



Maths ▶ Analyse ▶ Déivation

Maths ▶ Analyse ▶ Taylor

## Taylor-Lagrange

Théorème de Taylor-Lagrange, et conditions d'application.

---

Soit  $f : [a, b] \rightarrow \mathbb{R}$ ,  $C^n$  sur  $[a, b]$  et  $D^{n+1}$  sur  $]a, b[$

Il existe  $c \in ]a, b[$  tel que

$$f(b) = \sum_{k=0}^n f^{(k)}(a) \frac{(b-a)^k}{k!}$$

$$+ f^{(n+1)}(c) \frac{(b-a)^{n+1}}{(n+1)!}$$

Maths ▶ Analyse ▶ Intégration

Maths ▶ Analyse ▶ Taylor

## Taylor reste intégrale

Théorème de Taylor reste intégrale, et conditions d'application.

---

Soit  $f : [a, b] \rightarrow \mathbb{R}, C^{n+1}$

$$f(b) = \sum_{k=0}^n f^{(k)}(a) \frac{(b-a)^k}{k!} + \int_a^b f^{(n+1)}(t) \frac{(b-t)^n}{n!} dt$$

Maths ▶ Analyse ▶ Réels

Maths ▶ Analyse ▶ Complexes

## Inégalité Triangulaire

Inégalité triangulaire première  
et deuxième forme.

---

Soit  $a, b \in \mathbb{C}$

$$|a + b| \leq |a| + |b|$$

$$||a| - |b|| \leq |a - b| \leq |a| + |b|$$

## Formule de Moivre

Formule de Moivre.

---

Soit  $\theta \in \mathbb{R}$

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

## Formules d'addition trigonométrique

Formules d'additions  
trigonométriques.

---

Soient  $\theta, \varphi \in \mathbb{R}$

$$\cos(\theta + \varphi) = \cos \theta \cos \varphi - \sin \theta \sin \varphi$$

$$\sin(\theta + \varphi) = \cos \theta \sin \varphi + \sin \theta \cos \varphi$$

$$\tan(\theta + \varphi) = \frac{\tan \theta + \tan \varphi}{1 - \tan \theta \tan \varphi}$$

Maths ▶ Analyse ▶ Complexes  
Maths ▶ Trigonométrie ▶  
Euclidienne

# Formules de duplication trigonométrique

Formules de duplication trigonométriques.

---

Soit  $\theta \in \mathbb{R}$

$$\cos(2\theta) = \cos^2 \theta - \sin^2 \theta$$

$$\sin(2\theta) = 2 \cos \theta \sin \theta$$

$$\tan(2\theta) = \frac{2 \tan \theta}{1 - \tan^2 \theta}$$

# Formules de linéarisation trigonométrique

Formules de linéarisation trigonométriques.

---

Soient  $a, b \in \mathbb{R}$

$$\cos a \cos b = \frac{1}{2}[\cos(a + b) + \cos(a - b)]$$

$$\sin a \sin b = \frac{1}{2}[\cos(a - b) - \cos(a + b)]$$

$$\cos a \sin b = \frac{1}{2}[\sin(a + b) - \sin(a - b)]$$

Maths ▶ Analyse ▶ Complexes  
Maths ▶ Trigonométrie ▶  
Euclidienne

# Formules de factorisation trigonométrique

Formules de factorisation trigonométriques.

---

Soient  $p, q \in \mathbb{R}$

$$\cos p + \cos q = 2 \cos\left(\frac{p+q}{2}\right) \cos\left(\frac{p-q}{2}\right)$$

$$\cos p - \cos q = -2 \sin\left(\frac{p+q}{2}\right) \sin\left(\frac{p-q}{2}\right)$$

$$\sin p + \sin q = 2 \sin\left(\frac{p+q}{2}\right) \cos\left(\frac{p-q}{2}\right)$$

Maths ▶ Analyse ▶ Complexes  
Maths ▶ Trigonométrie ▶  
Euclidienne

## Formules en tangente de theta sur deux

Formules en  $\tan \frac{\theta}{2}$ .

---

Soit  $\theta \in \mathbb{R}$

$$\cos \theta = \frac{1 - \tan^2 \frac{\theta}{2}}{1 + \tan^2 \frac{\theta}{2}}$$

$$\sin \theta = \frac{2 \tan \frac{\theta}{2}}{1 + \tan^2 \frac{\theta}{2}}$$

$$\tan \theta = \frac{2 \tan \frac{\theta}{2}}{1 - \tan^2 \frac{\theta}{2}}$$

# Formules de parité et périodicité trigonométriques

Formules de parité et périodicité trigonométriques.

---

Soit  $\theta \in \mathbb{R}$

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

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

$$\cos(\pi + \theta) = -\cos \theta$$

$$\sin(\pi + \theta) = -\sin \theta$$

# Formules de somme d'entiers consécutifs

Forme explicites des sommes suivantes :

$$\sum_{k=1}^n k = ?$$

$$\sum_{k=1}^n k^2 = ?$$

$$\sum_{k=1}^n k^3 = ?$$

---

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

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

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

## Formule de newton

Soit  $n \in \mathbb{N}$ ,  $x, a, b \in \mathbb{C}$

$$x^n - 1 = ?$$

$$a^n - b^n = ?$$

---

$$x^n - 1 = (x - 1) \sum_{k=0}^{n-1} x^k$$

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

# Formules sur les coéfficients binomiaux

Soit  $k, n, p \in \mathbb{N}$

$$\binom{n}{0} = ? \quad \binom{n}{n} = ?$$

$$\sum_{k=0}^n \binom{n}{k} = ? \quad k \binom{n}{k} = ?$$

$$\binom{n}{n-k} = ? \quad \binom{k}{p} \binom{n}{k} = ?$$

$$\binom{n}{k} + \binom{n}{k+1} = ?$$

Soit  $k, n, p \in \mathbb{N}$

$$\binom{n}{0} = \binom{n}{n} = 1$$

$$\sum_{k=0}^n \binom{n}{k} = 2^n$$

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

$$k \binom{n}{k} = n \binom{n-1}{k-1}$$

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

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

# Formule du crible

Formule du crible : soit  $A_1, \dots, A_n \subseteq E$

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


---

Soit  $A_1, \dots, A_n \subseteq E$

$$\begin{aligned}
 \left| \bigcup_{k=1}^n A_k \right| &= |A_1| + |A_2| + \dots + |A_n| \\
 &\quad - |A_1 \cap A_2| - \dots - |A_{n-1} \cap A_n| \\
 &\quad + |A_1 \cap A_2 \cap A_3| + \dots + |A_{n-2} \cap A_{n-1} \cap A_n| \\
 &\quad \vdots \\
 &\quad + (-1)^n |A_1 \cap A_2 \cap \dots \cap A_n|
 \end{aligned}$$

$$= \sum_{k=1}^n (-1)^{k+1} \sum_{1 \leq i_1 < \dots < i_k \leq n} \left| \bigcap_{j=1}^k A_{i_j} \right|$$

# Majorant, borne supérieure, élément maximale

Soit  $(E, \leq)$  un ensemble ordonné et  $A \subseteq E$ , définitions de

- Majorant
  - Maximum
  - Borne supérieure
  - Élément maximale
- 

Soit  $(E, \leq)$  un ensemble ordonné et  $A \subseteq E$ .

**Majorant**  $M \in E$  est un majorant de  $A$  si  $\forall x \in A, x \leq M$

**Maximum**  $M$  est le maximum de  $A$  si  $M$  est un majorant de  $A$  et  $M \in A$ . S'il existe il est unique.

**Borne supérieure**  $B$  est la borne supérieure de  $A$  si  $B$  est le plus petit majorant de  $A$  :  $\forall M \in E, (\forall x \in A, x \leq M) \Rightarrow B \leq M$ . Si elle existe elle est unique.

