \quad \gamma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

REMARQUE:

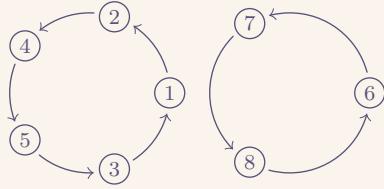
Avec $N = 4$ et

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$



Avec $N = 8$ et

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 1 & 5 & 3 & 7 & 8 & 6 \end{pmatrix}$$



Définition: Soit $\sigma \in S_N$ et $x \in \llbracket 1, N \rrbracket$.

L'orbite de x pour σ est

$$\{x, \sigma(x), \sigma^2(x), \dots\} = \{\sigma^i(x) \mid i \in \mathbb{N}\}.$$

On note l'ordre d de σ : si $\sigma \neq \text{id}$, $\begin{cases} \sigma^d = \text{id}, \\ \sigma^{d-1} \neq \text{id}. \end{cases}$ L'orbite de x est

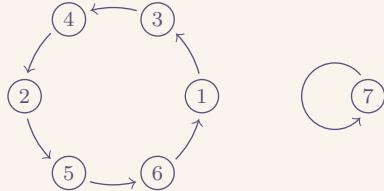
$$\{x, \sigma(x), \dots, \sigma^{d-1}(x)\}.$$

Les orbites de σ partitionnent $\llbracket 1, N \rrbracket$.

Définition: Soit $\gamma \in S_N$. On dit que γ est un k -cycle si γ a $N - k$ points fixes et les k autres éléments sont dans une même orbite.

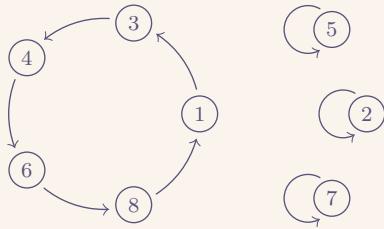
EXEMPLE:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 4 & 2 & 6 & 1 & 7 \end{pmatrix}$$



σ est un 6-cycle.

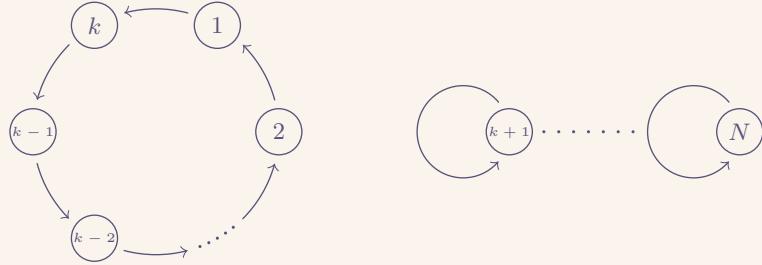
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 6 & 5 & 8 & 7 & 1 \end{pmatrix}$$



σ est un 5-cycle.

EXEMPLE:

$$\gamma_k = \begin{pmatrix} 1 & 2 & 3 & \cdots & k & k+1 & \cdots & N \\ k & 1 & 2 & \cdots & k-1 & k+1 & \cdots & N \end{pmatrix}$$



γ_k est un k -cycle.

REMARQUE (Notation):

Soit γ un k -cycle tel que $\gamma(x) \neq x$. On note

$$\gamma = (x \quad \gamma(x) \quad \gamma^2(x) \quad \cdots \quad \gamma^{k-1}(x)).$$

EXEMPLE:

Avec

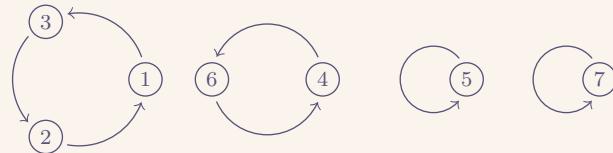
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 6 & 5 & 8 & 7 & 1 \end{pmatrix}$$

On a donc

$$\begin{aligned} \sigma &= (6 \quad 8 \quad 1 \quad 3 \quad 4) \\ &= (3 \quad 4 \quad 6 \quad 8 \quad 1) \end{aligned}$$

EXEMPLE:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 6 & 5 & 4 & 7 \end{pmatrix}$$



$$(1 \quad 3 \quad 2) \circ (4 \quad 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 6 & 5 & 4 & 7 \end{pmatrix} = \sigma.$$

$$(4 \quad 6) \circ (1 \quad 3 \quad 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 6 & 5 & 4 & 7 \end{pmatrix} = \sigma.$$

EXEMPLE:

Avec $N = 4$,

$$(1 \quad 2 \quad 3) (1 \quad 3 \quad 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

¶

$$(1 \quad 3 \quad 4) (1 \quad 2 \quad 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

Définition: Soit $\sigma \in S_n$. Le support de σ est

$$\text{Supp}(\sigma) = \{x \in \llbracket 1, n \rrbracket \mid \sigma(x) \neq x\}.$$

Théorème: Toute permutation de S_n est une composée de cycles à supports disjoints et ces cycles sont uniques.

EXEMPLE:

$$\begin{aligned}\sigma &= \left(\begin{array}{cccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 9 & 8 & 1 & 7 & 11 & 3 & 2 & 12 & 5 & 4 & 6 \end{array} \right) \\ &= (1 \ 10 \ 5 \ 7 \ 3 \ 8 \ 2 \ 9 \ 12 \ 6 \ 11 \ 4)\end{aligned}$$

EXEMPLE:

$$\begin{aligned}\sigma &= \left(\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 8 & 2 & 1 & 6 & 3 & 7 \end{array} \right) \\ &= (1 \ 4 \ 2 \ 5) (3 \ 8 \ 7)\end{aligned}$$

Preuve:

Soit $\sigma \in S_n$.

ANALYSE On suppose que

$$\sigma = \gamma_1 \gamma_2 \cdots \gamma_p$$

où $\forall i \in \llbracket 1, p \rrbracket$, γ_i est un cycle et $\forall i \neq j$, $\text{Supp}(\gamma_i) \cap \text{Supp}(\gamma_j) = \emptyset$.
On pose $\gamma_1 = (a_1 \ a_2 \ \cdots \ a_k)$. Donc

$$\begin{aligned}\sigma(a_1) &= \gamma_1 \circ \cdots \circ \gamma_p(a_1) \\ &= \gamma_1 \circ \cdots \circ \gamma_{p-1}(a_1) (\text{ car } a_1 \in \text{Supp}(\gamma_1) \text{ donc } a_1 \notin \text{Supp}(\gamma_p)) \\ &\quad \vdots \\ &= \gamma_1(a_1) = a_2.\end{aligned}$$

De même,

$$\sigma(a_2) = \gamma_1(a_2) = a_3$$

\vdots

$$\sigma(a_{k-1}) = \gamma_1(a_{k-1}) = a_k$$

$$\sigma(a_k) = \gamma_1(a_k) = a_1$$

De même,

$$\forall i \in \llbracket 1, p \rrbracket, \text{ Supp}(\gamma_i) \text{ est un orbite de } \sigma.$$

En d'autres termes, si σ a pour orbites $O(x_1), O(x_2), \dots, O(x_p), \{x_{p+1}\}, \dots, \{x_q\}$

avec $x_1, \dots, x_p \in \text{Supp}(\sigma)$ alors

$$\left\{ \begin{array}{l} \gamma_1 = \begin{pmatrix} x_1 & \sigma(x_1) & \sigma^2(x_1) & \dots \end{pmatrix} \\ \gamma_2 = \begin{pmatrix} x_2 & \sigma(x_2) & \sigma^2(x_2) & \dots \end{pmatrix} \\ \vdots \\ \gamma_p = \begin{pmatrix} x_p & \sigma(x_p) & \sigma^2(x_p) & \dots \end{pmatrix} \end{array} \right.$$

Synthèse ok!

□

Proposition: Soit γ un k -cycle.

Alors l'ordre de γ est k :

$$\left\{ \begin{array}{l} \gamma^k = \text{id} \\ \forall \ell \in \llbracket 1, k-1 \rrbracket, \gamma^\ell \neq \text{id} \end{array} \right.$$

Preuve:

On pose $\gamma = (a_1 \ a_2 \ \dots \ a_k)$ avec

$$\forall i \neq j, a_i \neq a_j.$$

Soit $\ell \in \llbracket 1, k-1 \rrbracket$. Alors

$$\gamma^\ell = a_{1+\ell} \neq a_1 \text{ car } 1 + \ell \leq k$$

donc $\gamma^\ell \neq \text{id}$.

Soit $i \in \llbracket 1, k \rrbracket$. Alors

$$\gamma^k(a_i) = a_j$$

$$\text{avec } \begin{cases} j \in \llbracket 1, k \rrbracket \\ j \equiv i+k \pmod{k} \end{cases} \quad \text{donc } a_j = a_i.$$

$$\forall x \notin \{a_1, \dots, a_k\}, \gamma(x) = x$$

donc $\gamma^k(x) = x$ et donc $\gamma^k = \text{id}$.

□

Proposition: Soit $\gamma = (a_1 \ \dots \ a_k)$ un k -cycle et $\sigma \in S_n$. Alors

$$\sigma \gamma \sigma^{-1} = (\sigma(a_1) \ \dots \ \sigma(a_k))$$

est un k -cycle.

Preuve:

Soit $x \notin \{\sigma(a_1), \dots, \sigma(a_k)\}$. σ est bijective : soit $y \in \llbracket 1, n \rrbracket$ tel que $\sigma(y) = x$.

De plus, $y \notin \{a_1, \dots, a_k\}$.

D'où

$$\begin{aligned}\sigma\gamma\sigma^{-1} &= \sigma\gamma\sigma^{-1}(\sigma(y)) \\ &= \sigma\gamma(y) \\ &= \sigma(y) \\ &= x.\end{aligned}$$

Soit $i \in \llbracket 1, k-1 \rrbracket$.

$$\begin{aligned}\sigma\gamma\sigma^{-1}(\sigma(a_i)) &= \sigma\gamma(a_i) = \sigma(a_{i+1}) \\ \sigma\gamma\sigma^{-1}(\sigma(a_k)) &= \sigma\gamma(a_k) = \sigma(a_1).\end{aligned}$$

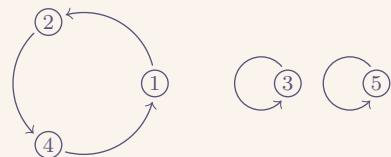
□

3 Transpositions

Définition: Une transposition est un cycle de longueur 2 : $(a \quad b)$ avec $a \neq b$.

EXEMPLE:

Avec $n = 5$ et $\gamma = (2 \quad 4 \quad 1)$.



$$\gamma = (1 \quad 4) (1 \quad 2)$$

$$\text{Avec } n = 6 \text{ et } \gamma = (1 \quad 3 \quad 5 \quad 6 \quad 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix}.$$

Donc,

$$\gamma = (1 \quad 2) (1 \quad 6) (1 \quad 5) (1 \quad 3)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 1 & 6 \\ 3 & 2 & 5 & 4 & 6 & 1 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix}$$

Et,

$$\gamma = (1 \quad 3) (2 \quad 3) (3 \quad 5) (5 \quad 6)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 6 & 5 \\ 1 & 2 & 5 & 4 & 6 & 3 \\ 1 & 3 & 5 & 4 & 6 & 2 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix}$$

EXEMPLE:

$$(1 \quad 4) = (1 \quad 2) (2 \quad 3) (3 \quad 4) (2 \quad 3) (1 \quad 2)$$

On n'a pas toujours le même nombre de transpositions mais la parité du nombre reste la même (proposition plus loin).

Théorème: Toute permutation se décompose en produit de transpositions.

Preuve:

Soit $\gamma = (a_1 \dots a_k)$ un k -cycle.

On remarque que

$$\gamma = (a_1 \ a_k) \cdots (a_1 \ a_4) (a_1 \ a_3) (a_1 \ a_2)$$

C'est un produit de transpositions. \square

EXEMPLE:

Avec $n = 10$ et $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 8 & 1 & 7 & 2 & 3 & 4 & 5 & 10 & 6 \end{pmatrix}$.

On a

$$\begin{aligned} \sigma &= (1 \ 9 \ 10 \ 6 \ 3) (2 \ 8 \ 5) (4 \ 7) \\ &= (1 \ 3) (1 \ 6) (1 \ 10) (1 \ 9) (2 \ 5) (2 \ 8) (4 \ 7) \end{aligned}$$

Vérification :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 2 & 3 & 7 & 5 & 6 & 4 & 8 & 9 & 10 \\ 1 & 8 & 3 & 7 & 5 & 6 & 4 & 2 & 9 & 10 \\ 1 & 8 & 3 & 7 & 2 & 6 & 4 & 5 & 9 & 10 \\ 9 & 8 & 3 & 7 & 2 & 6 & 4 & 5 & 1 & 10 \\ 9 & 8 & 3 & 7 & 2 & 6 & 4 & 5 & 10 & 1 \\ 9 & 8 & 3 & 7 & 2 & 1 & 4 & 5 & 10 & 6 \\ 9 & 8 & 1 & 7 & 2 & 3 & 4 & 5 & 10 & 6 \end{pmatrix}$$

4 Signature d'une permutation

Définition: Soit $\sigma \in S_n$.

Un inversion de σ est $(i, j) \in \llbracket 1, n \rrbracket^2$ tel que $i < j$ et $\sigma(i) > \sigma(j)$.

La signature de σ , notée $\varepsilon(\sigma)$ vaut $(-1)^k$ où k est le nombre d'inversions de σ .

EXEMPLE:

Avec $n = 10$ et $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 8 & 1 & 7 & 2 & 3 & 4 & 5 & 10 & 6 \end{pmatrix}$.

Les inversions de σ sont $(1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (1, 7), (1, 8), (1, 10), (2, 3), (2, 4), (2, 5), (2, 6), (2, 7), (2, 8), (2, 10), (4, 5), (4, 6), (4, 7), (4, 8), (4, 10), (9, 10)$.

Donc, $\varepsilon(\sigma) = (-1)^{21} = -1$.

Proposition: Soit τ une transposition. Alors $\varepsilon(\tau) = -1$.

Preuve:

On pose $\tau = (a \ b)$ avec $a < b$.

Donc

$$\tau = \begin{pmatrix} 1 & 2 & \cdots & a & \cdots & b & \cdots & n \\ 1 & 2 & \cdots & b & \cdots & a & \cdots & n \end{pmatrix}$$

τ a pour inversion $(a, a+1), (a, a+2), \dots, (a, b), (a+1, b), (a+2, b), \dots, (b-1, b)$.

Donc

$$\varepsilon(\tau) = (-1)^{b-a+b-a+1} = (-1)^{2(b-a)+1} = -1.$$

□

Théorème: $\varepsilon : (S_n, \circ) \rightarrow (\{-1, 1\}, \times)$ est un morphisme de groupes.

Preuve:

Soient $(\sigma_1, \sigma_2) \in (S_n)^2$. On a

$$\varepsilon(\sigma_1) = \prod_{i < j} \frac{\sigma_1(i) - \sigma_1(j)}{i - j}$$

donc

$$\begin{aligned} \varepsilon(\sigma_1 \sigma_2) &= \prod_{i < j} \frac{\sigma_1 \sigma_2(i) - \sigma_1 \sigma_2(j)}{i - j} \\ &= \prod_{i < j} \frac{\sigma_1(\sigma_2(i)) - \sigma_1(\sigma_2(j))}{\sigma_2(i) - \sigma_2(j)} \times \frac{\sigma_2(i) - \sigma_2(j)}{i - j} \\ &= \prod_{\substack{k, \ell \\ \sigma_2^{-1}(k) < \sigma_2^{-1}(\ell)}} \frac{\sigma_1(k) - \sigma_1(\ell)}{k - \ell} \times \varepsilon(\sigma_2) \\ &= \prod_{i < j} \frac{\sigma_1(i) - \sigma_1(j)}{i - j} \times \varepsilon(\sigma_2) \\ &= \varepsilon(\sigma_1) \varepsilon(\sigma_2). \end{aligned}$$

□

Définition: On dit qu'une permutation σ est paire si $\varepsilon(\sigma) = 1$, impaire si $\varepsilon(\sigma) = -1$.

Proposition – Définition: On note

$$A_n = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\}.$$

C'est un sous-groupe de S_n : on l'appelle groupe alterné.

Preuve:

$$A_n = \text{Ker}(\varepsilon)$$

□

EXEMPLE:

Avec

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}$$

donc

$$\begin{aligned} \prod_{i < j} \frac{\sigma(j) - \sigma(i)}{j - i} &= \frac{(3-1)(2-1)(5-1)(4-1)}{(2-1)(3-1)(4-1)(5-1)} \\ &\times \frac{(2-3)(5-3)(4-3)}{(3-2)(4-2)(5-2)} \\ &\times \frac{(5-2)(4-2)}{(4-3)(5-3)} \\ &\times \frac{4-5}{5-4} \\ &= -1. \end{aligned}$$

REMARQUE:

$$\#A_n = \frac{n!}{2}. \text{ En effet :}$$

$$\begin{aligned} A_n &\longrightarrow \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\} \\ \sigma &\longmapsto (1 \quad 2) \sigma \end{aligned}$$

est une bijection.

EXERCICE:

Problème :

Soit $\sigma \in S_n$. σ est-il un produit des cycles $\gamma_k = (k \quad k-1 \quad k-2 \quad \cdots \quad 1)$ avec $k \in \llbracket 1, N \rrbracket$?

Avec $N = 5$ et $\gamma = (2 \quad 3 \quad 5)$, $\left\{ \begin{array}{l} \gamma_2 = (1 \quad 2) \\ \gamma_3 = (3 \quad 2 \quad 1) \\ \gamma_4 = (4 \quad 3 \quad 2 \quad 1) \\ \gamma_5 = (5 \quad 4 \quad 3 \quad 2 \quad 1) \end{array} \right.$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \\ 1 & 3 & 5 & 2 & 4 \\ 2 & 3 & 5 & 1 & 4 \\ 1 & 2 & 5 & 4 & 3 \\ 3 & 1 & 5 & 4 & 2 \\ 2 & 3 & 5 & 4 & 1 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix} \begin{array}{l} \gamma_3 \\ \gamma_2 \\ \gamma_5 \\ \gamma_3 \\ \gamma_2 \\ \gamma_4 \\ \gamma_3 \\ \gamma_2 \end{array}$$

5 Bilan

$$\#S_n = n!.$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}.$$

On dit que d est l'ordre de σ si

$$\begin{cases} \sigma^d = \text{id}; \\ \forall i \in \llbracket 1, d-1 \rrbracket, \sigma^i \neq \text{id}. \end{cases}$$

Soit γ un k -cycle :

$$\gamma = (a_1 \dots a_n - k).$$

Alors, pour toute permutation σ ,

$$\sigma\gamma\sigma^{-1} = (\sigma(a_1) \dots \sigma(a_k)) I$$

et c'est un k -cycle.

L'orbite de σ pour $x \in \llbracket 1, n \rrbracket$ est

$$\{x, \sigma(x), \dots, \sigma^{d-1}(x)\}$$

où d est l'ordre de σ .

Une transposition est un cycle de longueur 2.

On dit que σ est un k -cycle si

- σ a $n-k$ points fixes ;
- les autres éléments sont dans une même orbite.

Toute permutation se décompose en produit de transpositions mais cette décomposition n'est pas unique.

Dans ce cas, σ est noté

$$\sigma = (x \quad \sigma(x) \quad \sigma^2(x) \quad \dots \quad \sigma^{k-1}(x))$$

et l'ordre de σ est k .

Une inversion est un couple (i, j) avec $i < j$ mais $\sigma(i) > \sigma(j)$.

Le support de σ est l'ensemble des éléments qui "changent" après l'application de σ :

$$\text{Supp}(\sigma) = \{x \in \llbracket 1, n \rrbracket \mid \sigma(x) \neq x\}.$$

La signature d'une permutation σ est $\varepsilon(\sigma) = (-1)^k$ où k est le nombre d'inversions. C'est un morphisme de groupes donc

$$\varepsilon\left(\prod_{i=1}^N \sigma_i\right) = \prod_{i=1}^N \varepsilon(\sigma_i).$$

La signature d'une transposition est -1 .

Toute permutation peut être décomposée, de manière unique, en cycles à supports disjoints.

Une permutation paire est une permutation de signature 1.

Une permutation impaire est une permutation de signature -1 .

L'ensemble des permutations paires forment un sous-groupe : le groupe alterné.

CHAPITRE

25

SÉRIES NUMÉRIQUES

1 Définitions et premières propriétés

Définition: Soit $(u_n)_{n \in \mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$. La suite des sommes partielles associée à (u_n) est

$$\forall n \in \mathbb{N}, S_n = \sum_{k=0}^n u_k.$$

Étudier la série des (u_n) , c'est étudier la convergence de la suite (S_n) .

On dit que la série $\sum u_n$ converge si (S_n) converge. Dans ce cas, $\lim_{n \rightarrow +\infty} S_n$ est notée $\sum_{n=0}^{+\infty} u_n$ et on l'appelle la somme de la série, et la suite définie par

$$\forall n \in \mathbb{N}, R_n = \sum_{k=n+1}^{+\infty} u_k$$

est appelée suite des restes partiels.

EXEMPLE (À connaître : série géométrique):

Soit $q \in \mathbb{C}$.

$$\forall n \in \mathbb{N}, \sum_{k=0}^n q_k = \begin{cases} \frac{1 - q^{n+1}}{1 - q} & \text{si } q \neq 1 \\ n + 1 & \text{si } q = 1 \end{cases}$$

Cette série converge si et seulement si $|q| < 1$, et dans ce cas $\sum_{k=0}^{+\infty} q^n = \frac{1}{1 - q}$.

Par exemple, avec $q = 1/2$, on a

$$\sum_{n=0}^{+\infty} \left(\frac{1}{2}\right)^n = \frac{1}{1 - \frac{1}{2}} = 2$$

et

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

Proposition: Soit $(v_n) \in \mathbb{C}^{\mathbb{N}}$.
La série $\sum(v_{n+1} - v_n)$ converge si et seulement si (v_n) .

Preuve:

$$\forall n \in \mathbb{N}, \sum_{k=0}^n (v_{k+1} - v_k) = v_{n+1} - v_0.$$

□

Proposition: Soit $\sum u_n$ une série.
Si $\sum u_n$ converge **ALORS** $u_n \rightarrow 0$.

REMARQUE:
La réciproque est **FAUSSE**.

CONTRE-EXEMPLE (série harmonique):
La série $\sum \frac{1}{n}$ diverge. En effet, on a vu en T.D. :

$$\forall n \in \mathbb{N}^*, \sum_{k=1}^n \frac{1}{k} = \ln(n) + \gamma + \underset{n \rightarrow +\infty}{\circ}(1)$$

où γ est la constante d'Euler.

Preuve:

On pose

$$\forall n \in \mathbb{N}, S_n = \sum_{k=0}^n u_k.$$

On suppose que (S_n) converge vers $S \in \mathbb{C}$. On a donc

$$\forall n \in \mathbb{N}^*, u_n = S_n - S_{n-1} \xrightarrow{n \rightarrow +\infty} S - S = 0.$$

□

REMARQUE:
Avec les notations précédentes, si $u_n \not\longrightarrow 0$, alors $\sum u_n$ diverge. On dit qu'elle diverge grossièrement.

2 Séries à termes positifs

Proposition: Soit $(u_n) \in (\mathbb{R}^+)^{\mathbb{N}}$. Alors $\left(\sum_{k=0}^n u_k \right)_{n \in \mathbb{N}}$ est croissante.

Preuve:

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

□

Théorème: Soient u et v deux suites réelles telles que

$$\forall n \in \mathbb{N}, 0 \leq u_n \leq v_n.$$

1. Si $\sum v_n$ converge, ALORS $\sum u_n$ converge
2. Si $\sum u_n$ diverge, ALORS $\sum v_n$ diverge.

Preuve: 1. On suppose que $\sum v_n$ converge. On note

$$\forall n \in \mathbb{N}, S_n(v) = \sum_{k=0}^n v_k.$$

Donc $(S_n(v))$ est majorée. Soit V un majorant et $n \in \mathbb{N}$.

$$\forall k, 0 \leq u_k \leq v_k$$

donc

$$\sum_{k=0}^n u_k \leq \sum_{k=0}^n v_k = S_n(v) \leq V$$

donc $\left(\sum_{k=0}^n u_k \right)_{n \in \mathbb{N}}$ est majorée. Or, elle est croissante, donc elle converge.

2. C'est la contraposée du 1.

□

CONTRE-EXEMPLE:

$\sum \frac{1}{n}$ diverge, $\sum \frac{1}{n^2}$ converge (vers $\frac{\pi^2}{6}$) et

$$\forall n \in \mathbb{N}, 0 \leq \frac{1}{n^2} \leq \frac{1}{n}.$$

Corollaire: Soient u, v deux suites réelles **POSITIVES** telles que $u = O(v)$.

1. Si $\sum v_n$ converge, alors $\sum u_n$ converge.
2. Si $\sum u_n$ diverge, alors $\sum v_n$ diverge.

[]

□

Théorème: Soient u et v deux suites réelles **POSITIVES** telles que $u = o(v)$.

1. Si $\sum v_n$ converge, alors $\sum u_n$ converge.
2. Si $\sum u_n$ diverge, alors $\sum v_n$ diverge.

□

Théorème (règle des équivalents): Soient u et v deux suites réelles **POSITIVES** telles que $u \sim v$. Alors

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

Preuve:

On suppose

$$u_n = v_n + o(v_n)$$

et donc

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, |u_n - v_n| \leq \varepsilon |v_n|$$

En particulier, on peut considérer $N \in \mathbb{N}$ tel que

$$\forall n \geq N, -\frac{1}{2}v_n \leq u_n - v_n \leq \frac{1}{2}v_n$$

et donc

$$\forall n \geq N, \frac{1}{2}v_n \leq u_n \leq \frac{3}{2}v_n$$

et donc $\begin{cases} u = O(v), \\ v = O(u). \end{cases}$

Si $\sum v_n$ converge, alors $\sum u_n$ converge car $u = O(v)$.

Si $\sum u_n$ converge, alors $\sum v_n$ converge car $v = O(u)$. □

EXEMPLE:

Déterminer la nature de $\sum \frac{1}{n^3 + n \ln(n)}$?

$$\forall n \geq 3, \frac{1}{n^3 + n \ln n} \geq 0.$$

et

$$\frac{1}{n^3 + n \ln n} \underset{n \rightarrow +\infty}{\sim} \frac{1}{n^3}.$$

$$\forall n \geq 1, \frac{1}{n^3} \leq \frac{1}{n^2}$$

$\sum \frac{1}{n^2}$ converge donc $\sum \frac{1}{n^3}$ converge donc $\sum \frac{1}{n^3 + n \ln n}$ converge.

3 Comparaison avec une intégrale

[]

Théorème: Soit $\alpha \in \mathbb{R}$.

$$\sum \frac{1}{n^\alpha} \text{ converge} \iff \alpha > 1$$

Dans ce cas, on note

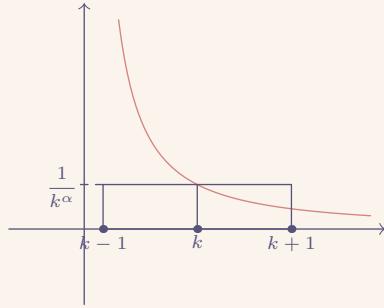
$$\zeta(\alpha) = \sum_{n=1}^{+\infty} \frac{1}{n^\alpha}.$$

Preuve:

$$\frac{1}{n^\alpha} \xrightarrow[n \rightarrow +\infty]{} \begin{cases} 0 & \text{si } \alpha > 0 \\ 1 & \text{si } \alpha = 0 \\ +\infty & \text{si } \alpha < 0 \end{cases}$$

donc $\sum \frac{1}{n^\alpha}$ diverge pour $\alpha \leq 0$.

On suppose $\alpha > 0$. Soit $f_\alpha : \mathbb{R}_*^+ \rightarrow \mathbb{R}$



Soit $k \in \mathbb{N}$ avec $k \geq 2$. comme f_α est décroissante,

$$\forall k \in [k, k+1], f_\alpha(x) \leq f_\alpha(k)$$

et donc

$$\int_k^{k+1} \frac{1}{x^\alpha} dx \leq \int_k^{k+1} \frac{1}{k^\alpha} dx = \frac{1}{k^\alpha}.$$

De même,

$$\forall k \in [k-1, k], f_\alpha(x) \geq f_\alpha(k)$$

et donc

$$\int_{k-1}^k \frac{1}{x^\alpha} dx \geq \int_{k-1}^k \frac{1}{k^\alpha} dx = \frac{1}{k^\alpha}.$$

Soit $n \in \mathbb{N}$ avec $n \geq 2$.

$$\forall k \in [\![2, n]\!], \int_k^{k+1} \frac{1}{x^\alpha} dx \leq \frac{1}{k^\alpha} \leq \int_{k-1}^k \frac{1}{x^\alpha} dx$$

donc

$$\int_2^{n+1} \frac{1}{x^\alpha} dx \leq \sum_{k=2}^n \frac{1}{k^\alpha} \leq \int_1^n \frac{1}{x^\alpha} dx$$

Cas1 On suppose $\alpha > 1$. Alors

$$\begin{aligned} \forall n \geq 2, \sum_{k=1}^n \frac{1}{k^\alpha} &\leq 1 + \int_1^n \frac{1}{x^\alpha} dx = 1 + \left[\frac{x^{-\alpha+1}}{-\alpha+1} \right]_1^n \\ &\leq 1 + \frac{1}{1-\alpha} \left(\frac{1}{n^{\alpha-1}} - 1 \right) \\ &\leq 1 + \frac{1}{\alpha-1} \left(1 - \frac{1}{n^{\alpha-1}} \right) \\ &\leq 1 + \frac{1}{\alpha-1}. \end{aligned}$$

La suite $\left(\sum_{k=1}^n \frac{1}{k^\alpha} \right)_n$ est croissante et majorée donc elle converge.

Cas2 On suppose $\alpha = 1$.

$$\forall n \geq 2, \sum_{k=1}^n \frac{1}{k} \geq 1 + \int_2^{n+1} \frac{1}{x} dx \geq \underbrace{1 + \ln(n+1) - \ln 2}_{n \rightarrow +\infty} \rightarrow +\infty$$

Par comparaison, $\sum_{k=1}^n \frac{1}{k} \xrightarrow{n \rightarrow +\infty} +\infty$.

Cas3 On suppose $\alpha < 1$.

$$\begin{aligned} \forall n \geq 2, \sum_{k=1}^n \frac{1}{k^\alpha} &\geq 1 + \int_2^{n+1} \frac{1}{x^\alpha} dx \\ &\geq 1 + \left[\frac{x^{-\alpha+1}}{-\alpha+1} \right]_2^{n+1} \\ &\geq 1 + \underbrace{\frac{1}{1-\alpha} \left(\frac{1}{(n+1)^{\alpha-1}} - \frac{1}{2^{\alpha-1}} \right)}_{n \rightarrow +\infty \text{ car } \alpha < 1} \end{aligned}$$

Donc, $\sum_{k=1}^n \frac{1}{k^\alpha} \xrightarrow{n \rightarrow +\infty} +\infty$.

□

Théorème: Soit $f : [a, +\infty[\rightarrow \mathbb{R}^+$ continue, décroissante de limite nulle, avec $a \in \mathbb{N}$.
Alors,

$$\sum_{n \geq a} f(n) \text{ converge} \iff \left(\int_a^n f(x) dx \right)_n \text{ converge.}$$

Preuve:

Soit $k \in \mathbb{N}$ tel que $k \geq a+1$.

$$\forall x \in [k, k+1], f(x) \leq f(k)$$

donc

$$\int_k^{k+1} f(x) dx \leq \int_k^{k+1} f(k) dx = f(k)$$

et

$$\forall x \in [k-1, k], f(x) \geq f(k)$$

et donc

$$\int_{k-1}^k f(x) \, dx \geq \int_{k-1}^k f(k) \, dx = f(k).$$

Donc, $\forall n \in \mathbb{N}$ avec $n \geq a+1$

$$\int_{a+1}^{n+1} f(x) \, dx \leq \sum_{a+1 \leq k \leq n} f(k) \leq \int_a^n f(x) \, dx.$$

CAS1 On suppose que $\left(\int_a^n f(x) \, dx \right)_n$ converge. Cette suite est croissante, donc majorée. Soit M un majorant donc

$$\forall n \geq a+1, \sum_{a \leq k \leq n} f(k) \leq f(a) + M.$$

donc la série converge.

— On suppose que $\left(\int_a^n f(x) \, dx \right)_n$ diverge donc, par croissance de cette suite,

$$\lim_{n \rightarrow +\infty} \int_a^n f(x) \, dx = +\infty$$

et donc

$$\begin{aligned} \forall n \geq a+1, \sum_{k=a}^n f(k) &= f(a) + \sum_{k=a+1}^n f(k) \\ &\geq \underbrace{f(a) + \int_a^n f(x) \, dx}_{n \rightarrow +\infty} - \underbrace{\int_a^{a+1} f(x) \, dx}_{\rightarrow +\infty} \end{aligned}$$

donc la série diverge.

□

EXERCICE:

Quelle est la nature de la série $\sum \frac{1}{n \ln(n)}$?

EXERCICE:

Quelle est la nature de la série $\sum \frac{\ln^\alpha(n)}{n^\beta}$ en fonction de α et β ?

4 Opérations sur les séries

Proposition: L'ensemble $E = \{u \in \mathbb{C}^{\mathbb{N}} \mid \sum u_n \text{ converge}\}$ est un sous-espace vectoriel de $\mathbb{C}^{\mathbb{N}}$ et

$$\begin{aligned} S : E &\longrightarrow \mathbb{C} \\ u &\longmapsto \sum_{n=0}^{+\infty} u_n \end{aligned}$$

est une forme linéaire. □

REMARQUE:

La somme d'une série convergente et d'une série divergente diverge. Le produit d'une série divergente par un scalaire non nul diverge.

5 Séries absolument convergente

Théorème: Soit $(u_n) \in \mathbb{C}^{\mathbb{N}}$. Si $\sum |u_n|$ converge, ALORS $\sum u_n$ converge.

REMARQUE:

La réciproque est FAUSSE. On a vu en exercice que la série harmonique alternée $\sum \frac{(-1)^{n+1}}{n}$ converge vers $\ln 2$, alors que $\sum \frac{1}{n}$ diverge.

Preuve: CAS1 On suppose $u \in \mathbb{R}^{\mathbb{N}}$. On pose

$$\forall n \in \mathbb{N}, u_n^+ = \begin{cases} u_n & \text{si } u_n \geq 0 \\ 0 & \text{si } u_n < 0 \end{cases}$$

et

$$u_n^- = \begin{cases} -u_n & \text{si } u_n \leq 0 \\ 0 & \text{si } u_n > 0. \end{cases}$$

Ainsi,

$$\forall n \in \mathbb{N}, \begin{cases} u_n^+ \geq 0, \\ u_n^- \geq 0, \\ u_n = u_n^+ - u_n^-, \\ |u_n| = u_n^+ + u_n^-. \end{cases}$$

On suppose que $\sum |u_n|$ converge. Or,

$$\forall n \in \mathbb{N}, 0 \leq u_n^+ \leq u_n^+ + u_n^- = |u_n|$$

donc $\sum u_n^+$ converge. De même,

$$\forall n \in \mathbb{N}, 0 \leq u_n^- \leq u_n^- + u_n^+ = |u_n|$$

donc $\sum u_n^-$ converge. Par linéarité, $\sum u_n$ converge.
CAS2 $u \in \mathbb{C}^{\mathbb{N}}$. On suppose que $\sum |u_n|$ converge. On pose

$$\forall n \in \mathbb{N}, \begin{cases} v_n = \Re(u_n) \in \mathbb{R} \\ w_n = \Im(u_n) \in \mathbb{R} \end{cases}$$

Or,

$$\forall n \in \mathbb{N}, 0 \leq |v_n| \leq |u_n|$$

donc $\sum |v_n|$ converge donc d'après le CAS 1, $\sum v_n$ converge.
De même,

$$\forall n \in \mathbb{N}, 0 \leq |w_n| \leq |u_n|$$

donc $\sum w_n$ converge.

Par linéarité, $\sum u_n$ converge.

□

Définition: Soit $u \in \mathbb{C}^{\mathbb{N}}$. On dit que $\sum u_n$ converge absolument si $\sum |u_n|$ converge. On dit que $\sum u_n$ est semi-convergente si

$$\begin{cases} \sum u_n \text{ converge,} \\ \sum |u_n| \text{ diverge.} \end{cases}$$

Corollaire: Soit $u \in \mathbb{C}^{\mathbb{N}}$ et $v \in (\mathbb{R}^+)^{\mathbb{N}}$ telles que $u = O(v)$.
Si $\sum v_n$ converge, alors $\sum u_n$ converge absolument.

□

EXEMPLE:

Quelle est la nature de la série $\sum_{n \geq 1} \frac{(-1)^n}{n^2} \sin\left(\frac{1}{n}\right)$?

$$\left| \frac{(-1)^n}{n^2} \sin\left(\frac{1}{n}\right) \right| = \frac{1}{n^2} \left| \sin\frac{1}{n} \right| \sim \frac{1}{n^3}$$

donc $\sum \frac{(-1)^n}{n^2} \sin\left(\frac{1}{n}\right)$ converge.

EXEMPLE:

Quelle est la nature de $\sum (-1)^n \sin\left(\frac{1}{n}\right)$?

$$\sin\frac{1}{n} = \frac{1}{n} + O\left(\frac{1}{n^2}\right)$$

donc

$$(-1)^n \sin\frac{1}{n} = \frac{(-1)^n}{n} + O\left(\frac{1}{n^2}\right).$$

$\sum O\left(\frac{1}{n^2}\right)$ converge absolument donc converge.

$\sum \frac{(-1)^n}{n}$ converge.

Par linéarité, $\sum (-1)^n \sin\frac{1}{n}$ converge.

6 Séries alternées

Théorème: Soit $u \in (\mathbb{R}^+)^{\mathbb{N}}$ décroissante de limite nulle. Alors $\sum (-1)^n u_n$ converge.

Preuve:

On pose

$$\forall n \in \mathbb{N}, S_n = \sum_{k=0}^n (-1)^k u_k$$

Montrons que (S_{2n}) et (S_{2n+1}) sont adjacentes.— Soit $n \in \mathbb{N}$.

$$\begin{aligned} S_{2n+2} - S_{2n} &= (-1)^{2n+1} u_{2n+1} + (-1)^{2n+2} u_{2n+2} \\ &= u_{2n+2} - u_{2n+1} \leq 0 \end{aligned}$$

Donc $(S_{2n})_n$ est décroissante.— Soit $n \in \mathbb{N}$.

$$S_{2n+3} - S_{2n+1} = u_{2n+2} - u_{2n+3} \geq 0$$

Donc la suite $(S_{2n+1})_n$ est croissante.— $\forall n \in \mathbb{N}, S_{2n+1} - S_{2n} = -u_{2n+1} \xrightarrow{n \rightarrow +\infty} 0$.