**Élément maximale**  $M$  est un élément maximale de  $A$  si  $M$  n'est plus petit que personne :  $\nexists x \in A, M \leq x$ . Dans le cas d'un ensemble totalement ordonné, seul un maximum est élément maximale, dans le cas d'un ensemble non totalement ordonné, il peut en exister plusieurs.

## EDL d'ordre 1

Soit  $a, b \in \mathbb{C}$ ,  $c(x)$  et  $C(x)$  tel que  $C'(x) = c(x)$ .

$$(E_1) : \quad y' = ay + b$$

$$(E_2) : \quad y' = a(x)y$$

---

Les solutions  $S_1$  et  $S_2$  de  $(E_1)$  et  $(E_2)$  sont

$$S_1 = \left\{ x \mapsto \lambda e^{ax} - \frac{b}{a}, \lambda \in \mathbb{R} \right\}$$

$$S_2 = \left\{ x \mapsto \lambda e^{A(x)}, \lambda \in \mathbb{R} \right\}$$

# Méthode de séparation des variables

Soit  $a(x) \in D^1$

$$\frac{dy}{dx} = a(x)y$$

$$y(x) = ?$$


---

Soient  $a(x) \in D^1$  et  $A(x)$  une primitive de  $a(x)$ .

$$\frac{dy}{dx} = a(x)y$$

$$\frac{dy}{y} = a(x) dx$$

$$\int_{y_0}^y \frac{dy}{y} = \int_{x_0}^x a(x) dx$$

$$\ln y - \ln y_0 = A(x) - A(x_0)$$

$$y = \underbrace{y_0 e^{-A(x_0)}}_{\lambda} e^{A(x)}$$

# Méthode de variation de la constante

Soient  $a(x), b(x) : \mathbb{R} \rightarrow \mathbb{R}$  et  $A(x)$  une primitive de  $a(x)$ .

$$y' = a(x)y + b(x)$$

$$f_h : \quad y(x) = \lambda e^{A(x)}$$

Trouver  $f_p$ , solution particulière par la variation de la constante.

---

Soient  $a(x), b(x) : \mathbb{R} \rightarrow \mathbb{R}$  et  $A(x)$  une primitive de  $a(x)$ .

$$y' = a(x)y + b(x)$$

$$f_h : \quad y(x) = \lambda e^{A(x)}$$

On fait varier la constante :  $\lambda \rightarrow \lambda(x)$  :

$$f_p(x) = \lambda(x)e^{A(x)}$$

$$f_{p'}(x) = a(x)f_{p(x)} + b(x)$$

$$= \lambda'(x)e^{A(x)} + \lambda(x)a(x)e^{A(x)}$$

$$= \lambda(x)a(x)e^{A(x)} + b(x)$$

$$\lambda'(x) = b(x)e^{-A(x)}$$

$$\lambda(x) = \int b(x)e^{-A(x)} dx$$

## EDL d'ordre 2

Soient  $a, b, c \in \mathbb{C}$ , résolution de l'équation homogène :

$$ay'' + by' + cy = 0$$


---

Soient  $a, b, c \in \mathbb{C}$

$$ay'' + by' + cy = 0$$

On appelle équation caractéristique

$$(EC) : az^2 + bz + c = 0$$

- Si  $\Delta > 0$ , soit  $r_1, r_2$  les racines (réelles) de  $(EC)$

$$f_{h(x)} = \lambda e^{r_1 x} + \mu e^{r_2 x}, \quad \lambda, \mu \in \mathbb{R}$$

- Si  $\Delta = 0$ , soit  $r$  la racine double de  $(EC)$

$$f_{h(x)} = (\lambda + \mu x)e^{rx}, \quad \lambda, \mu \in \mathbb{R}$$

- Si  $\Delta < 0$ , soit  $a + i\beta$  et  $a - i\beta$  les racines complexes de  $(EC)$

$$f_{h(x)} = e^{ax}(\lambda \cos(\beta x) + \mu \sin(\beta x))$$

## Axiomes d'un groupe

Soit  $G$  un ensemble muni d'une opération interne  $*$ , quels axiomes pour que  $(G, *)$  ait une structure de groupe ?

---

Soit  $G$  un ensemble et  $*$  une opération interne,  $(G, *)$  forme un groupe si

i) Associativité :

$$\forall x, y, z \in G, x * (y * z) = (x * y) * z$$

ii) Existence d'un neutre :

$$\exists e \in G, \forall x \in G, x * e = e * x = x$$

iii) Existence d'inverse :

$$\forall x \in G, \exists y \in G, x * y = y * x = e$$

# Vocabulaire d'ensemble structuré

Définitions du vocabulaire suivant

- Magma
- Semi-groupe
- Monoïde
- Groupe

Ensemble	Loi interne	Associative	Neutre	Inverse	Nom
x	x				Magma
x	x	x			Semi-groupe
x	x	x	x		Monoïde
x	x	x	x	x	Groupe

## Axiomes d'un sous-groupe

Soit  $(G, *)$  un groupe, quels axiome pour que  $H \subseteq G$  soit un sous-groupe ?

---

Soit  $(G, *)$  un groupe et  $H \subseteq G$ ,  $H$  est un sous-groupe de  $G$  si

i) Présence du neutre :

$$e \in H$$

ii) Stable par  $*$  :

$$\forall x, y \in H, x * y \in H$$

iii) Stable par inverse :

$$\forall x \in H, x^{-1} \in H$$

## Théorème de Lagrange

Énoncer le théorème de Lagrange sur les groupes.

---

Soit  $(G, \cdot)$  un groupe fini et  $H$  un sous-groupe de  $G$

$$|H| \mid |G|$$

# Démonstration du Théorème de Lagrange

## Démonstration du théorème de Lagrange

---

Soit  $(G, \cdot)$  un groupe fini et  $H$  un sous-groupe.

- Relation quotienté par  $H$  :  $x \mathcal{R} y$  si  $yx^{-1} \in H$  (relation d'équivalence). On note  $G/H$  l'ensemble des classes d'équivalences.
- Soit  $x \in G$ ,  $\bar{x}$  sa classe d'équivalence pour  $\mathcal{R}$ .  $\bar{x} = Hx = \{hx, h \in H\}$ .

Par double inclusion :

- $Hx \subseteq \bar{x}$  : Soit  $y \in Hx$ ,  $y = hx$  avec  $h \in H$ , donc  $yx^{-1} = h \in H$  d'où  $y \mathcal{R} x$  et  $y \in \bar{x}$ .
- $\bar{x} \subseteq Hx$  : Soit  $y \in \bar{x}$ ,  $yx^{-1} = h \in H$ , donc  $y = hx \in Hx$ .
- Donc  $\forall x \in G$ ,  $\bar{x} = Hx \simeq H$  d'où  $|\bar{x}| = |H|$ .
- Enfin par le lemme du berger :  $|G/H| = \frac{|G|}{|H|}$  et donc  $|H| \mid |G|$ .

## Relation de cardinal pour un morphisme de groupe

Soient  $(G_1, +)$ ,  $(G_2, \cdot)$  des groupes et  $\varphi : G_1 \rightarrow G_2$  un morphisme, avec  $G_1$  fini. Que peut on dire de  $|G_1|$  ?

---

Soient  $(G_1, +)$ ,  $(G_2, \cdot)$  des groupes et  $\varphi : G_1 \rightarrow G_2$  un morphisme, avec  $G_1$  fini.

$$|G_1| = |\ker \varphi| \cdot |\text{im } \varphi|$$

## Axiomes d'un anneau

Soit  $A$  muni de deux opérations internes  $+$  et  $\cdot$ , quels axiomes pour que  $(A, +, \cdot)$  soit un anneau ?