Ainsi, (S_{2n}) et (S_{2n+1}) convergent et ont la même limite, donc (S_n) converge. On note
 $S = \lim_{n \rightarrow +\infty} S_n$:

$$\forall n \in \mathbb{N}, S_{2n+1} \leq S \leq S_{2n}$$

donc

$$\forall n \in \mathbb{N}, R_{2n+1} \geq 0 \geq R_{2n}.$$

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

$$|R_{2n+1}| = R_{2n+1} = S - S_{2n+1} \leq S_{2n} - S_{2n+1} = u_{2n+1},$$

$$|R_{2n}| = -R_{2n} = S_{2n} - S \leq S_{2n} - S_{2n+1} \leq u_{2n+1} \leq u_{2n}.$$

Ainsi,

$$\forall n \in \mathbb{N}, |R_n| \leq u_n.$$

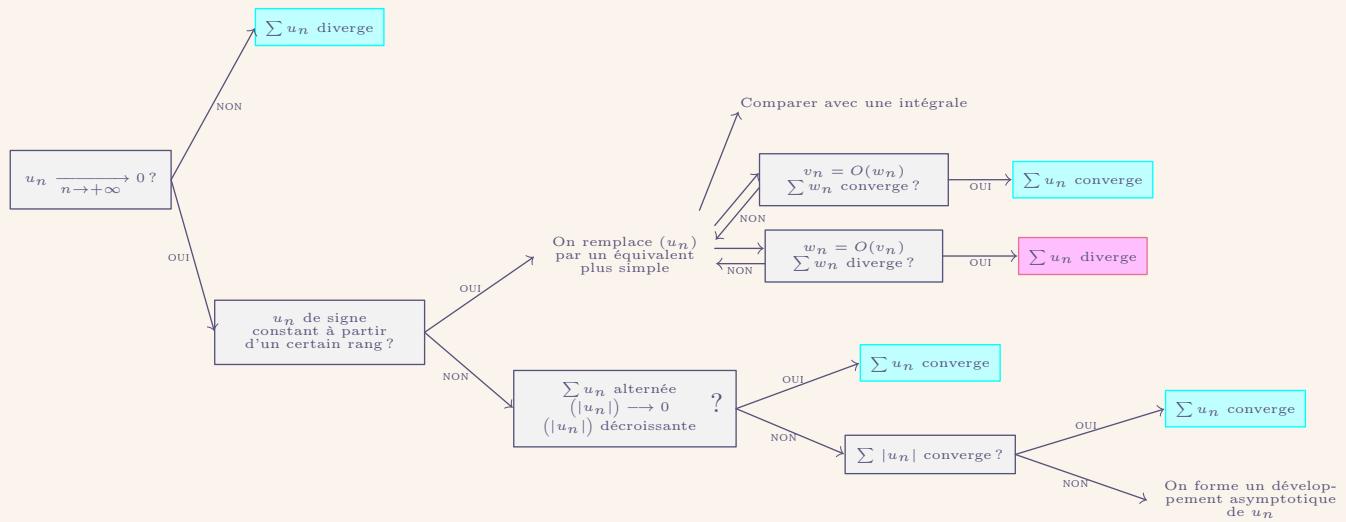
□

Proposition: Soit u une suite de signe constant telle que $(|u_n|)_n$ est décroissante de limite nulle. Alors, $\sum (-1)^n u_n$ converge et

$$\forall n \in \mathbb{N}, R_n \text{ est du signe de } (-1)^{n+1} u_{n+1} \text{ et } |R_n| \leq |u_n|$$

□

7 Résumé et exemples



EXERCICE: 1. $\forall n \in \mathbb{N}^*, u_n = \sqrt[n]{n+1} - \sqrt[n]{n}$,

$$2. \forall n \geq 2, u_n = \ln \left(1 + \frac{(-1)^n}{n} \right),$$

$$3. \forall n \in \mathbb{N}^*, u_n = \sin \left(\frac{\pi}{2n} \right),$$

$$4. \forall n \in \mathbb{N}^*, u_n = \frac{1}{\sum_{k=1}^n \frac{1}{k^\alpha}}.$$

1. Pour $n \in \mathbb{N}^*$,

$$f_n : x \mapsto x^{\frac{1}{n}} = e^{\frac{1}{n} \ln x}$$

donc

$$\forall x > 0, f'_n(x) = \frac{1}{nx} e^{\frac{1}{n} \ln(x)} = \frac{1}{nx} e^{\frac{1}{n} \ln x}.$$

D'après le théorème des accroissements finis,

$$\exists c_n \in [n, n+1], f_n(n+1) - f(n) = f'_n(c_n)$$

donc

$$u_n = \frac{1}{c_n} e^{\frac{1}{n} \ln c_n}.$$

$$\forall n, 1 \leq \frac{c_n}{n} \leq 1 + \frac{1}{n}$$

donc $c_n \underset{n \rightarrow +\infty}{\sim} n$ donc $c_n = n + o(n)$:

$$\begin{aligned} \ln c_n &= \ln(n + o(n)) \\ &= \ln(n(1 + o(1))) \\ &= \ln n + \ln(1 + o(1)) \\ &= \ln(n) + o(1) \\ &\sim \ln n \end{aligned}$$

$$\text{donc } \frac{\ln c_n}{n} \sim \frac{\ln n}{n} \xrightarrow{n \rightarrow +\infty} 0$$

$$\text{donc } e^{\frac{1}{n} \ln c_n} \underset{n \rightarrow +\infty}{\sim} 1$$

$$\text{donc } u_n \sim \frac{1}{n^2}$$

donc $\sum u_n$ converge.

2.

$$\forall n \geq 2, u_n = \frac{(-1)^n}{n} + O\left(\frac{1}{n^2}\right)$$

$\sum \frac{(-1)^n}{n}$ converge et $\sum O\left(\frac{1}{n^2}\right)$ converge absolument. Donc, $\sum u_n$ converge.

3. $u_n \underset{n \rightarrow +\infty}{\sim} \frac{\pi}{2n} \geq 0$ donc $\sum u_n$ diverge.

4.

$$\lim_{n \rightarrow +\infty} \sum_{k=1}^n \frac{1}{k^\alpha} = \begin{cases} \zeta(\alpha) & \text{si } \alpha > 1, \\ \zeta(\alpha) & \text{si } \alpha < 1, \\ +\infty & \text{si } \alpha \leq 1, \end{cases}$$

donc

$$u_n \rightarrow \begin{cases} \frac{1}{\zeta(\alpha)} & \text{si } \alpha > 1, \\ 0 & \text{si } \alpha \leq 1, \end{cases}$$

Si $\alpha > 1$, alors $\sum u_n$ diverge. On suppose $\alpha \leq 1$.

Équivalent de $\sum_{k=1}^n \frac{1}{k^\alpha}$?

Si $\alpha < 1$,

$$\underbrace{\frac{1}{1-\alpha} ((n+1)^{1-\alpha} - 2^{1-\alpha})}_{\sim \frac{n^{1-\alpha}}{1-\alpha}} = \int_2^{n+1} \frac{1}{x^\alpha} dx \leq \sum_{k=2}^n \frac{1}{k^\alpha} \leq \int_1^n \frac{1}{x^\alpha} dx = \underbrace{\frac{1}{1-\alpha} (n^{1-\alpha} - 1)}_{\sim \frac{n^{1-\alpha}}{1-\alpha}}$$

donc

$$\sum_{k=1}^n \frac{1}{k^\alpha} \sim \frac{n^{1-\alpha}}{1-\alpha}$$

donc

$$u_n \sim \frac{1-\alpha}{n^{1-\alpha}}$$

$$\begin{aligned} \sum u_n \text{ converge} &\iff 1-\alpha > 1 \\ &\iff \alpha < 0 \end{aligned}$$

Si $\alpha = 1$, $\sum_{k=1}^n \frac{1}{k} \sim \ln n$ et donc $u_n \sim \frac{1}{\ln n}$.

A-t-on $u_n = o\left(\frac{1}{n^\beta}\right)$ avec $\beta > 1$ ou $\frac{1}{n^\beta} = o(u_n)$ avec $\beta \leq 1$?

Si $\beta \geq 0$,

$$n^\beta u_n \sim \frac{n^\beta}{\ln(n)} \rightarrow +\infty$$

En particulier avec $\beta = \frac{1}{2}$:

$$\frac{1}{n^{\frac{1}{2}}} = o(u_n)$$

et $\sum \frac{1}{n^{\frac{1}{2}}}$ diverge car $\frac{1}{2} < 1$. Donc, $\sum u_n$ diverge.

On a donc

- avec $\alpha \leq 0$, $\sum u_n$ converge,
- avec $\alpha > 0$, $\sum u_n$ diverge.

8 Applications

8.1 Formule de Stirling

Proposition: On a :

$$n! \underset{n \rightarrow +\infty}{\sim} \sqrt{2\pi n} \left(\frac{n}{e}\right)^n ?.$$

Preuve:

$$\forall n \in \mathbb{N}^*, \ln(n!) = \sum_{k=1}^n \ln k.$$

$x \mapsto \ln x$ est strictement croissante sur $[1, +\infty[$ donc

$$\forall k \in \mathbb{N}^*, \forall x \in [k, k+1], \ln x \geq \ln k$$

donc

$$\forall k \in \mathbb{N}^*, \int_k^{k+1} \ln x \, dx \geq \int_k^{k+1} \ln k \, dx = \ln k$$

et

$$\forall k \geq 2, \forall x \in [k-1, k], \ln x \leq \ln k$$

et donc

$$\forall k \geq 2, \int_{k-1}^k \ln x \, dx \leq \int_{k-1}^k \ln k \, dx = \ln k$$

Ainsi

$$\forall n \geq 2, \int_1^n \ln x \, dx \geq \sum_{k=2}^n \leq \int_2^{n+1} \ln x \, dx$$

Or

$$\begin{aligned} \forall n \geq 2, \int_1^n \ln x \, dx &= [x \ln x]_0^n \\ &= n \ln(n) - n + 1 \\ &\underset{n \rightarrow +\infty}{\sim} n \ln n \\ \int_2^{n+1} \ln x \, dx &= (n+1) \ln(n+1) - (n+1) - 2 \ln(2) + 2 \\ &\underset{n \rightarrow +\infty}{\sim} (n+1) \ln(n+1) \\ &\underset{n \rightarrow +\infty}{\sim} n \ln n \end{aligned}$$

car

$$\begin{aligned} \ln(n+1) &= \ln \left(n \left(1 + \frac{1}{n} \right) \right) \\ &= \ln n + \ln \left(1 + \frac{1}{n} \right) \\ &= \ln n + \frac{1}{n} + o\left(\frac{1}{n}\right) \\ &\sim \ln n \end{aligned}$$

Donc

$$\ln(n!) \underset{n \rightarrow +\infty}{\sim} n \ln n$$

Cependant, on a un problème :

$$\begin{aligned} \ln(n!) &= n \ln n + o(n \ln n) \\ \text{donc } n! &= n^n \underbrace{e^{o(n \ln n)}}_? \end{aligned}$$

On pose

$$\forall n \in \mathbb{N}^*, u_n = \ln(n!) - n \ln n$$

(u_n) a même nature que $\sum(u_{n+1} - u_n)$ et

$$\begin{aligned} \forall n \in \mathbb{N}^*, u_{n+1} - u_n &= \ln \left(\frac{(n+1)!}{n!} \right) - (n+1) \ln(n+1) + n \ln n \\ &= n(\ln n - \ln(n+1)) \\ &= n \ln \left(\frac{n}{n+1} \right) \\ &= n \ln \left(1 - \frac{1}{n+1} \right) \\ &\sim -\frac{n}{n+1} \sim -1 < 0 \end{aligned}$$

$\sum(-1)$ diverge donc (u_n) diverge.

Conjecture

$$u_n = \sum_{k=1}^{n-1} (u_{k+1} - u_k) \underset{\downarrow}{\sim} \sum_{k=1}^{n-1} (-1) = -(n-1) \sim -n$$

On n'a absolument pas le droit !

On pose

$$\forall n \in \mathbb{N}^*, v_n = u_n + n$$

et donc

$$\begin{aligned} \forall n \in \mathbb{N}^*, v_{n+1} - v_n &= n \ln \left(1 - \frac{1}{n+1} \right) + 1 \\ &= n \left(-\frac{1}{n+1} - \frac{1}{2(n+1)^2} + o \left(\left(\frac{1}{n+1} \right)^2 \right) \right) + 1 \\ &= n \left(-\frac{1}{n(1+\frac{1}{n})} - \frac{1}{2n^2(1+\frac{1}{n^2})} + o \left(\frac{1}{n^2} \right) \right) + 1 \\ &= - \left(\frac{1}{1+\frac{1}{n}} - \frac{1}{2n} \times \frac{1}{(1+\frac{1}{n})^2} + o \left(\frac{1}{n} \right) \right) \\ &= - \left(1 - \frac{1}{n} + \frac{1}{2n} + o \left(\frac{1}{n} \right) \right) + 1 \\ &= \frac{1}{2n} + o \left(\frac{1}{n} \right) \\ &\sim \frac{1}{2n} > 0. \end{aligned}$$

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

On pose

$$\forall n \in \mathbb{N}^*, w_n = v_n - \frac{1}{2} \ln n$$

et donc

$$\begin{aligned} \forall n \in \mathbb{N}^*, w_{n+1} - w_n &= n \ln \left(1 + \frac{1}{n+1} \right) - \frac{1}{2} \ln(n+1) + \frac{1}{2} \ln(n) + 1 \\ &= n \left(-\frac{1}{n+1} - \frac{1}{2(n+1)^2} - \frac{1}{3(n+1)^3} + o \left(\frac{1}{(n+1)^3} \right) \right) \\ &\quad + 1 + \frac{1}{2} \ln \left(1 - \frac{1}{n+1} \right) \\ &= -1 - \frac{1}{2(n+1)} - \frac{1}{3(n+1)^2} + o \left(\frac{1}{(n+1)^2} \right) \\ &\quad + \frac{1}{n+1} + \frac{1}{2(n+1)^2} + 1 \\ &\quad + \frac{1}{2} \left(-\frac{1}{n+1} - \frac{1}{2(n+1)^2} + o \left(\frac{1}{(n+1)^2} \right) \right) \quad \sim -\frac{1}{12(n+1)^2} \\ &\sim -\frac{1}{12n^2} < 0 \end{aligned}$$

donc $\sum (w_{n+1} - w_n)$ converge et donc (w_n) converge.

On pose $\ell = \lim_{n \rightarrow +\infty} w_n$. Ainsi,

$$\forall n \in \mathbb{N}^*, w_n = \ell + o(1)$$

et donc

$$\forall n \in \mathbb{N}^*, \ln(n!) = n \ln n - n + \frac{1}{2} \ln(n) + \ell + o(1)$$

et alors

$$\begin{aligned} \forall n \in \mathbb{N}^*, n! &= n^n e^{-n} \sqrt{n} e^\ell \underbrace{e^{o(1)}}_{n \rightarrow +\infty} \\ &\sim \left(\frac{n}{e}\right)^n \sqrt{n} \times K \end{aligned}$$

avec $K = e^\ell$.

On pose

$$\forall n \in \mathbb{N}^*, I_n = \int_0^{\frac{\pi}{2}} \sin^n x \, dx \sim \sqrt{\frac{\pi}{2n}}$$

et

(c.f. TD5 / Exercice 8)

$$I_{2n} = \frac{(2n)!}{(2^n n!)^2} \times \frac{\pi}{2}.$$

$$\begin{aligned} I_{2n} &\sim \frac{\pi}{2} \left(\frac{2n}{2e}\right)^{2n} \sqrt{2n} K \left(\frac{e}{n}\right)^{2n} \frac{1}{n} \times \frac{1}{K^2} \\ &\sim \frac{\pi}{K \sqrt{2n}}. \end{aligned}$$

Or

$$I_{2n} \sim \sqrt{\frac{\pi}{4n}}.$$

Donc

$$\frac{\sqrt{\frac{\pi}{4n}}}{\frac{\pi}{K \sqrt{2n}}} \xrightarrow[n \rightarrow +\infty]{} 1$$

donc

$$\frac{K}{\sqrt{2\pi}} \xrightarrow[n \rightarrow +\infty]{} 1$$

et donc $K = \sqrt{2\pi}$. □

8.2 Développement décimal

EXEMPLE: — Avec $x = 0, \underline{5454} \dots$, que vaut $2x$?

— Avec $x = 0, \underline{3333} \dots$, que vaut $3x$?

— $0.9999 \dots$?

— $3 \times \frac{1}{3} = 1$?

Proposition: Soit $(a_n)_{n \in \mathbb{N}}$ telle que

$$\begin{cases} a_0 \in \mathbb{Z}, \\ \forall n \geq 1, a_n \in \llbracket 0, 9 \rrbracket \end{cases}$$

La série $\sum \frac{a_n}{10^n}$ converge.

Preuve:

$$\forall n \geq 1, 0 \leq \frac{a_n}{10^n} \leq \frac{9}{10^n}$$

$\sum \frac{1}{10^n}$ converge car $\frac{1}{10} \in [0, 1[$. Donc $\sum_{n \geq 1} \frac{a_n}{10^n}$ converge donc $\sum_{n \geq 1} \frac{a_n}{10^n}$ converge. \square

Définition: Soit $x \in \mathbb{R}$. On dit que x admet un développement décimal si

$$\exists a_0 \in \mathbb{Z}, (a_n)_{n \geq 1} \in [\![0, 9]\!]^N, x = \sum_{n=0}^{+\infty} \frac{a_n}{10^n}.$$

Théorème: Tou réel $x \in [0, 1[$ admet un développement décimal :

$$x = \sum_{n=1}^{+\infty} \frac{\lfloor 10^n x \rfloor - 10 \lfloor 10^{n-1} x \rfloor}{10^n}$$

Preuve:

$$\begin{aligned} \forall n \geq 1, \quad & 10^n x - 1 < \lfloor 10^n x \rfloor \leq 10^n x \\ & -10^n x + 10 > -10 \lfloor 10^{n-1} x \rfloor \geq -10^n x \end{aligned}$$

donc

$$-1 < \lfloor 10^n x \rfloor - 10 \lfloor 10^{n-1} x \rfloor < 10$$

et donc

$$\lfloor 10^n x \rfloor - 10 \lfloor 10^{n-1} x \rfloor \in [\![0, 9]\!].$$

De plus,

$$\begin{aligned} \sum_{k=1}^n \frac{\lfloor 10^k x \rfloor - 10 \lfloor 10^{k-1} x \rfloor}{10^k} &= \sum_{k=1}^n \left(\frac{\lfloor 10^k x \rfloor}{10^k} - \frac{\lfloor 10^{k-1} x \rfloor}{10^{k-1}} \right) \\ &= \frac{\lfloor 10^n x \rfloor}{10^n} - \underbrace{\lfloor x \rfloor}_{=0} \\ &\xrightarrow[n \rightarrow +\infty]{} x. \end{aligned}$$

\square

Théorème: Soit $x \in]0, 1[$.

1. Si x n'est pas décimal (i.e. on ne peut pas l'écrire comme $p/10^n$ avec $p \in \mathbb{Z}$ et $n \in \mathbb{N}$), alors x a un unique développement décimal.
2. Si x est décimal, alors x a exactement 2 développements décimaux :
 - il y en a un où, à partir d'un certain rang, tous les chiffres sont nuls,
 - et un autre où tous les chiffres sont égaux à 9 à partir d'un certain rang.

Preuve:

Soit $(a_n)_{n \geq 1} \in [\![0, 9]\!]^{\mathbb{N}^*}$ et $(b_n)_{n \geq 1} \in [\![0, 9]\!]^{\mathbb{N}^*}$ telles que

$$x = \sum_{n=1}^{+\infty} \frac{a_n}{10^n} = \sum_{n=1}^{+\infty} \frac{b_n}{10^n}$$

On pose $n_0 = \min\{n \in \mathbb{N}^* \mid a_n \neq b_n\}$:

$$\begin{cases} \forall n < n_0, a_n = b_n, \\ a_{n_0} \neq b_{n_0}. \end{cases}$$

Sans perte de généralité, on suppose $a_{n_0} < b_{n_0}$. On a donc

$$0 < \frac{b_{n_0} - a_{n_0}}{10^{n_0}} = \sum_{n=n_0+1}^{+\infty} \frac{a_n - b_n}{10^n}$$

$$\forall n \geq n_0, \begin{cases} 0 \leq a_n \leq 9 \\ 0 \leq b_n \leq 9 \end{cases}$$

donc

$$\forall n \geq n_0, -9 \leq a_n - b_n \leq 9$$

donc

$$-9 \sum_{n=n_0+1}^{+\infty} \frac{1}{10^n} \leq \sum_{n=n_0+1}^{+\infty} \frac{a_n - b_n}{10^n} \leq 9 \sum_{n=1}^{+\infty} \frac{1}{10^n}.$$

Or,

$$\begin{aligned} \sum_{n=n_0+1}^{+\infty} \frac{1}{10^n} &= \frac{1}{10^{n_0+1}} \sum_{n=0}^{+\infty} \frac{1}{10^n} \\ &= \frac{1}{10^{n_0+1}} \times \frac{1}{1 - \frac{1}{10}} \\ &= \frac{1}{9 \times 10^{n_0}} \end{aligned}$$

D'où,

$$0 < \frac{b_{n_0} - a_{n_0}}{10^{n_0}} \leq \frac{1}{10^{n_0}}$$

donc

$$0 < \underbrace{b_{n_0} - a_{n_0}}_{\in \mathbb{Z}} \leq 1$$

donc $b_{n_0} - a_{n_0} = 1$ et donc

$$\sum_{n=n_0+1}^{+\infty} \frac{a_n - b_n}{10^n} = \frac{1}{10^{n_0}}$$

donc

$$\forall n > n_0, a_n - b_n = 9$$

et donc

$$\forall n > n_0, \begin{cases} a_n = 9 \\ b_n = 0 \end{cases}$$

Comme

$$\forall n > n_0, b_n = 0$$

x est décimal et les deux développements de x sont alors

$$\begin{aligned} x &= 0, a_1 \dots a_{n_0-1} a_{n_0} \underline{9} \dots \\ &= 0, a_1 \dots a_{n_0-1} (a_{n_0} + 1) \underline{0} \dots \end{aligned}$$

□

REMARQUE:

Avec $x = 0,54\underline{54} \dots$, $100x = 54,54\underline{54} \dots = 54 + x$. On a donc $x = \frac{54}{99}$.

Avec $x = 0,987\ 123\ \underline{123} \dots$, on a

$$\begin{aligned} x &= \frac{987}{1000} + 0,000\ \underline{123} \dots \\ &= \frac{987}{1000} + \frac{1}{10^3} \underbrace{(0,\underline{123} \dots)}_y \end{aligned}$$

On a $1000y = 123 + y$ et donc $y = \frac{123}{999}$ et donc $x = \frac{987 + \frac{123}{999}}{1000}$.

8.3 Exponentielle

Proposition:

$$\forall x \in \mathbb{R}, \sum_{n=0}^{+\infty} \frac{x^n}{n!} = e^x$$

Preuve:

(formule de Taylor avec reste intégral)

$$e^x = \sum_{k=0}^n \frac{x^k}{k!} + \int_0^x e^t \frac{(x-t)^n}{n} dt$$

$$\begin{aligned} \left| e^x - \sum_{k=0}^n \frac{x^k}{k!} \right| &\leq \int_0^x e^t \frac{|x-t|^n}{n!} dt \\ &\leq \int_0^x e^x \frac{(x-t)^n}{n!} dt \\ &\leq e^x \left[-\frac{(x-t)^{n+1}}{(n+1)!} \right]_0^x \\ &\leq e^x \frac{x^{n+1}}{(n+1)!} \xrightarrow[n \rightarrow +\infty]{} 0 \end{aligned}$$

car

MÉTHODE 1

$$\begin{aligned} \frac{x^n}{n!} &\sim \frac{x^n}{\sqrt{2\pi n} \left(\frac{n}{e}\right)^n} = \frac{1}{\sqrt{2\pi n}} \left(\frac{ex}{n}\right)^n \\ &= \frac{1}{\sqrt{2\pi n}} e^{n \ln(\frac{ex}{n})} \xrightarrow[n \rightarrow +\infty]{} 0 \end{aligned}$$

MÉTHODE 2

$$\frac{\frac{x^{n+1}}{(n+1)!}}{\frac{x^n}{n!}} = \frac{x}{n+1} \xrightarrow{n \rightarrow +\infty} 0 < 1.$$

□

Proposition:

$$\forall z \in \mathbb{C}, \sum_{n=0}^{+\infty} \frac{z^n}{n!} = e^z$$

□

CHAPITRE

26

DÉTERMINANT

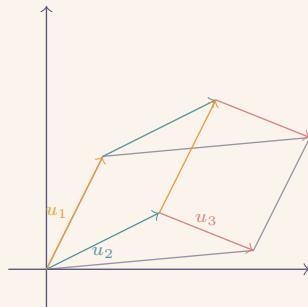
1 Motivation

Soit E un espace vectoriel de dimension n , $\mathcal{B} = (e_1, \dots, e_n)$ une base de E .

Soit $\mathcal{C} = (u_1, \dots, u_n)$ une famille de E . On souhaite trouver un “calcul” sur les coordonnées des vecteurs de \mathcal{C} qui nous dira si \mathcal{C} est un base ou non de E .

EXEMPLE:

Avec $E = \mathbb{R}^2$, $\mathcal{B} = (e_1, e_2)$ base canonique de \mathbb{R}^2 , $\mathcal{C} = (u_1, u_2)$ avec $u_1 = (x, y)$ et $u_2 = (x', y')$.



On note A l’aire orientée (ou algébrique) du parallélogramme engendré par u_1 et u_2 .

Cette aire vérifie :

$$\begin{cases} A(u_1 + u_3, u_2) = A(u_1, u_2) + A(u_3, u_2) \\ A(\lambda u_1, u_2) = \lambda A(u_1, u_2) \\ A(u_2, u_1) = -A(u_1, u_2) \\ A(e_1, e_2) = 1 \end{cases}$$

$$\begin{aligned}
A(u_1, u_2) &= A(xe_1 + ye_2, u_2) \\
&= xA(e_1, u_2) + yA(e_2, u_2) \\
&= xA(e_1, x'e_1 + y'e_2) + yA(e_2, x'e_1 + y'e_2) \\
&= xx'A(e_1, e_1) + xy'A(e_1, e_2) + yx'A(e_2, e_1) + yy'A(e_2, e_2) \\
&= xy' - yx'
\end{aligned}$$

$$(u_1, u_2) \text{ base de } \mathbb{R}^2 \iff xy' - yx' \neq 0$$

REMARQUE:

$$\text{Mat}_{\mathcal{B}}(\mathcal{C}) = \begin{pmatrix} x & x' \\ y & y' \end{pmatrix}$$

EXEMPLE:

$E = \mathbb{R}^3$, (e_1, e_2, e_3) base canonique, $\mathcal{C} = (u_1, u_2, u_3)$ famille de E .

Soit V le volume algébrique du parallélépipède orienté engendré par u_1, u_2 et u_3 .

V est trilinéaire et

$$\begin{cases} V(u_2, u_1, u_3) = -V(u_1, u_2, u_3) \\ V(u_3, u_1, u_2) = V(u_1, u_2, u_3) \\ V(e_1, e_2, e_3) = 1 \end{cases}$$

$$\text{On pose } \begin{cases} u_1 = (x_1, y_1, z_1) \\ u_2 = (x_2, y_2, z_2) \\ u_3 = (x_3, y_3, z_3). \end{cases}$$

$$\begin{aligned}
V(u_1, u_2, u_3) &= V(x_1e_1 + y_1e_2 + z_1e_3, u_2, u_3) \\
&= x_1V(e_1, u_2, u_3) + y_1V(e_2, u_2, u_3) + z_1V(e_3, u_2, u_3) \\
&= x_1y_2z_3V(e_1, e_2, e_3) + x_1z_2y_3V(e_1, e_3, e_2) + y_1x_2z_3V(e_2, e_1, e_3) \\
&\quad + y_1z_2x_3V(e_2, e_3, e_1) + z_1x_2y_3V(e_3, e_1, e_2) + z_1y_2x_3V(e_3, e_2, e_1) \\
&= x_1y_2z_3 + y_1z_2x_3 + z_1x_2y_3 - x_1z_2y_3 - y_1x_2z_3 - z_1y_2x_3
\end{aligned}$$

C'est la formule de Sarrus (hors-programme).

2 Définitions

Définition: Soit E un \mathbb{K} -espace vectoriel de dimension $n < +\infty$ et $f : E^n \rightarrow \mathbb{K}$. On dit que f est multilinéaire si

$$\forall i \in [\![1, n]\!], \forall (u_1, \dots, u_{i-1}, u_{i+1}, \dots, u_n) \in E^{n-1},$$

l'application $\begin{array}{ccc} E & \longrightarrow & \mathbb{K} \\ u & \longmapsto & f(u_1, \dots, u_{i-1}, u, u_{i+1}, \dots, u_n) \end{array}$ est linéaire.

On dit que f est antisymétrique si

$$\begin{aligned}
&\forall i < j, \forall (u_1, \dots, u_n) \in E^n, \\
&f(u_1, \dots, u_{i-1}, u_{\textcolor{red}{j}}, u_{i+1}, \dots, u_{j-1}, u_{\textcolor{violet}{i}}, u_{j+1}, \dots, u_n) \\
&= -f(u_1, \dots, u_{i-1}, u_{\textcolor{violet}{i}}, u_{i+1}, \dots, u_{j-1}, u_{\textcolor{red}{j}}, u_{j+1}, \dots, u_n).
\end{aligned}$$

On dit que f est alternée si

$$\forall (u_1, \dots, u_n) \in E^n, (\exists i < j, u_i = u_j \implies f(u_1, \dots, u_n) = 0).$$

Proposition: Soit \mathbb{K} un corps tel que $1+1 \neq 0$, E un \mathbb{K} -espace vectoriel de dimension n et $f : E^n \rightarrow \mathbb{K}$ une forme multilinéaire.

Alors,

$$f \text{ alternée} \iff f \text{ antisymétrique.}$$

Preuve: “ \implies ” On suppose f alternée.

Soit $(u_1, \dots, u_n) \in E^n$ et $(i, j) \in \llbracket 1, n \rrbracket^2$ avec $i < j$.

$$\begin{aligned} 0 &= f(u_1, \dots, u_{i-1}, u_i + u_j, u_{i+1}, \dots, u_{j-1}, u_i + u_j, u_{j+1}, \dots, u_n) \\ &= f(u_1, \dots, u_{i-1}, u_i, u_{i+1}, \dots, u_{j-1}, u_i + u_j, u_{j+1}, \dots, u_n) \\ &\quad + f(u_1, \dots, u_{i-1}, u_j, u_{i+1}, \dots, u_{j-1}, u_i + u_j, u_{j+1}, \dots, u_n) \\ &= f(u_1, \dots, u_{i-1}, u_i, u_{i+1}, \dots, u_{j-1}, u_i, u_{j+1}, \dots, u_n) \\ &\quad + f(u_1, \dots, u_{i-1}, u_i, u_{i+1}, \dots, u_{j-1}, u_j, u_{j+1}, \dots, u_n) \\ &\quad + f(u_1, \dots, u_{i-1}, u_j, u_{i+1}, \dots, u_{j-1}, u_i, u_{j+1}, \dots, u_n) \\ &\quad + f(u_1, \dots, u_{i-1}, u_j, u_{i+1}, \dots, u_{j-1}, u_j, u_{j+1}, \dots, u_n) \end{aligned}$$

donc

$$\begin{aligned} &f(u_1, \dots, u_{i-1}, u_j, u_{i+1}, u_{i+1}, \dots, u_{j-1}, u_i, u_{j+1}, \dots, u_n) \\ &= -f(u_1, \dots, u_{i-1}, u_i, u_{i+1}, u_{i+1}, \dots, u_{j-1}, u_j, u_{j+1}, \dots, u_n). \end{aligned}$$

Donc, f est antisymétrique.

“ \iff ” On suppose f antisymétrique. Soit $(u_1, \dots, u_n) \in E^n$ et $(i, j) \in \llbracket 1, n \rrbracket^2$ tels que $i < j$ et $u_i < u_j$.

$$\begin{aligned} &f(u_1, \dots, u_{i-1}, u_i, u_{i+1}, \dots, u_{j-1}, u_j, u_{j+1}, \dots, u_n) \\ &= f(u_1, \dots, u_{i-1}, u_j, u_{i+1}, \dots, u_{j-1}, u_i, u_{j+1}, \dots, u_n) \\ &= -f(u_1, \dots, u_{i-1}, u_i, u_{i+1}, \dots, u_{j-1}, u_j, u_{j+1}, \dots, u_n) \end{aligned}$$

D'où,

$$f(u_1, \dots, u_n) \underbrace{(1+1)}_{\neq 0} = 0$$

donc $f(u_1, \dots, u_n) = 0$.

□

Dans le reste du chapitre, \mathbb{K} est un corps avec $1+1 \neq 0$.

Théorème: Soit E un \mathbb{K} -espace vectoriel de dimension n . L'ensemble des formes multilinéaires alternées de E est un sous-espace vectoriel de $\mathbb{K}^{(E^n)}$ de dimension 1.

Preuve (pas exigible):

Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E . Soit f une forme multilinéaire alternée. Soit $(u_1, \dots, u_n) \in E^n$.

$$\forall j \in [\![1, n]\!], \exists (a_{i,j})_{1 \leq i \leq n}, u_j = \sum_{i=1}^n a_{i,j} e_i$$

$$\begin{aligned} f(u_1, \dots, u_n) &= f\left(\sum_{i=1}^n a_{i,1} e_i, u_2, \dots, u_n\right) \\ &= \sum_{i=1}^n a_{i,1} f(e_i, u_2, \dots, u_n) \\ &= \sum_{i_1=1}^n a_{i_1,1} f\left(e_{i_1}, \sum_{i_2=1}^n a_{i_2,2} e_{i_2}, u_3, \dots, u_n\right) \\ &= \sum_{i_1=1}^n \sum_{i_2=1}^n a_{i_1,1} a_{i_2,2} f(e_{i_1}, e_{i_2}, u_3, \dots, u_n) \\ &\quad \vdots \\ &= \sum_{i_1=1}^n \sum_{i_2=1}^n \cdots \sum_{i_n=1}^n a_{i_1,1} a_{i_2,2} \cdots a_{i_n,n} f(e_{i_1}, e_{i_2}, \dots, e_{i_n}) \\ &= \sum_{\sigma \in S_n} a_{\sigma(1),1} a_{\sigma(2),2} \cdots a_{\sigma(n),n} f(e_{\sigma(1)}, e_{\sigma(2)}, \dots, e_{\sigma(n)}) \\ &= \underbrace{\sum_{\sigma \in S_n} \left(\varepsilon(\sigma) \prod_{j=1}^n a_{\sigma(j),j} \right)}_{A(u_1, \dots, u_n)} \underbrace{f(e_1, \dots, e_n)}_{\in \mathbb{K}} \end{aligned}$$

D'où, $f = f(e_1, \dots, e_n) A$.

Donc, l'ensemble des formes multilinéaires alternées est $\text{Vect}(A)$. De plus,

$$\begin{aligned} A(e_1, \dots, e_n) &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{j=1}^n \delta_{\sigma(j),j} \\ &= \varepsilon(\text{id}) \prod_{j=1}^n 1 = 1 \neq 0. \end{aligned}$$

□

Définition: Soit E un \mathbb{K} -espace vectoriel de dimension n et $\mathcal{B} = (e_1, \dots, e_n)$ une base de E .

Il existe une unique forme f multilinéaire alternée sur E telle que $f(e_1, \dots, e_n) = 1$. Elle est donnée par la formule

$$\forall (u_1, \dots, u_n) \in E^n, f(u_1, \dots, u_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{j=1}^n a_{\sigma(j),j}$$

où

$\forall i, j, a_{i,j}$ est la i -ème coordonnée de u_j dans la base \mathcal{B} .

Cette application est appelée déterminant dans la base \mathcal{B} et noté $\det_{\mathcal{B}}$.

Proposition: Soient $\mathcal{B} = (e_1, \dots, e_n)$ et $\mathcal{C} = (u_1, \dots, u_n)$ deux bases de E . Alors

$$\det_{\mathcal{C}} = \det_{\mathcal{C}}(e_1, \dots, e_n) \det_{\mathcal{B}}$$

i.e.

$$\forall (v_1, \dots, v_n) \in E^n, \det_{\mathcal{C}}(v_1, \dots, v_n) = \det_{\mathcal{C}}(e_1, \dots, e_n) \det_{\mathcal{B}}(v_1, \dots, v_n).$$

Preuve:

On sait que $\det_{\mathcal{B}}$ et $\det_{\mathcal{C}}$ sont colinéaires :

$$\exists \lambda \in \mathbb{K}, \forall (v_1, \dots, v_n) \in E^n, \det_{\mathcal{C}}(v_1, \dots, v_n) = \lambda \det_{\mathcal{B}}(v_1, \dots, v_n).$$

En particulier,

$$\det_{\mathcal{C}}(e_1, \dots, e_n) = \lambda \det_{\mathcal{B}}(e_1, \dots, e_n) = \lambda.$$

□

REMARQUE (notation):

Avec les notations précédentes, on note $\det_{\mathcal{B}}(\mathcal{C})$ au lieu de $\det_{\mathcal{B}}(u_1, \dots, u_n)$.

Corollaire: Avec les notations précédentes, $\det_{\mathcal{B}}(\mathcal{C}) \neq 0$ et

$$\det_{\mathcal{B}}(\mathcal{C}) = (\det_{\mathcal{C}}(\mathcal{B}))^{-1}$$

Preuve:

On sait que

$$\forall (v_1, \dots, v_n) \in E^n, \det_{\mathcal{C}}(v_1, \dots, v_n) = \det_{\mathcal{B}}(\mathcal{C}) \det_{\mathcal{B}}(v_1, \dots, v_n).$$

En particulier,

$$1 = \det_{\mathcal{C}}(\mathcal{C}) = \det_{\mathcal{C}}(\mathcal{B}) \det_{\mathcal{B}}(\mathcal{C}).$$

□

Théorème: Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E , $\mathcal{C} = (u_1, \dots, u_n)$ une famille liée (i.e. \mathcal{C} n'est pas libre). Alors $\det_{\mathcal{B}}(\mathcal{C}) = 0$.

Preuve:

Sans perte de généralité, on peut supposer que $u_n \in \text{Vect}(u_1, \dots, u_{n-1})$:

$$u_n = \sum_{k=1}^{n-1} \lambda_k u_k \text{ où } \lambda_1, \dots, \lambda_{n-1} \in \mathbb{K}.$$

$$\begin{aligned}\det_{\mathcal{B}}(u_1, \dots, u_{n-1}, u_n) &= \sum_{k=1}^{n-1} \lambda_k \underbrace{\det_{\mathcal{B}}(u_1, \dots, u_{n-1}, u_k)}_{=0} \\ &= 0\end{aligned}$$

□

3 Déterminant d'un endomorphisme

Proposition: Soit $f \in \mathcal{L}(E)$, $\mathcal{B} = (e_1, \dots, e_n)$ une base de E . Alors,

$$\exists ! \lambda \in \mathbb{K}, \forall (u_1, \dots, u_n) \in E, \det_{\mathcal{B}}(f(u_1), \dots, f(u_n)) = \lambda \det_{\mathcal{B}}(u_1, \dots, u_n).$$

Preuve:

Soit $g : \begin{matrix} E^n \\ (u_1, \dots, u_n) \end{matrix} \xrightarrow{\quad} \mathbb{K} \quad \det_{\mathcal{B}}(f(u_1), \dots, f(u_n))$. g est clairement alternée.

Soit $i \in \llbracket 1, n \rrbracket$, $(u_1, \dots, u_i, u_{i+1}, \dots, u_n) \in E^{n-1}$. L'application $u \mapsto g(u_1, \dots, u_{i-1}, u, u_{i+1}, \dots, u_n)$ est la composée de f et de $v \mapsto \det_{\mathcal{B}}(f(u_1), \dots, f(u_{i-1}), v, f(u_{i+1}), \dots, f(u_n))$ donc elle est linéaire.

Donc, g est une forme multilinéaire alternée donc colinéaire à $\det_{\mathcal{B}}$.

□

Proposition: Soit $f \in \mathcal{L}(E)$, \mathcal{B} et \mathcal{C} deux bases de E . Soient $(\lambda, \mu) \in \mathbb{K}^2$ tel que

$$\forall (u_1, \dots, u_n) \in E^n, \begin{cases} \det_{\mathcal{B}}(f(u_1), \dots, f(u_n)) = \lambda \det_{\mathcal{B}}(u_1, \dots, u_n), \\ \det_{\mathcal{C}}(f(u_1), \dots, f(u_n)) = \mu \det_{\mathcal{C}}(u_1, \dots, u_n). \end{cases}$$

Alors, $\lambda = \mu$.

Preuve:

On pose $\mathcal{B} = (e_1, \dots, e_n)$.

$$\det_{\mathcal{C}}(f(e_1), \dots, f(e_n)) = \mu \det_{\mathcal{C}}(e_1, \dots, e_n) = \mu \det_{\mathcal{C}}(\mathcal{B})$$

||

$$\det_{\mathcal{C}}(\mathcal{B}) \det_{\mathcal{B}}(f(e_1), \dots, f(e_n))$$

||

$$\lambda \underbrace{\det_{\mathcal{C}}(\mathcal{B})}_{\neq 0} \underbrace{\det_{\mathcal{B}}(\mathcal{B})}_{=1}$$

donc $\lambda = \mu$.

□

Définition: Soit $f \in \mathcal{L}(E)$. Le déterminant de f est le seul scalaire vérifiant,

$$\forall \mathcal{B} \text{ base de } E, \forall (u_1, \dots, u_n), \det_{\mathcal{B}}(f(u_1), \dots, f(u_n)) = \lambda \det_{\mathcal{B}}(u_1, \dots, u_n)$$

et on le note $\lambda = \det(f)$.

REMARQUE:

Si $n = 2$,

$$\text{Aire}(f(u_1), f(u_2)) = \det(f) \text{ Aire}(u_1, u_2).$$

Proposition: Soient f et g deux endomorphismes de E . Alors,

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

Preuve:

Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E .

$$\begin{aligned} \det_{\mathcal{B}}(f \circ g(e_1), \dots, f \circ g(e_n)) &= \det(f \circ g) \det_{\mathcal{B}}(e_1, \dots, e_n) = \det(f \circ g) \\ &\quad \| \\ \det_{\mathcal{B}}(f(g(e_1)), \dots, f(g(e_n))) &\\ &\quad \| \\ (\det f) \det_{\mathcal{B}}(g(e_1), \dots, g(e_n)) &\\ &\quad \| \\ (\det f) (\det g) \underbrace{\det_{\mathcal{B}}(e_1, \dots, e_n)}_{=1}. & \end{aligned}$$

□

Corollaire: Si $f \in \text{GL}(E)$, alors $\det(f) \neq 0$ et $\det(f^{-1}) = \det(f)^{-1}$.

Preuve:

On suppose $f \in \text{GL}(E)$:

$$f \circ f^{-1} = \text{id}_E.$$

Donc,

$$\det(f) \det(f^{-1}) = \det(f \circ f^{-1}) = \det(\text{id}_E).$$

Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E .

$$\det_{\mathcal{B}}(\text{id}_E(e_1), \dots, \text{id}_E(e_n)) = \det(\text{id}_E) \times 1$$

$$\begin{aligned} &\quad \| \\ \det_{\mathcal{B}}(\mathcal{B}) &= 1 \end{aligned}$$

□

Proposition: Soit $f \in \mathcal{L}(E)$. On suppose $f \notin \text{GL}(E)$. Alors $\det(f) = 0$.

Preuve:

Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E .

$$\det(f) = \det_{\mathcal{B}}(f(e_1), \dots, f(e_n)).$$

f n'est pas surjective donc $\text{rg}(f(e_1), \dots, f(e_n)) < n$ donc $(f(e_1), \dots, f(e_n))$ est liée

donc $\det_{\mathcal{B}}(f(e_1), \dots, f(e_n)) = 0$. □

4 Déterminant d'une matrice carrée

Définition: Soit $A = (a_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} \in \mathcal{M}_n(\mathbb{K})$.

Le déterminant de A est

$$\det(A) = \begin{vmatrix} a_{11} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{vmatrix} = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{j=1}^n a_{\sigma(j),j}$$

Proposition: Soit E un \mathbb{K} -espace vectoriel de dimension n , $\mathcal{B} = (e_1, \dots, e_n)$ une base de E , $(u_1, \dots, u_n) \in E^n$ et $A = \text{Mat}_{\mathcal{B}}(u_1, \dots, u_n)$.

Alors,

$$\det_{\mathcal{B}}(u_1, \dots, u_n) = \det(A).$$

Proposition: Soit E un \mathbb{K} -espace vectoriel de dimension n , $\mathcal{B} = (e_1, \dots, e_n)$ une base de E , $f \in \mathcal{L}(E)$ et $A = \text{Mat}_{\mathcal{B}}(f)$. Alors, $\det(A) = \det(f)$.

Preuve:

$$\det(f) = \det_{\mathcal{B}}(f(e_1), \dots, f(e_n)), \quad A = \text{Mat}_{\mathcal{B}}(f(e_1), \dots, f(e_n)).$$

$$\begin{aligned} \det A &= \det_{\mathcal{B}}(f(e_1), \dots, f(e_n)) \\ &= \det(f). \end{aligned}$$

□

Proposition: Soit $(A, B) \in \mathcal{M}_n(\mathbb{K})^2$.

$$\det(AB) = \det(A) \det(B).$$

Preuve:

Soit $E = \mathbb{K}^n$, $\mathcal{B} = (e_1, \dots, e_n)$ la base canonique de E , $f \in \mathcal{L}(E)$ tel que $A = \text{Mat}_{\mathcal{B}}(f)$ et $g \in \mathcal{L}(E)$ tel que $B = \text{Mat}_{\mathcal{B}}(g)$.

$$\begin{aligned} \det(AB) &= \det(f \circ g) = (\det f)(\deg g) \\ &= \det(A) \det(B). \end{aligned}$$

□

Proposition: Soit $A \in \mathcal{M}_n(\mathbb{K})$.

$$A \in \mathrm{GL}_n(\mathbb{K}) \iff \det(A) \neq 0$$

Dans ce cas, $\det(A^{-1}) = \det(A)^{-1}$. □

Proposition:

$$\forall A \in \mathcal{M}_n(\mathbb{K}), \det({}^t A) = \det(A).$$

Preuve:

Soit $A \in \mathcal{M}_n(\mathbb{K})$.

$$\begin{aligned} \det({}^t A) &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{j=1}^n a_{j, \sigma(j)} \\ &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{k=1}^n a_{\sigma^{-1}(k), k} \\ &= \sum_{\sigma' \in S_n} \varepsilon(\sigma'^{-1}) \prod_{k=1}^n a_{\sigma'(k), k} \\ &= \sum_{\sigma' \in S_n} \varepsilon(\sigma') \prod_{k=1}^n a_{\sigma'(k), k} \\ &= \det(A) \end{aligned}$$

car

$$\begin{aligned} \forall \sigma' \in S_n, \varepsilon(\sigma'^{-1}) &= \varepsilon(\sigma')^{-1} = \begin{cases} 1 & \text{si } \varepsilon(\sigma') = 1 \\ -1 & \text{si } \varepsilon(\sigma') = -1 \end{cases} \\ &= \varepsilon(\sigma'). \end{aligned}$$
□

Proposition: Soit $A \in \mathcal{M}_n(\mathbb{K})$, C une opération sur les colonnes et A' la matrice obtenue en appliquant C sur les colonnes A .

1. Si $C = c_i \longleftrightarrow c_j$ (avec $i \neq j$), alors $\det(A') = -\det(A)$.
2. Si $C = c_i \longleftrightarrow \lambda c_i$, alors $\det(A') = \lambda \det(A)$.
3. Si $C = c_i \longleftrightarrow c_i + \lambda c_j$ (avec $i \neq j$), alors $\det(A') = \det(A)$.

Preuve:

Soit $(u_1, \dots, u_n) \in (\mathbb{K}^n)^n$ tel que

$$\forall i \in [\![1, n]\!], c_i = \mathrm{Mat}_{\mathcal{B}}(u_i)$$

où \mathcal{B} est la base canonique de \mathbb{K}^n et c_i la i -ème colonne de A .

1.

$$\begin{aligned} -\det(A) &= -\det_{\mathcal{B}}(u_1, \dots, u_n) \\ &\quad \| \\ \det(A') &= \det_{\mathcal{B}}(u_1, \dots, u_{i-1}, u_j, u_{i+1}, \dots, u_{j-1}, u_i, u_{j+1}, \dots, u_n). \end{aligned}$$

2.

$$\begin{aligned} \det(A') &= \det_{\mathcal{B}}(u_1, \dots, u_{i-1}, \lambda u_i, u_{i+1}, \dots, u_n) \\ &= \lambda \det_{\mathcal{B}}(u_1, \dots, u_{i-1}, u_i, u_{i+1}, \dots, u_n) \\ &= \lambda \det(A). \end{aligned}$$

3.

$$\begin{aligned} \det(A') &= \det_{\mathcal{B}}(u_1, \dots, u_{i-1}, u_i + \lambda u_j, u_{i+1}, \dots, u_n) \\ &= \det_{\mathcal{B}}(u_1, \dots, u_{i-1}, u_i, u_{i+1}, \dots, u_n) + \lambda \det_{\mathcal{B}}(u_1, \dots, u_{i-1}, u_j, u_{i+1}, \dots, u_n) \\ &= \det(A) \end{aligned}$$

car, comme u_j apparaît deux fois dans le second détermiant, il vaut 0.

□

Corollaire: Le déterminant d'une matrice triangulaire est le produit de ses coefficients diagonaux.

Preuve:

Soit $T = \begin{pmatrix} \lambda_1 & * & \cdots & * \\ 0 & \ddots & \ddots & \vdots \\ & & \ddots & * \\ & & & \lambda_n \end{pmatrix}$. S'il existe $i \in \llbracket 1, n \rrbracket$, avec $\lambda_i = 0$, alors $\text{rg}(T) < n$ et

donc $T \notin \text{GL}_n(\mathbb{K})$ et donc $\det(T) = 0 = \prod_{k=1}^n \lambda_k$.

On suppose que $\forall i, \lambda_i \neq 0$. On a

$$\frac{1}{\lambda_1} \det(T) = \det \begin{pmatrix} 1 & * & \cdots & * \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}$$

et

$$\frac{1}{\lambda_1 \lambda_2} \det(T) = \det \begin{pmatrix} 1 & * & \cdots & \cdots & * \\ 0 & 1 & \ddots & & \vdots \\ \vdots & 0 & \lambda_3 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & * \\ 0 & 0 & \cdots & 0 & \lambda_n \end{pmatrix}$$

D'où

$$\begin{aligned} \frac{1}{\lambda_1 \cdots \lambda_n} \det(T) &= \begin{vmatrix} 1 & & & * \\ & \ddots & \ddots & \ddots \\ & & (0) & \ddots \\ & & & 1 \end{vmatrix} \\ &= \begin{vmatrix} 1 & & & (0) \\ & \ddots & \ddots & \ddots \\ & & (0) & \ddots \\ & & & 1 \end{vmatrix} \\ &= 1 \end{aligned}$$

donc $\det(T) = \lambda_1 \cdots \lambda_n$. □

Proposition: Soit $A \in \mathcal{M}_n(\mathbb{K})$, L une opération sur les lignes, A' la matrice obtenue en appliquant L sur les lignes de A .

1. Si $L = \ell_i \longleftrightarrow \ell_j$ (avec $i \neq j$), $\det(A') = -\det(A)$.
2. Si $L = \ell_i \longleftrightarrow \lambda \ell_i$, $\det(A') = \lambda \det(A)$.
3. Si $L = \ell_i \longleftrightarrow \ell_i + \lambda \ell_j$ (avec $i \neq j$), $\det(A') = \det(A)$.

□

EXEMPLE:
 $(a, b, c) \in \mathbb{C}^3$

$$\begin{aligned} \begin{vmatrix} a & b & c \\ b & a & c \\ c & a & b \end{vmatrix} &= \begin{vmatrix} a+b+c & b & c \\ a+b+c & a & c \\ a+b+c & a & b \end{vmatrix} \\ &= (a+b+c) \begin{vmatrix} 1 & b & c \\ 1 & a & c \\ 1 & a & b \end{vmatrix} \\ &= (a+b+c) \begin{vmatrix} 1 & b & c \\ 0 & a-b & 0 \\ 0 & 0 & b-c \end{vmatrix} \\ &= (a+b+c)(a-b)(b-c) \end{aligned}$$

5 Développement suivant une ligne ou une colonne

EXEMPLE:

$$\begin{vmatrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ - & + & - & + \end{vmatrix}$$

$$\begin{aligned}
& \left| \begin{array}{c|cc|c} 1 & 2 & 3 & 0 \\ 4 & 5 & 6 & -1 \\ 7 & 8 & 9 & -2 \\ 3 & 2 & 1 & 0 \end{array} \right| = -2 \left| \begin{array}{ccc} 4 & 6 & -1 \\ 7 & 9 & -2 \\ 3 & 1 & 0 \end{array} \right| + 5 \left| \begin{array}{ccc} 1 & 3 & 0 \\ 7 & 9 & -2 \\ 3 & 1 & 0 \end{array} \right| - 8 \left| \begin{array}{ccc} 1 & 3 & 0 \\ 4 & 6 & -1 \\ 3 & 1 & 0 \end{array} \right| + 2 \left| \begin{array}{ccc} 1 & 3 & 0 \\ 4 & 6 & -1 \\ 7 & 9 & -2 \end{array} \right| \\
& \left| \begin{array}{c|cc|c} 1 & 2 & 3 & 0 \\ 4 & 5 & 6 & -1 \\ 7 & 8 & 9 & -2 \\ 3 & 2 & 1 & 0 \end{array} \right| = -1 \left| \begin{array}{ccc} 1 & 2 & 3 \\ 7 & 8 & 9 \\ 3 & 2 & 1 \end{array} \right| + 2 \left| \begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 3 & 2 & 1 \end{array} \right| \\
& \left| \begin{array}{c|cc|c} 1 & 2 & 3 & 0 \\ 4 & 5 & 6 & -1 \\ 7 & 8 & 9 & -2 \\ 3 & 2 & 1 & 0 \end{array} \right| = -3 \left| \begin{array}{ccc} 2 & 3 & 0 \\ 5 & 6 & -1 \\ 8 & 9 & -1 \end{array} \right| + 2 \left| \begin{array}{ccc} 1 & 3 & 0 \\ 4 & 6 & -1 \\ 7 & 9 & -2 \end{array} \right| - \left| \begin{array}{ccc} 1 & 2 & 0 \\ 4 & 5 & -1 \\ 7 & 8 & 9 \end{array} \right|
\end{aligned}$$

$E = \mathbb{C}^4$ et $\mathcal{B} = (e_1, e_2, e_3, e_4)$ base canonique de E .

On pose $\begin{cases} u_1 = (1, 4, 7, 3), \\ u_2 = (2, 5, 8, 2), \\ u_3 = (3, 6, 9, 1), \\ u_4 = (0, -1, -2, 0). \end{cases}$ et $A = \text{Mat}_{\mathcal{B}}(u_1, u_2, u_3, u_4) = \text{Mat}_{\mathcal{B}}(u_1, 2e_1 + 5e_2 + 8e_3 + 2e_4, u_3, u_4)$.

Donc,

$$\begin{aligned}
\det A &= \det_{\mathcal{B}}(u_1, 2e_1 + 5e_2 + 8e_3 + 2e_4, u_3, u_4) \\
&= 2 \det_{\mathcal{B}}(u_1, e_1, u_3, u_4) \\
&\quad + 5 \det_{\mathcal{B}}(u_1, e_2, u_3, u_4) \\
&\quad + 9 \det_{\mathcal{B}}(u_1, e_3, u_3, u_4) \\
&\quad + 2 \det_{\mathcal{B}}(u_1, e_4, u_3, u_4).
\end{aligned}$$

$$\begin{aligned}
\det_{\mathcal{B}}(u_1, e_1, u_3, u_4) &= \left| \begin{array}{cccc} 1 & 1 & 3 & 0 \\ 4 & 0 & 6 & -1 \\ 7 & 0 & 9 & -2 \\ 3 & 0 & 1 & 0 \end{array} \right| \\
&= - \left| \begin{array}{cccc} \boxed{1} & 1 & 3 & 0 \\ 0 & 4 & 6 & -1 \\ 0 & 7 & 9 & -2 \\ 0 & 3 & 1 & 0 \end{array} \right| \\
&= - \left| \begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 4 & 6 & -1 \\ 0 & 7 & 9 & -2 \\ 0 & 3 & 1 & 0 \end{array} \right| \\
&= \dots \\
&= - \left| \begin{array}{c|cc} 1 & 0 \\ \hline 0 & * \\ 0 & (0) \end{array} \right|
\end{aligned}$$

Idem pour e_2, e_3, e_4 .

Proposition (Laplace): Soit $A = (a_{ij}) \in \mathcal{M}_n(\mathbb{K})$.

$$\forall j \in \llbracket 1, n \rrbracket, \det(A) = \sum_{i=1}^n (-1)^{i+j} a_{i,j} m_{i,j}$$

où $m_{i,j}$ est le mineur d'indices (i, j) , i.e. le déterminant de la matrice obtenue en supprimant la ligne i et la colonne j de la matrice A .

$$\forall i \in \llbracket 1, n \rrbracket, \det(A) = \sum_{j=1}^n (-1)^{i+j} a_{i,j} m_{i,j}.$$

□

Proposition (Vandermonde): Soient $(a_1, \dots, a_n) \in \mathbb{K}^n$.

$$\begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{vmatrix} = \prod_{j < i} (a_j - a_i)$$

Preuve (par récurrence sur n): — Soit $n \in \mathbb{N}$. Soient $a_1, \dots, a_{n+1} \in \mathbb{K}$. On pose

$$\Delta_{n+1} = \begin{vmatrix} 1 & a_1 & \cdots & a_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_{n+1} & \cdots & a_{n+1}^n \end{vmatrix}$$

On développe Δ_{n+1} suivant la dernière ligne et on obtient une expression polynomial en a_{n+1} :

$$\Delta_{n+1} = P(a_{n+1}) \text{ avec } P \in \mathbb{K}_n[X]$$

et le coefficient devant X^n est Δ_n .

CAS 1 On suppose $\Delta_n \neq 0$. D'après l'hypothèse de récurrence :

$$\begin{cases} \forall i, j \in \llbracket 1, n \rrbracket, i \neq j \implies a_i \neq a_j \\ \text{dom}(P_n) = \Delta_n = \prod_{n \geq j > i \geq 1} (a_j - a_i) \\ \deg(P_n) = n \\ \forall i \in \llbracket 1, n \rrbracket, P(a_i) = 0 \end{cases}$$

donc

$$P = \Delta_n (X - a_1) \cdots (X - a_n)$$

donc

$$\begin{aligned} \Delta_{n+1} &= \prod_{n \geq j > i \geq 1} (a_j - a_i) (a_{n+1} - a_1) \cdots (a_{n+1} - a_n) \\ &= \prod_{n+1 \geq j > i \geq 1} (a_j - a_i) \end{aligned}$$

CAS 2 On suppose $\Delta_n = 0$:

$$\exists i, j \in \llbracket 1, n \rrbracket, i \neq j \text{ et } a_i = a_j.$$

Alors,

$$\Delta_{n+1} = 0 = \prod_{n+1 \geq j > i \geq 1} (a_j - a_i).$$

□

Proposition – Définition: Soit $A \in \mathcal{M}_n(\mathbb{K})$, et $\text{com}(A)$ la comatrice de A : c'est la matrice

$$((-1)^{i+j} m_{i,j})_{1 \leq i, j \leq n}$$

où $m_{i,j}$ est le mineur d'indices (i, j) de A .

On a

$$A^t \text{com}(A) = {}^t \text{com}(A) A = \det(A) I_n.$$

Si $\det A \neq 0$, alors

$$A^{-1} = \frac{1}{\det(A)} {}^t \text{com}(A).$$

EXEMPLE:

Avec $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, on a $\det A = ad - bc$.

$$\text{com } A = \begin{pmatrix} +d & -b \\ -c & +a \end{pmatrix} \text{ donc } {}^t \text{com}(A) = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

Si $\det(A) \neq 0$,

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

EXEMPLE:

Avec $A = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$, on a

$$\text{com } A = \begin{pmatrix} b_2 c_3 - b_3 c_2 & a_3 c_2 - a_2 c_3 & a_2 b_3 - a_3 b_2 \\ c_1 b_3 - b_1 c_3 & a_1 c_3 - a_3 c_1 & a_3 b_1 - a_1 b_3 \\ b_1 c_2 - b_2 c_1 & a_2 c_1 - a_1 c_2 & a_1 b_2 - a_2 b_1 \end{pmatrix}$$

Preuve:

On note $C = A^t \text{com}(A) = (c_{i,j})$.

$$\forall i \in \llbracket 1, n \rrbracket, c_{ii} = \sum_{j=1}^n a_{ij} (-1)^{i+j} m_{ij} = \det(A).$$

Soient $i \in \llbracket 1, n \rrbracket$, $j \in \llbracket 1, n \rrbracket$ avec $i \neq j$.

$$c_{ij} = \sum_{k=1}^n a_{ik} (-1)^{j+k} m_{jk}.$$

C'est le déterminant de la matrice obtenue en remplaçant la j -ème ligne de A par la i -ème, qui a donc 2 lignes identiques donc $c_{ij} = 0$.

L'autre formule " ${}^t \text{com}(A) A = \det(A) I_n$ " se démontre de la même façon. □

REMARQUE:

En pratique, on n'utilise jamais cette formule pour trouver A^{-1} (sauf si $n = 2$).

EXERCICE (Formules de Cramer):

INUTILES ET HORS-PROGRAMME

Soit S le système $AX = B$ avec $A \in \mathrm{GL}_n(\mathbb{K})$ et $B \in \mathcal{M}_{n,1}(\mathbb{K})$.

L'unique solution du système S est donnée par

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ où } \forall i, x_i = \frac{\det A_i}{\det A}$$

où A_i est obtenue en remplaçant la i -ème colonne de A par B .

Solution : Soit (x_1, \dots, x_n) l'unique solution de S .

$$\sum_{i=1}^n x_i C_i(A) = B$$

où $C_i(A)$ est la i -ème colonne de A .

$$\begin{aligned} \forall j, \det(A_j) &= \det(C_1(A), C_2(A), \dots, C_{j-1}(A), B, C_{j+1}(A), \dots, C_n(A)) \\ &= \sum_{i=1}^n x_i \det(C_1(A), \dots, C_{j-1}(A), C_i(A), C_{j+1}(A), \dots, C_n(A)) \\ &= x_j \det(A) \end{aligned}$$

Retour sur la diagonalisation

Soit $A \in \mathcal{M}_n(\mathbb{K})$. On cherche $P \in \mathrm{GL}_n(\mathbb{K})$ telle que

$$P A P^{-1} = \begin{pmatrix} \lambda_1 & & & \\ & \ddots & & (0) \\ & & \ddots & \\ (0) & & & \lambda_n \end{pmatrix}$$

Soit $f \in \mathcal{L}(\mathbb{K}^n)$ telle que $\mathrm{Mat}_{\mathcal{B}}(f) = A$ où \mathcal{B} est la base canonique de \mathbb{K}^n . On cherche $\mathcal{C} = (u_1, \dots, u_n) \in \mathbb{K}^n$ telle que

$$\exists \lambda_i, f(u_i) = \lambda_i u_i$$

$$\begin{aligned} &\exists \lambda \in \mathbb{K}, \exists u \neq 0, f(u) = \lambda u \\ \iff &\exists \lambda \in \mathbb{K}, \exists u \neq 0, u \in \mathrm{Ker}(f - \lambda \mathrm{id}_{\mathbb{K}^n}) \\ \iff &\exists \lambda \in \mathbb{K}, f - \lambda \mathrm{id}_{\mathbb{K}^n} \text{ n'est pas injective} \\ \iff &\exists \lambda \in \mathbb{K}, f - \lambda \mathrm{id}_{\mathbb{K}^n} \notin \mathrm{GL}(\mathbb{K}^n) \\ \iff &\exists \lambda \in \mathbb{K}, \det(\lambda - \mathrm{id}_{\mathbb{K}^n}) = 0 \\ \iff &\exists \lambda \in \mathbb{K}, \underbrace{\det(A - \lambda I_n)}_{\text{polynôme caractéristique de } A} = 0 \end{aligned}$$

CHAPITRE

27

ESPACE PROBABILISÉ FINI

1 Définitions

Définition: Soit Ω un ensemble fini. Une probabilité sur Ω est une application

$$P : \mathcal{P}(\Omega) \longrightarrow [0, 1]$$

telle que

1. $P(\Omega) = 1,$
2. $\forall A, B \in \mathcal{P}(\Omega), A \cap B = \emptyset \implies P(A \cup B) = P(A) + P(B).$

Dans ce cas, on dit que (Ω, P) est un espace probabilisé.

EXEMPLE (équiprobabilité):

Soit Ω un ensemble fini non vide. Soit

$$\begin{aligned} P : \mathcal{P}(\Omega) &\longrightarrow [0, 1] \\ A &\longmapsto \frac{\#A}{\#\Omega}. \end{aligned}$$

En effet,

1. $P(\Omega) = \frac{\#\Omega}{\#\Omega} = 1.$
2. Soient $A, B \in \mathcal{P}(\Omega)$ avec $A \cap B = \emptyset.$

$$\begin{aligned} P(A \cup B) &= \frac{\#(A \cup B)}{\#\Omega} \\ &= \frac{\#A + \#B}{\#\Omega} \\ &= P(A) + P(B) \end{aligned}$$

De plus, on pose $n = \#\Omega.$

$$\forall \omega \in \Omega, P(\{\omega\}) = \frac{1}{n} \text{ et ne dépend pas de } \omega.$$

Définition: Soit (Ω, P) un espace probabilisé.

L'ensemble Ω est appelé univers, les singletons $\{\omega\}$ avec $\omega \in \Omega$ sont appelés événements élémentaires, les parties de Ω sont appelées événements, \emptyset est appelé événement impossible et Ω est appelé événement certain.

Soient $A, B \in \mathcal{P}(\Omega)$. On dit que A et B sont incompatibles si $A \cap B = \emptyset$.

Proposition: Soit $\Omega = \{\omega_1, \dots, \omega_n\}$ un ensemble de cardinal n et $(p_1, \dots, p_n) \in [0, 1]^n$ tel que $\sum_{i=1}^n p_i = 1$. Il existe une unique probabilité P sur Ω que

$$\forall i \in \llbracket 1, n \rrbracket, P(\{\omega_i\}) = p_i.$$

Preuve: Éxistence On pose

$$P : \mathcal{P}(\Omega) \longrightarrow [0, 1]$$

$$A \longmapsto \sum_{i \in I_A} p_i$$

où $I_A = \{i \in \llbracket 1, n \rrbracket \mid \omega_i \in A\}$.
— Soit $a \in \mathcal{P}(\Omega)$.

$$0 \leq P(A) = \sum_{i \in I_A} p_i \leq \sum_{i=1}^n p_i = 1$$

— $P(\Omega) = \sum_{i \in I_\Omega} p_i = \sum_{i=1}^n p_i = 1$.
— Soient $A, B \in \mathcal{P}(\Omega)$ incompatibles.

$$\begin{aligned} I_{A \cup B} &= \{i \in \llbracket 1, n \rrbracket, \omega_i \in A \cup B\} \\ &= I_A \cup I_B \end{aligned}$$

$$P(A \cup B) = \sum_{i \in I_{A \cup B}} p_i = \sum_{i \in I_A} p_i + \sum_{i \in I_B} p_i = P(A) + P(B).$$

Unicité Soit Q une probabilité sur Ω tel que

$$\forall i \in \llbracket 1, n \rrbracket, Q(\{\omega_i\}) = p_i.$$

Soit $A \in \mathcal{P}(\Omega)$.

$$A = \bigcup_{\omega \in A} \{\omega\} = \bigcup_{i \in I_A} \{\omega_i\}.$$

En utilisant le lemme suivant,

$$\begin{aligned} Q(A) &= Q\left(\bigcup_{i \in I_A} \{\omega_i\}\right) = \sum_{i \in I_A} Q(\{\omega_i\}) \\ &= \sum_{i \in I_A} p_i = P(A). \end{aligned}$$

□

Lemme: Soit P une probabilité sur Ω et $(A_i)_{1 \leq i \leq n}$ une famille d'événements 2 à 2 incompatibles. Alors

$$P\left(\bigcup_{i=1}^n A_i\right) = \sum_{i=1}^n P(A_i).$$

Preuve:
par récurrence sur n .

□

Proposition: Soit P une probabilité sur Ω .

1. $P(\emptyset) = 0$;
2. $\forall A, B \in \mathcal{P}(\Omega), A \subset B \implies P(A) \leq P(B)$;
3. $\forall A, B \in \mathcal{P}(\Omega), P(A \cup B) = P(A) + P(B) - P(A \cap B)$.

Preuve: 1. $\Omega = \emptyset \cup \Omega$ donc $P(\Omega) = P(\emptyset) + P(\Omega)$ donc $P(\emptyset) = 0$.

2. Soient $A, B \in \mathcal{P}(\Omega)$ avec $A \subset B$. On pose $C = B \setminus A$:

$$\begin{cases} B = A \cup C; \\ A \cap C = \emptyset. \end{cases}$$

Donc, $P(B) = P(A) + \underbrace{P(C)}_{\geq 0} \geq P(A)$.

3. On pose $\begin{cases} A' = A \setminus (A \cap B), \\ B' = B \setminus (A \cap B), \\ C = A \cap B. \end{cases}$

$$\begin{cases} A' \cup B' \cup C = A \cup B \\ A' \cap C = B' \cap C = A' \cap B' = \emptyset \end{cases}$$

donc

$$P(A \cup B) = P(A') + P(B') + P(C).$$

De plus,

$$\begin{cases} A = A' \cup C \text{ donc } P(A) = P(A') + P(C); \\ B = B' \cup C \text{ donc } P(B) = P(B') + P(C). \end{cases}$$

D'où

$$\begin{aligned} P(A \cup B) &= P(A) - P(C) + P(B) - \cancel{P(C)} + \cancel{P(C)} \\ &= P(A) + P(B) - P(A \cap B). \end{aligned}$$

□

2 Probabilité conditionnelle

Proposition – Définition: Soit (Ω, P) un espace probabilisé et $A \in \mathcal{P}(\Omega)$ tel que $P(A) \neq 0$.

L'application

$$\begin{aligned}\mathcal{P}(\Omega) &\longrightarrow [0, 1] \\ X &\longmapsto \frac{P(A \cap X)}{P(A)}\end{aligned}$$

est une probabilité. Elle est notée P_A et est appelée probabilité sachant A .

Elle est parfois notée $P(A | B)$.

Preuve: — Soit $X \in P(\Omega)$.

$$0 \leq P(A \cap X) \leq P(A) \text{ car } A \cap X \subset A$$

Comme $P(A) > 0$,

$$0 \leq \frac{P(A \cap X)}{P(A)} \leq 1$$

—

$$\frac{P(A \cap \Omega)}{P(A)} = \frac{P(A)}{P(A)} = 1$$

— Soient $X, Y \in P(\Omega)$ avec $X \cap Y = \emptyset$.

$$\begin{aligned}\frac{P(A \cap (X \cup Y))}{P(A)} &= \frac{P((X \cap A) \cup (Y \cap A))}{P(A)} \\ &= \frac{P(A \cap X) + P(A \cap Y)}{P(A)}\end{aligned}$$

□

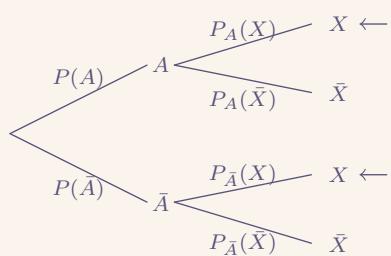
Proposition: Soit (Ω, P) un espace probabilisé et $A \in \mathcal{P}(\Omega)$ tel que $P(A) \neq 0$.

$$\forall X \in \mathcal{P}(\Omega), P(A \cap X) = P(A) P_A(X).$$

□

Proposition: Soit (Ω, P) un espace probabilisé, $A \in \mathcal{P}(\Omega)$ tel que $P(A) \in]0, 1[$.

$$\forall X \in \mathcal{P}(\Omega), P(X) = P(A) P_A(X) + P(\bar{A}) P_{\bar{A}}(X).$$



Preuve:
Soit $X \in \mathcal{P}(\Omega)$.

$$\begin{aligned} X &= X \cap \Omega \\ &= X \cap (A \cup \bar{A}) \\ &= (X \cap A) \cup (X \cap \bar{A}) \end{aligned}$$

donc

$$\begin{aligned} P(X) &= P(X \cap A) + P(X \cap \bar{A}) \\ &= P(A) P_A(X) + P(\bar{A}) P_{\bar{A}}(X). \end{aligned}$$

□

Définition: Soit (Ω, P) un espace probabilisé. Un système complet d'événements est une partition de Ω .

Proposition (probabilités totales): Soit (Ω, P) un espace probabilisé, $(A_i)_{1 \leq i \leq n}$ un système complet d'événements tel que

$$\forall i \in \llbracket 1, n \rrbracket, P(A_i) > 0.$$

Alors,

$$\forall x \in \mathcal{P}(\Omega), P(x) = \sum_{i=1}^n P(A_i) P_{A_i}(x).$$

Preuve:
Soit $X \in \mathcal{P}(\Omega)$.

$$\begin{aligned} P(X) &= P(X \cap \Omega) \\ &= P\left(X \cap \left(\bigcup_{i=1}^n A_i\right)\right) \\ &= P\left(\bigcup_{i=1}^n (X \cap A_i)\right) \\ &= \sum_{i=1}^n P(X \cap A_i) \\ &= \sum_{i=1}^n P(A_i) P_{A_i}(X) \end{aligned}$$

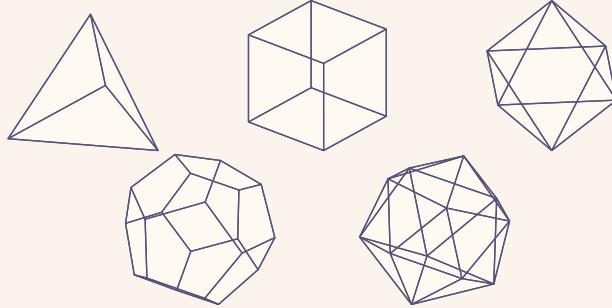
□

EXEMPLE:

On dispose de 5 dés : un à 4 faces, un à 6 faces, un à 8 faces, un à 8 faces, un à 12 faces et un à 20 faces que l'on suppose bien équilibré.

Pour qu'un dé soit bien équilibré, il faut que ce soit un polyèdre régulier, aussi appelé polyèdre

de Platon. Il y en a 5 : le tétraèdre, le cube, l'octaèdre, le dodécaèdre, et l'icosaèdre.



On choisit au hasard l'un de ces dés, on le lance et on note le résultat.

Quelle est la probabilité que ce résultat soit égal à 7?

Modélisation 1 : $\Omega = \llbracket 1, 20 \rrbracket$, $P = ?$.

Modélisation 2 : $\Omega = \left\{ (x, y) \mid x \in \{4, 6, 8, 12, 20\} \text{ et } y \in \llbracket 1, x \rrbracket \right\}$ et P une probabilité sur Ω .
On pose $\forall x \in \overbrace{\{4, 6, 8, 12, 20\}}^X$, $A_x = \{x\} \times \llbracket 1, x \rrbracket$. On suppose que

$$\forall x \in X, P(A_x) = \frac{1}{5}.$$

On note

$$\forall y \in \llbracket 1, 20 \rrbracket, B_y = \{(x, y) \mid x \in X \text{ et } y \leq x\}$$

et donc

$$\forall x \in X, \forall y \in \llbracket 1, x \rrbracket, P_{A_x}(B_y) = \begin{cases} \frac{1}{x} & \text{si } y \leq x, \\ 0 & \text{si } y > x. \end{cases}$$

Implémentation en Python de l'expérience :

```
import random as rd

def exp():
    faces = rd.choice([4, 6, 8, 12, 20])
    result = rd.randint(1, faces)
    return result == 7

def proba(N = 1000):
    cpt = 0
    for _ in range(N):
        if exp():
            cpt += 1
    return cpt / N
```

Solution :

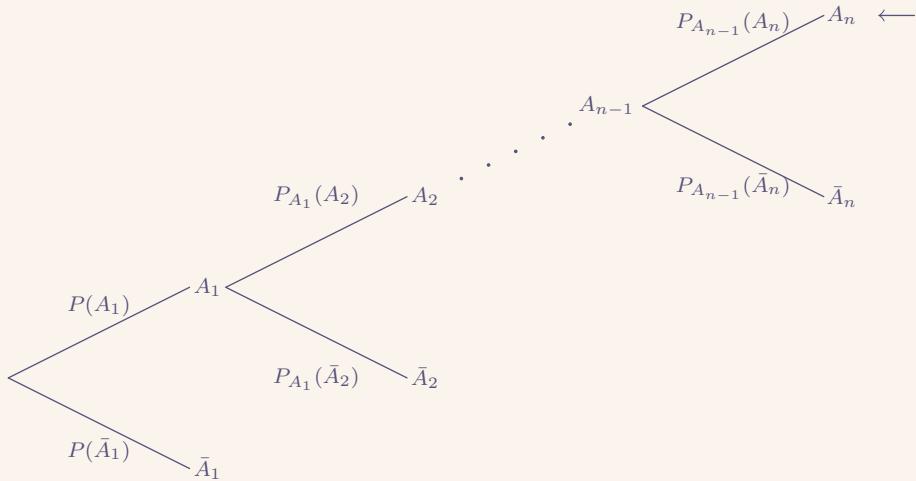
$$\begin{aligned} P(B_7) &= \sum_{x \in X} P_{A_x}(B_7)P(A_x) \\ &= \frac{1}{5} (P_{A_8}(B_7) + P_{A_{12}}(B_7) + P_{A_{20}}(B_7)) \\ &= \frac{1}{5} \left(\frac{1}{8} + \frac{1}{12} + \frac{1}{20} \right). \end{aligned}$$

Proposition (probabilités composées): Soit (Ω, P) un espace probabilisé, $(A_i)_{1 \leq i \leq n}$ des événements tels que

$$P(A_1 \cap \cdots \cap A_{n-1}) \neq 0.$$

Alors,

$$P(A_1 \cap \cdots \cap A_n) = P(A_1) P_{A_1}(A_2) P_{A_1 \cap A_2}(A_3) \cdots P_{A_1 \cap \cdots \cap A_{n-1}}(A_n)$$



Preuve:

$$\forall i, A_1 \cap \cdots \cap A_i \supset A_1 \cap \cdots \cap A_n \text{ donc } P(A_1 \cap \cdots \cap A_i) > 0.$$

$$\begin{aligned} & P(A_1) P_{A_1}(A_2) P_{A_1 \cap A_2}(A_3) \cdots P_{A_1 \cap \cdots \cap A_{n-1}}(A_n) \\ &= P(A_1) \frac{P(A_2 \cap A_1)}{P(A_1)} \frac{P(A_3 \cap A_2 \cap A_1)}{P(A_1 \cap A_2)} \cdots \frac{P(A_n \cap A_{n-1} \cap \cdots \cap A_1)}{P(A_1 \cap \cdots \cap A_{n-1})} \\ &= P(A_1 \cap \cdots \cap A_n) \end{aligned}$$

□

EXEMPLE:

On reprend l'expérience précédente aléatoire précédente. On sait qu'on a obtenu 7.

Quel dé a été utilisé ?

On veut calculer $P_{B_7}(A_x)$ pour tout x . Soit $x \in X$.

$$\begin{aligned} P_{B_7}(A_x) &= \frac{P(A_x \cap B_7)}{P(B_7)} \\ &= \frac{P_{A_x}(B_7) P(A_x)}{P(B_7)} \\ &= \begin{cases} 0 & \text{si } x \in \{4, 6\} \\ \frac{\frac{1}{8} \times \frac{1}{5}}{P(B_7)} & \text{si } x = 8 \\ \frac{\frac{1}{2} \times \frac{1}{5}}{P(B_7)} & \text{si } x = 12 \\ \frac{\frac{1}{20} \times \frac{1}{5}}{P(B_7)} & \text{si } x = 20 \end{cases} \end{aligned}$$

On a utilisé la formule de Bayes.

Proposition (Bayes): Soit (Ω, P) un espace probabilisé, $A, B \in \mathcal{P}(\Omega)$ tels que $P(A) \neq 0$ et $P(B) \in]0, 1[$.

$$P_A(B) = \frac{P_B(A) P(B)}{P(A)} = \frac{P_B(A) P(B)}{P_B(A) P(B) + P_{\bar{B}}(A) P(\bar{B})}.$$

□

REMARQUE:

On appelle $P_A(B)$ la vraisemblance (*likelihood* en anglais), $P(A)$ la probabilité a-priori (*prior distribution*), et $P_B(A)$ la probabilité a-posteriori (*posterior distribution*).