---

$(A, +, \cdot)$  est un anneau si :

- i)  $(A, +)$  est un groupe abélien
  - a) Associativité de  $+$
  - b) Existence d'un neutre additif ( $0_A$ )
  - c) Existence d'opposés ( $-x$ )
  - d) Commutativité de  $+$
- ii) Associativité de  $\cdot$
- iii) Existence d'un neutre multiplicatif ( $1_A$ )
- iv) Distributivité de  $\cdot$  sur  $+$

$$x(y + z) = xy + xz$$

$$(x + y)z = xz + yz$$

## Diviseur de zéro

Définition de diviseur de 0 dans un anneau.

---

Soit  $(A, +, \cdot)$  un anneau,  $x \in A$  est dit diviseur de 0 (à gauche) si  $x \neq 0$  et  $\exists y \neq 0, xy = 0$

## Intégrité d'un anneau

Définition d'un anneau intègre.

---

Un anneau  $(A, +, \cdot)$  est dit intègre si

- $A$  est commutatif
- $A$  n'admet aucun diviseur de 0

## Groupe des inversibles

Définition de groupe des inversibles d'un anneau.

---

Le groupe des inversibles d'un anneau  $(A, +, \cdot)$ , est le groupe  $(A^\times, \cdot)$ .

## Idéal d'un anneau

Définition d'un idéal d'un anneau, propriétés élémentaires.

---

Soit  $(A, +, \cdot)$  un anneau et  $I \subseteq A$ ,  $I$  est un idéal de  $A$  si

- $I$  est un sous-groupe additif de  $A$
- $I$  est stable par produit externe :  $\forall x \in I, \forall a \in A, ax \in I$

Propriétés :

- Si  $1 \in I$  idéal de  $A$ , alors  $I = A$ .
- Plus généralement s'il existe  $x \in I$  inversible,  $I = A$ .
- Une intersection quelconque d'idéaux est un idéal.
- Une somme finie d'idéaux est un idéal.
- Si  $\varphi : A_1 \rightarrow A_2$  un morphisme d'anneau avec  $A_1$  commutatif,  $\ker \varphi$  est un idéal de  $A_1$ .
- Pour tout  $b \in A$ ,  $bA$  est un idéal de  $A$ .
- Un idéal engendré par un ensemble est le plus petit idéal le contenant, dans le cas d'un singleton  $\{a\} \subset A$ , il s'agit de  $aA$ .

## Axiomes d'un corps

Soit  $K$  muni de deux opérations internes  $+$  et  $\cdot$ , quels axiomes pour que  $(K, +, \cdot)$  soit un corps ?

---

$(K, +, \cdot)$  est un corps si :

- i)  $(K, +)$  est un groupe abélien
  - a) Associativité de  $+$
  - b) Existence d'un neutre additif ( $0$ )
  - c) Existence d'opposés ( $-x$ )
  - d) Commutativité de  $+$
- ii) Associativité de  $\cdot$
- iii) Commutativité de  $\cdot$
- iv) Existence d'un neutre multiplicatif ( $1$ )
- v) Distributivité de  $\cdot$  sur  $+$
- vi) Existence d'inverses (sauf pour  $0$ )

$$\forall x \in K \setminus \{0\}, \exists x^{-1} \in K$$

$$xx^{-1} = x^{-1}x = 1$$

## **Corps gauche, anneau à division**

Qu'est-ce qu'un “corps gauche” ou “anneau à division” ?

---

Un corps gauche ou anneau à division est un anneau non commutatif dont tous les éléments sont inversible sauf 0. C'est un corps dont le produit n'est pas commutatif.

## Axiomes d'un sous-corps

Soit  $(K, +, \times)$  un corps, axiomes pour que  $L \subseteq K$  soit un sous-corps ?

---

$(K, +, \times)$  un corps,  $L \subseteq K$  est un sous-corps si :

- i)  $0 \in L$
- ii)  $1 \in L$
- iii) Stable par  $+$
- iv) Stable par  $-$  ou stable par opposé
- v) Stable par  $\times$
- vi) Stable par  $\div$  ou stable par inverse

## Primalité de la caractéristique d'un corps

Si  $(K, +, \cdot)$  est un corps de caractéristique non nulle, que peut-on dire sur celle ci ?

---

$(K, +, \cdot)$  un corps, notons  $p$  sa caractéristique, si  $p \neq 0$  alors  $p$  est premier

Démonstration:

Notons  $p = ab$  avec  $a, b \in \mathbb{N}$

$$\begin{aligned} \left( \sum_{k=1}^a 1 \right) \left( \sum_{k=1}^b 1 \right) &= \sum_{k=1}^a \sum_{k=1}^b 1 \\ &= \sum_{k=1}^{ab=p} 1 \\ &= 0 \end{aligned}$$

Or un corps n'admet pas de diviseurs de 0, donc  $\sum_{k=1}^a 1 = 0$  ou  $\sum_{k=1}^b 1 = 0$ , d'où

$$\text{ou } \begin{cases} a = p, b = 1 \\ p = b, a = 1 \end{cases}$$

Donc  $p$  est premier.

## Corps des fractions

Définition du corps des fractions d'un anneau intègre.

$(A, +', \cdot)$  un anneau intègre.

- Soit  $(a, b), (c, d) \in A \times A \setminus \{0\}$ , on définit la relation d'équivalence suivante :

$$(a, b) \mathcal{R} (d, c) \text{ si } ad = bc$$

- On note  $\frac{a}{b}$  la classe d'équivalence de  $(a, b)$ .
- On définit les opérations  $+$ ,  $\times$  sur les fractions

$$\frac{a}{b} + \frac{c}{d} = \frac{ad +' cb}{bd}$$

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

Le corps des fractions de  $A$  est le corps

$$(A \times A \setminus \{0\}, +, \times)$$

## Théorème de Gauss

Théorème de Gauss.

---

Soit  $a, b, c \in \mathbb{N}$ , si  $a \mid bc$  et  $a \wedge b = 1$  alors  $a \mid c$

# Équations diophantiennes

Résolutions d'une équation de la forme  $ax + by = c$  dans  $\mathbb{Z}$ .

Soit  $a, b, c \in \mathbb{Z}$

$$(E) : ax + by = c$$

- **Solution homogène :** On cherche un couple  $(u, v) \in \mathbb{Z}^2$  (Bézout) tel que

$$au + bv = 0$$

- **Solution particulière :** il en existe si

$$a \wedge b \mid c$$

- **Les solutions sont**

$$S = \begin{cases} x = x_p - kb' \\ y = y_p + ka' \end{cases}$$

avec  $(x_p, y_p)$  solution particulière

$$\text{et } a' = \frac{a}{a \wedge b}, \quad b' = \frac{b}{a \wedge b}$$

# Nombres de Fermat

Que sont les nombres de Fermat, et quelques propriétés.

---

Le  $n$ -ème nombre de Fermat est

$$F_n = 2^{2^n} + 1$$

Ils sont impaires et premier entre eux :

Soit  $n < m \in \mathbb{N}$ ,

$$\begin{aligned} & (2^{2^n} - 1) \cdot F_n \quad \cdots \cdot F_{n+1} \cdots F_{m-1} \\ & (2^{2^n} - 1) \cdot (2^{2^n} + 1) \quad \cdots \cdot F_{n+1} \cdots F_{m-1} \\ & \qquad \qquad \qquad (2^{2^{n+1}} - 1) \cdot F_{n+1} \cdots F_{m-1} \\ & \qquad \qquad \qquad \vdots \\ & \qquad \qquad \qquad 2^{2^m} - 1 = F_m - 2 \end{aligned}$$

Donc  $F_n \mid F_m - 2$ , d'où  $F_m \wedge F_n \mid F_m - 2$ , donc  $F_m \wedge F_n \mid 2$ , mais ils sont impaire donc premier entre eux.