EXEMPLE (filtre bayésien):

On peut utiliser cette formule pour filtrer les SPAMs dans les emails. On utilise des données de la forme :

	mot 1	mot 2	...	mot p	spam ?
mail 1					
mail 2					
⋮					
mail n					

On peut donc calculer la probabilité qu'un email soit un SPAM en fonction des mots qu'il contient :

$$\begin{aligned} P_{(\text{mot 1}, \text{mot 2}, \dots)}(\text{spam}) &= \frac{P(\text{spam}) P_{\text{spam}}(\overline{\text{mot 1}}, \overline{\text{mot 2}}, \dots)}{P(\text{mot 1}, \text{mot 2}, \dots)} \\ &\approx \frac{P_{\text{spam}}(\text{mot 1}) \times P_{\text{spam}}(\overline{\text{mot 2}}) \times \dots}{P(\text{mot 1}, \text{mot 2}, \dots)}. \end{aligned}$$

EXEMPLE (Test médical):

On estime qu'une personne sur 10 000 est atteinte d'une certaine maladie. On invente un test T .

$$\begin{cases} P_{\text{malade}}(T = \text{positif}) = \frac{99}{100}, \\ P_{\overline{\text{malade}}}(T = \text{positif}) = \frac{1}{1000}. \end{cases}$$

On fait un test et il revient positif. Quelle est la probabilité d'avoir la maladie : $P_{T+}(M)$?

$$\begin{aligned}
P_{T^+}(M) &= \frac{P_M(T^+) P(M)}{P(T)} \\
&= \frac{\frac{99}{100} \times \frac{1}{10000}}{\frac{99}{100} \times \frac{1}{10000} \times \frac{9999}{10000}} \\
&= \frac{990}{990 + 9999} \simeq 9\%
\end{aligned}$$

On a 9 % d'avoir la maladie : le test n'est pas très précis.

EXEMPLE (QCM):

On a un QCM de 20 questions où l'on peut répondre par vrai ou faux (donc c'est pas vraiment un QCM). Si un étudiant connaît la réponse, il répond correctement. Sinon, il choisit l'une des réponses au hasard.

Soit p la probabilité qu'il connaisse la réponse à une question. Cela représente le niveau du candidat : un élève ayant travaillé aura une valeur de p plus importante qu'un élève n'ayant pas travaillé.

L'étudiant obtient 13/20. Estimer p .

Comme $p \in [0, 1]$, on découpe l'intervalle en 10 : on pose

$$\forall k \in \llbracket 0, 9 \rrbracket, A_k : "p = \frac{k + 0,5}{10}".$$

On pose aussi

$$\begin{cases} \forall i \in \llbracket 1, 20 \rrbracket, B_i : \text{"la } i\text{-ème réponse est correcte"}, \\ \forall j \in \llbracket 0, 20 \rrbracket, C_j : \text{"l'étudiant a } j/20"} \end{cases},$$

On cherche donc $P_{C_{13}}(A_k)$. S'il n'y a pas de "pic" de probabilité (en fonction de k), il faut changer le QCM : augmenter le nombre de questions, mettre des questions plus faciles / difficiles...

On utilise la formule de Bayes :

$$P_{C_{13}}(A_k) = \frac{P_{A_k}(C_{13}) P(A_k)}{P(C_{13})}.$$

On peut choisir $P(A_k)$: c'est subjectif. On peut avoir une distribution uniforme, ou suivant une courbe de Gauß, ...

On choisit $P(A_k) = \frac{1}{10}$: distribution uniforme.

$$\begin{aligned}
P(C_{13}) &= \sum_{k=0}^9 P_{A_k}(C_{13}) P(A_k); \\
P_{A_k}(C_{13}) &= \binom{20}{13} \left(\frac{p+1}{2}\right)^{13} \left(1 - \frac{p+1}{2}\right)^7.
\end{aligned}$$

Proposition (Bayes): Soit (Ω, P) un espace probabilisé et $(A_k)_{k \in K}$ un système complet d'événements tel que

$$\forall k \in K, P(A_k) \neq 0.$$

Soit $X \in \mathcal{P}(\Omega)$ tel que $P(X) \neq 0$. On a

$$\forall k \in K, P_X(A_k) = \frac{P_{A_k}(X) P(A_k)}{\sum_{j \in K} P_{A_j}(X) P(A_j)}.$$

□

[]

3 Événements indépendants

Définition: Soient A et B deux événements d'un espace probabilisé (Ω, P) . On dit que A et B sont indépendants si

$$P(A \cap B) = P(A) P(B).$$

REMARQUE:

L'indépendance d'événements au sens mathématique n'est pas la même chose que l'indépendance dans le sens commun : elle dépend de la probabilité utilisé !

EXEMPLE:

On considère un objet, qui est défectueux avec une probabilité $p \in]0, 1[$. On effectue deux contrôles indépendants. Chaque contrôle permet de détecter un défaut (s'il y en a un) avec une probabilité q (il n'y a pas de faux positifs : on ne peut pas trouver un défaut s'il n'y en a pas).

Les deux contrôles sont négatifs. Quelle est la probabilité qu'il y ait quand même un défaut ?

SIMULATIONEN PYTHON :

```
import random as rd

def experience(p, q):
    defaut = bernoulli(p)
    controles = [False, False]

    for i in range(2):
        if defaut:
            controles[i] = bernoulli(q)

    return (controles, defaut)

def proba(p, q, N = 10000):
    cpt = 0
    pr = 0
    while cpt < N:
        c, d = experience(p, q)
        if not any(c): # deux controles negatifs
            cpt += 1

        if d:
            pr += 1
    return pr / N
```

Pour générer une variable aléatoire de probabilité p en Python, on génère un réel $x \in [0, 1]$ et on le compare à p :

```
def bernoulli(p):
    return rd.random() < p
```

MODÉLISATION : $\Omega = \{0, 1\}^3$;
 $D = \{0, 1\}^2 \times \{1\}$ et $P(D) = p$;
 $C_1 = \{1\} \times \{0, 1\}^2$ et $P_D(C_1) = q$;
 $C_2 = \{0, 1\} \times \{1\} \times \{0, 1\}$ et $P_D(C_2) = q$.

On sait que $P_{\bar{D}}(C_1) = P_{\bar{D}}(C_2) = 0$.

On suppose que C_1 et C_2 indépendants relativement à P_D .

$$P_{\bar{C}_1 \cap \bar{C}_2}(D) = \frac{P_D(\bar{C}_1 \cap \bar{C}_2) P(D)}{P(\bar{C}_1 \cap \bar{C}_2)}.$$

On a :

$$\begin{aligned} P_D(\bar{C}_1 \cap \bar{C}_2) &= P_D(\bar{C}_1) P_D(\bar{C}_2) \\ &= (1-q)^2, \end{aligned}$$

$$P(D) = p,$$

et

$$\begin{aligned} P(\bar{C}_1 \cap \bar{C}_2) &= P_D(\bar{C}_1 \cap \bar{C}_2) P(D) + P_{\bar{D}}(\bar{C}_1 \cap \bar{C}_2) P(\bar{D}) \\ &= p(1-q)^2 + 1-p. \end{aligned}$$

Or,

$$\begin{aligned} P(\bar{C}_1) P(\bar{C}_2) &= ((1-q)p + 1-p)^2 \\ &\neq P(\bar{C}_1 \cap \bar{C}_2) \text{ en général.} \end{aligned}$$

Finalement,

$$P_{\bar{C}_1 \cap \bar{C}_2}(D) = \frac{p(1-q)^2}{p(1-q)^2 + 1-p}.$$

Si $q = 1$, on a $P_{\bar{C}_1 \cap \bar{C}_2}(D) = 0$. Si $q = 0$, on a $P_{\bar{C}_1 \cap \bar{C}_2}(D) = p$.

Définition: Soit (Ω, P) un espace probabilisé et $(A_i)_{i \in I}$ une famille finie d'événements.

1. On dit que ces événements sont 2 à 2 indépendants si

$$\forall i \neq j, \quad P(A_i \cap A_j) = P(A_i) P(A_j)$$

2. On dit qu'ils sont mutuellement indépendants si

$$\forall J \in \mathcal{P}(I) \setminus \{\emptyset\}, \quad P\left(\bigcap_{j \in J} A_j\right) = \prod_{j \in J} P(A_j).$$

EXAMPLE:

À faire

$\Omega = \dots, P = \dots, A, B, C = \dots$ tels que

$$\begin{cases} P(A \cap B) = P(A) P(B) \\ P(A \cap C) = P(A) P(C) \\ P(B \cap C) = P(B) P(C) \end{cases}$$

mais

$$P(A \cap B \cap C) \neq P(A) P(B) P(C).$$

EXERCICE:

Soit (Ω, P) un espace probabilisé fini, A et B deux événements indépendants (par rapport à P).

1. Montrer que A et \bar{B} sont indépendants.

2. Montrer que \bar{A} et \bar{B} sont indépendants.

SOLUTION :

1. On suppose $P(A) \neq 0$.

$$\begin{aligned} P(A \cap \bar{B}) &= P_A(\bar{B}) P(A) \\ &= P(A)(1 - P_A(B)) \\ &= P(A)(1 - P(B)) \\ &= P(A) P(\bar{B}) \end{aligned}$$

On suppose $P(A) = 0$. $A \cap \bar{B} \subset A$ donc

$$0 \leq P(A \cap \bar{B}) \leq P(A) = 0$$

et donc

$$P(A \cap \bar{B}) = 0 = P(A) P(\bar{B}).$$

2. C'est une conséquence du 1. : on remplace B par A et A par \bar{B} .

Proposition: Soit (Ω, P) un espace probabilisé et $(A_i)_{i \in I}$ une famille d'événements mutuellement indépendants. Soit $J \in \mathcal{P}(I)$ et on pose

$$\forall i \in I, B_i = \begin{cases} \bar{A}_i & \text{si } i \in J \\ A_i & \text{sinon.} \end{cases}$$

Alors, $(B_i)_{i \in I}$ est une famille d'événements mutuellement indépendants.

Preuve:

Pour $n \in \mathbb{N}^*$, on pose

$$\mathcal{P}(n) : \text{ "}\forall K \subset I \text{ avec } \#K = n, P\left(\bigcap_{i \in K} B_i\right) = \prod_{i \in K} P(B_i)\text{"}.$$

□

4 Bilan

Une probabilité est une application de la forme

$$P : \mathcal{P}(\Omega) \longrightarrow [0, 1]$$

vérifiant

1. $P(\Omega) = 1$;
2. $\forall A, B, P(A \cup B) = P(A) + P(B)$.

Si $A \cap B = \emptyset$, on dit qu'il sont incompatibles.

Si on associe à chaque événement élémentaire ω_i une "valeur" (\simeq probabilité) p_i , alors il existe une unique probabilité P sur Ω vérifiant $P(\omega_i) = p_i$.

Équiprobabilité

$$P : \mathcal{P}(\Omega) \longrightarrow [0, 1]$$

$$A \longmapsto \frac{\#A}{\#\Omega}.$$

$$P\left(\bigcup_{i=1}^n A_i\right) = \sum_{i=1}^n P(A_i).$$

$$\forall A, B, P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Probabilité conditionnelle

Pour tout événement A de Ω de probabilité non nulle,

$$P_A : \mathcal{P}(\Omega) \rightarrow [0, 1]$$

$$X \mapsto \frac{P(A \cap X)}{P(A)}.$$

Un système complet d'événements est une partition de Ω .

Probabilités totales

$$\forall X \in \mathcal{P}(\Omega), P(X) = \sum_{i=1}^n P(A_i) P_{A_i}(X).$$

A et B sont deux événements indépendants si

$$P(A \cap B) = P(A) P(B).$$

$(A_i)_{i \in I}$ est une famille finie d'événements mutuellement indépendants si

$$P\left(\bigcap_{i \in I} A_i\right) = \prod_{i \in I} P(A_i).$$

Probabilités composées

$$P(A_1 \cap \dots \cap A_n) = P(A_1) P_{A_1}(A_2) P_{A_1 \cap A_2}(A_3) \dots P_{A_1 \cap \dots \cap A_{n-1}}(A_n).$$

Bayes

$$P_A(B) = \frac{P_B(A) P(A)}{P(A)}.$$

Pour plusieurs événements

$$\forall k \in K, P_X(A_k) = \frac{P_{A_k}(X) P(A_k)}{\sum_{j \in K} P_{A_j}(X) P(A_j)}.$$

CHAPITRE

28

SOUS-ESPACES AFFINES D'UN ESPACE VECTORIEL

1 Espace affine (HORS PROGRAMME)

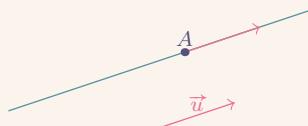
MOTIVATION GÉOMÉTRIQUE :

Dans les petites classes, la géométrie du plan distingue deux types d'objets élémentaires :

- le point
- le vecteur

reliés par la notion de translation.

Par exemple, une droite peut être décrite avec un point et un vecteur :



Soit \mathbb{K} un corps.

Définition: Un \mathbb{K} -espace affine est un triplet (E, \vec{E}, τ) où

- E est un ensemble ;

- \vec{E} est un \mathbb{K} -espace vectoriel ;

— $\tau : E \times \vec{E} \rightarrow E$ telle que

$$\begin{cases} \forall M \in E, \tau(M, \vec{0}) = M, \\ \forall M \in E, \forall (\vec{u}, \vec{v}) \in \vec{E}^2, \tau(\tau(M, \vec{u}), \vec{v}) = \tau(M, \vec{u} + \vec{v}), \\ \forall (A, B) \in E^2, \exists! \vec{u} \in \vec{E}, \tau(A, \vec{u}) = B. \end{cases}$$

Les éléments de E sont appelés points, ceux de \vec{E} vecteurs.

Pour tout $\vec{u} \in \vec{E}$, l'application

$$\begin{array}{ccc} E & \longrightarrow & E \\ M & \longmapsto & \tau(M, \vec{u}) \end{array}$$

est la translation de vecteur \vec{u} .

En général, pour $M \in E$ et $\vec{u} \in \vec{E}$, au lieu d'écrire $\tau(M + \vec{u})$, on écrit $M + \vec{u}$. Soient $(A, B) \in E^2$. L'unique vecteur \vec{u} tel que $A + \vec{u} = B$ est noté $\vec{AB} = B - A$.

EXEMPLE: 1. On pose

$$(\mathcal{E}) : \quad y' = xy + xe^x$$

Soit E l'ensemble des solutions de (\mathcal{E}) , \vec{E} le \mathbb{R} -espace vectoriel des solutions de

$$(\mathcal{H}) : \quad y' = xy,$$

et

$$\begin{aligned} \tau : E \times \vec{E} &\longrightarrow E \\ (f, \vec{u}) &\longmapsto f + \vec{u} \end{aligned}$$

où $+$ correspond à l'addition de fonctions.

— $\forall f \in E, \tau(f, \vec{0}) = f + 0 = f$.

—

$$\begin{aligned} \forall f \in E, \forall (h_1, h_2) \in \vec{E}^2, \tau(\tau(f, h_1), h_2) &= \tau(f + h_1, h_2) \\ &= (f + h_1) + h_2 \\ &= f + (h_1 + h_2) \\ &= \tau(f, \tau(h_1, h_2)) \end{aligned}$$

— Soient $(f_1, f_2) \in E^2$. On pose $h = f_2 - f_1 \in \vec{E}$ ($-$ est la soustraction de fonctions) et alors $\tau(f_1, h) = f_2$ et h est unique.

2. On pose $E = \mathbb{R}^2$, $\vec{E} = \mathbb{R}^2$ et

$$\begin{aligned} \tau : E \times \vec{E} &\longrightarrow E \\ ((x, y), (u, v)) &\longmapsto (x + u, y + v). \end{aligned}$$

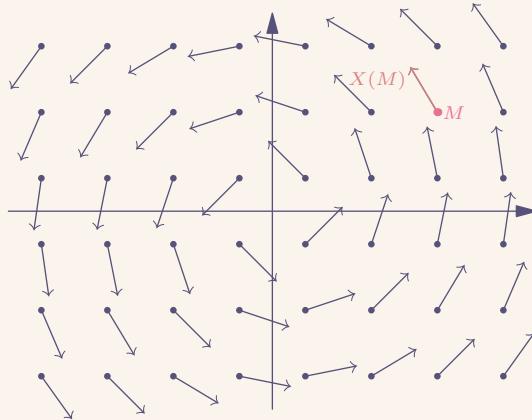
(E, \vec{E}, τ) est un \mathbb{R} -espace affine.

Proposition: Soit E un \mathbb{K} -espace vectoriel. Alors $(E, E, +)$ est un \mathbb{K} -espace affine. \square

EXEMPLE:

Soit E un \mathbb{K} -espace vectoriel. Un champ de vecteur est une application

$$X : \begin{array}{c} E \longrightarrow E \\ \uparrow \quad \uparrow \\ \text{points} \quad \text{vecteurs} \end{array}$$



EXEMPLE:

Avec $F = \mathbb{R}^2$ et $E = \{(x, y) \in F \mid 2x + 3y = 5\}$, $(E, +, \cdot)$ n'est pas un \mathbb{R} -espace vectoriel : $(0, 0) \notin E$.

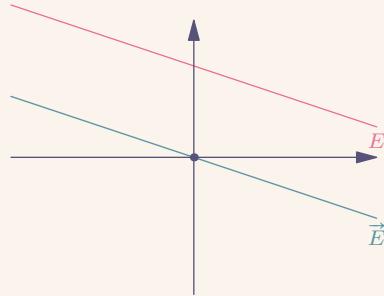
On pose $\vec{E} = \{(x, y) \in F \mid 2x + 3y = 0\}$, c'est un sous-espace vectoriel de F . On pose

$$\begin{aligned}\tau : E \times \vec{E} &\longrightarrow E \\ ((x, y), (u, v)) &\longmapsto (x + u, y + v).\end{aligned}$$

En effet,

$$\begin{aligned}\forall (x, y) \in E, \forall (u, v) \in \vec{E}, 2(x + u) + 3(y + v) &= 2x + 3y + 2u + 3v \\ &= 5 + 0 = 5\end{aligned}$$

donc $\tau((x, y), (u, v)) \in E$.



EXEMPLE:

Avec E les solutions de $y' = 3y + e^x$, $\vec{E} = \mathbb{R}$, et

$$\begin{aligned}\tau : E \times \vec{E} &\longrightarrow E \\ (y, \lambda) &\longmapsto (x \mapsto y(x) + \lambda e^{3x}).\end{aligned}$$

Proposition: Soit (E, \vec{E}, τ) un \mathbb{K} -espace affine. Si $E \neq \emptyset$,

$$\vec{E} = \{\overrightarrow{AB} \mid (A, B) \in \vec{E}\}.$$

Preuve: — $\forall A, B \in E, \overrightarrow{AB} \in \vec{E}$.

— Soit $\vec{u} \in \vec{E}$. Comme $E \neq \emptyset$, on choisit $A \in E$. On pose $B = A + \vec{u}$. D'où $\vec{u} = \overrightarrow{AB}$.

□

REMARQUE:

On a même démontré que, pour tout $A \in E$, l'application

$$\begin{aligned}\varphi_A : \vec{E} &\longrightarrow E \\ \vec{u} &\longmapsto A + \vec{u}\end{aligned}$$

est bijective. On dit qu'on a vectorialisé E au point A :

$$\begin{cases} M + N := A + \overrightarrow{AM} + \overrightarrow{AN} \\ \lambda N := A + \lambda \overrightarrow{AM} \end{cases}$$

Proposition: Soit (E, \vec{E}, τ) un \mathbb{K} -espace affine.

1. $\forall A \in E, \overrightarrow{AA} = \vec{0}$;
2. $\forall A, B, C \in E, \overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$;
3. $\forall A, B \in E, \overrightarrow{BA} = -\overrightarrow{AB}$.

Preuve: 1. Soit $A \in E$. $\tau(A, \overrightarrow{AA}) = A = \tau(A, \vec{0})$ donc $\overrightarrow{AA} = \vec{0}$.

2. Soient $A, B, C \in E$. On pose $\vec{u} = \overrightarrow{AB}$ et $\vec{v} = \overrightarrow{BC}$.

$$\tau(\tau(A, \vec{u}), \vec{v}) = \tau(B, \vec{v}) = C = \tau(A, \overrightarrow{AC})$$

$$\begin{matrix} \| \\ \tau(A, \vec{u} + \vec{v}) \end{matrix}$$

3. Soient $A, B \in E$. D'après 1. $\overrightarrow{AA} = \vec{0}$ et, d'après 2. $\overrightarrow{AA} = \overrightarrow{AB} + \overrightarrow{BA}$. Donc $\overrightarrow{AB} = -\overrightarrow{BA}$.

□

2 Sous-espaces affines

Définition: Soit (E, \vec{E}, τ) un \mathbb{K} -espace affine et $F \in \mathcal{P}(E) \setminus \{\emptyset\}$.

Pour tout $A \in F$, on pose $\overrightarrow{F_A} = \{\overrightarrow{AB} \mid B \in F\}$. On dit que F est un sous-espace affine de (E, \vec{E}, τ) s'il existe $A \in F$ tel que $\overrightarrow{F_A}$ est un sous-espace vectoriel de \vec{E} .

Proposition: Avec les notations précédentes, $(F, \overrightarrow{F_A}, \tau|_{F \times \overrightarrow{F_A}})$ est un espace affine.

Preuve: — Soit $M \in F$, $\vec{u} \in \overrightarrow{F_A}$.

$$M + \vec{u} = A + \underbrace{\overrightarrow{AM}}_{\in \overrightarrow{F_A}} + \underbrace{\overrightarrow{u}}_{\in \overrightarrow{F_A}} = A + \underbrace{\overrightarrow{AB}}_{B \in F} = B \in F.$$

— Soit $M \in F$, $\vec{u}, \vec{v} \in \overrightarrow{F_A}$.

$$(M + \vec{u}) + \vec{v} = M + (\vec{u} + \vec{v})$$

car $M \in E$ et $\vec{u}, \vec{v} \in \overrightarrow{E}$.

— Soient $M, N \in F \subset E$. On sait que

$$\exists! \vec{u} \in \overrightarrow{E}, M + \vec{u} = N.$$

$$\begin{aligned} \vec{u} &= \overrightarrow{MN} = \overrightarrow{MA} + \overrightarrow{AN} \\ &= \underbrace{\overrightarrow{AN}}_{\in \overrightarrow{F_A}} - \underbrace{\overrightarrow{AM}}_{\in \overrightarrow{F_A}} \in \overrightarrow{F_A} \end{aligned}$$

□

Proposition: Soit F un sous-espace affine de $(E, \overrightarrow{E}, \tau)$. Alors

$$\forall (A, B) \in F^2, \overrightarrow{F_A} = \overrightarrow{F_B}.$$

Preuve:

Soit A comme dans la définition ($\overrightarrow{F_A}$ sous-espace vectoriel de \overrightarrow{E}) et $B \in F$. Soit $\vec{u} \in \overrightarrow{F_B}$. Alors $\vec{u} = \overrightarrow{BM}$ avec $M \in F$.

$$\vec{u} = \overrightarrow{BA} + \overrightarrow{AM} = \overrightarrow{AM} - \overrightarrow{AB} \in \overrightarrow{F_A}.$$

Soit $\vec{v} \in \overrightarrow{F_A}$. On pose $M = \underbrace{M}_{\in \overrightarrow{F_A}} + \underbrace{\vec{v}}_{\in \overrightarrow{F_A}} \in F$. Donc $\vec{v} = \overrightarrow{BM} \in \overrightarrow{F_B}$. □

Corollaire: Soit $f \in \mathcal{L}(E, F)$ et $y \in F$.

Les solutions de l'équation $f(x) = y$ est un sous-espace affine de direction $\text{Ker } f$. □

Proposition: Soit $(F_i)_{i \in I}$ une famille de sous-espaces affines de F . Alors, $\bigcap_{i \in I} F_i$ est soit vide, soit un sous-espace affine de F .

De même que pour les groupes et les espaces vectoriels, on peut définir le sous-espace engendré par une partie de E .

Proposition – Définition: Soit $A \in \mathcal{P}(E)$. Le sous-espace affine engendré par A est

$$\bigcap_{\substack{F \text{ sous-espace affine de } E \\ A \subset F}} F.$$

C'est le plus petit (au sens de l'inclusion) sous-espace affine contenant A .

REMARQUE:

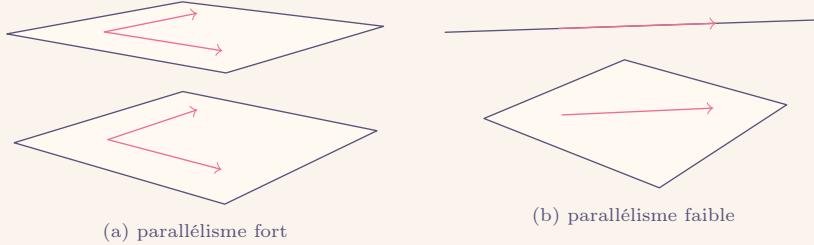
Si E est un \mathbb{K} -espace vectoriel et F un sous-espace affine de E , alors

$$\begin{cases} \forall A \in F, F = A + \vec{F} = \{A + \vec{u} \mid \vec{u} \in \vec{F}\}, \\ \vec{F} \text{ sous-espace vectoriel de } E. \end{cases}$$

3 Parallélisme et hyperplans

Définition: Soit (E, \vec{E}, τ) un espace affine, F et G deux sous-espaces affines de E .

1. On dit que F et G sont fortement parallèles si $\vec{F} = \vec{G}$.
2. On dit que F et G sont faiblement parallèles si $\vec{F} \subset \vec{G}$ ou $\vec{G} \subset \vec{F}$.



Définition: Soit F un sous-espace affine de (E, \vec{E}, τ) . L'espace

$$\vec{F} = \{\overrightarrow{AB} \mid A, B \in F\}$$

est appelé direction de F .

On dit que

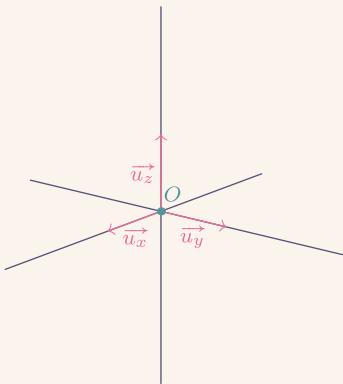
- F est une droite affine si \vec{F} est une droite vectorielle,
- F est une plan affine si \vec{F} est un plan vectoriel,
- F est une hyperplan affine si \vec{F} est un hyperplan vectoriel.

4 Repère affine

Définition: Soit F un sous-espace affine de E . Un repère de F est la donnée d'un point $A \in F$ ("l'origine du repère") et d'une base $\mathcal{B} = (\vec{e}_i)_{i \in I}$ de \vec{F} ("vecteurs direction").

EXEMPLE (mécanique – physique):

On pose $E = (\mathbb{R}^3, \mathbb{R}^3, +)$, un \mathbb{R} -espace affine. $(O, \vec{u_x}, \vec{u_y}, \vec{u_z})$ est une base de E : la base cartésienne. Il existe plusieurs bases de E : $(O, \vec{u_r}, \vec{u_\theta}, \vec{u_z})$ (base cylindrique) et $(O, \vec{u_r}, \vec{u_\theta}, \vec{u_\varphi})$ (base sphérique) sont deux autres bases de E .



Proposition – Définition: Soit F un sous-espace affine de E , et $\mathcal{R} = (A, \vec{e}_1, \dots, \vec{e}_n)$ un repère de F . Alors, pour tout $B \in F$,

$$\exists! (\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n, B = A + \sum_{i=1}^n \lambda_i \vec{e}_i.$$

On dit que $(\lambda_1, \dots, \lambda_n)$ sont les coordonées de B .

REMARQUE:

Les solutions d'un problème linéaire forment un espace sous-affine de direction les solutions du système homogène associé.

CHAPITRE

29

PRODUIT SCALAIRES

Dans ce chapitre, E désigne un \mathbb{R} -espace vectoriel.

On sait déjà calculer le produit scalaire en dimension 2 et 3 mais l'objectif de ce chapitre est de le généraliser en dimension potentiellement infinie.

1 Définitions

Définition: Un produit scalaire sur E est une forme bilinéaire symétrique définie positive :

$$f : E \times E \longrightarrow \mathbb{R}$$

1. $\forall (u_1, u_2, v) \in E^3, \forall (\alpha, \beta) \in \mathbb{R}^2, f(\alpha u_1 + \beta u_2, v) = \alpha f(u_1, v) + \beta f(u_2, v)$, (bilinéaire)
2. $\forall (u, v) \in E^2, f(u, v) = f(v, u)$, (symétrie)
3. $\forall u \in E, f(u, u) \geq 0$, (positive)
4. $\forall u \in E, (f(u, u) = 0 \iff u = 0_E)$. (définie)

On dit alors que (E, f) est un espace préhilbertien. Si, de plus, E est de dimension finie, alors on dit que (E, f) est un espace euclidien.

En général, on note $\langle u | v \rangle$, $\langle u, v \rangle$ ou $(u | v)$ à la place de $f(u, v)$.

REMARQUE:

Même si elle est utilisée (notamment au lycée), la notation $u \cdot v$ est dangereuse car elle peut être facilement confondue par la multiplication.

EXEMPLE: 1. Avec $E = \mathbb{R}^2$, on a $\langle (x, y) | (x', y') \rangle = xx' + yy'$.

2. Avec $E = \mathbb{R}^n$, on a $\langle (x_1, \dots, x_n) | (y_1, \dots, y_n) \rangle = \sum_{i=1}^n x_i y_i$.

3. Avec $E = C^0([a, b], \mathbb{R})$, on a $\langle f | g \rangle = \int_a^b f(t)g(t) dt$.

4. Avec $E = \ell^1(\mathbb{R}) = \{u \in \mathbb{R}^{\mathbb{N}} \mid \sum |u_n| \text{ converge}\}$, on a $\langle u | v \rangle = \sum_{n=0}^{+\infty} u_n v_n$. En effet,

$v \in E$ donc $\sum |v_n|$ converge et donc $v_n \xrightarrow{n \rightarrow +\infty} 0$. On a donc

$$\exists N \in \mathbb{N}, \forall n \geq N, |v_n| \leq 1$$

donc

$$\exists N \in \mathbb{N}, \forall n \geq N, |u_n v_n| \leq |u_n|.$$

Comme $\sum |u_n|$ converge, on en déduit que $\sum |u_n v_n|$ aussi.

5. Avec $E = \mathbb{R}^2$, on a $\langle (x, y) | (x', y') \rangle = xx' + 2xy' + 2yx' + 5yy'$.

— On fixe $(x', y') \in E$. Soient $(x_1, y_1) \in E$, $(x_2, y_2) \in E$ et $(\lambda_1, \lambda_2) \in \mathbb{R}^2$.

$$\begin{aligned} \langle \lambda_1(x_1, y_1) + \lambda_2(x_2, y_2) | (x', y') \rangle &= \langle (\lambda_1 x_1 + \lambda_2 x_2, \lambda_1 y_1 + \lambda_2 y_2) | (x', y') \rangle \\ &= (\lambda_1 x_1 + \lambda_2 x_2)x' + 2(\lambda_1 x_1 + \lambda_2 x_2)y' \\ &\quad + 2(\lambda_1 y_1 + \lambda_2 y_2)x' + 5(\lambda_1 y_1 + \lambda_2 y_2)y' \\ &= \lambda_1(x_1 x' + 2x_1 y' + 2y_1 x' + 5y_1 y') \\ &\quad + \lambda_2(x_2 x' + 2x_2 y' + 2y_2 x' + 5y_2 y') \\ &= \lambda_1 \langle (x_1, y_1) | (x', y') \rangle + \lambda_2 \langle (x_2, y_2) | (x', y') \rangle \end{aligned}$$

— Soit $(x, y) \in E$ et $(x', y') \in E$.

$$\begin{aligned} \langle (x', y') | (x, y) \rangle &= x'x + 2x'y + 2y'x + 3y'y \\ &= \langle (x, y) | (x', y') \rangle \end{aligned}$$

— Soit $(x, y) \in E$.

$$\begin{aligned} \langle (x, y) | (x, y) \rangle &= x^2 + 4xy + 5y^2 \\ &= (x + 2y)^2 + y^2 \geq 0 \end{aligned}$$

— Soit $(x, y) \in E$.

$$\begin{aligned} \langle (x, y) | (x, y) \rangle = 0 &\iff (x + 2y)^2 + y^2 = 0 \\ &\iff \begin{cases} y^2 = 0 \\ (x + 2y)^2 = 0 \end{cases} \\ &\iff \begin{cases} y = 0 \\ x = 0 \end{cases} \end{aligned}$$

Définition: Soit $(E, \langle \cdot | \cdot \rangle)$ un espace préhilbertien. Soit $x \in E$.

La norme (euclidienne) de x est

$$\sqrt{\langle x | x \rangle} = \|x\|.$$

Proposition:	1. $\forall x \in E, \ x\ = 0 \iff x = 0_E$	(séparation)
	2. $\forall x \in E, \forall \lambda \in \mathbb{R}, \ \lambda x\ = \lambda \ x\ $	(homogénéité positive)
	3. $\forall (x, y) \in E^2, \ x + y\ \leq \ x\ + \ y\ $	(inégalité triangulaire)

□

L'inégalité triangulaire sera prouvée dans la suite du chapitre (paragraphe 2.).

Définition: Soit $(x, y) \in E^2$. On dit que x et y sont orthogonaux si $\langle x | y \rangle = 0$. On note cette situation $x \perp y$.

EXEMPLE:

Avec $E = C^0([-1, 1], \mathbb{R})$ et $\langle f | g \rangle = \int_{-1}^1 f(t)g(t) dt$. Soit f paire et g impaire. Alors $f \perp g$. Dans ce cas, on peut appliquer le théorème de Pythagore (vu dans la suite du chapitre) :

$$\|f + g\|^2 = \|f\|^2 + \|g\|^2.$$

2 Quelques formules

Dans ce paragraphe, $(E, \langle \cdot | \cdot \rangle)$ est un espace préhilbertien.

Proposition: Soient $x, y \in E$.

- 1. $\|x + y\|^2 = \|x\|^2 + \|y\|^2 + 2\langle x | y \rangle$.
- 2. $\|x + y\|^2 + \|x - y\|^2 = 2(\|x\|^2 + \|y\|^2)$. (identité du parallélogramme)
- 3. $\langle x | y \rangle = \frac{1}{4} (\|x + y\|^2 - \|x - y\|^2)$. (polarisation)

Preuve: 1.

$$\begin{aligned} \|x + y\|^2 &= \langle x + y | x + y \rangle \\ &= \langle x | x + y \rangle + \langle y | x + y \rangle \\ &= \langle x | x \rangle + \langle x | y \rangle + \langle y | x \rangle + \langle y | y \rangle \\ &= \|x\|^2 + \|y\|^2 + 2\langle x | y \rangle \end{aligned}$$

2.

$$\begin{aligned} \|x + y\|^2 + \|x - y\|^2 &= \|x\|^2 + \|y\|^2 + 2\langle x | y \rangle \\ &\quad + \|x\|^2 + \|y\|^2 + 2\langle x | -y \rangle \\ &= 2\|x\|^2 + 2\|y\|^2 \end{aligned}$$

3.

□

Théorème (inégalité de Cauchy-Schwarz): Soient $x, y \in E$. Alors

$$|\langle x | y \rangle| \leq \|x\| \|y\|$$

et

$$|\langle x | y \rangle| = \|x\| \|y\| \iff x \text{ et } y \text{ sont colinéaires.}$$

Preuve:

On fixe $(x, y) \in E^2$.

— On suppose $y \neq 0_E$. Soit

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ t &\longmapsto \|x + ty\|. \end{aligned}$$

$$\begin{aligned} \forall t \in \mathbb{R}, f(t) &= \|x\|^2 + 2\langle x \mid ty \rangle + \|ty\|^2 \\ &= \|x\|^2 + 2t\langle x \mid y \rangle + t^2\|y\|^2. \end{aligned}$$

Comme $y \neq 0_E$, $\|y\|^2 \neq 0$ et f est donc une fonction polynomiale de degré 2.
En outre,

$$\forall t \in \mathbb{R}, f(t) \geq 0.$$

Donc le discriminant Δ de f est négatif ou nul. Or,

$$\Delta = 4\langle x \mid y \rangle^2 - 4\|x\|^2\|y\|^2.$$

Ainsi

$$\langle x \mid y \rangle^2 \leq \|x\|^2\|y\|^2$$

et donc

$$|\langle x \mid y \rangle| \leq \|x\|\|y\|.$$

On suppose que $|\langle x \mid y \rangle| = \|x\|\|y\|$. Dans ce cas, $\Delta = 0$. Soit $\lambda \in \mathbb{R}$ tel que $f(\lambda) = 0$, i.e. $\|x + \lambda y\| = 0$ et donc $x = -\lambda y$, donc x et y sont colinéaires.

La réciproque est immédiate.

— On suppose $y = 0_E$.

$$|\langle x \mid y \rangle| = |\langle x \mid 0_E \rangle| = 0 \quad \text{et} \quad \|x\|\|y\| = \|x\| \times 0 = 0.$$

On a bien

$$\left\{ \begin{array}{l} |\langle x \mid y \rangle| \leq \|x\|\|y\|; \\ y \text{ et } x \text{ sont colinéaires.} \end{array} \right.$$

□

Corollaire (inégalité triangulaire): Soit $(x, y) \in E^2$.

1. $\|x + y\| \leq \|x\| + \|y\|$.
2. $\|x + y\| = \|x\| + \|y\| \iff \exists \lambda \in \mathbb{R}^+, (x = \lambda y \text{ ou } y = \lambda x)$.

Preuve: 1.

$$\begin{aligned} \|x + y\|^2 &= \|x\|^2 + \|y\|^2 + 2\langle x \mid y \rangle \\ &\leq \|x\|^2 + \|y\|^2 + 2|\langle x \mid y \rangle| \\ &\leq \|x\|^2 + \|y\|^2 + 2\|x\|\|y\| \\ &\leq (\|x\| + \|y\|)^2. \end{aligned}$$

D'où

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

2.

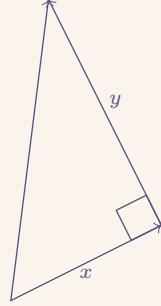
$$\begin{aligned}
 \|x + y\| = \|x\| + \|y\| &\iff \|x + y\|^2 = (\|x\| + \|y\|)^2 \\
 &\iff \|x\|^2 + \|y\|^2 + 2\langle x | y \rangle = \|x\|^2 + \|y\|^2 + 2\|x\|\|y\| \\
 &\iff \langle x | y \rangle = \|x\|\|y\| \\
 &\iff \begin{cases} \langle x | y \rangle \geq 0 \\ |\langle x | y \rangle| = \|x\|\|y\| \end{cases} \\
 &\iff \begin{cases} \exists \lambda \in \mathbb{R}, x = \lambda y \text{ ou } y = \lambda x \\ \langle x | y \rangle \geq 0 \end{cases} \\
 &\iff \exists \lambda \in \mathbb{R}^+, x = \lambda y \text{ ou } y = \lambda x.
 \end{aligned}$$

□

3 Familles orthogonales

Théorème (Pythagore): Soit $(x, y) \in E^2$.

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2 \iff x \perp y.$$



Preuve:

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2 \iff 2\langle x | y \rangle = 0 \iff x \perp y.$$

□

Définition: Soit $(e_i)_{i \in I}$ une famille de vecteurs. On dit que cette famille est orthogonale si

$$\forall i \neq j \ e_i \perp e_j.$$

Si, en plus, on a

$$\forall i \in I, \|e_i\| = 1,$$

alors on dit que la famille est orthonormale ou orthonormée.

Proposition (Pythagore): Soit (e_1, \dots, e_n) une famille orthogonale. Alors

$$\left\| \sum_{i=1}^n e_i \right\|^2 = \sum_{i=1}^n \|e_i\|^2.$$

Théorème: Toute famille orthogonale de vecteurs non nuls est libre.

Preuve:

Soit $(e_i)_{i \in I}$ une famille orthogonale telle que

$$\forall i \in I, e_i \neq 0_E.$$

Soit $n \in \mathbb{N}^*$, $(\lambda_1, \dots, \lambda_n) \in \mathbb{R}^n$. On suppose

$$\sum_{k=1}^n \lambda_k e_{i_k} = 0_E.$$

Soit $j \in \llbracket 1, n \rrbracket$.

$$\begin{aligned} 0 &= \left\langle \sum_{k=1}^n \lambda_k e_{i_k} \mid e_{i_j} \right\rangle \\ &= \sum_{k=1}^n \lambda_k \langle e_{i_k} \mid e_{i_j} \rangle \\ &= \lambda_j \underbrace{\|e_{i_j}\|^2}_{\neq 0} \end{aligned}$$

donc $\lambda_j = 0$. □

Algorithme (Orthonormalisation de Gram–Schmidt): On suppose E de dimension finie. Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E .

— Étape 1 : On pose $v_1 = \frac{e_1}{\|e_1\|}$ de sorte que $\|v_1\| = 1$.

— Étape 2 : On pose

$$u_2 = e_2 - \langle e_2 \mid v_1 \rangle v_1.$$

Ainsi,

$$\begin{aligned} \langle u_2 \mid v_1 \rangle &= \langle e_2 - \langle e_2 \mid v_1 \rangle v_1 \mid v_1 \rangle \\ &= \langle e_2 \mid v_1 \rangle - \langle e_2 \mid v_1 \rangle \langle v_1 \mid v_1 \rangle \\ &= 0. \end{aligned}$$

On pose $v_2 = \frac{u_2}{\|u_2\|}$ donc $v_2 \perp v_1$ et $\|v_2\| = 1$.

— Étape 3 : On pose

$$u_3 = e_3 - \langle e_3 \mid v_1 \rangle v_1 - \langle e_3 \mid v_2 \rangle v_2.$$

Ainsi,

$$\begin{aligned} \langle u_3 \mid v_1 \rangle &= \langle e_3 \mid v_1 \rangle - \langle e_3 \mid v_1 \rangle \underbrace{\langle v_1 \mid v_1 \rangle}_{=1} - \langle e_3 \mid v_2 \rangle \underbrace{\langle v_2 \mid v_1 \rangle}_{=0} \\ &= 0 \end{aligned}$$

et

$$\begin{aligned}\langle u_3 \mid v_2 \rangle &= \langle e_3 \mid v_2 \rangle - \langle e_3 \mid v_1 \rangle \underbrace{\langle v_1 \mid v_2 \rangle}_{=0} - \langle e_3 \mid v_2 \rangle \underbrace{\langle v_2 \mid v_2 \rangle}_{=1} \\ &= 0.\end{aligned}$$

On pose $v_3 = \frac{u_3}{\|u_3\|}$ de sorte que $v_3 \perp v_1$, $v_3 \perp v_2$ et $\|v_3\| = 1$.

— Étape i + 1 : On pose

$$u_{i+1} = e_{i+1} - \sum_{k=1}^i \langle e_{i+1} \mid v_k \rangle v_k.$$

Ainsi, pour tout $j \in \llbracket 1, i \rrbracket$, on a

$$\begin{aligned}\langle u_{i+1} \mid v_j \rangle &= \langle e_{i+1} \mid v_j \rangle - \sum_{k=1}^i \langle e_{i+1} \mid v_k \rangle \langle v_k \mid v_j \rangle \\ &= \langle e_{i+1} \mid v_j \rangle - \langle e_{i+1} \mid v_j \rangle \|v_j\|^2 \\ &= 0.\end{aligned}$$

$$\text{On pose } v_{i+1} = \frac{u_{i+1}}{\|u_{i+1}\|}.$$

EXEMPLE:

Avec $E = \mathbb{R}_3[X]$, $\langle P \mid Q \rangle = \int_0^1 P(t) Q(t) dt$ et $\mathcal{B} = (1, X, X^2, X^3)$.

$$1. \quad \|1\|^2 = \langle 1 \mid 1 \rangle = \int_0^1 1 dt = 1 \text{ et donc } v_1 = 1.$$

$$2. \quad u_2 = X - \langle X \mid v_1 \rangle v_1. \text{ Or, } \langle X \mid v_1 \rangle = \int_0^1 t dt = \frac{1}{2}. \text{ D'où } u_2 = X - \frac{1}{2}.$$

$$\begin{aligned}\|u_2\|^2 &= \int_0^1 \left(t - \frac{1}{2} \right)^2 dt \\ &= \int_0^1 \left(t^2 - t + \frac{1}{4} \right) dt \\ &= \frac{1}{3} - \frac{1}{2} + \frac{1}{4} \\ &= \frac{1}{12}\end{aligned}$$

On en déduit que $v_2 = \sqrt{12} \left(X - \frac{1}{2} \right)$.

$$3. \quad u_3 = X^2 - \langle X^2 \mid v_1 \rangle v_1 - \langle X^2 \mid v_2 \rangle v_2. \text{ On a}$$

$$\langle X^2 \mid v_1 \rangle = \int_0^1 t^2 dt = \frac{1}{3}$$

et

$$\begin{aligned}\langle X^2 \mid v_2 \rangle &= \sqrt{12} \int_0^1 t^2 \left(t - \frac{1}{2} \right) dt \\ &= \frac{\sqrt{12}}{12}.\end{aligned}$$

D'où

$$\begin{aligned} u_3 &= X^2 - \frac{1}{3} - \frac{\sqrt{12}}{12} \sqrt{12} \left(X - \frac{1}{2} \right) \\ &= X^2 - \frac{1}{3} - X + \frac{1}{2} \\ &= X^2 - X + \frac{1}{6}. \end{aligned}$$

$$\begin{aligned} \|u_3\|^2 &= \int_0^1 \left(t^2 - t + \frac{1}{6} \right) dt \\ &= \int_0^1 \left(t^4 + t^2 + \frac{1}{36} - 2t^3 + \frac{t^2}{3} - \frac{t}{3} \right) dt \\ &= \frac{1}{5} + \frac{1}{3} + \frac{1}{36} - \frac{1}{2} + \frac{1}{9} - \frac{1}{6} \\ &= \frac{36 + 60 + 5 - 90 + 20 - 30}{180} \\ &= \frac{1}{180} \end{aligned}$$

On en déduit que

$$v_3 = 6\sqrt{5} \left(X^2 - X + \frac{1}{6} \right).$$

4. Exercice : calculer v_4 .

Proposition: Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E et \mathcal{C} la base obtenue par le procédé d'orthonormalisation de Gram–Schmidt. Alors,

$$\forall i \in \llbracket 1, n \rrbracket, \text{Vect}(e_1, \dots, e_i) = \text{Vect}(v_1, \dots, v_i).$$

□

EXEMPLE (orthogonalisation):

$$\begin{aligned} \left. \begin{aligned} u_2 \in \text{Vect}(e_1, e_2) \\ u_2 \perp u_1 \end{aligned} \right\} &\iff \left\{ \begin{aligned} u_2 = ae_1 + be_2 &\quad (a, b) \in \mathbb{R}^2 \\ \langle u_1 \mid u_2 \rangle = 0 \end{aligned} \right. \\ &\iff \left\{ \begin{aligned} u_2 = a + bX \\ \int_0^1 (a + bt) dt = 0. \end{aligned} \right. \end{aligned}$$

$$\begin{aligned} \int_0^1 (a + bt) dt = 0 &\iff a + \frac{b}{2} = 0 \\ &\iff a = -\frac{b}{2} \\ &\iff u_2 = -\frac{b}{2} + bX. \end{aligned}$$

Par exemple, $u_2 = -1 + 2X$.

$$-\left\{ \begin{aligned} u_3 \in \text{Vect}(e_1, e_2, e_3) \\ u_3 \perp u_1 \\ u_3 \perp u_2 \end{aligned} \right.$$

On pose $u_3 = a + bX + cX^2$ avec $(a, b, c) \in \mathbb{R}^3$.

$$\begin{aligned} \left. \begin{aligned} \int_0^1 (a + bt + ct^2) dt &= 0 \\ \int_0^1 (a + bt + ct^2)(2t - 1) dt &= 0 \end{aligned} \right\} &\iff \begin{cases} a + \frac{b}{2} + \frac{c}{3} = 0 \\ \int_0^1 (2ct^3 + (-c + 2b)t^2 + (2a - b)t - a) dt = 0 \end{cases} \\ &\iff \begin{cases} a + \frac{b}{2} + \frac{c}{3} = 0 \\ \frac{c}{2} + \frac{2b - c}{3} + \frac{2a - b}{2} - a = 0 \end{cases} \\ &\iff \begin{cases} a = -\frac{b}{2} - \frac{c}{3} = \frac{c}{2} - \frac{c}{3} = \frac{c}{6} \\ b = -c. \end{cases} \end{aligned}$$

On en déduit que

$$u_3 = 1 - 6X + 6X^2.$$

Corollaire (théorème de la base orthonormée incomplète): Soit (e_1, \dots, e_k) une base orthonormée d'un espace euclidien. On peut trouver e_{k+1}, \dots, e_n tels que $(e_1, \dots, e_k, e_{k+1}, \dots, e_n)$ soit une base orthonormée de E .

Preuve:

On sait que (e_1, \dots, e_k) est libre. On complète (e_1, \dots, e_k) en une base \mathcal{B} de E . On orthonormalise \mathcal{B} : on obtient une base orthonormée \mathcal{C} de E . En détaillant l'algorithme de Gram–Schmidt, on s'aperçoit que les k premiers vecteurs de \mathcal{C} sont ceux de \mathcal{B} . \square

Théorème: Soit E un espace euclidien et $\mathcal{B} = (e_1, \dots, e_n)$ une base orthonormée de E . Soit $(x, y) \in E^2$. On pose $(x_1, \dots, x_n) \in \mathbb{R}^n$ et $(y_1, \dots, y_n) \in \mathbb{R}^n$ tels que

$$x = \sum_{i=1}^n x_i e_i \quad y = \sum_{i=1}^n y_i e_i.$$

Alors

$$\langle x | y \rangle = \sum_{i=1}^n x_i y_i.$$

Soit $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ et $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$. Alors,

$$\langle x | y \rangle = X^\top Y.$$

Preuve:

$$\begin{aligned}
\langle x \mid y \rangle &= \left\langle \sum_{i=1}^n x_i e_i \mid y \right\rangle \\
&= \sum_{i=1}^n x_i \langle e_i \mid y \rangle \\
&= \sum_{i=1}^n x_i \left\langle e_i \mid \sum_{j=1}^n y_j e_j \right\rangle \\
&= \sum_{i=1}^n x_i \sum_{j=1}^n y_j \underbrace{\langle e_i \mid e_j \rangle}_{\delta_i^j} \\
&= \sum_{i=1}^n x_i y_i.
\end{aligned}$$

□

Proposition: Soit E un espace euclidien et $\mathcal{B} = (e_1, \dots, e_n)$ une base orthonormée de E . Alors,

$$\forall x \in E, x = \sum_{i=1}^n \langle x \mid e_i \rangle e_i.$$

Preuve:

Soit $x \in E$. On pose

$$x = \sum_{i=1}^n x_i e_i$$

avec $(x_1, \dots, x_n) \in \mathbb{R}^n$. Soit $j \in \llbracket 1, n \rrbracket$. On a

$$\begin{aligned}
\langle x \mid e_j \rangle &= \left\langle \sum_{i=1}^n x_i e_i \mid e_j \right\rangle \\
&= \sum_{i=1}^n x_i \langle e_i \mid e_j \rangle \\
&= x_j.
\end{aligned}$$

□

4 Projection orthogonale

Dans ce paragraphe, $(E, \langle \cdot \mid \cdot \rangle)$ est un espace préhilbertien (de dimension quelconque).

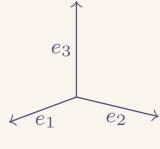
Définition: Soit $A \in \mathcal{P}(E)$. L'orthogonal de A est

$$A^\perp = \{u \in E \mid \forall a \in A, a \perp u\}.$$

EXEMPLE: 1. $\emptyset^\perp = E$; $\{0_E\}^\perp = E$; $E^\perp = \{0_E\}$.

Attention \triangle , $(\emptyset^\perp)^\perp = \{0_E\} \neq \emptyset$.

2. Avec $E = \mathbb{R}^3$, et $A = \{e_3\}$.



$$A^\perp = \text{Vect}(e_1, e_2)$$

et

$$A^{\perp\perp} = \text{Vect}(e_1, e_2)^\perp = \text{Vect}(e_3) \neq A.$$

Proposition:

$\forall A \in \mathcal{P}(E)$, A^\perp est un sous-espace vectoriel de E .

Preuve:

Soit $A \in \mathcal{P}(E)$.

- $\forall a \in A$, $\langle a \mid 0_E \rangle = 0$ donc $0_E \in A^\perp$ et donc $A^\perp \neq \emptyset$.
- Soient $(u, v) \in A^\perp$, $(\alpha, \beta) \in \mathbb{R}^2$. Soit $a \in A$.

$$\begin{aligned} \langle \alpha u + \beta v \mid a \rangle &= \alpha \langle u \mid a \rangle + \beta \langle v \mid a \rangle \\ &= \alpha \times 0 + \beta \times 0 \\ &= 0. \end{aligned}$$

□

Théorème: Soit F un sous-espace vectoriel de dimension finie de E . Alors

$$F \oplus F^\perp = E.$$

Preuve:

Soit $\mathcal{B} = (e_1, \dots, e_p)$ une base orthonormée de F .

ANALYSE Soit $x \in E$. On suppose $x = u + v$ avec $u \in F$ et $v \in F^\perp$. On pose

$$u = \sum_{i=1}^p u_i e_i. \text{ De plus,}$$

$$\forall i \in \llbracket 1, p \rrbracket, \langle v \mid e_i \rangle = 0.$$

Soit $i \in \llbracket 1, p \rrbracket$.

$$\begin{aligned} \langle x \mid e_i \rangle &= \langle u + v \mid e_i \rangle \\ &= \langle u \mid e_i \rangle + \langle v \mid e_i \rangle \\ &= \left\langle \sum_{j=1}^p u_j e_j \mid e_i \right\rangle \\ &= \sum_{j=1}^p u_j \langle e_j \mid e_i \rangle \\ &= u_i \end{aligned}$$

D'où

$$\begin{cases} u = \sum_{i=1}^p \langle x | e_i \rangle e_i \\ v = x - \sum_{i=1}^p \langle x | e_i \rangle e_i. \end{cases}$$

Synthèse Soit $x \in E$. On pose

$$\begin{cases} u = \sum_{i=1}^p \langle x | e_i \rangle e_i \\ v = x - \sum_{i=1}^p \langle x | e_i \rangle e_i \end{cases}$$

On a clairement $u + v = x$ et $u \in F$.

Soit $a \in F$. On pose $a = \sum_{i=1}^p a_i e_i$.

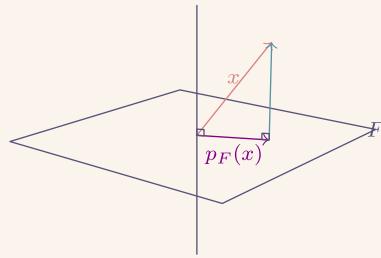
$$\begin{aligned} \langle v | a \rangle &= \langle x | a \rangle - \sum_{i=1}^p \langle x | e_i \rangle \underbrace{\langle e_i | a \rangle}_{=a_i} \\ &= \sum_{i=1}^p a_i \langle x | e_i \rangle - \sum_{i=1}^p a_i \langle x | e_i \rangle \\ &= 0 \end{aligned}$$

donc $v \in F^\perp$.

□

Définition: Dans les conditions précédentes, F^\perp est appelé le supplémentaire orthogonal de F .

La projection sur F parallèlement à F^\perp est appelée projection orthogonale sur F . On la note p_F .



Proposition (inégalité de Bessel): Soit F de dimension finie. Alors,

$$\forall x \in E, \|p_F(x)\| \leq \|x\|.$$

Preuve:

Comme F est de dimension finie :

$$F \oplus F^\perp = E.$$

Soit $x \in E$. On a

$$x = p_F(x) + (x - p_F(x))p_F(x) \in Fx - p_F(x) \in F^\perp.$$

Donc, $x - p_F(x) \perp p_F(x)$ car $p_F(x) \in F$ et $x - p_F(x) \in F^\perp$.

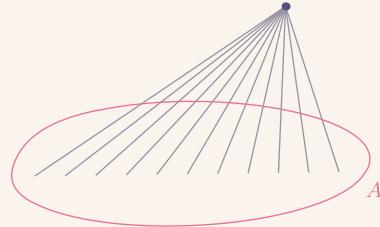
D'après le théorème de Pythagore,

$$\begin{aligned} \|x\|^2 &= \|p_F(x)\|^2 + \underbrace{\|x - p_F(x)\|}_{\geq 0}^2 \\ &\geq \|p_F(x)\|^2. \end{aligned}$$

□

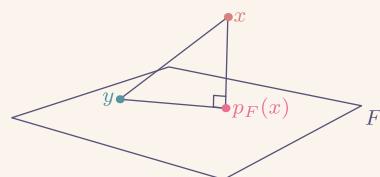
Définition: Soit $A \in \mathcal{P}(E)$ non vide et $x \in E$. La distance de x à A est

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



Théorème: Soit F un sous-espace vectoriel de E de dimension finie et $x \in E$. Alors,

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



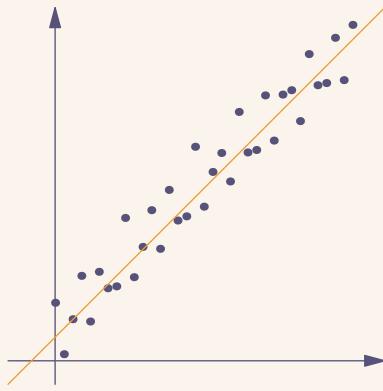
Preuve:

Soit $y \in F$.

$$\begin{aligned}\|x - y\|^2 &= \|\underbrace{x - p_F(x)}_{\in F^\perp} + \underbrace{p_F(x) - y}_{\in F}\|^2 \\ &= \|x - p_F(x)\|^2 + \|p_F(x) - y\|^2 \\ &\geq \|x - p_F(x)\|^2.\end{aligned}$$

□

EXEMPLE (droite des moindres carrés – régression linéaire):



On cherche $(a, b) \in \mathbb{R}^2$ qui minimise $\sum_{i=1}^n (y_i - (ax_i - b))^2$.

On pose $y = (y_1, \dots, y_n) \in \mathbb{R}^n$, $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ et $\mathbf{1} = (1, \dots, 1) \in \mathbb{R}^n$. On suppose que x et $\mathbf{1}$ ne sont pas colinéaires.

Soit $\langle \cdot | \cdot \rangle$ le produit scalaire canonique de \mathbb{R}^n .

$$\begin{aligned}\sum_{i=1}^n (y_i - (ax_i - b))^2 &= \|y - \underbrace{(ax - b\mathbf{1})}_{\in \text{Vect}(x, \mathbf{1}) = F}\|^2. \\ \min_{(a,b) \in \mathbb{R}^2} \sum_{i=1}^n (y_i - (ax_i + b))^2 &= \|y - p_F(y)\|^2.\end{aligned}$$

On veut les coordonnées de $p_F(y)$ dans la base $(x, \mathbf{1})$ de F .

Proposition: Soit F un sous-espace vectoriel de E de dimension finie et $\mathcal{B} = (e_1, \dots, e_p)$ une base orthonormée de F . Alors,

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

Preuve: — $\sum_{i=1}^p \langle x | e_i \rangle e_i \in F$ car $e_1, \dots, e_p \in F$.

— On pose $u = x - \sum_{i=1}^p \langle x \mid e_i \rangle e_i$. Montrons que $u \in F^\perp$. Soit $a \in F$. On peut écrire

$$a = \sum_{i=1}^p \langle a \mid e_i \rangle e_i.$$

$$\begin{aligned} \langle u \mid a \rangle &= \langle x \mid a \rangle - \langle p_F(x) \mid a \rangle \\ &= \sum_{i=1}^p \langle a \mid e_i \rangle \langle x \mid e_i \rangle - \sum_{i=1}^p \sum_{j=1}^p \langle a \mid e_i \rangle \langle x \mid e_j \rangle \langle e_i \mid e_j \rangle \\ &= \sum_{i=1}^p \langle a \mid e_i \rangle \langle x \mid e_i \rangle - \sum_{i=1}^p \langle a \mid e_i \rangle \langle x \mid e_i \rangle \\ &= 0. \end{aligned}$$

□

EXEMPLE (suite de l'exemple précédent – régression linéaire):
On orthonormalise la base $(\mathbb{1}, x)$ de F .

$$\|\mathbb{1}\|^2 = \sum_{i=1}^n 1^2 = n.$$

On pose donc $v_1 = \frac{\mathbb{1}}{\|\mathbb{1}\|} = \frac{1}{\sqrt{n}}(1, \dots, 1)$.

Soit $u_2 = x - \langle x \mid v_1 \rangle v_1$.

$$\langle x \mid v_1 \rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^n x_i = \sqrt{n}\bar{x} \text{ où } \bar{x} = \frac{1}{n} = \frac{1}{n} \sum_{i=1}^n x_i.$$

D'où,

$$\begin{aligned} u_2 &= (x_1, \dots, x_n) - \bar{x}(1, \dots, 1) \\ &= (x_1 - \bar{x}, \dots, x_n - \bar{x}). \end{aligned}$$

On a $\|u_2\|^2 = \sum_{i=1}^n (x_i - \bar{x})^2 = n\sigma_x^2$. On en déduit donc que

$$v_2 = \frac{u_2}{\|u_2\|} = \frac{1}{\sqrt{n}\sigma_x}(x_1 - \bar{x}, \dots, x_n - \bar{x}).$$

$$\begin{aligned} p_F(y) &= \langle y \mid v_1 \rangle v_1 + \langle y \mid v_2 \rangle v_2 \\ &= \frac{1}{n} \sum_{i=1}^n y_i (1, \dots, 1) + \frac{1}{n\sigma_x^2} \sum_{i=1}^n y_i (x_i - \bar{x})(x_1 - \bar{x}, \dots, x_n - \bar{x}) \\ &= (\bar{y}, \dots, \bar{y}) - \frac{1}{n\sigma_x^2} \left(\sum_{i=1}^n (y_i - \bar{y})(x_i - \bar{x}) + \bar{y} \sum_{i=1}^n (x_i - \bar{x}) \right) (x_1 - \bar{x}, \dots, x_n - \bar{x}) \\ &= (\bar{y}, \dots, \bar{y}) + \frac{1}{\sigma_x^2} \text{Cov}(x, y)(x_1 - \bar{x}, \dots, x_n - \bar{x}) \\ &= \left(\bar{y} - \frac{\text{Cov}(x, y)}{\sigma_x^2} \bar{x} \right) (1, \dots, 1) + \frac{\text{Cov}(x, y)}{\sigma_x^2} (x_1, \dots, x_n). \end{aligned}$$

Donc,

$$\begin{cases} a = \frac{\text{Cov}(x, y)}{\sigma_x^2}; \\ b = \bar{y} - a\bar{x}. \end{cases}$$

Proposition: Soit F un sous-espace vectoriel de E de dimension finie. Alors,

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

Preuve:

Clairement, $F \subset (F^\perp)^\perp$.

Soit $\mathcal{B} = (e_1, \dots, e_p)$ une base orthonormée de F et $x \in (F^\perp)^\perp$.

On sait que

$$\begin{cases} x = \underbrace{p_F(x)}_{\in F} + \underbrace{x - p_F(x)}_{\in F^\perp} \\ p_F(x) = \sum_{i=1}^p \langle x | e_i \rangle e_i \end{cases}.$$

$$\begin{aligned} x - p_F(x) &\in F^\perp \text{ donc } x \perp (x - p_F(x)) \\ \text{donc } \langle x | x - p_F(x) \rangle &= 0 \\ \text{donc } \|x\|^2 - \langle x | p_F(x) \rangle &= 0 \\ \text{donc } \|x\|^2 &= \sum_{i=1}^p \langle x | e_i \rangle \langle x | e_i \rangle = \|p_F(x)\|^2 \end{aligned}$$

Or,

$$\begin{aligned} \|x\|^2 &= \|p_F(x)\|^2 + \|x - p_F(x)\|^2 \\ \text{donc } \|x - p_F(x)\| &= 0 \\ \text{donc } x &= p_F(x) \in F. \end{aligned}$$

□

5 Annexe

Dans ce chapitre, beaucoup des résultats ne seront pas prouvés, et sont, en grande majorité, hors-programme (pour l'année de MP2I).

5.1 Produit vectoriel

Théorème (Riesz): Soit $(E, \langle \cdot | \cdot \rangle)$ un espace euclidien. L'application

$$\begin{aligned} \varphi : E &\longrightarrow E^* \\ a &\longmapsto \langle a | \cdot \rangle \end{aligned}$$

est un isomorphisme.

Preuve:

Soient $(a, b) \in E^2$ et $(\alpha, \beta) \in \mathbb{R}^2$.

$$\begin{aligned}\forall x \in E, \varphi(\alpha a + \beta b)(x) &= \langle \alpha a + \beta b \mid x \rangle \\ &= \alpha \langle a \mid x \rangle + \beta \langle b \mid x \rangle \\ &= \alpha \varphi(a)(x) + \beta \varphi(b)(x) \\ &= (\alpha \varphi(a) + \beta \varphi(b))(x)\end{aligned}$$

Donc $\varphi \in \mathcal{L}(E, E^*)$.

Soit $a \in \text{Ker}(\varphi)$, alors $\varphi(a) = 0_{E^*}$ et donc,

$$\forall x \in E, \varphi(a)(x) = 0$$

donc

$$\forall x \in E, \langle a \mid x \rangle = 0.$$

On a donc $\langle a \mid a \rangle = 0$ et donc $a = 0_E$.

On en déduit que φ est injective.

Comme $\dim(E) = \dim(E^*) < +\infty$ et donc $\varphi \in \text{GL}(E, E^*)$. \square

EXEMPLE:

Soit P un plan de \mathbb{R}^3 et $n \in P^\perp$.

$$\begin{aligned}u \in P &\iff u \perp n \\ &\iff \langle u \mid n \rangle = 0.\end{aligned}$$

Ici, $E = \mathbb{R}^3$ muni de son produit scalaire canonique.

Définition: Soient u et v linéairement indépendants dans E . Soit $\mathcal{B} = (e_1, e_2, e_3)$ la base canonique de E .

L'application

$$\begin{aligned}f : E &\longrightarrow \mathbb{R} \\ w &\longmapsto \det_{\mathcal{B}}(u, v, w)\end{aligned}$$

est linéaire. D'après le théorème de Riesz,

$$\exists! a \in E, f = \langle a \mid \cdot \rangle.$$

On considère un tel vecteur $a \in E$. Donc,

$$\forall w \in E, \det_{\mathcal{B}}(u, v, w) = \langle a \mid w \rangle.$$

On en déduit que

$$\begin{aligned}(u, v, w) \text{ base de } E &\iff \langle a \mid w \rangle \neq 0 \\ &\iff w \not\perp a.\end{aligned}$$

Comme $a \not\perp a$, (u, v, a) est une base de E . a est le produit vectoriel de u et v et est noté $u \wedge v$.

$$\forall w \in E, \det_{\mathcal{B}}(u, v, w) = \underbrace{\langle u \wedge v \mid w \rangle}_{\substack{\text{produit mixte} \\ \text{noté } [u, v, w]}}.$$

Proposition: Soit $(u, v) \in E^2$ avec u et v linéairement indépendants.

1. $(u \wedge v) \perp u$;
2. $(u \wedge v) \perp v$;
3. $(u, v, u \wedge v)$ est une base directe (i.e. $\det(u, v, u \wedge v) > 0$) ;
4. $\|u \wedge v\| = \|u\| \|v\| \sin(\widehat{u, v})$.

Preuve: 1. $\langle u \wedge v | u \rangle = \det_{\mathcal{B}}(u, v, u) = 0$.

$$2. \langle u \wedge v | v \rangle = \det_{\mathcal{B}}(u, v, v) = 0.$$

$$3. \det_{\mathcal{B}}(u, v, u \wedge v) = \langle u \wedge v | u \wedge v \rangle = \|u \wedge v\|^2 > 0.$$

$$4. \|u \wedge v\|^2 = \det_{\mathcal{B}}(u, v, u \wedge v) = \|u \wedge v\| \|u\| \|v\| \sin(\widehat{u, v}).$$

□

Proposition: Soient $u = (a, b, c)$ et $v = (\alpha, \beta, \gamma)$. Alors,

$$u \wedge v = (b\gamma - c\beta, \alpha c - \gamma a, a\beta - b\alpha).$$

Preuve:

On pose $u \wedge v = (x, y, z)$. Comme (e_1, e_2, e_3) est orthonormée, on a

$$\begin{aligned} x &= \langle u \wedge v | e_1 \rangle = \det_{\mathcal{B}}(u, v, e_1) = \begin{vmatrix} a & \alpha & 1 \\ b & \beta & 0 \\ c & \gamma & 0 \end{vmatrix} = \begin{vmatrix} b & \beta \\ c & \gamma \end{vmatrix}; \\ y &= \langle u \wedge v | e_2 \rangle = \begin{vmatrix} a & \alpha & 0 \\ b & \beta & 1 \\ c & \gamma & 0 \end{vmatrix} = - \begin{vmatrix} a & \alpha \\ c & \gamma \end{vmatrix}; \\ z &= \langle u \wedge v | e_3 \rangle = \begin{vmatrix} a & \alpha & 0 \\ b & \beta & 0 \\ c & \gamma & 1 \end{vmatrix} = a\beta - b\alpha. \end{aligned}$$

□

5.2 Calcul différentiel

Définition: Soit $f : D \subset \mathbb{R}^n \rightarrow \mathbb{R}$ où D est un ouvert. Soit $a \in D$. S'il existe $\ell_a \in \mathcal{L}(\mathbb{R}^n, \mathbb{R})$ telle que

$$\forall h \in \mathbb{R}^n \text{ avec } \|h\| \text{ assez petite, } f(a + h) = f(a) + \ell_a(h) + o(\|h\|)$$

alors on dit que f est differentiable en a et ℓ_a est la differentielle de f en a . Si c'est le cas, alors

$$\exists! g_a \in \mathbb{R}^n, \forall h, \ell_a(h) = \langle g_a | h \rangle.$$

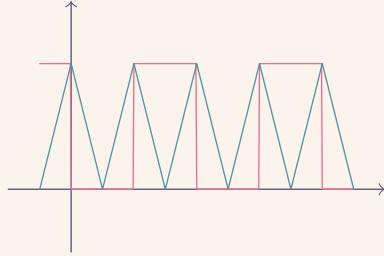
On dit que g_a est le gradient de f au point a .

Donc,

$$f(a + h) - f(a) \simeq \langle g_a | h \rangle.$$

Les résultats vus au chapitre 22 peuvent se retrouver avec cette nouvelle définition du gradient.

5.3 Séries de Fourier



Soit E un \mathbb{C} -espace vectoriel de dimension infinie et $\langle \cdot | \cdot \rangle$ une application de E^2 dans \mathbb{C} vérifiant

1. linéarité à gauche;
2. $\forall (u, v) \in E^2, \langle v | u \rangle = \overline{\langle u | v \rangle}$; (symétrie hermitienne)
3. $\forall u \in E, \langle u | u \rangle \geq 0$;
4. $\forall u \in E, \langle u | u \rangle = 0 \iff u = 0_E$.

Proposition: $\langle \cdot | \cdot \rangle$ est semi-linéaire à droite :

$$\langle u | \alpha v + \beta w \rangle = \bar{\alpha} \langle u | v \rangle + \bar{\beta} \langle u | w \rangle.$$

$\langle \cdot | \cdot \rangle$ est donc sesquilinear.

$\langle \cdot | \cdot \rangle$ est dit produit héermitien.

EXEMPLE:

Avec $E = C^0([a, b], \mathbb{C})$, on a $\langle f | g \rangle = \frac{1}{b-a} \int_a^b f(t) \overline{g(t)} dt$.

Définition: Soit $\mathcal{B} = (e_n)_{n \in \mathbb{Z}}$ une famille de E . On dit que \mathcal{B} est une base hilbertienne si

$$\begin{cases} \forall x \in E, \exists! (c_n)_{n \in \mathbb{Z}}, x = \sum_{n=-\infty}^{+\infty} c_n e_n; \\ \forall n \in \mathbb{Z}, \|e_n\| = 1; \\ \forall p \neq q, \langle e_p | e_q \rangle = 0. \end{cases}.$$

Dans ce cas, $c_n = \langle x | e_n \rangle$.

EXEMPLE:

On pose

$$\begin{aligned} \forall n \in \mathbb{Z}, \quad e_n : [0, 2\pi] &\longrightarrow \mathbb{C} \\ t &\longmapsto e^{int} \end{aligned}$$

$$\begin{aligned}
\langle e_p | e_q \rangle &= \frac{1}{2\pi} \int_0^{2\pi} e^{ipt} e^{-iqt} dt \\
&= \frac{1}{2\pi} \int_0^{2\pi} e^{i(p-q)t} dt \\
&= \begin{cases} 1 & \text{si } p = q \\ \frac{1}{2\pi} \left[\frac{e^{i(p-q)t}}{i(p-q)} \right]_0^{2\pi} = 0 & \text{si } p \neq q \end{cases}
\end{aligned}$$

Soit

$$F = \left\{ \sum_{n \in \mathbb{Z}} c_n e_n \mid (c_n) \in \mathbb{C}^{\mathbb{Z}} \text{ tel que } \forall t, \sum c_n e_n(t) \text{ converge} \right\}.$$

Soit f 2π -périodique. On a

$$p_F(f) = \sum_{n=-\infty}^{+\infty} c_n e_n$$

$$\text{où } c_n = \langle f | e_n \rangle = \frac{1}{2\pi} \int_0^{2\pi} f(t) e^{-int} dt.$$

On en déduit que

$$\Re(c_n) = \frac{1}{2\pi} \int_0^{2\pi} f(t) \cos(nt) dt.$$

5.4 Espace-temps de Minkowsky

On modélise l'espace-temps par $E = \mathbb{R}^4$; c'est un espace affine et on y crée un "produit scalaire" (en utilisant une "norme") :

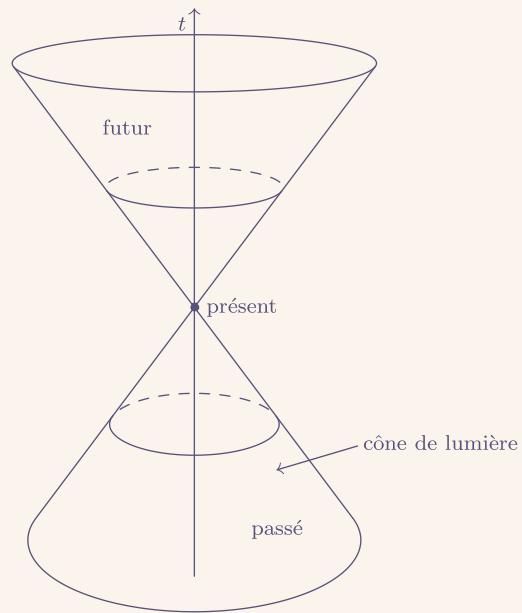
$$q(x, y, z, t) = x^2 + y^2 + z^2 - c^2 t^2.$$

On en déduit que

$$\langle (x, y, z, t) | (x', y', z', t') \rangle = xx' + yy' + zz' - c^2 tt'.$$

Ce "produit scalaire" n'en est pas vraiment un : il est bilinéaire, symétrique **MAIS** pas positif.

$$(x, y, z, t) \text{ isotrope} \iff x^2 + y^2 + z^2 = c^2 t^2.$$



Toute information contenue dans le cône passé nous est accessible ; s'il est sur sa surface, il faut que l'information y voyage à la vitesse de la lumière. Par contre, comme le temps n'est pas symétrique, on ne peut pas voir l'information future.

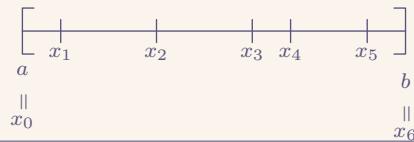
CHAPITRE

30

INTÉGRALE DE RIEMANN

1 Intégrale d'une fonction en escaliers

Définition: Une subdivision du segment $[a, b]$ est une suite finie $a = x_0 < x_1 < x_2 < \dots < x_n = b$.



REMARQUE (Notation):

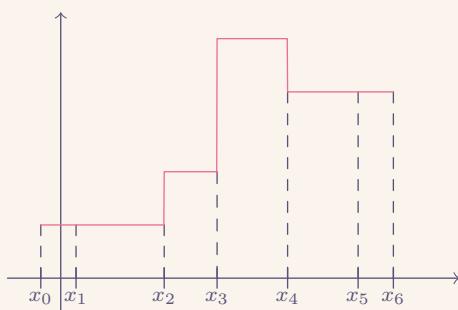
Dans ce chapitre, l'ensemble des subdivisions de $[a, b]$ est noté $\mathfrak{S}_{[a,b]}$.

Définition: Soit $f : [a, b] \rightarrow \mathbb{R}$.

On dit que f est en escalier s'il existe $\sigma = (x_0, \dots, x_n) \in \mathfrak{S}_{[a,b]}$ et $(c_0, \dots, c_{n-1}) \in \mathbb{R}^n$ tels que

$$\forall i \in \llbracket 0, n-1 \rrbracket, \forall x \in]x_i, x_{i+1}[, f(x) = c_i.$$

On dit alors que σ est adaptée à f .



Définition: Soient $\sigma = (x_0, x_1, \dots, x_n) \in \mathfrak{S}_{[a,b]}$ et $\sigma' = (x'_0, x'_1, \dots, x'_p) \in \mathfrak{S}_{[a,b]}$. On dit alors que σ' est plus fine que σ si $\{x_0, x_1, \dots, x_n\} \subset \{x'_0, x'_1, \dots, x'_n\}$. On note alors $\sigma' \prec \sigma$.

Proposition: Soient σ_1, σ_2 deux subdivisions de $[a, b]$. Alors il existe une subdivision σ_3 plus fine que σ_1 et σ_2 .

Preuve:

Soit $\sigma_1 = (x_0, x_1, \dots, x_n) \in \mathfrak{S}_{[a,b]}$ et $\sigma_2 = (x'_0, x'_1, \dots, x'_p) \in \mathfrak{S}_{[a,b]}$.

On pose $A = \{x_0, \dots, x_n\} \cup \{x'_0, \dots, x'_p\}$. On ordonne dans l'ordre croissant les éléments de A :

$$A = \{x_0'', x_1'', \dots, x_q''\}$$

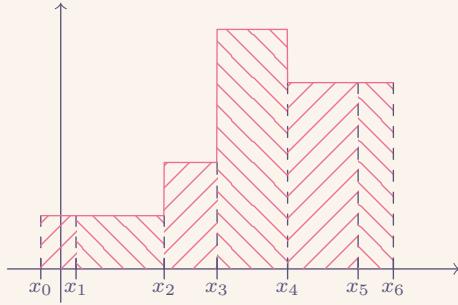
avec $a = x_0'' < x_1'' < \cdots < x_q'' = b$. On pose $\sigma_3 = (x_0'', x_1'', \dots, x_q'') \in \mathfrak{S}_{[a,b]}$. On a bien $\sigma_3 \prec \sigma_2$ et $\sigma_3 \prec \sigma_1$. \square

Proposition – Définition: Soit $f : [a, b] \rightarrow \mathbb{R}$ une fonction en escaliers. Soit $\sigma = (x_0, \dots, x_n)$ une subdivision adaptée à f . Pour $i \in \llbracket 0, n-1 \rrbracket$, on pose c_i la valeur constante de f sur $]x_i, x_{i+1}[\text{.}$

Alors,

$$\sum_{i=1}^{n-1} (x_{i+1} - x_i) c_i$$

ne dépend pas de la subdivision adaptée. On dit que c'est l'intégrale de f sur $[a, b]$. On note ce nombre $\int_{[a,b]} f$.



Preuve:

Soit $\sigma' = (x'_0, \dots, x'_p)$ une subdivision adaptée à f . On considère σ'' une subdivision de $[a, b]$ plus fine que σ et σ' . On pose

$$\sigma'' = (a, x_{1,1}, x_{1,2}, \dots, \overset{\parallel}{x_{1,i_1}}, x_{2,1}, \dots, x_{2,i_2}, \dots, b)$$

On a

$$\forall k \in \llbracket 0, n-1 \rrbracket, \forall j \in \llbracket 0, u_k - 1 \rrbracket, \forall x \in]x_{k,j}, x_{k,j+1}[, f(x) = c_k.$$

$$\begin{aligned} \sum_{k=0}^{n-1} \sum_{j=0}^{i_k-1} (x_{k,j+1} - x_{k,j}) c_k &= \sum_{k=0}^{n-1} c_k \sum_{j=0}^{i_k-1} (x_{k,j+1} - x_{k,j}) \\ &= \sum_{k=0}^{n-1} (x_{k,i_k} - x_{k,0}) \\ &= \sum_{k=0}^{n-1} c_k (x_{k+1} - x_k) \end{aligned}$$

De même, comme $\sigma \prec \sigma'$, on a aussi l'égalité avec $\sum_{k=0}^{p-1} c'_k (x'_{k+1} - x'_k)$ où c'_k est la valeur de f sur $]x'_k, x'_{k+1}[$. \square

Pour définir l'intégrale d'une fonction continue, on peut utiliser deux méthodes :

1. L'intégrale d'une fonction continue est la limite d'une suite de fonctions en escaliers. Ces résultats seront vus l'année prochaine en *MPI*.
2. Les sommes de Darboux ; c'est la définition que l'on va utiliser.