## Lemme d'Euclide

Théorème du lemme d'Euclide.

---

Soit  $p \in \mathbb{P}$ ,  $a, b \in \mathbb{Z}$ ,

$$p \mid ab \Rightarrow p \mid a \text{ ou } p \mid b$$

Plus algébriquement :

$\mathbb{Z}/p\mathbb{Z}$  est un anneaux intègre :

$$ab \equiv 0 [p] \Rightarrow a \equiv 0 [p] \text{ ou } b \equiv 0 [p]$$

## Formule du nombre de diviseurs

Formule du nombre de diviseurs d'un entier.

---

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

$$\text{nombre de diviseurs} = \prod_{i=1}^k (a_k + 1)$$

# Théorème des restes chinois

Théorème des restes chinois.

---

Soit  $n, m \in \mathbb{N}^*$  premiers entre eux

- Formulation arithmétique :

$$\forall a \in \llbracket 0, m-1 \rrbracket, \forall b \in \llbracket 0, n-1 \rrbracket,$$

$$\exists! x \in \llbracket 0, nm-1 \rrbracket,$$

$$x \equiv a \pmod{m} \text{ et } x \equiv b \pmod{n}$$

- Formulation algébrique :

$$\begin{array}{ccc} \varphi : & \mathbb{Z}/mn\mathbb{Z} & \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ & x & \mapsto \begin{pmatrix} x[m] \\ x[n] \end{pmatrix} \end{array}$$

est un isomorphisme  
d'anneaux.

- Structure de preuve : injectivité par  $\ker \varphi$  + argument de cardinal.

# Petit théorème de Fermat

Petit théorème de Fermat.

---

- Première formulation :

$$\forall p \in \mathbb{P}, \forall a \in \mathbb{Z},$$

$$a \wedge p = 1 \Rightarrow a^{p-1} \equiv 1 [p]$$

- Deuxième formulation (moins forte) :

$$\forall p \in \mathbb{P}, \forall a \in \mathbb{Z},$$

$$a^p \equiv a [p]$$

- Démo : On étudie  $(\mathbb{Z}/p\mathbb{Z})^\times$  :

$$\forall a \in (\mathbb{Z}/p\mathbb{Z})^\times$$

$\text{ord}(a) \mid p - 1$  (Lagrange)

$$\text{donc } a^{p-1} \equiv 1 [p]$$

# Indicatrice d'Euler

Définition de l'indicatrice d'Euler, et propriétés.

La fonction indicatrice d'Euler est

$$\varphi : \begin{matrix} \mathbb{N}^* \rightarrow \mathbb{N} \\ n \mapsto |(\mathbb{Z}/n\mathbb{Z})^\times| \end{matrix}$$

Quelques propriétés :

$$\varphi(p) = p - 1$$

$$\varphi(p^a) = p^a - p^{a-1}$$

$$m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$$

$$\varphi(n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) = \prod_{i=1}^k (p_i^a - p_i^{a-1})$$

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

$$\sum_{d \in \text{Div}(n)} \varphi(d) = n$$

Pour se convaincre de la dernière :

$$\frac{1}{n} + \frac{2}{n} + \cdots + \frac{n}{n}$$

Sous formes irréductibles ( $p_i \wedge q_i = 1$ )

$$\frac{p_1}{q_1} + \frac{p_2}{q_2} + \cdots + \frac{p_n}{q_n}$$

Il y a  $n$  fractions, les  $q_i \in \text{Div}(n)$ , et pour chaque  $q_i$ , on a tous les  $p_i \leq q_i$ , qui sont premiers avec eux :

$$\underbrace{\sum_{d \in \text{Div}(n)}}_{\substack{\text{somme sur} \\ \text{tous les} \\ \text{dénominateur}}} \underbrace{\varphi(d)}_{\substack{\text{nombre de} \\ \text{fractions pour le} \\ \text{dénominateur } d}} = \underbrace{n}_{\substack{\text{nombre de} \\ \text{fractions}}}$$

Enfin, une généralisation du petit théorème de Fermat :

$$a \wedge n = 1 \Rightarrow a^{\varphi(n)} \equiv 1 [n]$$

# Théorème de Bézout

Énoncé et preuve du théorème de Bézout.

---

- Soient  $a, b \in \mathbb{N}$  et  $d = a \wedge b$  alors il existe  $u, v \in \mathbb{Z}$  tel que  $au + bv = d$ .
- Preuve : Soit  $I = \{au + bv, (u, v) \in \mathbb{Z}\}$

$I$  est un idéal de  $\mathbb{Z}$ , donc  $\exists d \in \mathbb{Z}, I = d\mathbb{Z}$  (principalité de  $\mathbb{Z}$ ).  
Donc  $d \mid a$  et  $d \mid b$ .

Soit  $\partial$  tel que  $\partial \mid a$  et  $\partial \mid b$ .  $\forall x \in I, \partial \mid x$ , en particulier  $\partial \mid d$  d'où  $\partial \leq d$ .

$a \wedge b = d \in I$  d'où  $\exists u, v \in \mathbb{Z}, d = au + bv$

## Propriétés diviseurs communs

Soit  $a, b \in \mathbb{Z}$

$x \mid a$  et  $x \mid b$  ssi ?

$a \mid y$  et  $b \mid y$  ssi ?

$a\mathbb{Z} + b\mathbb{Z} = ?$

$a\mathbb{Z} \cap b\mathbb{Z} = ?$

---

Soit  $a, b \in \mathbb{Z}$

$x \mid a$  et  $x \mid b$  ssi  $x \mid (a \wedge b)$

$a \mid y$  et  $b \mid y$  ssi  $m \mid (a \vee b)$

$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$

$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$

## Corps totalement ordonné

Définition d'un corps totalement ordonné.

---

Soit  $(K, +, \cdot)$  un corps et un ordre  $\leq$ .

1.  $\forall x, y, z \in K, x \leq y \Rightarrow x + z \leq y + z$
2.  $\forall x, y \in K, x \geq 0$  et  $y \geq 0 \Rightarrow xy \geq 0$

$\mathbb{R}$  et  $\mathbb{Q}$  sont ordonnés,  $\mathbb{C}$  ne l'est pas. Mais il existe un seul corps totalement ordonné (à isomorphisme près) :  $\mathbb{R}$ .

# Propriété fondamentale des réels

Propriété fondamentale des réels.

---

Toute partie non vide majoré de  $\mathbb{R}$  admet une borne sup. De même pour minoré.

On en déduit (car  $\mathbb{R}$  est totalement ordonné) que

- $x \geq 0 \Rightarrow -x \leq 0$
- Loi du signe de produit
- $x^2 \geq 0$
- $1 > 0$
- $x > 0 \Rightarrow \frac{1}{x} > 0$
- $0 < x \leq y \Rightarrow \frac{1}{x} \geq \frac{1}{y}$

## Propriété de la borne supérieure

Propriété de la borne supérieure.

---

Soit  $A \subseteq \mathbb{R}$  non vide majoré,  $S = \sup A$  ssi

1.  $\forall x \in A, x \leq S$
2.  $\forall \varepsilon > 0, \exists y \in A, s - \varepsilon < y$

## Partie convexe de $\mathbb{R}$

Définition de partie convexe.

---

Une partie convexe de  $\mathbb{R}$  est un ensemble  $C \subseteq \mathbb{R}$  tel que

$$\forall x \leq y \in C, [x, y] \subseteq C$$

Les parties convexes de  $\mathbb{R}$  sont des intervalles.

## Densité

Définition de densité.

---

Soit  $D \subseteq \mathbb{R}$ ,  $D$  est dense dans  $\mathbb{R}$  si

$$\forall a < b \in \mathbb{R}, ]a, b[ \cap D \neq \emptyset$$

$\mathbb{Q}$  est dense dans  $\mathbb{R}$ , preuve : saut de grenouille.