2 Sommes de Darboux

Définition: Soit $f : [a, b] \rightarrow \mathbb{R}$. Soit $\sigma = (x_0, x_1, \dots, x_n) \in \mathfrak{S}_{[a,b]}$. La somme de Darboux supérieur de f associé à σ est

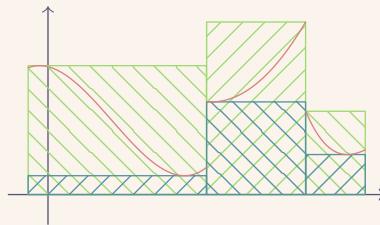
$$S_\sigma^+(f) = \sum_{i=1}^{n-1} (x_{i+1} - x_i) M_i$$

où $\forall i \in \llbracket 0, n-1 \rrbracket, M_i = \sup_{]x_i, x_{i+1}[} f$.

La somme de Darboux inférieure de f associé à σ est

$$S_\sigma^-(f) = \sum_{i=0}^{n-1} (x_{i+1} - x_i) m_i$$

où $m_i = \inf_{]x_i, x_{i+1}[} f$.



Proposition: Soit $f : [a, b] \rightarrow \mathbb{R}$ bornée, σ et σ' deux subdivisions de $[a, b]$ avec

$$\left| \begin{array}{l} \sigma' \prec \sigma. \text{ Alors} \\ \left\{ \begin{array}{l} S_{\sigma'}^+(f) \leq S_\sigma^+(f); \\ S_{\sigma'}^-(f) \geq S_\sigma^-(f). \end{array} \right. \end{array} \right.$$

Preuve:

On pose $\sigma = (x_0, \dots, x_n)$.

$$\forall i \in \llbracket 0, n-1 \rrbracket,]x_i, x_{i+1}[= \bigcup_{k=0}^{\ell-1}]y_k, y_{k+1}[$$

avec $y_k \in \sigma'$ pour tout k .

$$\forall x \in]y_k, y_{k+1}[, f(x) \leq M_i.$$

donc M_i majore $f([y_k, y_{k+1}[)$ et donc $\sup_{]y_k, y_{k+1}[} f \leq M_i$. Donc,

$$\sum_{k=0}^{\ell-1} (y_{k+1} - y_k) \sup_{]y_k, y_{k+1}[} f \leq M_i \sum_{k=0}^{\ell-1} (y_{k+1} - y_k) = M_i (x_{i+1} - x_i).$$

Ainsi,

$$S_{\sigma'}^+(f) \leq \sum_{i=0}^{n-1} M_i (x_{i+1} - x_i) = S_\sigma^+(f).$$

De même pour la somme de Darboux inférieure. \square

Définition: Soit $f : [a, b] \rightarrow \mathbb{R}$ bornée.

L'intégrale supérieure de f est

$$I_{[a, b]}^+(f) = \inf_{\sigma \in \mathfrak{S}_{[a, b]}} (S_\sigma^+(f)).$$

L'intégrale inférieure de f est

$$I_{[a, b]}^-(f) = \sup_{\sigma \in \mathfrak{S}_{[a, b]}} (S_\sigma^-(f)).$$

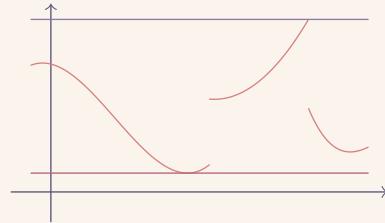
REMARQUE (justification de l'existence des bornes inférieures et supérieures):

Soit $m = \inf_{[a, b]} f$. $\forall i \in \llbracket 0, n-1 \rrbracket, M_i \geq m$ et

donc

$$\begin{aligned} S_\sigma^+(f) &= \sum_{i=0}^{n-1} (x_{i+1} - x_i) M_i \\ &\geq \sum_{i=0}^{n-1} (x_{i+1} - x_i) m \\ &\geq m(b-a). \end{aligned}$$

De même, avec $M = \sup_{[a, b]} f, \forall \sigma \in \mathfrak{S}_{[a, b]}, S_\sigma^-(f) \leq M(b-a)$.



EXEMPLE: 1. Soit $f : [a, b] \rightarrow \mathbb{R}$ en escaliers.

$$I_{[a,b]}^+(f) = \int_{[a,b]} f = I_{[a,b]}^-(f).$$

2. On pose

$$\begin{aligned} f : [0, 1] &\longrightarrow \mathbb{R} \\ x &\longmapsto \begin{cases} 0 & \text{si } x \notin \mathbb{Q} \\ 1 & \text{si } x \in \mathbb{Q}. \end{cases} \end{aligned}$$

Rappel : on a $f = \mathbb{1}_{\mathbb{Q}}$.

On a $I_{[0,1]}^+(f) = 1$ et $I_{[0,1]}^-(f) = 0$.

3. On pose

$$\begin{aligned} f : [0, 1] &\longrightarrow \mathbb{R} \\ x &\longmapsto x \end{aligned}$$

Soit $\sigma_n = \left(0, \frac{1}{n}, \frac{2}{n}, \dots, \frac{n-1}{n}, 1\right)$.

$$S_{\sigma_n}^+(f) = \sum_{i=0}^n \frac{1+1}{n} \times \frac{i}{n} = \frac{1}{n^2} \times \frac{n(n+1)}{2} = \frac{n-1}{2n}.$$

On a, pour tout n non nul, $I_{[0,1]}^+ f \leq \frac{n+1}{n}$ donc $I_{[a,b]}^+ \leq \frac{1}{2}$.

De même,

$$S_{\sigma_n}^-(f) = \sum_{i=0}^{n-1} \frac{1}{n} \times \frac{i}{n} = \frac{n(n-1)}{2} = \frac{n-1}{2n}.$$

D'où, pour tout n non nul, $I_{[0,1]}^- f \geq \frac{n-1}{2n}$ et donc $I_{[0,1]}^- f \geq \frac{1}{2}$.

Or, $\frac{1}{2} \leq I_{[0,1]}^-(f) \leq I_{[0,1]}^+(f) \leq \frac{1}{2}$ (voir ci-après). Et donc,

$$I_{[0,1]}^-(f) = I_{[0,1]}^+(f) = \frac{1}{2}.$$

Proposition: Soit $f : [a, b] \rightarrow \mathbb{R}$ bornée. Alors

$$I_{[a,b]}^-(f) \leq I_{[a,b]}^+(f).$$

Preuve:

Soit $\sigma \in \mathfrak{S}_{[a,b]}$. Soit $\sigma' \in \mathfrak{S}_{[a,b]}$. On considère $\sigma'' \in \mathfrak{S}_{[a,b]}$ telle que $\sigma'' \prec \sigma$ et $\sigma'' \prec \sigma'$.
On a donc

$$S_{\sigma'}^-(f) \leq S_{\sigma''}^-(f) \leq S_{\sigma''}^+(f) \leq S_{\sigma}^+(f).$$

On fixe $\sigma \in \mathfrak{S}_{[a,b]}$.

$$\forall \sigma' \in \mathfrak{S}_{[a,b]}, S_{\sigma'}^-(f) \leq S_{\sigma}^+(f)$$

donc $S_{\sigma}^+(f)$ majore toutes les sommes de Darboux inférieures de f donc

$$I_{[a,b]}^-(f) \leq S_{\sigma}(f)$$

donc $I_{[a,b]}^-(f)$ minore toutes les sommes de Darboux supérieures de f . On a donc

$$I_{[a,b]}^+(f) \geq I_{[a,b]}^-(f).$$

□

Définition: Soit $f : [a, b] \rightarrow \mathbb{R}$ bornée. On dit que f est Riemann-intégrable si $I_{[a,b]}^-(f) = I_{[a,b]}^+(f)$. Dans ce cas, ce nombre est noté $\int_{[a,b]} f$.

3 Propriétés de l'intégrale

Proposition: Soient f et g deux fonctions définies de $[a, b]$ à valeurs dans \mathbb{R} . Si $f \leq g$, alors

$$I_{[a,b]}^-(f) \leq I_{[a,b]}^-(g).$$

Preuve:

On suppose $f \leq g$.

$$\begin{aligned} I^-(f) \leq I^-(g) &\iff \sup_{\sigma \in \mathfrak{S}} S_\sigma^-(f) \leq \sup_{\sigma \in \mathfrak{S}} S_\sigma^-(g) \\ &\iff \forall \sigma \in \mathfrak{S}, S_\sigma^-(f) \leq \sup_{\sigma' \in \mathcal{S}} I_{\sigma'}^-(g) \end{aligned}$$

Soit $\sigma \in \mathfrak{S}$. On pose $\sigma = (x_0, x_1, \dots, x_n)$ et, pour tout $i \in \llbracket 0, n-1 \rrbracket$, $m_i = \inf_{]x_i, x_{i+1}[} f$. Alors,

$$S_\sigma^-(f) = \sum_{i=1}^{n-1} (x_{i+1} - x_i) m_i.$$

On pose aussi, pour tout $i \in \llbracket 0, n-1 \rrbracket$, $m'_i = \inf_{]x_i, x_{i+1}[} (g)$.

Soit $i \in \llbracket 0, n-1 \rrbracket$.

$$\begin{aligned} m_i \leq m'_i &\iff \inf_{]x_i, x_{i+1}[} (f) \leq \inf_{]x_i, x_{i+1}[} (g) \\ &\iff \forall x \in]x_i, x_{i+1}[, \inf_{]x_i, x_{i+1}[} (f) \leq g(x) \end{aligned}$$

Soit $x \in]x_i, x_{i+1}[$. On sait que

$$\inf_{]x_i, x_{i+1}[} (f) \leq f(g) \leq g(x).$$

On en déduit que

$$S_\sigma^-(f) \leq \sum_{i=0}^{n-1} (x_{i+1} - x_i) m'_i = S_\sigma^-(g) \leq \sup_{\sigma' \in \mathcal{S}} S_{\sigma'}^-(g).$$

□

EXERCICE:

Démontrer le même résultat avec les sommes de Darboux supérieures :

$$I_{[a,b]}^+(f) \leq I_{[a,b]}^+(g).$$

Corollaire: Soient f et g deux fonctions intégrables définies sur $[a, b]$ à valeurs dans \mathbb{R} . Si $f \leq g$, alors

$$\int_{[a,b]} f \leq \int_{[a,b]} g.$$

□

Proposition (Chasles): Soit f une fonction définie sur $[a, b]$ à valeurs dans \mathbb{R} . Soit $c \in]a, b[$. Alors,

$$\begin{cases} I_{[a,b]}^-(f) = I_{[a,c]}^-(f) + I_{[c,b]}^-(f) \\ I_{[a,b]}^+(f) = I_{[a,c]}^+(f) + I_{[c,b]}^+(f). \end{cases}$$

Preuve:

— $I_{[a,b]}^-(f) \leq I_{[a,c]}^-(f) + I_{[c,b]}^-(f) \iff \forall \sigma \in \mathfrak{S}_{[a,b]}, S_\sigma^-(f) \leq I_{[a,c]}^-(f) + I_{[c,b]}^-(f)$.

Soit $\sigma \in \mathfrak{S}_{[a,b]}$. On pose $\sigma = (x_0, x_1, \dots, x_n)$. On note $k \in \llbracket 0, n-1 \rrbracket$ tel que $x_k \leq c \leq x_{k+1}$.

On pose aussi $\sigma_1 = (x_0, x_1, \dots, x_k, c) \in \mathfrak{S}_{[a,c]}$ et $\sigma_2 = (c, x_{k+1}, \dots, x_n) \in \mathfrak{S}_{[c,b]}$. $\sigma_1 \cup \sigma_2$ est une subdivision plus fine que σ . On en déduit que

$$S_\sigma^-(f) \leq S_{\sigma_1 \cup \sigma_2}^-(f) = \underbrace{S_{\sigma_1}^-(f)}_{\diagup \diagdown} + \underbrace{S_{\sigma_2}^-(f)}_{\diagup \diagdown}.$$

$$I_{[a,c]}^-(f) \quad I_{[c,b]}^-(f)$$

—

$$\begin{aligned} I_{[a,b]}^-(f) &\geq I_{[a,c]}^-(f) + I_{[c,b]}^-(f) \iff I_{[a,c]}^-(f) \geq I_{[a,b]}^-(f) - I_{[c,b]}^-(f) \\ &\iff \forall \sigma_1 \in \mathfrak{S}_{[a,c]}, S_{\sigma_1}^-(f) \leq I_{[a,b]}^-(f) - I_{[c,b]}^-(f) \\ &\iff \forall \sigma_1 \in \mathfrak{S}_{[a,c]}, I_{[c,b]}^-(f) \leq I_{[a,b]}^-(f) - S_{\sigma_1}^-(f) \\ &\iff \forall \sigma_1 \in \mathfrak{S}_{[a,c]}, \forall \sigma_2 \in \mathfrak{S}_{[c,b]}, S_{\sigma_2}^-(f) \leq I_{[a,b]}^-(f) - S_{\sigma_1}^-(f). \end{aligned}$$

Soient $\sigma \in \mathfrak{S}_{[a,c]}$ et $\sigma_2 \in \mathfrak{S}_{[c,b]}$.

$$S_{\sigma_1}^-(f) + S_{\sigma_2}^-(f) = S_{\sigma_1 \cup \sigma_2}^-(f) \leq I_{[a,b]}^-(f).$$

□

Corollaire: Soit f une fonction définie sur $[a, b]$ à valeurs dans \mathbb{R} . Soit $c \in]a, b[$. Alors,

$$\int_{[a,b]} f = \int_{[a,c]} f + \int_{[c,b]} f.$$

□

Proposition: Soient f et g deux fonctions intégrables définies sur $[a, b]$ à valeurs dans \mathbb{R} . Alors,

$$\begin{cases} I_{[a,b]}^-(f+g) \geq I_{[a,b]}^-(f) + I_{[a,b]}^-(g) \\ I_{[a,b]}^+(f+g) \leq I_{[a,b]}^+(f) + I_{[a,b]}^+(g) \end{cases}$$

Preuve:

$$\begin{aligned}
 I^-(f+g) &\geq I^-(f) + I^-(g) \iff I^-(f) \leq I^-(f+g) - I^-(g) \\
 &\iff \forall \sigma \in \mathfrak{S}_{[a,b]}, S_\sigma^-(f) \leq I^-(f+g) - I^-(g) \\
 &\iff \forall \sigma \in \mathfrak{S}, I^-(g) \leq I^-(f+g) - S_\sigma^-(f) \\
 &\iff \forall \sigma \in \mathfrak{S}, \forall \sigma' \in \mathfrak{S}, S_{\sigma'}^-(g) \leq I^-(f+g) - I_\sigma^-(f) \\
 &\iff \forall \sigma \in \mathfrak{S}, \forall \sigma' \in \mathfrak{S}, S_\sigma^-(f) + S_{\sigma'}^-(g) \leq I^-(f+g)
 \end{aligned}$$

Soit $\sigma, \sigma' \in \mathfrak{S}$. On considère $\sigma'' \in \mathfrak{S}$ telle que $\sigma'' \prec \sigma'$ et $\sigma'' \prec \sigma$. On a

$$\begin{cases} S_\sigma^-(f) \geq S_{\sigma''}^-(f) \\ S_{\sigma'}^-(g) \leq S_{\sigma''}^-(g) \end{cases}$$

donc

$$S_\sigma^-(f) + S_{\sigma'}^-(g) \leq S_{\sigma''}^-(f) + S_{\sigma''}^-(g).$$

On pose $\sigma'' = (x_0, \dots, x_n)$ et, pour $i \in \llbracket 0, n-1 \rrbracket$,

$$\begin{cases} m_i(f) = \inf_{]x_i, x_{i+1}[}(f) \\ m_i(g) = \inf_{]x_i, x_{i+1}[}(g) \\ m_i(f+g) = \inf_{]x_i, x_{i+1}[}(f+g). \end{cases}$$

Alors,

$$\begin{aligned}
 S_{\sigma''}^-(f) + S_{\sigma''}^-(g) &= \sum_{i=0}^{n-1} (x_{i+1} - x_i) m_i(f) + \sum_{i=0}^{n-1} (x_{i+1} - x_i) m_i(g) \\
 &= \sum_{i=0}^{n-1} (x_{i+1} - x_i) (m_i(f) + m_i(g)).
 \end{aligned}$$

Soit $i \in \llbracket 0, n-1 \rrbracket$.

$$\begin{aligned}
 m_i(f) + m_i(g) \leq m_i(f+g) &\iff \inf_{]x_i, x_{i+1}[}(f) + \inf_{]x_i, x_{i+1}[}(g) \leq \inf_{]x_i, x_{i+1}[}(f+g) \\
 &\iff \forall x \in]x_i, x_{i+1}[, \inf_{]x_i, x_{i+1}[}(f) + \inf_{]x_i, x_{i+1}[}(g) \leq (f+g)(x)
 \end{aligned}$$

Soit $x \in]x_i, x_{i+1}[$.

$$\begin{aligned}
 (f+g)(x) &= f(x) + g(x) \\
 &\geq \inf_{]x_i, x_{i+1}[}(f) + \inf_{]x_i, x_{i+1}[}(g).
 \end{aligned}$$

D'où

$$\begin{aligned}
 S_{\sigma''}^-(f) + S_{\sigma''}^-(g) &\leq \sum_{i=0}^{n-1} (x_{i+1} - x_i) m_i(f+g) \\
 &\leq S_{\sigma''}^-(f+g) \leq I^-(f+g).
 \end{aligned}$$

□

||

Proposition: Soit $\lambda \in \mathbb{R}$. On a

$$I_{[a,b]}^-(\lambda f) = \begin{cases} \lambda I_{[a,b]}^-(f) & \text{si } \lambda \geq 0 \\ \lambda I_{[a,b]}^+(f) & \text{si } \lambda \leq 0 \end{cases}$$

et

$$I_{[a,b]}^+(\lambda f) = \begin{cases} \lambda I_{[a,b]}^+(f) & \text{si } \lambda \geq 0 \\ \lambda I_{[a,b]}^-(f) & \text{si } \lambda \leq 0 \end{cases}.$$

Preuve: — On suppose $\lambda > 0$.

$$I^-(\lambda f) \leq \lambda I^-(f) \iff \forall \sigma \in \mathfrak{S}, S_\sigma^-(\lambda f) \leq \lambda I^-(f).$$

Soit $\sigma = (x_0, \dots, x_n) \in \mathfrak{S}$. On pose, pour $i \in \llbracket 0, n-1 \rrbracket$, $m_i(f) = \inf_{]x_i, x_{i+1}[}(f)$ et $m_i(\lambda f) = \inf_{]x_i, x_{i+1}[}(\lambda f)$. Soit $i \in \llbracket 0, n-1 \rrbracket$.

$$\begin{aligned} m_i(\lambda f) \leq \lambda m_i(f) &\iff m_i(f) \geq m_i(f) \geq \frac{1}{\lambda} m_i(\lambda f) \\ &\iff \forall x \in]x_i, x_{i+1}[, \frac{1}{\lambda} m_i(\lambda f) \leq f(x) \end{aligned}$$

Soit $x \in]x_i, x_{i+1}[$. On a

$$f(x) = \frac{1}{\lambda} (\lambda f(x)) \geq \frac{1}{\lambda} m_i(\lambda f).$$

Donc,

$$\begin{aligned} S_\sigma^-(\lambda f) &= \sum_{i=0}^{n-1} (x_{i+1} - x_i) m_i(\lambda f) \\ &\leq \sum_{i=0}^{n-1} \lambda (x_{i+1} - x_i) m_i(f) \\ &\leq \lambda S_\sigma^-(f) \\ &\leq \lambda I^-(f). \end{aligned}$$

En outre,

$$\begin{aligned} I^-(f) &= I^-\left(\frac{1}{\lambda} \lambda f\right) \\ &\leq \frac{1}{\lambda} I^-(\lambda f) \end{aligned}$$

donc

$$\lambda I^-(f) \leq I^-(\lambda f).$$

— On suppose $\lambda < 0$.

$$I^-(\lambda f) \leq \lambda I^-(f) \iff \forall \sigma \in \mathfrak{S}, S_\sigma^-(\lambda f) \leq \lambda I^+(f).$$

Soit $\sigma \in \mathfrak{S}$. On pose $\sigma = (x_0, \dots, x_n)$. Alors,

$$S_\sigma^-(\lambda f) = \sum_{i=0}^{n-1} (x_{i+1} - x_i) m_i(\lambda f).$$

Soit $i \in \llbracket 0, n-1 \rrbracket$. Soit $x \in]x_i, x_{i+1}[\cdot$.

$$\begin{aligned} f(x) &= \frac{1}{\lambda} \left(\underbrace{\lambda f(x)}_{\geq \inf(\lambda f)} \right) \leq \frac{1}{\lambda} m_i(\lambda f) \\ \text{donc } \frac{1}{\lambda} m_i(\lambda f) &\text{ majore } f \text{ sur }]x_i, x_{i+1}[\\ \text{donc } \frac{1}{\lambda} m_i(\lambda f) &\geq \sup_{]x_i, x_{i+1}[} (f) = M_i(f) \\ \text{et donc } m_i(\lambda f) &\leq \lambda M_i(f). \end{aligned}$$

D'où

$$\begin{aligned} S_\sigma^-(\lambda f) &\leq \sum_{i=0}^{n-1} \lambda(x_{i+1} - x_i) M_i(f) \\ &\leq \lambda S_\sigma^+(f) \\ &\leq \lambda I^+(f) \end{aligned}$$

car $\lambda < 0$ et $I^+(f) \leq S_\sigma^+(f)$.

De plus,

$$I^-\left(\frac{1}{\lambda} \lambda f\right) \leq \frac{1}{\lambda} I^+(\lambda f)$$

donc

$$\lambda I^-(f) \geq I^+(\lambda f).$$

Il reste à prouver (pour $\lambda < 0$) que

$$\begin{cases} I^-(\lambda f) \geq \lambda I^+(f) \\ I^+(\lambda f) \geq \lambda I^-(f). \end{cases}$$

□

4 Théorème fondamental de l'Analyse

Théorème: Soit $f : [a, b] \rightarrow \mathbb{R}$ continue. Alors f est Riemann-intégrable.

Preuve:

f est continue sur $[a, b]$; elle est donc bornée. Soient

$$\begin{aligned} \varphi^- : [a, b] &\longrightarrow \mathbb{R} \\ x &\longmapsto I_{[a, x]}^-(f) \end{aligned}$$

et

$$\begin{aligned} \varphi^+ : [a, b] &\longrightarrow \mathbb{R} \\ x &\longmapsto I_{[a, x]}^+(f). \end{aligned}$$

Soit $x \in]a, b[$ et $h > 0$ tel que $x + h \in [a, b]$.

$$\varphi^-(x + h) - \varphi^-(x) = I_{[x, x+h]}^-(f) \leq I_{[x, x+h]}^+(f) = \varphi^+(x + h) - \varphi^+(x)$$

donc

$$\begin{cases} \frac{1}{h}(\varphi^-(x+h) - \varphi^-(x)) = \frac{1}{h}I_{[x,x+h]}^-(f) \geqslant \frac{1}{h}\inf_{[x,x+h]} f \times (x+h-x); \\ \frac{1}{h}(\varphi^+(x+h) - \varphi^-(x)) = \frac{1}{h}I_{[x,x+h]}^+(f) \leqslant \frac{1}{h}\sup_{[x,x+h]} f \times (x+h-x); \end{cases}$$

d'où

$$\inf_{[x,x+h]}(f) = \frac{1}{h}I_{[x,x+h]}^-(f) \leqslant \frac{1}{h}I_{[x,x+h]}^+(f) \leqslant \sup_{[x,x+h]}(f).$$

f est continue sur $[x, x+h]$ donc $\inf_{[x,x+h]}(f) = f(c_h)$ avec $c_h \in [x, x+h]$. $x \leqslant c_h \leqslant x+h$
donc $c_h \xrightarrow[h \rightarrow 0]{>} x$. Comme f est continue, $f(c_h) \xrightarrow[h \rightarrow 0]{>} f(x)$.

De même, $\sup_{[x,x+h]}(f) = f(d_h)$ avec $d_h \in [x, x+h]$ donc $d_h \xrightarrow[h \rightarrow 0]{>} x$ et donc $f(d_h) \xrightarrow[h \rightarrow 0]{>} f(x)$.

On en déduit que

$$\begin{cases} \frac{\varphi^-(x+h) - \varphi^-(x)}{h} \xrightarrow[h \rightarrow 0]{>} f(x) \\ \frac{\varphi^+(x+h) - \varphi^+(x)}{h} \xrightarrow[h \rightarrow 0]{>} f(x). \end{cases}$$

De même,

$$\begin{cases} \frac{\varphi^-(x+h) - \varphi^-(x)}{h} \xrightarrow[h \rightarrow 0]{<} f(x) \\ \frac{\varphi^+(x+h) - \varphi^+(x)}{h} \xrightarrow[h \rightarrow 0]{<} f(x). \end{cases}$$

Donc φ^- et φ^+ sont deux primitives de f sur l'intervalle $[a, b]$.

Donc,

$$\exists C \in \mathbb{R}, \forall x \in [a, b], \varphi^-(x) = \varphi^+(x) + C.$$

En évaluant en $x = a$, on a

$$\underbrace{\varphi^-(a)}_{=0} = \underbrace{\varphi^+(a)}_{=0} + C$$

et donc $C = 0$ donc $\varphi^-(b) = \varphi^+(b)$ et donc f est intégrable. \square

On a aussi démontré le théorème suivant :

Théorème: Soit $f : [a, b] \rightarrow \mathbb{R}$ continue. Alors

$$x \mapsto \int_{[a, x]} f$$

est une primitive de f . \square

REMARQUE (Notation):

Soit $f : [a, b] \rightarrow \mathbb{R}$ continue. On note plutôt $\int_a^b f(t) dt$ à la place de $\int_{[a, b]} f$.

On note aussi $\int_b^a f(t) dt = - \int_{[a, b]} f$.

Corollaire: Soit $f : [a, b] \rightarrow \mathbb{R}$ continue et F une primitive de f . Alors

$$\int_a^b f(t) dt = F(b) - F(a).$$

Preuve:

Soit $\varphi : x \mapsto \int_a^x f(t) dt$. On sait que φ est une primitive de f . Or,

$$\varphi' = f = F' \text{ donc } (\varphi - F)' = 0$$

On en déduit que

$$\exists C \in \mathbb{R}, \forall x \in [a, b], \varphi(x) = F(x) + C.$$

En particulier,

$$0 = \varphi(a) = F(a) + C$$

donc $C = -F(a)$.

D'où

$$\int_a^b f(t) dt = \varphi(b) = F(b) + C = F(b) - F(a).$$

□

5 Fonctions continues par morceaux

Définition: Soit $f : [a, b] \rightarrow \mathbb{R}$. On dit que f est continue par morceaux si,

$$\exists \sigma = (x_0, \dots, x_n) \in \mathfrak{S}_{[a, b]}, \begin{cases} \forall i \in \llbracket 0, n-1 \rrbracket, f|_{[x_i, x_{i+1}]} \text{ est continue;} \\ \forall i \in \llbracket 1, n-1 \rrbracket, \lim_{x \rightarrow x_i^-} f(x) \in \mathbb{R} \text{ et } \lim_{x \rightarrow x_i^+} f(x) \in \mathbb{R}; \\ \lim_{\substack{x \rightarrow a^+} f(x) \in \mathbb{R}; \lim_{\substack{x \rightarrow b^-} f(x) \in \mathbb{R}.} \end{cases}$$

Théorème: Toute fonction continue par morceaux sur un segment est Riemann-intégrable sur ce segment. □

Définition: Soit $f : I \subset \mathbb{R} \rightarrow \mathbb{R}$. On dit que f est continue par morceaux sur I si f est continue par morceaux sur tout segment inclus dans I .

REMARQUE:



$$\begin{aligned}\delta : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto \begin{cases} 0 & \text{si } x \neq 0, \\ 1 & \text{si } x = 0. \end{cases}\end{aligned}$$

δ est continue par morceaux sur \mathbb{R} . On a $\int_{[0,1]} \delta = 0$, et $\forall x \in [0, 1]$, $f(x) \geq 0$. Mais, $\delta \neq 0$.

6 Sommes de Riemann

Théorème: Soit $f : [a, b] \longrightarrow \mathbb{R}$ continue par morceaux.

À faire : schéma 1

$$\lim_{n \rightarrow +\infty} \left(\sum_{i=0}^{n-1} \frac{b-a}{n} f \left(a + i \frac{b-a}{n} \right) \right) = \int_a^b f(t) dt.$$

Preuve (dans le cas où f est continue) :

$$\begin{aligned}\forall n \in \mathbb{N}^*, 0 &\leqslant \left| \int_a^b f(t) dt - \sum_{i=0}^{n-1} \frac{b-a}{n} f \left(\overbrace{a + i \frac{b-a}{n}}^{x_i} \right) \right| \\ &= \left| \sum_{i=0}^{n-1} \int_{x_i}^{x_{i+1}} f(t) dt - \sum_{i=0}^{n-1} \frac{b-a}{n} f(x_i) \right| \\ &= \left| \sum_{i=0}^{n-1} \left(\int_{x_i}^{x_{i+1}} f(t) dt - \frac{b-a}{n} f(x_i) \right) \right| \\ &= \left| \sum_{i=0}^{n-1} \left(\int_{x_i}^{x_{i+1}} f(t) dt - \int_{x_i}^{x_{i+1}} f(x_i) dt \right) \right| \\ &= \left| \sum_{i=0}^{n-1} \int_{x_i}^{x_{i+1}} (f(t) - f(x_i)) dt \right| \\ &\leqslant \sum_{i=0}^{n-1} \int_{x_i}^{x_{i+1}} |f(t) - f(x_i)| dt.\end{aligned}$$

f est continue sur $[a, b]$, donc uniformément continue sur $[a, b]$:

$$\forall \varepsilon > 0, \exists \eta > 0, \forall x, y \in \mathcal{D}_f, |x - y| \leq \eta \implies |f(x) - f(y)| \leq \varepsilon.$$

Soit $\varepsilon > 0$. On considère $\eta > 0$ comme ci-dessus. On a $\frac{b-a}{n} \rightarrow 0$ donc, il existe $N \in \mathbb{N}^*$ tel que

$$\forall n \geq N, \frac{b-a}{n} \leq \eta.$$

On considère un tel $N \in \mathbb{N}^*$. On suppose $n \geq N$.

$$\forall i \in \llbracket 0, n-1 \rrbracket, \forall x \in [x_i, x_{i+1}], |x - x_i| \leq x_{i+1} - x_i = \frac{b-a}{n} \leq \eta$$

et donc

$$|f(x) - f(x_i)| \leq \varepsilon.$$

Donc,

$$\forall n \geq N, \left| \int_a^b f(x) dx - \frac{b-a}{n} \sum_{i=0}^{n-1} f(x_i) \right| \leq \sum_{i=0}^{n-1} \int_{x_i}^{x_{i+1}} \varepsilon dt = \varepsilon(b-a).$$

□

Proposition: Soit $f : [a, b] \rightarrow \mathbb{R}$ continue par morceaux et $n \in \mathbb{N}^*$.

$$\frac{b-a}{n} \sum_{i=1}^n f\left(\underbrace{a + i \frac{b-a}{n}}_{x_i}\right) \xrightarrow{n \rightarrow +\infty} \int_a^b f(t) dt.$$

□

REMARQUE:

On suppose à présent f de classe \mathcal{C}^1 sur $[a, b]$. f' est continue sur $[a, b]$: on considère

$$M = \max_{x \in [a, b]} |f'(x)|.$$

$$\begin{aligned} \forall n \in \mathbb{N}^*, \left| \int_a^b f(t) dt - \frac{b-a}{n} \sum_{i=0}^{n-1} f(x_i) \right| &= \left| \sum_{i=0}^{n-1} \int_{x_i}^{x_{i+1}} (f(t) - f(x_i)) dt \right| \\ &\leq \sum_{i=0}^{n-1} \int_{x_i}^{x_{i+1}} |f(t) - f(x_i)| dt \\ &\leq \sum_{i=0}^{n-1} \int_{x_i}^{x_{i+1}} M |t - x_i| dt \\ &\leq M \sum_{i=0}^{n-1} \frac{(x_{i+1} - x_i)^2}{2} \\ &\leq \frac{M}{2} \left(\frac{b-a}{n} \right)^2 n \\ &= \frac{M(b-a)^2}{2n}. \end{aligned}$$

Par exemple, on veut calculer une valeur approchée de $\ln 2$ à 10^{-3} près :

$$\ln 2 = \int_1^2 \frac{1}{t} dt.$$

Soit $f : t \mapsto \frac{1}{t}$ de classe \mathcal{C}^1 sur $[1, 2]$.

$$\forall t \in [1, 2], |f'(t)| = \frac{1}{t^2} \leq 1$$

d'où $M = 1$.

On cherche $n \in \mathbb{N}^*$ tel que

$$\frac{1(2-1)^2}{2n} \leq 10^{-3}$$

i.e. $n \geq 500$.

Donc, $\frac{1}{500} \sum_{i=0}^{499} \frac{1}{1 + \frac{i}{500}} \simeq 0,693$ est une valeur approchée de $\ln 2$ à 10^{-3} près.

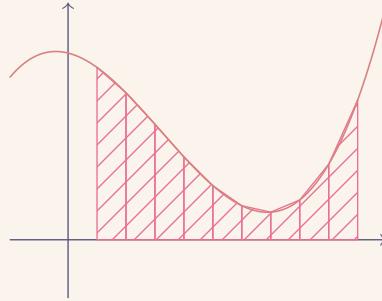
EXEMPLE:

$$\text{Que vaut } \lim_{n \rightarrow +\infty} \sum_{i=1}^n \frac{n}{n^2 + k^2} ?$$

$\sum_{1 \leq k \leq n} \frac{n}{n^2 + k^2}$ n'est pas une série! En effet, en passant de n à $n+1$, on modifie les termes précédents.

$$\begin{aligned} \forall n \in \mathbb{N}^*, \sum_{k=1}^n \frac{n}{n^2 + k^2} &= \sum_{k=1}^n \frac{\frac{1}{n}}{1 + \left(\frac{k}{n}\right)^2} \\ &= \frac{1}{n} \sum_{k=1}^n \frac{1}{1 + \left(\frac{k}{n}\right)^2} \\ &\xrightarrow{n \rightarrow +\infty} \int_0^1 \frac{1}{1+t^2} dt = \arctan 1 - \arctan 0 = \frac{\pi}{4}. \end{aligned}$$

REMARQUE (Méthode des trapèzes):



Au lieu d'approximer l'intégrale par des rectangles, on utilise des trapèzes.

7 Retour sur les formules de Taylor

Proposition: Soit $f : I \subset \mathbb{R} \rightarrow \mathbb{R}$ continue et F une primitive de f . On suppose

$$f(x) = \sum_{i=0}^n \alpha_i (x-a)^i + \underset{x \rightarrow a}{\circ} ((x-a)^n).$$

Alors,

$$F(x) = F(a) + \sum_{i=0}^n \alpha_i \frac{(x-a)^{i+1}}{i+1} + \underset{x \rightarrow a}{\circ} ((x-a)^{n+1}).$$

Preuve:

Soit $\varepsilon > 0$. On sait qu'il existe $\eta > 0$ tel que

$$\forall x \in [a-\eta, a+\eta], \left| f(x) - \sum_{i=0}^n \alpha_i (x-a)^i \right| \leq \varepsilon |x-a|^n.$$

On considère un tel $\eta > 0$. Soit $x \in [a - \eta, a + \eta]$.

$$\begin{aligned} \overbrace{\left| F(x) - F(a) - \sum_{i=0}^n \alpha_i \frac{(x-a)^{i+1}}{i+1} \right|}^{(*)} &= \left| \int_a^x f(t) dt - \sum_{i=0}^n \alpha_i \int_a^x (t-a)^i dt \right| \\ &= \left| \int_a^x \left(f(t) - \sum_{i=0}^n \alpha_i (t-a)^i \right) dt \right| \end{aligned}$$

On suppose $x \geq a$, donc

$$\begin{aligned} (*) &\leq \int_a^x \left| f(t) - \sum_{i=0}^n \alpha_i (t-a)^i \right| dt \\ &\leq \int_a^x \varepsilon |t-a|^n dt \\ &\leq \varepsilon \int_a^x (t-a)^n dt \\ &= \frac{\varepsilon}{n+1} (x-a)^{n+1} \end{aligned}$$

On suppose $x < a$.

$$\begin{aligned} (*) &= \left| \int_x^a \left(f(t) - \sum_{i=0}^n \alpha_i (t-a)^i \right) dt \right| \\ &\leq \int_x^a \left| f(t) - \sum_{i=0}^n \alpha_i (t-a)^i \right| dt \\ &\leq \int_x^a \varepsilon |t-a|^n dt \\ &\leq \varepsilon \int_x^a (a-t)^n dt \\ &\leq \varepsilon \left[-\frac{(a-t)^{n+1}}{n+1} \right]_x^a \\ &\leq \varepsilon \frac{(a-x)^{n+1}}{n+1} \\ &= \frac{\varepsilon}{n+1} |x-a|^{n+1} \end{aligned}$$

□

Corollaire: Soit $f : I \xrightarrow{\text{fin}} \mathbb{R}$ de classe \mathcal{C}^n . Alors,

$$f(x) = \sum_{i=0}^n \frac{f^{(i)}(a)}{i!} (x-a)^i + {}_{x \rightarrow a} \circ ((x-a)^n).$$

Preuve:
par récurrence sur n .

□

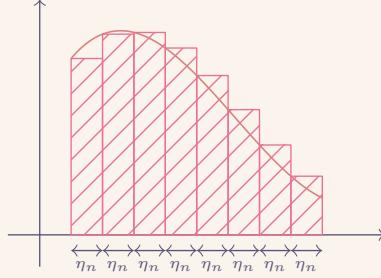
8 Fonctions réglées

Soit $f : [a, b] \rightarrow \mathbb{R}$ continue. Cette fonction est donc uniformément continue (théorème de Heine) :

$$\forall \varepsilon > 0, \exists \eta > 0, \forall (x, y) \in [a, b]^2, |x - y| \leq \eta \implies |f(x) - f(y)| \leq \varepsilon.$$

D'où

$$\forall n \in \mathbb{N}^*, \exists \eta_n > 0, |x - y| \leq \eta_n \implies |f(x) - f(y)| \leq \frac{1}{n}.$$



Cependant, contrairement au somme de Darboux, cette construction utilise des notions que l'on admet : notamment, la convergence d'une suite de fonctions.

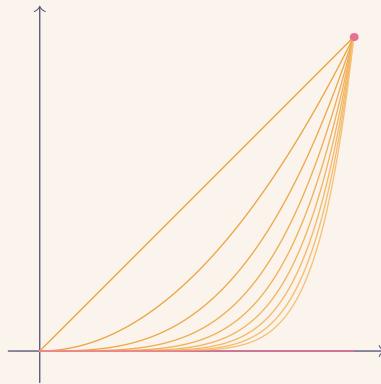
EXEMPLE (convergence d'une suite de fonctions):

Pour $n \in \mathbb{N}$, on pose

$$\begin{aligned} f_n : [0, 1] &\longrightarrow \mathbb{R} \\ x &\longmapsto x^n \end{aligned}$$

$$\forall x \in [0, 1], f_n(x) \xrightarrow[n \rightarrow +\infty]{} \begin{cases} 0 & \text{si } x < 1 \\ 1 & \text{sinon.} \end{cases}$$

Pour $n \in \mathbb{N}$, f_n est continue mais $\lim_{n \rightarrow +\infty} f_n$ ne l'est pas :



CHAPITRE

31

VARIABLES ALÉATOIRES

1 Définitions

Définition: Une variable aléatoire est une application sur un espace probabilisé (Ω, P) dans E où E est un ensemble quelconque :

$$X : \Omega \longrightarrow E.$$

Si $E \subset \mathbb{R}$, on dit que X est réelle.