## Voisinage

Définition de voisinage.

---

Soit  $x \in \overline{\mathbb{R}}$ ,  $V \subseteq \mathbb{R}$  est un voisinage de  $x$  si

$$\exists \varepsilon > 0, ]x - \varepsilon, x + \varepsilon[ \subseteq V$$

On note  $\mathcal{V}(x)$  l'ensemble des voisinages de  $x$ .

# Adhérence

Définition et propriétés de l'adhérence d'un ensemble.

---

Soit  $A \subseteq \mathbb{R}$ ,  $x \in \overline{\mathbb{R}}$ ,  $x \in \mathbb{R}$  est adhérent à  $A$  si

$$\forall V \in \mathcal{V}(x), V \cap A \neq \emptyset$$

L'adhérence de  $A$  est alors

$$\begin{aligned}\text{adh}(A) &= \{x \in \mathbb{R} \mid x \text{ adhérent à } A\} \\ &= \{x \in \mathbb{R} \mid \forall \varepsilon > 0, ]x - \varepsilon, x + \varepsilon[ \cap A \neq \emptyset\}\end{aligned}$$

Propriétés :

- $A \subseteq \text{adh}(A)$
- Si  $A$  non vide borné :  
 $\{\inf A, \sup A\} \subseteq A$
- $\text{adh}(]a, b[) = [a, b]$
- $D$  est dense dans  $\mathbb{R}$  ssi  $\text{adh}(D) = \mathbb{R}$
- $\text{adh}(\text{adh}(A)) = \text{adh}(A)$

# Suites arithmético-géométriques

Formule explicite d'une suite arithmético-géométrique.

---

Soit  $a, b \in \mathbb{R}$  et  $(u_n)$  une suite tel que

$$\forall n \in \mathbb{N}, u_{n+1} = au_n + b$$

On note  $f(x) = ax + b$ , on trouve le point fixe  $w = \frac{b}{1-a}$ . Soit  $v_n = u_n - w$ .

$$\begin{aligned} v_{n+1} &= au_n + b - \underbrace{(aw + b)}_{-w} \\ &= a(u_n - w) = av_n \end{aligned}$$

$$v_n = a^n v_0$$

$$u_n = a^n(v_0 - w) + w$$

# Suites récurrentes d'ordre 2

Formule explicite d'une suite récurrente d'ordre 2.

---

Soit  $a, b \in \mathbb{R}$ ,  $(u_n)$  une suite tel que

$$u_{n+2} = au_{n+1} + bu_n$$

On résout l'équation caractéristique

$$x^2 = ax + b$$

- Deux racines  $r_1, r_2$

$$u_n = \lambda r_1^n + \mu r_2^n$$

- Racine double  $r$

$$u_n = (\lambda + \mu n)r^n$$

Avec  $\lambda, \mu \in \mathbb{R}$  déterminés par  $u_0$  et  $u_1$ .

# Caractérisation séquentielle de l'adhérence

Caractérisation séquentielle de l'adhérence et la borne supérieure.

---

Soit  $A \subseteq \mathbb{R}$ .

- Si  $(u_n)$  une suite à valeur dans  $A$  et  $u_n \rightarrow l$ , alors  $l \in \text{adh}_{\overline{\mathbb{R}}}(A)$ .
- Si  $x \in \text{adh}_{\overline{\mathbb{R}}}$ , alors il existe  $(u_n) \in A^{\mathbb{N}}$  tel que  $u_n \rightarrow x$ .

Ainsi

$$\begin{aligned} \text{adh}(A) \\ = \{x \in \mathbb{R} \mid \exists (u_n) \in A^{\mathbb{N}}, u_n \rightarrow x\} \end{aligned}$$

Et  $S = \sup A$  existe si  $A$  non vide majoré par  $S$  et il existe  $(u_n) \in A^{\mathbb{N}}$  tel que  $u_n \rightarrow S$ .

# Suites adjacentes, emboitées

Définition et théorème des suites adjacentes et emboitées.

---

- **Adjacentes :**

Deux suites  $(a_n)$  et  $(b_n)$  sont adjacentes si

$$(a_n) \nearrow, \quad (b_n) \searrow \\ \text{et } \lim_{n \rightarrow \infty} (b_n - a_n) = 0$$

Théorème :  $(a_n)$  et  $(b_n)$  et  
 $\lim a_n = \lim b_n$ .

Preuve : Théorème de la limite croissante pour la convergence.

- **Emboitées :**

La même chose avec des segments.

Théorème :

$$\bigcap_{n=0}^{\infty} [a_n, b_n] = \{x\}$$

avec  $x = \lim a_n = \lim b_n$

# Théorème de Bolzano-Weierstrass

Théorème de Bolzano-Weierstrass et démonstration.

Toute suite réelle bornée admet une sous-suite convergente. Dans  $\mathbb{R}^n$  (et  $\mathbb{C}$ ), il suffit d'être borné en norme ou module.

Preuve :

Soit  $(u_n)$  une suite bornée par  $a_0$  et  $b_0$ , notons  $A = \{u_n, n \in \mathbb{N}\}$ . Par récurrence :

- Ini :  $|[a_0, b_0] \cap A| = \infty$
- Héré : On suppose  $|[a_n, b_n] \cap A| = \infty$ , et on coupe en  $m = \frac{a_n + b_n}{2}$  :
  - Si  $|[a_n, m] \cap A| = \infty$ ,  $\begin{cases} a_{n+1} = a_n \\ b_{n+1} = m \end{cases}$
  - Si  $|[m, b_n] \cap A| = \infty$ ,  $\begin{cases} a_{n+1} = m \\ b_{n+1} = b_n \end{cases}$

Par le théorème des suites emboitées :

$$\exists l \in [a_0, b_0], \bigcap_{n=0}^{\infty} [a_n, b_n] = \{l\}$$

Soit  $\varphi$  une extractrice, par récurrence :

- Ini :  $\varphi(0) = 0$
- Héré :  $[a_{n+1}, b_{n+1}]$  est infini, donc il existe  $m > \varphi(n)$  tel que  $u_m \in [a_{n+1}, b_{n+1}]$ . On prend  $\varphi(n+1) = m$ .

Donc  $a_n \leq u_{\varphi(n)} \leq b_n$  d'où  $\lim u_{\varphi(n)} = l$ .

## Moyennes de Cesàro

Définition, propriétés des moyennes de Cesàro.

---

Soit  $(u_n)$  une suite. La suite des moyennes de Cesàro de  $u_n$  est

$$\sigma_n = \frac{a_1 + a_2 + \cdots + a_n}{n}$$

Si  $u_n \rightarrow l \in \overline{\mathbb{R}}$ , alors  $\sigma_n \rightarrow l$ .

Preuve :

- / fini : Découpage pour  $n < N$  et  $n \geq N$  et inégalité triangulaire.
- / infini : majoration.

# Manipulations asymptotiques

Manipulations asymptotiques élémentaires.

---

- $\sim$  : relation d'équivalence
  - produit, quotient, exposant
  - **pas** de somme, de composition, ...
- $o(1) \Leftrightarrow$  tend vers 0,  $O(1) \Leftrightarrow$  borné
- $O$  et  $o$  transitifs
- $O$  et  $o$  mangent les constantes
- $u_n \sim v_n$  ssi  $u_n = v_n + o(v_n)$
- Si  $u_n \sim v_n$  (ou  $O, o$ ), alors  $u_{\varphi(n)} \sim v_{\varphi(n)}$  (ou  $O, o$ )
- $o$  et  $\sim$  sont des cas particuliers de  $O$ .