Si E est un espace vectoriel, on dit que X est un vecteur aléatoire.

Si $E \subset \mathcal{M}_{n,p}(\mathbb{K})$, on dit que X est une matrice aléatoire.

EXEMPLE:

On lance 2 dés bien équilibrés et on note S la somme des points sur ces deux dés.

On pose $\Omega = \llbracket 1, 6 \rrbracket^2$, P l'équiprobabilité et

$$\begin{aligned} S : \Omega &\longrightarrow \mathbb{R} \\ (\omega_1, \omega_2) &\longmapsto \omega_1 + \omega_2. \end{aligned}$$

$S(\Omega) = \llbracket 2, 12 \rrbracket$.

λ	2	3	4	5	6	7	8	9	10	11	12
$P(S = \lambda)$	$\frac{1}{36}$	$\frac{2}{36}$	$\frac{3}{36}$	$\frac{4}{36}$	$\frac{5}{36}$	$\frac{6}{36}$	$\frac{5}{36}$	$\frac{4}{36}$	$\frac{3}{36}$	$\frac{2}{36}$	$\frac{1}{36}$

Dans la suite du chapitre, (Ω, P) est un espace probabilisé.

Proposition: Soit $X : \Omega \rightarrow E$ une variable aléatoire avec $E = X(\Omega)$. L'application

$$\begin{aligned} P_X : \mathcal{P}(E) &\longrightarrow [0, 1] \\ A &\longmapsto P(X^{-1}(A)) \end{aligned}$$

est une probabilité sur E .

Preuve:

- $\forall A \in \mathcal{P}(E), X^{-1}(A) \in \mathcal{P}(\Omega)$ donc $P(X^{-1}(A)) \in [0, 1]$.
- $P_X(E) = P(X^{-1}(E)) = P(\Omega) = 1$.
- Soient $A, B \in \mathcal{P}(E)$ avec $A \cap B = \emptyset$.

$$\begin{aligned} P_X(A \cup B) &= P(X^{-1}(A \cup B)) \\ &= P(X^{-1}(A) \cup X^{-1}(B)) \\ &= P(X^{-1}(A)) + P(X^{-1}(B)) \\ &= P_X(A) + P_X(B). \end{aligned}$$

□

Définition: Soit $X : \Omega \rightarrow E$ une variable aléatoire. P_X est la loi de X .

REMARQUE (Notations):

Soit $X : \Omega \rightarrow E$ une variable aléatoire.

- Soit $A \in \mathcal{P}(E)$. $X^{-1}(A)$ est noté $(X \in A)$. D'où $P_X(A) = P(X \in A)$.
- Soit $x \in E$. $X^{-1}(\{x\})$ est noté $(X = x)$; $P_X(\{x\}) = P(X = x)$.
- Si $E \subset \mathbb{R}$, $X^{-1}([-\infty, x])$ est noté $(X \leq x)$ et donc $P(X^{-1}([-\infty, x])) = P(X \leq x)$.
De même avec les autres inégalités strictes et larges.

REMARQUE (Notation):

On note $X \sim Y$ si X et Y suivent la même loi, i.e. $P_X = P_Y$.

2 Exemples de lois

Définition: Soit $X : \Omega \rightarrow E$ une variable aléatoire. On dit que X suit une loi uniforme si P_X est l'équiprobabilité sur $X(\Omega)$. On note alors $X \sim \mathcal{U}(X(\Omega))$.

Définition: Soit $X : \Omega \rightarrow \{0, 1\}$. On note $p = P(X = 1) \in [0, 1]$. On dit que X suit la loi de Bernoulli de paramètre p . On note alors $X \sim \mathcal{B}(p)$.

Définition: Soit $X : \Omega \rightarrow \llbracket 0, n \rrbracket$. On dit que X suit la loi binomiale de paramètres n et p si

$$\forall k \in \llbracket 0, n \rrbracket, P(X = k) = \binom{n}{k} p^k (1-p)^{n-k}.$$

On note alors $X \sim \mathcal{B}(n, p)$.

Théorème: On considère une expérience aléatoire qui n'a que deux issues possibles : succès ou échec. On répète n fois à l'identique cette expérience, et on note X le nombre de succès. Alors $X \sim \mathcal{B}(n, p)$ où P est la probabilité de succès. □

3 Couples de variables aléatoires

EXEMPLE:

On lance 2 dés bien équilibrés; on note S la somme des points sur ces deux dés et M le maximum.

$S \backslash M$	1	2	3	4	5	6	loi de S
2	$1/36$	0	0	0	0	0	$1/36$
3	0	$2/36$	0	0	0	0	$2/36$
4	0	$1/36$	$2/36$	0	0	0	$3/36$
5	0	0	$2/36$	$2/36$	0	0	$4/36$
6	0	0	$1/36$	$2/36$	$2/36$	0	$5/36$
7	0	0	0	$0/36$	$2/36$	$2/36$	$6/36$
8	0	0	0	$1/36$	$2/36$	$2/36$	$5/36$
9	0	0	0	0	$2/36$	$2/36$	$4/36$
10	0	0	0	0	$1/36$	$2/36$	$3/36$
11	0	0	0	0	0	$2/36$	$2/36$
12	0	0	0	0	0	$1/36$	$1/36$
loi de M	$1/36$	$3/36$	$5/36$	$7/36$	$9/36$	$11/36$	

Définition: Soient $X : \Omega \rightarrow E$ et $Y : \Omega \rightarrow F$ deux variables aléatoires.

La loi du couple (X, Y) est P_Z où

$$\begin{aligned} Z : \Omega &\longrightarrow E \times F \\ \omega &\longmapsto (X(\omega), Y(\omega)) \end{aligned}$$

i.e. c'est la donnée de

$$\forall x \in X(\Omega), \forall y \in Y(\Omega), P(X = x, Y = y) = P((X = x) \cap (Y = y)).$$

Définition: Soient $X : \Omega \rightarrow E$ et $Y : \Omega \rightarrow F$. Les lois marginales du couple (X, Y) sont P_X et P_Y .

Proposition: Avec les notations précédentes,

$$\begin{aligned} \forall x \in X(\Omega), P(X = x) &= \sum_{y \in Y(\Omega)} P(X = x, Y = y); \\ \forall y \in Y(\Omega), P(Y = y) &= \sum_{x \in X(\Omega)} P(X = x, Y = y). \end{aligned}$$

Preuve:
probabilités totales

□

REMARQUE:

Si

$$\forall y \in Y(\Omega), P(Y = y) \neq 0$$

alors

$$\forall x \in X(\Omega), P(X = x) = \sum_{y \in Y(\Omega)} P_{(Y=y)}(X = x) P(Y = y).$$

Définition: Soient $X : \Omega \rightarrow E$ et $Y : \Omega \rightarrow F$ deux variables aléatoires. On dit que X et Y sont indépendantes si

$$\forall A \subset X(\Omega), \forall B \subset Y(\Omega), P(X \in A, Y \in B) = P(X \in A) P(Y \in B).$$

On note alors $X \perp\!\!\!\perp Y$.

Proposition: Avec les notations précédentes,

$$X \perp\!\!\!\perp Y \iff \forall x \in X(\Omega), \forall y \in Y(\Omega), P(X = x, Y = y) = P(X = x)P(Y = y).$$

Preuve: “ \implies ” immédiat

“ \impliedby ” Soient $A = \{x_1, \dots, x_n\} \subset X(\Omega)$ et $B = \{y_1, \dots, y_p\} \subset Y(\Omega)$.

$$\begin{aligned} P(X \in A, Y \in B) &= P\left(\left(\bigcup_{i=1}^n (X = x_i)\right) \cap (Y \in B)\right) \\ &= P\left(\bigcup_{i=1}^n ((X = x_i) \cap (Y \in B))\right) \\ &= \sum_{i=1}^n P((X = x_i) \cap (Y \in B)) \\ &= \sum_{i=1}^n P\left((X = x_i) \cap \left(\bigcup_{j=1}^p (Y = y_j)\right)\right) \\ &= \sum_{i=1}^n P\left(\bigcup_{j=1}^p ((X = x_i) \cap (Y = y_j))\right) \\ &= \sum_{i=1}^n \sum_{j=1}^p P(X = x_i, Y = y_j) \\ &= \sum_{i=1}^n \sum_{j=1}^p P(X = x_i) P(Y = y_j) \\ &= \sum_{i=1}^n P(X = x_i) \sum_{j=1}^p P(Y = y_j) \\ &= P(X \in A) P(Y \in B). \end{aligned}$$

□

4 Familles de variables aléatoires

Définition: Soit $(X_i)_{i \in I} \in \prod_{i \in I} E_i^\Omega$ une famille de variables aléatoires. On dit que ces variables sont indépendantes si, pour toute partie finie J de I , et pour tout $(A_j)_{j \in J} \in$

$$\prod_{j \in J} \mathcal{P}(E_j),$$

$$P\left(\bigcap_{j \in J} (X_j \in A_j)\right) = \prod_{j \in J} P(X_j \in A_j).$$

Proposition: Avec les notations précédentes, $(X_i)_{i \in I}$ est une famille de variables aléatoires indépendantes si et seulement si

$$\forall J \subset I, J \text{ finie}, \forall (x_j)_{j \in J} \in \prod_{j \in J} X_j(\Omega), P\left(\bigcap_{j \in J} (X_j = x_j)\right) = \prod_{j \in J} P(X_j = x_j).$$

□

Proposition: Soit $(X_i)_{i \in \mathbb{N}}$ une suite de variables aléatoires suivant la même loi de Bernoulli $\mathcal{B}(p)$. Alors,

$$\forall n \in \mathbb{N}^*, \sum_{i=1}^n X_i \sim \mathcal{B}(n, p).$$

Proposition: Soient $X \sim \mathcal{B}(n, p)$ et $Y \sim \mathcal{B}(m, p)$.

Si $X \perp\!\!\!\perp Y$, alors $X + Y \sim \mathcal{B}(n + m, p)$.

□

5 Espérance d'une variable aléatoire

Dans ce paragraphe, toutes les variables aléatoires sont à valeurs réelles.

Définition: Soit $X : \Omega \rightarrow \mathbb{R}$. L'espérance de X est

$$E(X) = \sum_{x \in X(\Omega)} x P(X = x).$$

EXEMPLE (À connaître): 1. Avec $X \sim \mathcal{B}(p)$, on a $E(X) = \sum_{x \in \{0, 1\}} x P(X = x) = p$.

2. Avec $X \sim \mathcal{B}(n, p)$, on a

$$\begin{aligned} E(X) &= \sum_{k=0}^n k P(X = k) \\ &= \sum_{k=1}^n k \binom{n}{k} p^k (1-p)^{n-k} \\ &= n \sum_{k=1}^n \binom{n-1}{k-1} p^k (1-p)^{n-k} \\ &= np \sum_{k=0}^{n-1} \binom{n-1}{k} p^k (1-p)^{n-k-1} \\ &= np(p+1-p)^{n-1} \\ &= np \end{aligned}$$

Lemme: Soit $X : \Omega \rightarrow \mathbb{R}$.

$$E(X) = \sum_{\omega \in \Omega} X(\omega) P(\{\omega\}).$$

Preuve:

$$\begin{aligned} \sum_{\omega \in \Omega} X(\omega) P(\{\omega\}) &= \sum_{x \in X(\Omega)} \sum_{\substack{\omega \in \Omega \\ X(\omega)=x}} X(\omega) P(\{\omega\}) \\ &= \sum_{x \in X(\Omega)} \sum_{\substack{\omega \in \Omega \\ X(\omega)=x}} x P(\{\omega\}) \\ &= \sum_{x \in X(\Omega)} x \sum_{\substack{\omega \in \Omega \\ X(\omega)=x}} P(\{\omega\}) \\ &= \sum_{x \in X(\Omega)} x P\left(\bigcup_{\substack{\omega \in \Omega \\ X(\omega)=x}} \{\omega\}\right) \\ &= \sum_{x \in X(\Omega)} x P(X=x) \end{aligned}$$

□

Théorème (linéarité de l'espérance): Soient X et Y deux variables aléatoires réelles, et α, β deux réels. Alors,

$$E(\alpha X + \beta Y) = \alpha E(X) + \beta E(Y).$$

Preuve:

$$\begin{aligned} \alpha E(X) + \beta E(Y) &= \alpha \sum_{\omega \in \Omega} X(\omega) P(\{\omega\}) + \beta \sum_{\omega \in \Omega} Y(\omega) P(\{\omega\}) \\ &= \sum_{\omega \in \Omega} (\alpha X(\omega) + \beta Y(\omega)) P(\{\omega\}) \\ &= E(\alpha X + \beta Y). \end{aligned}$$

□

Corollaire: Soit X une variable aléatoire suivant la loi binomiale $\mathcal{B}(n, p)$. On a $E(X) = np$.

Preuve:

Soient X_1, \dots, X_n des variables indépendantes suivant toutes $\mathcal{B}(p)$.

On a

$$X \sim \sum_{i=1}^n X_i$$

donc

$$\begin{aligned} E(X) &= E\left(\sum_{i=1}^n X_i\right) \\ &= \sum_{i=1}^n E(X_i) \\ &= np \end{aligned}$$

□

EXEMPLE:

On pose $\Omega = S_n$ le groupe symétrique ; P l'équiprobabilité sur Ω et

$$\begin{aligned} X : \Omega &\longrightarrow [\![0, n]\!] \\ \omega &\longmapsto \text{le nombre de points fixes de } \omega \end{aligned}$$

Que vaut $E(X)$?

On pose, pour tout $\omega \in \Omega$, pour tout $i \in [\![0, n]\!]$, $X_i(\omega) = \begin{cases} 1 & \text{si } \omega(i) = i \\ 0 & \text{sinon.} \end{cases}$

Ainsi,

$$\forall \omega \in \Omega, \sum_{i=1}^n X_i(\omega) = X(\omega).$$

D'où

$$\begin{aligned} E(X) &= E\left(\sum_{i=1}^n X_i\right) \\ &= \sum_{i=1}^n E(X_i) \\ &= \sum_{i=1}^n P(X_i = 1) \\ &= \sum_{i=1}^n \frac{(n-1)!}{n!} \\ &= \sum_{i=1}^n \frac{1}{n} \\ &= \frac{n}{n} \\ &= 1 \end{aligned}$$

On n'a pas eu besoin de déterminer la loi de X pour déterminer l'espérance de X .

Définition: Soient $X : \Omega \rightarrow \mathbb{R}$ une variable aléatoire et $f : \mathbb{R} \rightarrow \mathbb{R}$.

$$\begin{array}{ccc} \Omega & \xrightarrow{X} & \mathbb{R} \\ & \searrow f & \downarrow \\ & & \mathbb{R} \end{array}$$

La composée $f \circ X$ est notée $f(X)$.

Théorème (formule de transfert): Avec les notations précédentes,

$$E(f(X)) = \sum_{x \in X(\Omega)} f(x) P(X = x).$$

Preuve:

$$\begin{aligned} E(f(X)) &= \sum_{\omega \in \Omega} f(X(\omega)) P(\{\omega\}) \\ &= \sum_{x \in X(\Omega)} \sum_{\substack{\omega \in \Omega \\ X(\omega)=x}} f(X(\omega)) P(\{\omega\}) \\ &= \sum_{x \in X(\Omega)} f(x) \sum_{\substack{\omega \in \Omega \\ X(\omega)=x}} P(\{\omega\}) \\ &= \sum_{x \in X(\Omega)} f(x) P(X = x). \end{aligned}$$

□

EXEMPLE:

Avec $X(\Omega) = \{-1, 0, 1\}$, $P(X = -1) = \frac{1}{2}$, $P(X = 0) = \frac{1}{4}$, $P(X = 1) = \frac{1}{4}$, que vaut $E(X^2)$?

— Loi de $X^2 : X^2(\Omega) = \{0, 1\}$ avec $P(X^2 = 0) = \frac{1}{4}$ et $P(X^2 = 1) = \frac{3}{4}$; d'où $E(X^2) = \frac{3}{4}$.

— Formule de transfert : $E(X^2) = \sum_{x=-1}^1 x^2 P(X = x) = \frac{3}{4}$.

6 Variance

Dans ce paragraphe, toutes les variables aléatoires sont à valeurs réelles.

Définition: Soit $X : \Omega \rightarrow \mathbb{R}$ une variable aléatoire. La variance de X est

$$V(X) = E((X - E(X))^2).$$

Proposition: Avec les notations précédentes,

$$V(X) \geq 0.$$

Preuve:
On pose $\mu = E(X)$.

$$V(X) = \sum_{x \in X(\Omega)} \underbrace{(x - \mu)^2 P(X = x)}_{\geq 0} \geq 0.$$

□

Définition: L'écart-type de X est

$$\sigma_X = \sqrt{V(X)}.$$

Définition: On dit que X vérifie presque sûrement une propriété si la probabilité que X vérifie cette propriété vaut 1.

Proposition:

$$V(X) = 0 \iff X \text{ est presque sûrement constante..}$$

□

Proposition (Koenig-Huygens):

$$V(X) = E(X^2) - E(X)^2.$$

Preuve:
On pose $\mu = E(X)$

$$\begin{aligned} V(X) &= E((X - \mu)^2) \\ &= E(X^2 - 2\mu X + \mu^2) \\ &= E(X^2) - 2\mu E(X) + \mu^2 E(1) \\ &= E(X^2) - 2\mu^2 + \mu^2 \\ &= E(X^2) - \mu^2 \end{aligned}$$

□

EXEMPLE: 1. Avec $X \sim \mathcal{B}(p)$, on a $X^2 \sim \mathcal{B}(p)$ d'où

$$V(X) = p - p^2 = p(1 - p) = pq \leq \frac{1}{4} \text{ avec } q = 1 - p$$

2. Avec $X \sim \mathcal{B}(n, p)$.

$$\begin{aligned} E(X^2) &= \sum_{k=0}^n k^2 \binom{n}{k} p^k q^{n-k} \\ &= \dots \end{aligned}$$

En faisant le calcul, on trouve $V(X) = npq$.

Théorème: Soit $X, Y : \Omega \rightarrow \mathbb{R}$.

$$V(X + Y) = V(X) + V(Y) + 2 \operatorname{Cov}(X, Y)$$

où $\operatorname{Cov}(X, Y) = E(XY) - E(X)E(Y)$ est la covariance de X et Y .

Preuve:

$$\begin{aligned} E((X + Y)^2) &= E(X^2 + Y^2 + 2XY) \\ &= E(X^2) + E(Y^2) + 2E(XY) \end{aligned}$$

et

$$\begin{aligned} (E(X + Y))^2 &= (E(X) + E(Y))^2 \\ &= E(X)^2 + E(Y)^2 + 2E(X)E(Y). \end{aligned}$$

D'où

$$V(X + Y) = V(X) + V(Y) + 2 \operatorname{Cov}(X, Y).$$

□

Proposition: Si $X \perp\!\!\!\perp Y$, alors $\operatorname{Cov}(X, Y) = 0$. D'où

$$V(X + Y) = V(X) + V(Y).$$

Preuve:

$$\begin{aligned} E(XY) &= \sum_{\substack{x \in X(\Omega) \\ y \in Y(\Omega)}} xy P(X = x, Y = y) \\ &= \sum_{x \in X(\Omega)} \sum_{y \in Y(\Omega)} xy P(X = x) P(Y = y) \\ &= \sum_{x \in X(\Omega)} x P(X = x) \sum_{y \in Y(\Omega)} y P(Y = y) \\ &= E(X)E(Y) \end{aligned}$$

□

Proposition: Soit $(X_i)_{1 \leq i \leq n}$ des variables aléatoires définies sur le même espace pro-

babilisé (Ω, P) . Alors

$$\begin{aligned} V\left(\sum_{i=1}^n X_i\right) &= \sum_{1 \leq i, j \leq n} \text{Cov}(X_i, X_j) \\ &= \sum_{i=1}^n V(X_i) + 2 \sum_{1 \leq i < j \leq n} \text{Cov}(X_i, X_j) \end{aligned}$$

□

Corollaire: Avec les notations précédentes, si les X_i sont deux à deux non corrélés (i.e. $\text{Cov}(X_i, X_j) = 0$ pour $i \neq j$), alors

$$V\left(\sum_{i=1}^n X_i\right) = \sum_{i=1}^n V(X_i).$$

□

Corollaire: Avec les notations précédentes, si les X_i sont indépendantes deux à deux, alors

$$V\left(\sum_{i=1}^n X_i\right) = \sum_{i=1}^n V(X_i).$$

□

Corollaire: Soit $X \sim \mathcal{B}(n, p)$. Alors,

$$V(X) = np(1 - p).$$

Preuve:

On pose $X \sim \sum_{i=1}^n X_i$ où les (X_i) sont mutuellement indépendants et $\forall i$, $X_i \sim \mathcal{B}(p)$.

$$\begin{aligned} V(X) &= V\left(\sum_{i=1}^n X_i\right) \\ &= \sum_{i=1}^n V(X_i) \\ &= \sum_{i=1}^n p(1 - p) \\ &= np(1 - p) \end{aligned}$$

□

Proposition (transfert): Soient X_1, \dots, X_n des variables aléatoires à valeurs réelles

toutes définies sur un même espace probabilisé (Ω, P) et $f : \mathbb{R}^n \rightarrow \mathbb{R}$

$$E(f(X_1, \dots, X_n)) = \sum_{x_1 \in X_1(\Omega)} \dots \sum_{x_n \in X_n(\Omega)} f(x_1, \dots, x_n) P(X_1 = x_1, \dots, X_n = x_n).$$

Preuve:

$$\begin{aligned} E(f(X_1, \dots, X_n)) &= \sum_{\omega \in \Omega} f(X_1(\omega), \dots, X_n(\omega)) P(\{\omega\}) \\ &= \sum_{x_1 \in X_1(\Omega)} \dots \sum_{x_n \in X_n(\Omega)} \sum_{\substack{\omega \in \Omega \\ \forall i, X_i(\omega) = x_i}} f(X_1(\omega), \dots, X_n(\omega)) P(\{\omega\}) \\ &= \sum_{x_1 \in X_1(\Omega)} \dots \sum_{x_n \in X_n(\Omega)} f(x_1, \dots, x_n) \sum_{\substack{\omega \in \Omega \\ \forall i, X_i(\omega) = x_i}} P(\{\omega\}) \\ &= \sum_{x_1 \in X_1(\Omega)} \dots \sum_{x_n \in X_n} f(x_1, \dots, x_n) P(X_1 = x_1, \dots, X_n = x_n) \end{aligned}$$

□

7 Covariance (HORS-PROGRAMME)

On se place dans une optique de Big Data. On dispose d'un tableau à N lignes : chaque ligne correspond à une observation et chaque colonne à une "mesure" (ou caractéristique).

Ces caractéristiques peuvent être corrélées plus ou moins fortement et contenir plus ou moins d'information.

Plus la variance est grande, plus il y a d'information.

Soient X et Y deux colonnes. D'après l'inégalité de Cauchy-Schwarz :

$$|\text{Cov}(X, Y)| \leq \sigma_X \sigma_Y \quad \text{donc} \quad -1 \leq \frac{\text{Cov}(X, Y)}{\sigma_X \sigma_Y} \leq 1.$$

$$\text{Si } Y = \alpha X + \beta : \quad \left| \frac{\text{Cov}(X, Y)}{\sigma_X, \sigma_Y} \right| = 1.$$

L'objectif est de modifier les colonnes de façon à extraire le plus d'informations possible sur le moins de colonnes possibles.

La matrice de covariance est

$$A = (\text{Cov}(X_i, X_j))_{\substack{1 \leq i \leq N \\ 1 \leq j \leq N}}.$$

On aimerait que la matrice A soit diagonale avec de grands coefficients diagonaux.

L'année prochaine, nous verrons le théorème suivant :

Théorème (théorème spectral): Toute matrice symétrique réelle est diagonalisable dans une base orthonormée de vecteurs propres.

Il existe donc des variables aléatoires Y_1, \dots, Y_k combinaisons linéaires des X_1, \dots, X_k telles

que

$$\text{Cov}(Y_i, Y_j) = \begin{pmatrix} \lambda_1 & & & \\ & \ddots & & (0) \\ & & \ddots & \\ (0) & & & \lambda_k \end{pmatrix}.$$

De plus, le maximum de $V(\alpha_1 X_1 + \dots + \alpha_k X_k)$ avec la condition que $\alpha_1^2 + \dots + \alpha_k^2 = 1$ est $V(Y_1) = \lambda_1$.

Définition (Multiplificateurs de Lagrange): Soit $f : U \subset \mathbb{R}^n \rightarrow \mathbb{R}$ où U est un ouvert de \mathbb{R}^n . On cherche $\max_{(x_i)_{i \in \llbracket 1, n \rrbracket} \in R^n} f(x_1, \dots, x_n)$ avec la contrainte $g(x_1, \dots, x_n)$.

On pose

$$F : \mathbb{R}^{n+1} \rightarrow \mathbb{R} \\ (x_1, \dots, x_n, \lambda) \mapsto f(x_1, \dots, x_n) + \lambda g(x_1, \dots, x_n).$$

On cherche les points critiques de F :

$$\nabla F(x_1, \dots, x_n, \lambda) = 0 \iff \begin{cases} \forall i, \frac{\partial F}{\partial x_i}(x_1, \dots, x_n, \lambda) = 0 \\ \frac{\partial F}{\partial \lambda}(x_1, \dots, x_n, \lambda) = 0 \end{cases} \\ \iff \begin{cases} \forall i, \frac{\partial f}{\partial x_i}(x_1, \dots, x_n) + \lambda \frac{\partial g}{\partial x_i}(x_1, \dots, x_n) = 0 \\ g(x_1, \dots, x_n) = 0 \end{cases}$$

Si $(x_1, \dots, x_n, \lambda)$ est le maximum de F , alors
 $\forall y_1, \dots, y_n, \mu \in \mathbb{R}^{n+1}$ $F(x_1, \dots, x_n, \lambda) \geq F(y_1, \dots, y_n, \mu)$
 $f(x_1, \dots, x_n) + \underbrace{\lambda g(x_1, \dots, x_n)}_{=0} \geq f(y_1, \dots, y_n)$

8 Loi des grands nombres

Lemme (inégalité de Markov^a): Soit $X : \Omega \rightarrow \mathbb{R}^+$ une variable aléatoire positive.

$$\forall t \in \mathbb{R}_+^*, P(X \geq t) \leq \frac{E(X)}{t}$$

ou encore,

$$\forall u \in \mathbb{R}_+^*, P(X \geq u E(X)) \leq \frac{1}{u}.$$

^a. Марков : Markov

Preuve:

Soit $t \in \mathbb{R}_+^*$.

$$\begin{aligned}
E(X) &= \sum_{x \in X(\Omega)} x P(X = x) \\
&= \sum_{\substack{x \in X(\Omega) \\ x \geq t}} x P(X = x) + \sum_{\substack{x \in X(\Omega) \\ x < t}} x P(X = x) \\
&\geq \sum_{\substack{x \in X(\Omega) \\ x \geq t}} t P(X = x) + \sum_{\substack{x \in X(\Omega) \\ x < t}} 0 \\
&\geq t P(X \geq t).
\end{aligned}$$

□

Lemme (inégalité de Bienaymé-Tchebychev^a): Soit $X : \Omega \rightarrow \mathbb{R}$ une variable aléatoire réelle. On pose $\mu = E(X)$ et $\sigma = \sigma_X$. Alors,

$$\forall t \in \mathbb{R}_+^*, P(|X - \mu| \geq t) \leq \frac{\sigma^2}{t^2}$$

ou encore

$$\forall u \in \mathbb{R}_+^*, P(|X - \mu| \geq u\sigma) \leq \frac{1}{u^2}.$$

^a. чебышёв : Tchebychev

Preuve:

On pose $Y = |X - \mu|^2$, Y est positive.

$$E(Y) = E((X - \mu)^2) = V(X) = \sigma^2.$$

Donc, d'après l'inégalité de Markov :

$$\forall y \in \mathbb{R}_+^*, P(Y \geq y) \leq \frac{\sigma^2}{y}$$

donc

$$\forall t > 0, P((X - \mu)^2 \geq t^2) \leq \frac{\sigma^2}{t^2}.$$

Or, $(|X - \mu| \geq t) = ((X - \mu)^2 \geq t^2)$, donc

$$P(|X - \mu| \geq t) \leq \frac{\sigma^2}{t^2}.$$

□

REMARQUE (Application):

On considère une expérience de Bernoulli de paramètre $p \in]0, 1[$. On répète n fois cette expérience à l'identique et on note Y_n le nombre moyen de succès.

On pose, pour $i \in \llbracket 1, n \rrbracket$,

$$X_i = \begin{cases} 1 & \text{si la } i\text{-ème expérience est un succès} \\ 0 & \text{sinon.} \end{cases}$$

Les (X_i) sont mutuellement indépendants ; d'où

$$Y_n = \frac{1}{n} \sum_{i=1}^n X_i.$$

Et donc

$$E(Y_n) = \frac{1}{n} \sum_{i=1}^n E(X_i) = \frac{1}{n} np = p.$$

Comme les (X_i) sont deux à deux indépendantes,

$$V(Y_n) = \frac{1}{n^2} \sum_{i=1}^n V(X_i) = \frac{1}{n^2} npq = \frac{pq}{n} \text{ où } q = 1 - p.$$

D'où, d'après l'inégalité de Bienaymé-чебышёв,

$$\forall \varepsilon > 0, P(|Y_n - p| \geq \varepsilon) \leq \frac{pq}{n\varepsilon^2} \xrightarrow[n \rightarrow +\infty]{} 0.$$

On en déduit que

$$\forall \varepsilon > 0, P(|Y_n - p| < \varepsilon) \geq 1 - \underbrace{\frac{pq}{n\varepsilon^2}}_{\substack{\lambda \\ \text{"seuil"}}}.$$

— Par exemple, avec $\varepsilon = 10^{-2}$ et $s = 95\%$, on a

$$\begin{aligned} \frac{95}{100} = s &= 1 - \frac{pq}{n \times 10^{-4}} \iff \frac{5}{100} = \frac{pq}{n 10^{-4}} \\ &\iff 20 = \frac{n 10^{-4}}{pq} \\ &\iff n = 20 \underbrace{\frac{pq}{10^4}}_{\leq \frac{1}{4}} \leq 5 \times 10^4. \end{aligned}$$

En répétant 50 000 fois l'expérience, on est sûr à 95 % que la valeur observée de $Y_{50\,000}$ est dans l'intervalle $[p - 10^{-2}, p + 10^{-2}]$.

— Avec $n = 12$ et $s = 95\%$, on a

$$\begin{aligned} \frac{95}{100} = s &= 1 - \frac{pq}{n\varepsilon^2} \iff \frac{pq}{n\varepsilon^2} = \frac{5}{100} \\ &\iff \frac{\varepsilon^2 n}{pq} = 20 \\ &\iff \varepsilon^2 = \frac{20}{n} pq \leq \frac{5}{12}. \end{aligned}$$

$$\text{Donc, } \varepsilon = \sqrt{\frac{5}{12}} \simeq 0,65.$$

— Avec $n = 12$ et $\varepsilon = 10^{-2}$,

$$\begin{aligned} P(|Y_{12} - p| < \varepsilon) &\geq 1 - \frac{pq}{12 \cdot 10^{-4}} \\ &\geq 1 - \frac{1}{48 \cdot 10^{-4}} \\ &\geq 1 - \underbrace{\frac{1}{48} \times 10^4}_{<0} \end{aligned}$$

Théorème (loi faible des grands nombres — HORS-PROGRAMME): Soit $(X_n)_{n \in \mathbb{N}}$ une suite de variables aléatoires indépendantes de même loi définies sur le même espace probabilisé (Ω, P) . On note μ leur espérance commune.

$$\forall \varepsilon > 0, \lim_{n \rightarrow +\infty} P(|\bar{X}_n - \mu| > \varepsilon) = 0$$

$$\text{où } \forall n, \bar{X}_n = \frac{1}{n} \sum_{i=1}^n X_i.$$

[]

Preuve:

$$\begin{aligned}\forall n \in \mathbb{N}^*, E(\bar{X}_n) &= \frac{1}{n} \sum_{i=1}^n E(X_i) = \mu \\ V(\bar{X}_n) &= \frac{1}{n^2} \sum_{i=1}^n V(X_i) = \frac{n\sigma^2}{n^2} = \frac{\sigma^2}{n}\end{aligned}$$

où σ^2 est la variance commune aux X_i .

Soit $\varepsilon > 0$.

$$0 \leq P(|\bar{X}_n - \mu| > \varepsilon) \leq \frac{\sigma^2}{n\varepsilon^2} \xrightarrow[n \rightarrow +\infty]{} 0..$$

□

Proposition (lemme des coalitions): Soient X_1, \dots, X_n des variables aléatoires à valeurs réelles d'un même ensemble probabilisé mutuellement indépendantes. Soient $f : \mathbb{R}^p \rightarrow \mathbb{R}$ et $g : \mathbb{R}^{n-p} \rightarrow \mathbb{R}$. Alors, $f(X_{i_1}, \dots, X_{i_p})$ et $g(X_{j_1}, \dots, X_{j_{n-p}})$ sont indépendantes si

$$\begin{cases} \{i_1, \dots, i_p\} \cap \{j_1, \dots, j_{n-p}\} = \emptyset \\ \forall k \neq \ell, i_k \neq i_\ell \text{ et } j_k \neq j_\ell. \end{cases}$$

CHAPITRE

32

FAMILLES SOMMABLES

1 Motivation

La série $\sum \frac{(-1)^n}{n}$ est semi-convergente. On a $\sum_{n=1}^{+\infty} \frac{(-1)^n}{n} = -\ln 2$, d'où,

$$-1 + \frac{1}{2} - \frac{1}{3} + \frac{1}{4} - \frac{1}{5} + \frac{1}{6} + \dots = -\ln 2.$$

On change l'ordre :

$$\begin{aligned} & \overbrace{-1 + \frac{1}{2} + \frac{1}{4}}^{-\frac{1}{2} + \frac{1}{4}} - \overbrace{\frac{1}{3} + \frac{1}{6} + \frac{1}{8}}^{-\frac{1}{6} + \frac{1}{8}} - \overbrace{\frac{1}{5} + \frac{1}{10} + \frac{1}{12}}^{-\frac{1}{10} + \frac{1}{12}} + \dots \\ &= \frac{1}{2} \left(-1 + \frac{1}{2} - \frac{1}{3} + \frac{1}{4} - \frac{1}{5} + \frac{1}{6} + \dots \right) \\ &= \frac{-\ln 2}{2} \end{aligned}$$

Théorème (réarrangement de Riemann): Soit $\sum u_n$ une série semi-convergente réelle.

$$\forall \ell \in \mathbb{R}, \exists \sigma : \mathbb{N} \xrightarrow{\text{bij}} \mathbb{N}, \sum_{n=1}^{+\infty} u_{\sigma(n)} = \ell.$$

2 Familles sommables positives

Dans ce paragraphe, toutes les familles considérées sont positives.

Définition: Soit $(u_i)_{i \in I} \in (\mathbb{R}^+)^I$.

Si $\left\{ \sum_{i \in J} u_i \mid \begin{array}{l} J \subset I \\ J \text{ fini} \end{array} \right\}$ est majorée, alors on dit qu'elle est sommable et on définit la somme des $(u_i)_{i \in I}$ par

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

Sinon, la famille n'est pas sommable et on définit

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

EXEMPLE: 1. Toute famille finie positive est sommable : avec $I = \llbracket 1, n \rrbracket$, on a

$$\sum_{i \in I} u_i = \sum_{i=1}^n u_i.$$

2. Soit $(u_n)_{n \in \mathbb{N}} \in (\mathbb{R}^+)^{\mathbb{N}}$.

Cas1 $\sum u_n$ converge. Soit $J \subset I = \mathbb{N}$ finie et

$$\sum_{j \in J} u_j \leq \sum_{i=0}^{\max(J)} u_i \leq \sum_{i=0}^{+\infty} u_i = S.$$

Or,

$$\forall \varepsilon > 0 \exists N \in \mathbb{N} \forall n \geq N, S - \varepsilon \leq \sum_{i=1}^n u_i$$

donc $S - \varepsilon$ ne majore pas $\left\{ \sum_{i \in J} u_i \mid \begin{array}{l} J \subset I \\ J \text{ fini} \end{array} \right\}$. Ainsi,

$$S = \sup_{\substack{J \subset I \\ J \text{ finie}}} \sum_{j \in J} u_j = \sum_{i \in \mathbb{N}} u_i.$$

Cas2 $\sum u_n$ diverge. Alors $\lim_{N \rightarrow +\infty} \sum_{i=0}^N u_i = +\infty$ et donc $\left\{ \sum_{i \in J} u_i \mid \begin{array}{l} J \subset I \\ J \text{ fini} \end{array} \right\}$ n'est pas majorée et donc $(u_n)_{n \in \mathbb{N}}$ n'est pas sommable et

$$\sum_{n \in \mathbb{N}} u_n = +\infty.$$

Théorème: Soit $(u_i)_{i \in I} \in (\mathbb{R}^+)^I$ sommable et soit $\sigma : I \rightarrow I$ une bijection. Alors

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

Preuve:

$$\begin{aligned} \left\{ \sum_{j \in J} u_{\sigma(j)} \mid \begin{array}{l} J \subset I \\ J \text{ fini} \end{array} \right\} &= \left\{ \sum_{k \in \sigma(J)} u_k \mid \begin{array}{l} J \subset I \\ J \text{ fini} \end{array} \right\} \\ &= \left\{ \sum_{k \in K} u_k \mid \begin{array}{l} K \subset I \\ K \text{ fini} \end{array} \right\} \end{aligned}$$

□

Corollaire (sommation par paquets): Soit $(u_i)_{i \in I} \in (\mathbb{R}^+)^I$ et $(I_j)_{j \in J}$ une partition de I :

$$I = \bigcup_{j \in J} I_j.$$

$$(u_i)_{i \in I} \text{ est sommable} \iff \left\{ \begin{array}{l} \forall j \in J, (u_i)_{i \in I_j} \text{ est sommable,} \\ \left(\sum_{i \in I_j} u_i \right)_{j \in J} \text{ est sommable.} \end{array} \right..$$

Dans ce cas,

$$\sum_{i \in I} u_i = \sum_{j \in J} \sum_{i \in I_j} u_i.$$

□

Corollaire (Fubini positif): Soit $(u_{i,j})_{\substack{i \in I \\ j \in J}} \in (\mathbb{R}^+)^{I \times J}$.

$$\sum_{i \in I} \sum_{j \in J} u_{i,j} = \sum_{j \in J} \sum_{i \in I} u_{i,j}.$$

Preuve: — On suppose $(u_{i,j})_{i \in I, j \in J}$ sommable. On pose $I \times J = \bigcup_{i \in I} K_i$ où $K_i = \{i\} \times$

$$J = \{(i, j) \mid j \in J\}.$$

Donc, $\forall i \in I$, $(u_{i,j})_{j \in J}$ est sommable, $\left(\sum_{j \in J} u_{i,j} \right)_{i \in I}$ est sommable et

$$\sum_{(i,j) \in I \times J} u_{i,j} = \sum_{i \in I} \sum_{j \in J} u_{i,j}.$$

On a aussi

$$I \times J = \bigcup_{j \in J} L_j \quad \text{où } L_j = I \times \{j\}.$$

$\forall j \in J$, $(u_{i,j})_{i \in I}$ est sommable, $\left(\sum_{i \in I} u_{i,j} \right)_{j \in J}$ est sommable et

$$\sum_{(i,j) \in I \times J} u_{i,j} = \sum_{j \in J} \sum_{i \in I} u_{i,j}.$$

— On suppose $(u_i)_{i \in I}$ non sommable et donc

$$\sum_{i \in I} \sum_{j \in I} u_{i,j} = +\infty = \sum_{j \in J} \sum_{i \in I} u_{i,j}.$$

□

Corollaire: Soient $(a_i)_{i \in I}$ et $(b_j)_{j \in J}$ deux familles sommables de réels positifs.

$$\sum_{\substack{i \in I \\ j \in J}} a_i b_j = \left(\sum_{i \in I} a_i \right) \left(\sum_{j \in J} b_j \right).$$

Preuve:

On pose, pour $i \in I$, pour $j \in J$, $u_{i,j} = a_i b_j$.

$$\begin{aligned} \sum_{\substack{i \in I \\ j \in J}} a_i b_j &= \sum_{(i,j) \in I \times J} u_{i,j} \\ &= \sum_{i \in I} \sum_{j \in J} u_{i,j} \\ &= \sum_{i \in I} \sum_{j \in J} a_i b_j \\ &= \sum_{i \in I} a_i \sum_{j \in J} b_j \end{aligned}$$

□

Dans la preuve précédente, on a utilisé la linéarité de la somme :

Proposition: Soient $(a_i)_{i \in I} \in (\mathbb{R}^+)^I$, $(b_i)_{i \in I} \in (\mathbb{R}^+)^I$ et $\lambda \in \mathbb{R}^+$.