# Comparaison asymptotiques usuelles

Comparaison asymptotiques usuelles, stirling

---

Soit  $k \in \mathbb{R}_+^*, q > 1$ , au voisinage de l'infini :

$$n^k = o(q^n)$$

$$q^n = o(n!)$$

$$n! \sim \sqrt{2\pi n} \frac{n^n}{e^n}$$

$$\ln(n!) \sim n \ln n$$

$$\sum_{k=1}^n \frac{1}{n} = \ln n + \gamma + o(1)$$

## Fonctions K-Lipschitziennes

Qu'est qu'une fonction  $K$ -lipschitzienne

---

Une fonction  $f : A \rightarrow \mathbb{R}$  est  $K$ -lipschitzienne si

$$\forall x, y \in A, |f(x) - f(y)| \leq K|x - y|$$

Lipschitz sur un segment implique uniformement continue.

## Théorème des bornes atteintes

Théorème des bornes atteintes et démonstration.

---

Si  $f$  est  $C^0([a, b])$ , alors  $f$  est bornée et atteint ses bornes.

Preuve :

Notons  $M = \sup f$ , quitte à avoir  $M \in \overline{\mathbb{R}}$ .  $M \in \text{adh}_{\overline{\mathbb{R}}}(f([a, b]))$ , donc il existe une suite  $(x_n)$  à valeur dans  $[a, b]$  tel que  $f(x_n) \rightarrow M$ .

Par Bolzano-Weierstrass, il existe  $\varphi$  tel que  $x_{\varphi(n)} \rightarrow l$  avec  $l \in [a, b]$  et donc nécessairement  $M \in \mathbb{R}$ .

## Théorème de Heine

Énoncé et démonstration du théorème de Heine.

---

Toute fonction continue sur un segment est uniformément continue.

Preuve :

Soit  $f \in C^0([a, b])$ . Supposons par l'absurde que  $f$  n'est pas uniformément continue.

$$\exists \varepsilon > 0, \forall \delta > 0, \exists x, y \in [a, b]$$

$$|x - y| < \delta \text{ et } |f(x) - f(y)| \geq \varepsilon$$

On prend  $(x_n), (y_n) \in [a, b]^{\mathbb{N}}$  tel que

$$\forall n \in \mathbb{N}, |x_n - y_n| < \frac{1}{n}$$

$$|f(x_n) - f(y_n)| \geq \varepsilon$$

Ces suites sont bornées donc par Bolzano-Weierstrass, il existe une extractrice  $\varphi$  tel que  $x_{\varphi(n)} \rightarrow l \in [a, b]$ .

Or  $|x_{\varphi(n)} - y_{\varphi(n)}| \rightarrow 0$  donc  $y_{\varphi(n)} \rightarrow l$ .

Mais par continuité de  $f$ ,

$$\begin{aligned} \lim_{n \rightarrow \infty} f(x_{\varphi(n)}) &= \lim_{n \rightarrow \infty} f(y_{\varphi(n)}) \\ &= f(l) \end{aligned}$$

Donc il existe  $N \in \mathbb{N}$  tel que

$$|f(x_{\varphi(n)}) - f(y_{\varphi(n)})| < \varepsilon$$

Qui est absurde.

# Fonctions trigonométriques réciproques

Domaine de définition et dérivées des fonctions trigonométrique réciproques.

---

$$\begin{aligned} \arccos &: [-1, 1] \rightarrow [0, \pi] \\ \arccos' &: ]-1, 1[ \rightarrow [-1, -\infty[ \\ x &\mapsto -\frac{1}{\sqrt{1-x^2}} \end{aligned}$$

$$\begin{aligned} \arcsin &: [-1, 1] \rightarrow [-\frac{\pi}{2}, \frac{\pi}{2}] \\ \arcsin' &: ]-1, 1[ \rightarrow [1, +\infty[ \\ x &\mapsto \frac{1}{\sqrt{1-x^2}} \end{aligned}$$

$$\begin{aligned} \arctan &: \mathbb{R} \rightarrow ]-\frac{\pi}{2}, \frac{\pi}{2}[ \\ \arctan' &: \mathbb{R} \rightarrow ]0, 1] \\ x &\mapsto \frac{1}{1+x^2} \end{aligned}$$

# Propriété des extrémum locaux

Que peut on dire si  $f : I \rightarrow \mathbb{R}$  est dérivable et admet un extrémum local en  $a \in I \setminus \{\inf I, \sup I\}$ .

---

Soit  $f : I \rightarrow \mathbb{R}$  dérivable qui admet un extrémum local en  $a$ , un point intérieur à  $I$ , alors  $f'(a) = 0$ .

Preuve : par hypothèse, pour un maximum (un minimum se traite de même)

$$\exists V \in \mathcal{V}(a), \forall x \in V, f(x) \leq f(a)$$

Étudions

$$\lim_{x \rightarrow a} \frac{f(x) - f(a)}{x - a}$$

Si  $x < a$  :

$$\frac{\overbrace{f(x) - f(a)}^{\leq 0}}{\underbrace{x - a}_{< 0}} \geq 0 \quad \frac{\overbrace{f(x) - f(a)}^{\leq 0}}{\underbrace{x - a}_{> 0}} \leq 0$$

Si  $x > a$  :

Donc  $f'(a) = 0$  (les deux limites sont égales par la dérivabilité de  $f$  en  $a$ ).

# Théorème de Rolle, théorème des acroissements finis

Énoncé et preuve des théorèmes de Rolle et des acroissements finis.

---

Soit  $f \in C^0([a, b])$  dérivable sur  $]a, b[$

**Rolle** Si  $f(a) = f(b)$ , alors

$$\exists c \in ]a, b[, f'(c) = 0$$

**TAF**

$$\exists c \in ]a, b[, f'(c) = \frac{f(b) - f(a)}{b - a}$$

Preuve :

- Rolle : théorème des bornes atteintes, propriétés des extrémum locaux avec une disjonction de cas si les extrémums sont aux bornes.
- TAF : Rolle en pente, on corrige par la pente pour se ramener à Rolle.

# Inégalité des accroissements finis et de Taylor-Lagrange

Inégalité des accroissements finis et de Taylor-Lagrange.

---

## Inégalité des accroissements finis

Soit  $f : I \rightarrow \mathbb{R}$  dérivable et  $a \in I$ , pour tout  $x \in I$

$$|f(x) - f(a)| \leq \sup_{[a,x]} |f'| \cdot |x - a|$$

## Inégalité de Taylor-Lagrange

Soit  $f : I \rightarrow \mathbb{R}$  qui est  $D^{n+1}$  et  $a \in I$ , pour tout  $x \in I$

$$\left| f(x) - \sum_{k=0}^n f^{(k)}(a) \frac{(x-a)^k}{k!} \right| \leq \sup_{[a,x]} |f^{(n+1)}| \cdot \frac{|x-a|^{n+1}}{(n+1)!}$$

Preuve :

On prend les théorème et on majore le paramètre.

# Intégration de l'inverse d'un trinôme

Méthode d'intégration pour l'inverse d'un trinôme du second degré.

On prend  $ax^2 + bx + c$  un trinôme du second degré, on vas intégrer  $\frac{1}{ax^2+bx+c}$ .

- $\Delta > 0$  : décomposition en éléments simples
- $\Delta = 0$  :

$$\int \frac{dx}{ax^2 + bx + c} = \int \frac{dx}{a(x - r)^2}$$

$$= -\frac{1}{a(x - r)}$$

- $\Delta < 0$  : on passe à la forme canonique

$$ax^2 + bx + c = a \left[ \left( x + \frac{b}{2a} \right)^2 + \frac{|\Delta|}{4a^2} \right]$$

Et on se ramène à  $\int \frac{du}{u^2+1} = \arctan u$ .

$$\int \frac{1}{ax^2 + bx + c} = \frac{2}{\sqrt{|\Delta|}} \arctan \left( \frac{2ax + b}{\sqrt{|\Delta|}} \right)$$

# Développements limités

$$\frac{1}{1-x} = ? \quad \text{ch}(x) = ?$$

$$\frac{1}{1+x} = ? \quad (1+x)^a = ?$$

$$\ln(1+x) = ? \quad \frac{1}{\sqrt{1-x^2}} = ?$$

$$e^x = ? \quad \arcsin(x) = ?$$

$$\cos(x) = ? \quad \arccos(x) = ?$$

$$\sin(x) = ? \quad \arctan(x) = ?$$

$$\tan(x) = ?$$


---

$$\frac{1}{1-x} = 1 + x + x^2 + o(x^2)$$

$$= \sum_{k=0}^n x^k + o(x^n)$$

$$\frac{1}{1+x} = 1 - x + x^2 + o(x^2)$$

$$= \sum_{k=0}^n (-x)^k + o(x^n)$$

$$\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} + o(x^3)$$

$$= \sum_{k=0}^n \frac{(-x)^{k+1}}{k+1} + o(x^n)$$

$$\cos(x) = 1 - \frac{x^2}{2} + \frac{x^4}{24} + o(x^5)$$

$$= \sum_{k=0}^n \frac{(-1)^k x^{2k}}{(2k)!} + o(x^{2k})$$

$$\sin(x) = x - \frac{x^3}{6} + \frac{x^5}{120} + o(x^6)$$

$$= \sum_{k=0}^n \frac{(-1)^k x^{2k+1}}{(2k+1)!} + o(x^{2k+1})$$

$$\text{ch}(x) = 1 + \frac{x^2}{2} + \frac{x^4}{24} + o(x^5)$$

$$= \sum_{k=0}^n \frac{x^k}{k!} \prod_{p=0}^{k-1} (a-p) + o(x^n)$$

$$\frac{1}{\sqrt{1-x^2}} = 1 + \frac{1}{2}x^2 + \frac{3}{8}x^4 + o(x^4)$$

$$= \sum_{k=1}^n \frac{1}{2^{2k}} \binom{2k}{k} x^{2k} + o(x^{2k})$$

$$\arcsin(x) = x + \frac{1}{2} \frac{x^3}{3} + \frac{3}{8} \frac{x^5}{5} + o(x^5)$$

$$= \sum_{k=1}^n \frac{\binom{2k}{k} x^{2k+1}}{2^{2k} (2k+1)} + o(x^{2k+1})$$

$$\arccos(x) = -x - \frac{1}{2} \frac{x^3}{3} - \frac{3}{8} \frac{x^5}{5} + o(x^5)$$

$$= \sum_{k=1}^n -\frac{\binom{2k}{k} x^{2k+1}}{2^{2k} (2k+1)} + o(x^{2k+1})$$

$$\arctan(x) = x - \frac{x^3}{3} + \frac{x^5}{5} + o(x^5)$$

$$= \sum_{k=1}^n \frac{(-1)^k x^{2k+1}}{2k+1} + o(x^{2k+1})$$

$$\tan(x) = x + \frac{1}{3}x^3 + \frac{2}{15}x^5 + \frac{17}{315}x^7 + o(x^8)$$

## Étude local et asymptotique de fonctions

Méthode pour étudier le comportement local et asymptotique d'une fonction.

**Local** au voisinage de  $a \in \mathbb{R}$

- Équivalent en  $a$  : premier terme
- Tangente en  $a$  :  $\text{DL}_1(a)$
- Signe de  $f$  en  $a$  : premier terme non nul.
- Position relative par rapport à la tangente : signe du premier terme non nul après l'ordre 1.

**Asymptotique** au voisinage de  $\pm\infty$

- Asymptote oblique :  $\text{DL}_1(\pm\infty)$
- Position relative : signe du terme suivant.

Rappelle :

$f$  admet une asymptote oblique d'équation  $ax + b$  si

$$\lim_{x \rightarrow \pm\infty} f(x) - ax - b = 0$$

# Suites récurrentes

Méthode pour les suites récurrentes de la forme  $u_{n+1} = f(u_n)$ .

---

Soit  $f$  une fonction et  $(u_n) \in \mathbb{R}^{\mathbb{N}}$  tel que  $u_{n+1} = f(u_n)$ .

1. Intervalle stable : on cherche  $I$  tel que  $f(I) \subseteq I$ .
2. Variations de  $(u_n)$ 
  - Signe de  $f(x) - x$  sur  $I$ 
    - + :  $(u_n)$  est croissante
    - - :  $(u_n)$  est décroissante
    - Sinon affiner  $I$
  - Monotonie de  $f$ 
    - Si  $f$  est croissante sur  $I$ ,  $(u_n)$  est monotone
    - Si  $f$  est décroissante sur  $I$ ,  $(u_{2n})$  et  $(u_{2n+1})$  sont monotone.
3. On montre l'existence de la limite (limite croissante)
4. On la détermine : il s'agit de l'un des points fixes de  $I$  (idéalement il n'y en a qu'un).

Dans le cas des fonctions décroissantes, on cherche les limites des deux sous-suites, points fixes de  $f \circ f$ .

# Propriétés de convexité

Définition et propriétés de convexité.

Soit  $f : I \rightarrow \mathbb{R}$ ,  $f$  est dite convexe si

$$\forall x, y \in I, \forall \lambda \in [0, 1]$$

$$f(\lambda x + (1 - \lambda)y)$$

$$\leq \lambda f(x) + (1 - \lambda)f(y)$$

Propriétés :

- Soit  $f : I \rightarrow \mathbb{R}$  convexe,

$$\forall x_1, \dots, x_n \in I$$

$$\forall \lambda_1, \dots, \lambda_n \in [0, 1], \lambda_1 + \dots + \lambda_n = 1 \Rightarrow$$

$$f\left(\sum_{i=1}^n \lambda_i x_i\right) \leq \sum_{i=1}^n \lambda_i f(x_i)$$

- Soit  $\Phi$  convexe,  $\forall f \in C^0([a, b])$

$$\Phi\left(\frac{1}{b-a} \int_a^b f(x) dx\right)$$

$$\leq \frac{1}{b-a} \int_a^b \Phi(f(x)) dx$$

- Soit  $f : I \rightarrow \mathbb{R}$ ,  $a \in I$ , on note

$$\begin{aligned} \tau_a : I \setminus \{a\} &\rightarrow \mathbb{R} \\ x &\mapsto \frac{f(x) - f(a)}{x - a} \end{aligned}$$

les taux d'acroissements en  $a$  de  $f$ .

$f$  est convexessi  $\forall a \in I$ ,  $\tau_a$  est croissante.

- Soit  $f : I \rightarrow \mathbb{R}$ , on appelle droite d'appuis en  $x_0$  de  $f$  une droite  $y = ax + b$  tel que

►  $\forall x \in I, ax + b \leq f(x)$

►  $f(x_0) = ax_0 + b$

Si  $f$  convexe,  $f$  admet des droites d'appuis en tout points.

# Théorème de caractérisation des matrices inversibles

Énoncé du théorème de caractérisation des matrices inversibles.

---

Soit  $A \in M_n(\mathbb{R})$ , les assertions suivantes sont équivalentes :

- $A$  est inversible.
- $A \stackrel{L}{\sim} I_n$ .
- $\text{rg } A = n$ .
- Le système homogène  $AX = 0$  admet une seule solution.
- $\forall Y \in \mathbb{R}^n$  le système homogène  $AX = Y$  admet au plus une solution.
- $\forall Y \in \mathbb{R}^n$  le système homogène  $AX = Y$  admet au moins une solution.

## Polynômes associés

Définition et propriétés des polynômes associés.