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

Preuve: Cas1 On suppose (a_i) et (b_i) sommables. Soit $J \subset I$ finie.

$$\sum_{i \in J} (a_i + b_i) = \sum_{i \in J} a_i + \sum_{i \in J} b_i \leq \sum_{i \in I} a_i + \sum_{i \in I} b_i.$$

Donc, $S = \sum_{i \in I} a_i + \sum_{i \in I} b_i$ majore $\left\{ \sum_{i \in J} (a_i + b_i) \mid \begin{array}{l} J \subset I \\ J \text{ fini} \end{array} \right\}$ et donc $(a_i + b_i)_{i \in I}$ est sommable.

Soit $\varepsilon > 0$. Il existe $J \subset I$ finie telle que

$$\sum_{j \in J} a_j \geq \sum_{i \in I} a_i - \frac{\varepsilon}{2}.$$

Également, il existe $J \subset I$ finie telle que

$$\sum_{i \in K} b_i \geq \sum_{i \in J} b_i - \frac{\varepsilon}{2}.$$

On pose $L = J \cup K$. $L \subset I$ et L est un ensemble fini.

$$\begin{aligned}
\sum_{i \in L} (a_i + b_i) &= \sum_{i \in L} a_i + \sum_{i \in L} b_i \\
&\geq \sum_{i \in J} a_i + \sum_{i \in K} b_i \\
&\geq \sum_{i \in I} a_i - \frac{\varepsilon}{2} + \sum_{i \in I} b_i - \frac{\varepsilon}{2} \\
&\geq S - \varepsilon.
\end{aligned}$$

Donc,

$$S = \sup_{\substack{J \subset I \\ J \text{ finie}}} \sum_{i \in J} (a_i + b_i) = \sum_{i \in I} (a_i + b_i).$$

□

Proposition: Soient $(a_i)_{i \in I}$ et $(b_i)_{i \in I}$ deux familles de réels positifs telles que

$$\forall i \in I, 0 \leq a_i \leq b_i.$$

Si $(b_i)_{i \in I}$ est sommable, alors $(a_i)_{i \in I}$ aussi, et, dans ce cas,

$$\sum_{i \in I} a_i \leq \sum_{i \in I} b_i.$$

Preuve:

Soit $J \subset I$ finie.

$$\begin{aligned}
\sum_{i \in J} a_i &\leq \sum_{i \in J} b_i \leq \sum_{i \in I} b_i \\
\text{donc } \sum_{i \in I} b_i &\text{ majore } \left\{ \sum_{i \in J} a_i \mid J \subset I \text{ fini} \right\} \\
\text{donc } (a_i) &\text{ est sommable et}
\end{aligned}$$

$$\sum_{i \in I} a_i \leq \sum_{i \in I} b_i.$$

□

3 Familles sommables réelles

Définition: Soit $(u_i)_{i \in I} \in \mathbb{R}^I$. On dit que $(u_i)_{i \in I}$ est sommable si $(|u_i|)_{i \in I}$ est sommable.

EXEMPLE: 1. Toute famille finie de réels est sommable.

2. Avec $I = \mathbb{N}$ et $(u_n) \in \mathbb{R}^{\mathbb{N}}$,

$$\begin{aligned}
(u_n)_{n \in \mathbb{N}} \text{ sommable} &\iff \sum |u_n| \text{ converge} \\
&\iff \sum u_n \text{ converge absolument.}
\end{aligned}$$

REMARQUE:

Une famille sommable n'est pas une famille dont on peut calculer la somme mais la somme des valeurs absolues.

Proposition – Définition: Soit $(u_i)_{i \in I} \in \mathbb{R}^I$. On pose, pour tout $i \in I$,

$$u_i^+ = \begin{cases} u_i & \text{si } u_i \geq 0, \\ 0 & \text{sinon;} \end{cases}$$

$$u_i^- = \begin{cases} -u_i & \text{si } u_i \leq 0, \\ 0 & \text{sinon.} \end{cases}$$

Alors,

$$(u_i) \text{ sommable} \iff (u_i^+) \text{ et } (u_i^-) \text{ sont sommables.}$$

Dans ce cas, on définit

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

Preuve: “ \implies ” On suppose (u_i) sommable. Par définition, $(|u_i|)_{i \in I}$ est sommable.

$$\forall i \in I, 0 \leq u_i^+ \leq |u_i|.$$

On en déduit que (u_i^+) est sommable. De même,

$$\forall i \in I, 0 \leq u_i^- \leq |u_i|$$

et donc (u_i^-) est sommable.

“ \impliedby ” On suppose (u_i^+) et (u_i^-) sommables.

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

Par linéarité, $(|u_i|)_{i \in I}$ est sommable et donc $(u_i)_{i \in I}$ est sommable.

□

Proposition: Soient $(a_i)_{i \in I}$ et $(b_i)_{i \in I}$ deux familles sommables et $\lambda \in \mathbb{R}$. Alors, $(a_i + b_i)_{i \in I}$ est sommable, $(\lambda a_i)_{i \in I}$ aussi et

$$\sum_{i \in I} (a_i + b_i) = \sum_{i \in I} a_i + \sum_{i \in I} b_i,$$

$$\sum_{i \in I} \lambda a_i = \lambda \sum_{i \in I} a_i.$$

En d'autres termes, $\ell^1(I)$ est un sous-espace vectoriel de \mathbb{R}^I et

$$S : \ell^1(I) \longrightarrow \mathbb{R}$$

$$(u_i)_{i \in I} \mapsto \sum_{i \in I} u_i$$

est linéaire où $\ell^1(I) = \{(u_i) \in \mathbb{R}^I \mid (u_i) \text{ sommable}\}$.

Preuve: — $\forall i \in I, |u_i + v_i| \leq |u_i| + |v_i|$. Or, par hypothèse, $(|u_i|)_{i \in I}$ et $(|v_i|)_{i \in I}$ sont sommables et positives donc $(|u_i| + |v_i|)_{i \in I}$ est sommable donc $(|u_i + v_i|)_{i \in I}$ est sommable et donc $(u_i + v_i)_{i \in I}$ est sommable.

Et,

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

Or,

$$\begin{aligned} \sum_{i \in I} (u_i + v_i) &= \sum_{i \in I} u_i + \sum_{i \in I} v_i \\ \iff \sum_{i \in I} (u_i + v_i)^+ - \sum_{i \in I} (u_i + v_i)^- &= \sum_{i \in I} u_i^+ - \sum_{i \in I} u_i^- + \sum_{i \in I} v_i^+ - \sum_{i \in I} v_i^- \\ \iff \sum_{i \in I} (u_i + v_i)^+ + \sum_{i \in I} u_i^- + \sum_{i \in I} v_i^- &= \sum_{i \in I} (u_i + v_i)^- + \sum_{i \in I} u_i^+ + \sum_{i \in I} v_i^+ \\ \iff \sum_{i \in I} ((u_i + v_i)^+ + u_i^- + v_i^-) &= \sum_{i \in I} ((u_i + v_i)^- + u_i^+ + v_i^+). \end{aligned}$$

On réalise une disjonction de cas : soit $i \in I$.

u_i	v_i	$u_i + v_i$	$(u_i + v_i)^+ + u_i^- + v_i^-$	$(u_i + v_i)^- + u_i^+ + v_i^+$
+	+	+	$u_i + v_i$	$u_i + v_i$
+	-	+	u_i	u_i
+	-	-	$-v_i$	$-v_i$
-	+	+	v_i	v_i
-	+	-	$-u_i$	$-u_i$
-	-	-	$-u_i - v_i$	$-u_i - v_i$

On remarque que, pour tout $i \in I$,

$$(u_i + v_i)^+ + u_i^- + v_i^- = (u_i + v_i)^- + u_i^+ + v_i^+.$$

- $\forall i \in I, |\lambda u_i| = |\lambda| |u_i|$, $(|u_i|)_{i \in I}$ est sommable, $|\lambda| \geq 0$ et donc $(|\lambda u_i|)_{i \in I}$ est sommable et donc $(\lambda u_i)_{i \in I}$ est sommable.

CAS1 $\lambda \geq 0$:

$$\begin{aligned} \sum_{i \in I} \lambda u_i &= \sum_{i \in I} (\lambda u_i)^+ - \sum_{i \in I} (\lambda u_i)^- \\ &= \sum_{i \in I} \lambda u_i^+ - \sum_{i \in I} \lambda u_i^- \\ &= \lambda \left(\sum_{i \in I} u_i^+ - \sum_{i \in I} u_i^- \right) \\ &= \lambda \sum_{i \in I} u_i. \end{aligned}$$

CAS2 $\lambda < 0$:

$$\begin{aligned} \sum_{i \in I} \lambda u_i &= \sum_{i \in I} (\lambda u_i)^+ - \sum_{i \in I}^- \\ &= \sum_{i \in I} \underbrace{(-\lambda)}_{\geq 0} u_i^- - \sum_{i \in I} \underbrace{(-\lambda)}_{\geq 0} u_i^+ \\ &= (-\lambda) \left(\sum_{i \in I} u_i^- - \sum_{i \in I} u_i^+ \right). \end{aligned}$$

Or,

$$\lambda \sum_{i \in I} u_i = \lambda \left(\sum_{i \in I} u_i^+ - \sum_{i \in I} u_i^- \right) = (-\lambda) \left(\sum_{i \in I} u_i^- - \sum_{i \in I} u_i^+ \right).$$

□

Proposition: Soit $(u_i)_{i \in I} \in \mathbb{R}^I$ sommable et $\sigma : I \rightarrow I$ une bijection. Alors $(u_{\sigma(i)})_{i \in I}$ est sommable et

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

Preuve:

D'après le paragraphe 1, $(|u_{\sigma(i)}|)_{i \in I}$ est sommable.

$$\begin{aligned} \sum_{i \in I} u_{\sigma(i)} &= \sum_{i \in I} u_{\sigma(i)}^+ - \sum_{i \in I} u_{\sigma(i)}^- \\ &= \sum_{i \in I} u_i^+ - \sum_{i \in I} u_i^- \\ &= \sum_{i \in I} u_i \end{aligned}$$

□

Corollaire (sommation par paquets): Soit $(u_i)_{i \in I} \in \mathbb{R}^I$ et $(I_j)_{j \in J}$ une partition de I .

$$(u_i)_{i \in I} \text{ sommable} \implies \left\{ \begin{array}{l} \forall j \in J, (u_i)_{i \in I_j} \text{ sommable}, \\ \left(\sum_{i \in I_j} u_i \right)_{j \in J} \text{ sommable.} \end{array} \right.$$

Dans ce cas,

$$\sum_{i \in I} u_i = \sum_{j \in J} \sum_{i \in I_j} u_i.$$

Corollaire (Fubini): Soit $(u_{i,j})_{\substack{i \in I \\ j \in J}} \in \mathbb{R}^{I \times J}$ sommable. Alors,

$$\sum_{i \in I} \sum_{j \in J} u_{i,j} = \sum_{j \in J} \sum_{i \in I} u_{i,j}.$$

Corollaire: Soient $(a_i)_{i \in I}$ et $(b_j)_{j \in J}$ deux familles sommables. Alors $(a_i b_j)_{\substack{i \in I \\ j \in J}}$ est sommable et

$$\sum_{i \in I} \sum_{j \in J} a_i b_j = \left(\sum_{i \in I} a_i \right) \left(\sum_{j \in J} b_j \right).$$

Preuve:

$$\text{On a } I \times J = \bigcup_{i \in I} (\{i\} \times J).$$

Alors,

$$\begin{aligned} (a_i b_j)_{\substack{i \in I \\ j \in J}} \text{ sommable} &\iff \begin{cases} \forall i \in I, (a_i b_j)_{j \in J} \text{ sommable} \\ \left(\sum_{j \in J} a_i b_j \right)_{i \in I} \text{ sommable} \end{cases} \\ &\iff \{(b_j)_{j \in J} \text{ sommable}, (a_i)_{i \in I} \text{ sommable}\}. \end{aligned}$$

De plus,

$$\begin{aligned} \sum_{(i,j) \in I \times J} &= \sum_{i \in I} \sum_{j \in J} (a_i b_j) \\ &= \sum_{i \in I} \left(a_i \sum_{j \in J} b_j \right) \\ &= \left(\sum_{i \in I} a_i \right) \left(\sum_{j \in J} b_j \right). \end{aligned}$$

□

4 Familles sommables de nombres complexes

Définition: Soit $(u_i)_{i \in I} \in \mathbb{C}^I$. On dit qu'elle est sommable si $(|u_i|)_{i \in I}$ est sommable.

Proposition: Soit $(u_i)_{i \in I} \in \mathbb{C}^I$.

$(u_i)_{i \in I}$ sommable $\iff (\Re(u_i))_{i \in I}$ et $(\Im(u_i))_{i \in I}$ sont sommables.

Preuve: “ \implies ” Pour tout $i \in I$, $|\Re(u_i)| \leq |u_i|$ et $|\Im(u_i)| \leq |u_i|$ donc $(\Re(u_i))_{i \in I}$ et $(\Im(u_i))_{i \in I}$ sont sommables.

“ \impliedby ” $\forall i \in I$, $|u_i| \leq |\Re(u_i)| + |\Im(u_i)|$ donc $(|u_i|)_{i \in I}$ est sommable.

□

Définition: Soit $(u_k)_{k \in I} \in \mathbb{C}^I$ sommable. On définit

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

On a exactement les mêmes propriétés que pour des familles réelles.

□

5 Produit de Cauchy de deux séries

RAPPEL:

Avec $P = \sum_{k=0}^p a_k X^k$ et $Q = \sum_{\ell=0}^q b_\ell X^\ell$, on a

$$\begin{aligned} PQ &= \sum_{k=0}^p \sum_{\ell=0}^q a_k b_\ell X^{k+\ell} \\ &= \sum_{m=0}^{p+q} \left(\sum_{k=0}^{\min(p,m)} a_k b_{m-k} \right) X^m. \end{aligned}$$

Définition: Soient $(u_n), (v_n) \in \mathbb{C}^{\mathbb{N}}$. Le produit de Cauchy des séries $\sum u_n$ et $\sum v_n$ est la série $\sum w_n$ où

$$\forall n \in \mathbb{N}, w_n = \sum_{k=0}^n u_k v_{n-k}.$$

Théorème: Soient $(u_n), (v_n) \in \mathbb{C}^{\mathbb{N}}$. Si $\sum u_n$ et $\sum v_n$ convergent absolument, alors leur produit $\sum w_n$ converge absolument et

$$\sum_{n=0}^{+\infty} w_n = \left(\sum_{n=0}^{+\infty} u_n \right) \left(\sum_{n=0}^{+\infty} v_n \right).$$

Preuve:

On sait que (u_n) et (v_n) sont sommables. On pose

$$\forall n \in \mathbb{N}, w_n = \sum_{k=0}^n u_k v_{n-k}.$$

$(u_n v_m)_{(n,m) \in \mathbb{N}^2}$ est donc sommable et

$$\begin{aligned} \left(\sum_{k=0}^{+\infty} u_n \right) \left(\sum_{k=0}^{+\infty} v_n \right) &= \sum_{(n,m) \in \mathbb{N}^2} u_n v_m \\ &= \sum_{n=0}^{+\infty} \sum_{a=n}^{+\infty} u_n v_{a-n} \\ &= \sum_{a=0}^{+\infty} \sum_{n=0}^a u_n v_{a-n} \\ &= \sum_{n=0}^{+\infty} \sum_{k=0}^n u_k v_{n-k} \\ &= \sum_{n=0}^{+\infty} w_n. \end{aligned}$$

□

EXEMPLE:

On préfère définir l'exponentielle complexe par

$$\forall z \in \mathbb{C}, e^z = \sum_{n=0}^{+\infty} \frac{z^n}{n!}$$

(au lieu de la définition du chapitre 4)

$$\text{Par définition, } e^0 = \sum_{n=0}^{+\infty} \frac{0^n}{n!} = 1.$$

Soient $(x, y) \in \mathbb{C}^2$. $\left(\frac{x^n}{n!}\right)_{n \in \mathbb{N}}$ et $\left(\frac{y^n}{n!}\right)_{n \in \mathbb{N}}$ sont sommables donc

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

CHAPITRE

33

ANNEXE

1 Algorithme de Metropolis-Hastings

On a un texte à déchiffrer. Il a été codé par substitution : on a remplacé une lettre par une autre (par exemple, “ $A \rightarrow W$ ” et “ $B \rightarrow U$ ”). L’algorithme de Metropolis-Hastings permet de déchiffrer ce type de message.

Cet algorithme fonctionne itérativement, et, pour chaque lettre, il tente de la permute avec une autre et il conserve la meilleur.

Pour comparer deux permutations, il utilise des *bigrammes* : un couple de deux lettres consécutives (où l’on a supprimé les espaces). Avec un entraînement sur un autre texte de la même langue, l’algorithme détermine la *plausibilité* de chaque bigramme. Au moment de comparer deux permutations, il compare les plausibilités des bigrammes obtenus à la suite des deux permutations.

On se place dans le groupe symétrique et la fonction qui donne la plausibilité associée à une permutation est une fonction du groupe symétrique dans les réels : $p : S_n \rightarrow \mathbb{R}$ (en français, $n = 26$).

L’algorithme ressemble donc à :

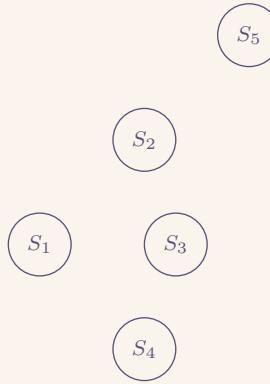
On choisit une permutation.

Si, en l’appliquant au texte, la plausibilité augmente, on conserve cette permutation.
Sinon, on ne la conserve pas.

Et on répète.

Cet algorithme utilise donc une marche aléatoire, il ne teste pas *toutes* les permutations (avec $n = 26$, on a $\#S_n \geq 10^{61}$).

Définition (Chaîne de Markov): Le système est dans un état E et peut passer dans d’autres états avec des probabilités associées. Ce changement d’état ne dépend **que** de l’état actuel, et n’utilise pas les états passés.



On associe à une chaîne de Markov une matrice de transition :

$$\begin{array}{c} i \\ \downarrow \\ \left(\begin{array}{c} P(S_j | S_i) \end{array} \right) \leftarrow j. \end{array}$$

On souhaite trouver $\max_{x \in S} f(x)$. Pour cela, on considère le changement $x \rightarrow x'$ et on pose $\alpha = \frac{f(x')}{f(x)}$. On ne conserve x' avec une probabilité de α , sinon, on revient à x .

Mais, la probabilité de transition est proportionnelle à $f(x')$ et donc, pour que ce choix soit marqué, il faut que la fonction f ait une grande variance.

Cette méthode de choix ne peut être appliquée que si la chaîne de Markov est symétrique et connexe. La symétrie de la chaîne de Markov est assurée par le fait qu'une permutation est bijective, on peut donc appliquer son inverse pour revenir à un état précédent.

2 Gradient automatique

On considère l'ensemble

$$D = \{a + b\varepsilon \mid (a, b) \in \mathbb{R}^2\}$$

où $\varepsilon \notin \mathbb{R}$ donc $\varepsilon \neq 0$ mais $\varepsilon^2 = 0$ (similaire à i dans les complexes).

Cet ensemble peut exister : avec $D = \mathbb{R}[X]/\sim$ où

$$\begin{aligned} P \sim Q &\iff P \equiv Q \ [X^2] \\ &\iff X^2 \mid P - Q. \end{aligned}$$

On définit donc $\varepsilon = \overline{X} \neq 0 : \varepsilon^2 = \overline{X^2} = \overline{0} = 0$. En appliquant la division euclidienne de P par X^2 , on a $P = X^2Q + R$ et donc $\overline{P} = \overline{R} = \overline{a + bX} = a + b\varepsilon$.

C'est comme ceci que l'on a défini \mathbb{C} : en effet, on a $\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$.

On essaie de multiplier deux duals avec la distributivité du produit :

$$(1 + 2\varepsilon)(3 + 4\varepsilon) = 3 + 4\varepsilon + 6\varepsilon + 8\varepsilon^2 = 3 + 10\varepsilon.$$

On considère maintenant une fonction réelle

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto 3x^2 - 5x^2 + 2x + 6 \end{aligned}$$

et on pose F l'extension de f dans l'anneau des nombres duals.

$$\begin{aligned}
F(x + \varepsilon) &= 3(x + \varepsilon)^3 - 5(x + \varepsilon)^2 + 2(x + \varepsilon) + 6 \\
&= 3(x^3 + 3x^2\varepsilon + 3x\varepsilon^2 + \cancel{\varepsilon^3}) - 5(x^2 + 2x\varepsilon + \cancel{\varepsilon^2}) + 2x + 2\varepsilon + 6 \\
&= \underbrace{(3x^3 - 5x^2 + 2x + 6)}_{f(x)} + \varepsilon \underbrace{(9x^2 - 10x + 2)}_{f'(x)} \\
&= f(x) + \varepsilon f'(x)
\end{aligned}$$

On généralise : soient f et g deux fonctions définies et dérivables sur $I \subset \mathbb{R}$ à valeurs réelles.
On pose

$$\forall x \in I, \forall y \in \mathbb{R}, \begin{cases} F(x + y\varepsilon) = f(x) + y\varepsilon f'(x), \\ G(x + y\varepsilon) = g(x) + y\varepsilon g'(x). \end{cases}$$

Soit $x \in I$ et $y \in \mathbb{R}$.

$$\begin{aligned}
F(x + \varepsilon) + G(x + \varepsilon) &= (f(x) + g(x)) + \varepsilon(f'(x) + g'(x)); \\
F(x + \varepsilon) \times G(x + \varepsilon) &= (f(x) + \varepsilon f'(x))(g(x) + \varepsilon g'(x)) \\
&= f(x)g(x) + \varepsilon(f'(x)g(x) + f(x)g'(x)) \\
&= (f \times g)(x) + \varepsilon(f \times g)'(x) \\
F(G(x + \varepsilon)) &= F(g(x) + \varepsilon g'(x)) \\
&= f(g(x)) + g'(x)\varepsilon f'(g(x))
\end{aligned}$$

Ces opérations sur les fonctions dans l'anneau dual sont compatibles avec les règles de dérivation habituelles.

EXEMPLE:

On calcule

$$\frac{d}{dx}(e^x \cos x - \cos(\ln x)).$$

On pose

$$\begin{cases} F(x + y\varepsilon) = e^x + y\varepsilon e^x, \\ G(x + y\varepsilon) = \cos(x) - y\varepsilon \sin x, \\ H(x + y\varepsilon) = \ln x + \frac{y\varepsilon}{x}. \end{cases}$$

$$\begin{aligned}
&F(x + \varepsilon)G(x + \varepsilon) - G(H(x + \varepsilon)) \\
&= (e^x + \varepsilon e^x)(\cos x - \varepsilon \sin x) - G\left(\ln x + \frac{\varepsilon}{x}\right) \\
&= e^x \cos x - \varepsilon \sin x e^x + \varepsilon \cos(x) e^x - \left(\cos(\ln x) - \frac{\varepsilon}{x} \times \sin(\ln x)\right) \\
&= e^x \cos(x) - \cos(\ln x) + \varepsilon \left(-\sin(x)e^x + \cos(x)e^x + \frac{1}{x} \sin(\ln x)\right)
\end{aligned}$$

On peut calculer les dérivées de fonctions. À la main, c'a prend autant de temps que d'utiliser les techniques habituelles. Cependant, informatiquement, le calcul de dérivée est simple ; en Python on peut le faire avec :

Par exemple, pour chercher $\min_{x \in \mathbb{R}} (x^4 + 3x^3 - 5x^2 + 2)$, on pose $f(x_0) = f(x_0 + \varepsilon f'(x_0))$ et $x_{n+1} = x_n - h f'(x_n)$ où $h > 0$. La suite (x_n) tends vers x^* où x^* est un minimum local.

```

class Dual:
    def __init__(self, x, y):
        self.x = x
        self.y = y

    def __add__(self, other):
        return Dual(self.x + other.x, self.y + other.y)

    def __mul__(self, other):
        return Dual(self.x * other.x, self.x * other.y + self.y * other.x)

    def exp(self):
        return Dual(exp(self.x), self.y * exp(self.x))

```

Ce calcul de dérivée est exact, on ne calcule pas $f'(x) \simeq \frac{f(x+h) - f(x)}{h}$.

Pour le calcul de gradient dans le cas de deux dimensions, on considère deux nombres vérifiant les propriétés de " ε " : ε_1 et ε_2 .

INDEX

- action (groupe), 206
- adaptation (subdivision), 483
- adhérent (dans \mathbb{R}^2), 368
- adjacence (suites), 170
- affixe (point), 25
- affixe (vecteur), 25
- alternée (application), 429
- anneau, 198
- anti symétrie (relation), 94
- antisymétrique (application), 428
- application, 84
- arccosinus (trigonométrie), 60
- archimédien, 107
- arcsinus (trigonométrie), 58
- arctangente (trigonométrie), 62
- p -arrangement, 388
- association (anneau), 201
- association (entiers), 136
- association (polynôme), 282
- associativité (loi de composition interne), 97
- automorphisme (d'anneaux), 202
- automorphisme (de groupes), 196
- automorphisme intérieur, 196
- base (espace vectoriel), 250
- bijective (application), 85
- borne inférieure, 95
- borné (ensemble), 97
- bornée (suite complexe), 182
- boule (de \mathbb{R}^2), 362
- boule fermée (de \mathbb{R}^2), 362
- boule ouverte (de \mathbb{R}^2), 362
- cardinal (ensemble), 382
- champ de vecteur, 456
- classe \mathcal{C}^∞ (fonction réelle), 260
- classe \mathcal{C}^n (fonction réelle), 258
- classe d'équivalence (relation), 90
- classe de similitude (matrices), 347
- colinéarité (espace vectoriel), 244
- comatrice, 440
- p -combinaison, 390
- combinaison linéaire, 236
- commutativité (loi de composition interne), 98
- complémentaire (ensemble), 83
- composition (application), 85
- composition (polynômes), 279
- condition nécessaire, 3
- condition suffisante, 3
- congruence (entiers), 138
- conjugaison, 196
- continuité (application complexe), 33
- continuité (dans \mathbb{R}^2), 366
- continuité en un point, 220
- continuité par morceaux, 494
- continuité par morceaux sur un intervalle, 494
- convergence (suites complexes), 180
- convergence (suites réelles), 157
- convergence (série), 407
- convergence absolue (série), 414
- coordonnées (espace affine), 461
- corps, 204
- corrélation (variables aléatoires), 510
- cosinus hyperbolique, 64
- cotangente (trigonométrie), 19
- couple, 101
- covariance (variables aléatoires), 509
- croissance (application), 97
- k -cycle (permutation), 398
- cyclique (groupe), 191
- densité (partie de \mathbb{R}), 108
- différence symétrique (ensemble), 83

- déifferentiable (application), 479
- déifferentielle, 479
- dimension (espace vectoriel), 267
- dimension finie (espace vectoriel), 264
- dimension infinie (espace vectoriel), 264
- direction (sous-espace affine), 460
- disque fermée (de \mathbb{R}^2), 362
- disque ouverte (de \mathbb{R}^2), 362
- distance (espace euclidien), 474
- distance (espace préhilbertien), 474
- divergence (suites réelles), 159
- diviseur (anneau), 201
- diviseur (entiers), 135
- diviseur (polynôme), 282
- diviseur de zéro (anneau), 204
- division (anneau), 201
- division (entiers), 135, 138
- division (polynômes), 282
- division euclidienne (entiers), 138
- division euclidienne (polynômes), 283
- domaine de validité (prédicat, logique), 5
- dominer (suites réelles), 177
- droite (vectorielle, espaces vectoriels), 244
- droite affine (espace affine), 460
- décroissance (application), 97
- définition explicite (suites), 157
- définition implicite (suites), 157
- définition par récurrence (suites), 157
- démontrer (proposition logique), 1
- dérivabilité (application complexe), 33
- dérivabilité (fonction complexe), 262
- dérivabilité (fonction réelle), 252
- dérivabilité sur un intervalle (fonction réelle), 252
- dérivé (polynôme), 280
- dérivée n -ième (fonction réelle), 258
- dérivée n -ième (polynôme), 282
- dérivée partielle (fonction à deux variables), 369
- dérivée selon un vecteur (fonction à deux variables), 370
- déterminant (d'une application), 432
- déterminant (d'une matrice), 434
- déterminant (dans une base \mathcal{B}), 431
- développement décimal, 423
- développement limité d'ordre n au voisinage de a , 76
- endomorphisme (d'anneaux), 202
- endomorphisme (de groupes), 196
- engendrer (groupe), 190
- ensemble, 80
- ensemble de toutes les parties d'un ensemble, 82
- ensemble ordonné, 94
- ensemble vide, 81
- \emptyset , 81
- entiers congrus, 138
- escalier (fonction), 483
- espace affine, 455
- espace dual, 310
- espace euclidien, 462
- espace probabilisé, 442
- espace préhilbertien, 462
- espace vectoriel, 233
- espace vectoriel des polynômes à coefficients inférieurs à n , 294
- espérance (variable aléatoire réelle), 504
- et (logique), 1
- exponentielle (réelle), 49
- exponentielle complexe, 32
- e^z avec $z \in \mathbb{C}$, 32
- exponentielle de base a , 17, 53
- e^{ia} , 22
- extension, 205
- extractrice (suites), 171
- extremum (ensemble), 97
- extremum local, 256
- famille (ensemble), 103
- famille génératrice (espace vectoriel), 245
- famille non sommable, 517
- famille orthogonale, 466
- famille orthonormale, 466
- famille orthonormée, 466
- famille sommable (complexe), 524
- famille sommable (positive), 517
- famille sommable (réelle), 520
- finesse (subdivision), 484
- fonction en escalier, 483
- fonction Riemann-intégrable, 488
- forme bilinéaire, 462
- forme définie, 462
- forme linéaire, 310
- forme positive, 462
- forme symétrique, 462
- gradient (fonction à deux variables), 372
- gradient d'une application de \mathbb{R}^n , 479
- graphe (application), 98
- groupe, 188
- groupe abélien, 188
- groupe alterné, 404
- groupe commutatif, 188
- groupe linéaire, 304
- groupe produit, 198
- groupe symétrique, 395
- générateur (groupe), 191
- homomorphisme (d'anneaux), 202
- homomorphisme (de corps), 206
- homomorphisme (de groupes), 193
- homothétie (complexe), 30
- homéomorphisme, 232
- hyperplan, 313
- hyperplan affine (espace affine), 460
- identité (application), 87
- image (application), 103
- image directe (application, ensemble), 87
- image réciproque (application, ensemble), 87
- implication (logique), 3
- inclusion (ensemble), 81
- indicatrice (ensemble), 99

- indépendance (événements d'un espace probabilisé), 451
 indépendance 2 à 2 (événements d'un espace probabilisé), 452
 indépendance linéaire (vecteurs), 247
 indépendance mutuelle (événements d'un espace probabilisé), 452
 injective (application), 85
 interpolateur de Lagrange (polynôme), 299
 intersection (ensemble), 82
 intégrité (anneau), 199
 intégrale (fonction en escaliers), 484
 intégrale de f , 69
 intérieur (dans \mathbb{R}^2), 364
 inverse (loi de composition interne), 100
 inversibilité (loi de composition interne), 100
 inversion (permutation), 403
 involution (application linéaire), 317
 irréductibilité (fraction rationnelles), 321
 irréductibilité (polynôme), 289
 isomorphisme (d'anneaux), 202
 isomorphisme (de groupes), 196
 liberté (famille de vecteurs), 247
 limite (dans \mathbb{R}^2), 365, 368
 limite finie (suites complexes), 180
 limite finie (suites réelles), 157
 limite infinie (suites réelles), 158
 linéarité (application), 301
 linéarité (problème), 302
 lipschitzienne, 229
 k -lipschitzienne, 229
 logarithme de base a , 54
 logarithme népérien, 44
 loi (couple de variables aléatoires), 502
 loi (variable aléatoire), 501
 loi binomiale (variables aléatoires), 501
 loi de Bernoulli (variables aléatoires), 501
 loi de composition interne, 97
 loi uniforme (variables aléatoires), 501
 lois marginales (couple de variables aléatoires), 502
 majorant (ensemble), 95
 majorer (ensemble), 95
 matrice aléatoire, 500
 matrice d'un vecteur, 336
 matrice d'une application linéaire, 340
 matrice d'une base, 337
 matrice de covariance, 511
 maximum (ensemble), 95
 maximum local, 256
 minimum (ensemble), 95
 minimum local, 256
 minorant (ensemble), 95
 minorer (ensemble), 95
 monogène (groupe), 191
 monoïde (groupe), 198
 morphisme (d'anneaux), 202
 morphisme (de corps), 206
 morphisme (de groupes), 193
 multilinéaire (application), 428
 multiple (anneau), 201
 multiple (entiers), 135
 multiple (polynôme), 282
 multiplication par un scalaire (fraction rationnelle), 324
 multiplicité (racine d'un polynôme), 290
 nombre dérivée (fonction réelle), 252
 norme (de \mathbb{R}^2), 361
 norme euclidienne, 463
 norme euclidienne (de \mathbb{R}^2), 361
 noyau (d'une application), 203
 négation (logique), 2
 négligeabilité (suites réelles), 178
 opposé (loi de composition interne), 100
 orbite (permutation), 398
 ordre (groupe), 192
 ordre (permutation), 398
 ordre total (relation d'ordre), 94
 orthogonal d'une partie, 471
 orthogonalité, 464
 ou (logique), 2
 ouvert (de \mathbb{R}^2), 362
 parallélisme faible (espace affine), 460
 parallélisme fort (espace affine), 460
 parité (permutation), 404
 k parmi n , 11
 partie d'un ensemble, 82
 partie entière, 108
 partie fermée (de \mathbb{R}^2), 362
 partie génératrice (groupe), 190
 Partie imaginaire (application), 33
 partie ouverte (de \mathbb{R}^2), 362
 Partie réelle (application), 33
 partition (ensemble), 93
 PGCD (polynôme), 286
 PGCD (polynômes), 287
 plan (vectoriel, espaces vectoriels), 244
 plan affine (espace affine), 460
 plus grand élément (ensemble), 95
 plus petit élément (ensemble), 95
 point (espace affine), 456
 point adhérent (dans \mathbb{R}^2), 368
 point critique, 256
 point critique (fonction à deux variables), 374
 point intérieur (dans \mathbb{R}^2), 364
 polynôme de matrices, 278
 polynôme unitaire, 287
 polynôme à coefficients dans \mathbb{K} , 272
 presque sûrement (variables aléatoires), 508
 probabilité, 442
 probabilité sachant A , 445
 produit (famille), 16
 produit (polynômes), 273
 produit cartésien (ensembles), 101
 produit de Cauchy, 525
 produit hermitien, 480
 produit scalaire, 462
 produit vectoriel, 478
 projecteur (application linéaire), 316

- projection (espace vectoriel), 315
- projection orthogonale (espace euclidien), 473
- projeté (espace vectoriel), 315
- prolongement (application), 89
- proposition, 1
- prédictat (logique), 5
- prédécesseur (\mathbb{N}), 132
- pôles (fraction rationnelle), 333
- quotient (division euclidienne, polynômes), 283
- quotient (entiers), 138
- quotient (relation, ensemble), 91
- racine (polynôme), 278
- racine double (polynôme), 290
- racine simple (polynôme), 290
- rand (système), 213
- rang (application linéaire), 309
- rang (matrice), 213
- relation (binaire), 90
- relation d'ordre, 94
- relation d'équivalence, 90
- remplacer (polynôme), 278
- repère (espace affine), 460
- reste (division euclidienne, polynômes), 283
- reste (entiers), 138
- restriction (application), 89
- Riemann-intégrable (fonction), 488
- rotation (complexe), 27
- réciproque (application), 87
- réflectivité (relation), 90
- réunion (ensemble), 82
- scalaire (espace vectoriel), 233
- scindé (polynôme), 297
- second membre (équation différentielle), 72
- semblable (matrices), 347
- semi convergence (série), 414
- semi-linéarité (application), 480
- sesquilineaire (application), 480
- signature (permutation), 403
- similitude (directe, complexe), 31
- simplifiabilité à droite, 99
- simplifiabilité à gauche, 99
- sinus hyperbolique, 64
- somme (espaces vectoriels), 238
- somme (famille d'espaces vectoriels), 239
- somme (famille sommable complexe), 524
- somme (famille sommable réelle), 521
- somme (famille), 15
- somme (familles sommables), 517
- somme (polynômes), 272
- somme (série), 407
- somme directe (espaces vectoriels), 239
- somme directe (famille d'espaces vectoriels), 243
- somme partielle (série), 407
- sous anneau, 201
- sous corps, 205
- sous espace vectoriel, 235
- sous espace vectoriel engendré, 243
- sous groupe, 188
- sous groupe engendré par A , 190
- sous suite, 171
- sous-espace affine, 458
- sous-espace affine engendré, 460
- sphère (de \mathbb{R}^2), 362
- spécialiser (polynôme), 278
- subdivision adaptée, 483
- subdivision d'un segment, 483
- subdivision plus fine, 484
- substituer (polynôme), 278
- successeur (\mathbb{N}), 132
- suite (ensemble), 103
- suite extraite, 171
- suite récurrente d'ordre 2, 175
- supplémentaire orthogonal (espace euclidien), 473
- supplémentarité (espaces vectoriels), 242
- support (permutation), 400
- surjective (application), 85
- symétrie (espace vectoriel), 317
- symétrie (relation), 90
- symétrique (loi de composition interne), 100
- symétrisabilité, 99
- symétrisabilité à droite, 99
- symétrisabilité à gauche, 99
- système complet d'événements, 446
- système de Cramer, 214
- système triangulaire, 216
- série, 407
- tangente (trigonométrie), 18
- tangente hyperbolique, 64
- tendre vers (dans \mathbb{R}^2), 365, 368
- trace (matrice), 350
- transitivité (relation), 90
- translation (complexe), 26
- translation (espace affine), 456
- transposition (permutation), 402
- transposée (matrice), 354
- triangulaire inférieur (matrice), 216
- triangulaire supérieur (matrice), 215
- un (\mathbb{N}), 132
- univers (probabilités), 443
- valeur critique, 256
- valeur critique (fonction à deux variables), 374
- variable aléatoire, 500
- variable aléatoire réelle, 500
- variance (variable aléatoire), 507
- vecteur (espace affine), 456
- vecteur (espace vectoriel), 233
- vecteur aléatoire, 500
- vectorialiser (espace affine), 458
- voisinage, 217
- voisinage (complexe), 231
- voisinage (dans \mathbb{R}^2), 364
- voisinage à droite, 218
- voisinage à gauche, 218
- zéro (\mathbb{N}), 132
- zéros (fraction rationnelle), 333

écart-type (variable aléatoire), 508
égalité (ensemble), 81
élément maximal (ensemble), 96
élément minimal (ensemble), 96
élément neutre (loi de composition interne),
 98
élément neutre à droite (loi de composition
 interne), 98
élément neutre à gauche (loi de composition
 interne), 98
équation caractéristique (suites), 175
équation différentielle, 72
équation différentielle linéaire d'ordre n , 72
équipotence (ensembles), 101
équivalence (fonctions réelles), 40
équivalence (matrices), 347
équivalence (propositions logiques), 2
équivalence (suites réelles), 179
évaluer (polynôme), 278
événement (probabilités), 443
événement certain (probabilités), 443
événement impossible (probabilités), 443
événement élémentaire (probabilités), 443
événements incompatibles (probabilités), 443