---

Soit  $P, Q \in \mathbb{K}[X]$ ,  $P$  et  $Q$  sont dit associé si  $P \mid Q$  et  $Q \mid P$ .

$P, Q$  sont associés ssi  $\exists \lambda \in \mathbb{K}^*, A = \lambda B$ . Toute class de polynômes associés contient un unique polynôme unitaire (à l'exception de  $\{0\}$ ).

# Propriétés des racines d'un polynôme

Propriétés des racines d'un polynôme.

Soit  $P \in \mathbb{K}[X]$ ,  $n = \deg P$

## En général

- Si  $P \neq 0$ ,  $P$  à au plus  $n$  racines (comptées avec multiplicités).
- L'unique polynôme qui à une infinité de racines est  $P = 0$ .
- Si  $Q \in \mathbb{K}_n[X]$  et  $\exists a_1, \dots, a_{n+1} \in \mathbb{K}$  tels que  $\forall k \in \llbracket 1, n+1 \rrbracket$ ,  $P(a_k) = Q(a_k)$ , alors  $P = Q$ .

## En caractéristique nulle

- $a \in \mathbb{K}$  est racine de  $P$  avec multiplicité  $m$  ssi

$$\forall k \in \llbracket 0, m-1 \rrbracket, P^{(k)}(a) = 0$$

$$\text{et } P^{(m)}(a) \neq 0$$

## Démonstration

- Si  $a_1, \dots, a_N \in \mathbb{K}$  sont des racines distinctes de  $P$ , et  $m_1, \dots, m_N \in \mathbb{N}^*$  leurs multiplicités.

Pour tout  $k \in \llbracket 1, N \rrbracket$ ,  $(X - a_k)^{m_k} \mid P$

Or pour  $i < j \in \llbracket 1, n \rrbracket$

$$(X - a_i) - (X - a_j) = a_j - a_i$$

Relation de Bézout ( $a_j - a_i$  associé à 1) donc premiers entre eux deux à deux.

D'où  $\prod_{k=1}^N (X - a_k)^{m_k} \mid P$  et  $n \geq \sum_{k=1}^N m_k$ .

- Par la propriété précédente, si  $P$  à une infinité de racine distincte il ne peut être de degré positif (ou il serait infini) donc il est nul.

- Par Taylor-Lagrange formel, pour tout  $j \in \llbracket 1, m-1 \rrbracket$

$$P = \underbrace{\sum_{k=0}^{j-1} P^{(k)}(a) \frac{(X-a)^k}{k!}}_{R_j(X) (\deg < j)} + \underbrace{\sum_{k=j}^n P^{(k)}(a) \frac{(X-a)^k}{k!}}_{(X-a)^j Q(X)}$$

D'où  $R_j$  le reste de la division euclidienne de  $P$  par  $(X - a)^j$ .

Or  $a$  est une racine de

multiplicité  $m$  ssi

$$\begin{cases} R_m = 0 \\ R_{m+1} \neq 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} \forall k \in \llbracket 0, m-1 \rrbracket, \frac{P^{(k)}(a)}{k!} = 0 \\ \exists k \in \llbracket 0, m \rrbracket, \frac{P^{(k)}(a)}{k!} \neq 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} \forall k \in \llbracket 0, m-1 \rrbracket, (P^{(k)}(a)) = 0 \\ P^{(m)}(a) \neq 0 \end{cases}$$

## Multiplicité d'une racine

Définition de multiplicité d'une racine.

---

Soit  $P \in \mathbb{K}[X]$ ,  $a \in \mathbb{K}$  une racine et  $n \in \mathbb{N}^*$ . On dit que  $a$  est de multiplicité  $n$  si (l'un ou l'autre) :

- $(X - a)^n \mid P$  mais  $(X - a)^{n+1} \nmid P$ .
- $\forall k \in \llbracket 0, n - 1 \rrbracket$ ,  $P^{(k)}(a) = 0$

# Polynômes scindés

Définition et propriétés des polynôme scindés.

---

Soit  $P \in \mathbb{K}[X]$ ,  $a_1, \dots, a_k$  ses racines et  $m_1, \dots, m_k$  leur multiplicités.

- $P$  est scindé si  $\deg P = \sum_{i=1}^k m_k$ .
- $P$  est scindé racines simples si  $P$  scindé et  $\forall i \in \llbracket 1, k \rrbracket, m_i = 1$ .

Propriétés :

- Si  $P$  est scindé racines simples sur  $\mathbb{R}$ ,  $P'$  aussi.
- Si  $P$  est scindé sur  $\mathbb{R}$ ,  $P'$  aussi.
- Tout polynôme  $P$  est scindé sur  $\mathbb{C}$  : théorème de Gauss-d'Alembert.

# Polynômes irréductibles

Définition et propriétés des polynômes irréductibles.

Soit  $P \in \mathbb{K}[X]$ ,  $P$  est dit irréductible si ses seuls diviseurs sont  $P$ , 1 et leurs associés.

1. Dans  $\mathbb{C}$ , les polynômes irréductibles sont les monômes (théorème de Gauss-d'Alembert).
2. Dans  $\mathbb{R}$ , les polynômes irréductibles sont les monômes et les polynômes de degré 2 avec  $\Delta < 0$ .
3. En général, un polynôme de degré 1 est toujours irréductible.
4. Dans  $\mathbb{K}[X]$ , un polynôme de degré 2 ou 3 est irréductible ssi il n'admet pas de racine dans  $\mathbb{K}$ .
5. Dans  $\mathbb{K}[X]$ , un polynôme de degré  $\geq 2$  ne peut être irréductible s'il admet une racine dans  $\mathbb{K}$ .
6. ( $\text{car}(\mathbb{K}) = 0$ ) Un polynôme  $P \in \mathbb{K}[X] \subset \mathbb{L}[X]$  irréductible ( $\mathbb{L}$  extension de corps de  $\mathbb{K}$ ) n'admet que des racines simples dans  $\mathbb{L}$  (et à fortiori dans  $\mathbb{K}$ ).

## Démonstration

2. Par les propriétés 3 et 4, on sait que ces polynômes sont irréductibles, montrons que ce sont les seuls.

Soit  $P \in \mathbb{R}[X]$  irréductible de degré  $\geq 2$ .

$P \in \mathbb{C}[X]$  donc on dispose de  $\lambda \in \mathbb{C} \setminus \mathbb{R}$  racine de  $P$ .

$$P(\bar{\lambda}) = \overline{P(\lambda)} = \overline{P(\lambda)} = 0$$

D'où  $(\text{car}(X - \lambda) \wedge (X - \bar{\lambda})) = 1$

$$Q = \underbrace{X^2 - 2\Re(\lambda)X + |\lambda|^2}_{\in \mathbb{R}[X]} \mid P$$

Comme  $P$  est irréductible,  $P$  et  $Q$  sont associés et  $\deg P = 2$ .

4. Soit  $P \in \mathbb{K}_3[X] \setminus \mathbb{K}_1[X]$ 
  - S'il est irréductible il n'admet pas de racine.
  - S'il n'est pas irréductible,

$$P = QR$$

- Soit  $\deg Q = 1$ ,  $Q = X - a$  et  $a$  racine de  $P$ .

- Soit  $\deg R = 1$ ,  $R = X - \beta$  et  $\beta$  racine de  $P$ .

6.  $0 \leq \deg P' \leq \deg P - 1$  et par irréductibilité de  $P$  dans  $\mathbb{K}[X]$

$$P \wedge P' = 1$$

Or le PGCD se conserve sur les extensions de corps, ils n'ont donc pas de racine communes (dans  $\mathbb{K}$  et  $\mathbb{L}$ ).

# Fonctions symétriques des racines

Définition des fonctions symétriques des racines et formules de Viete.

---

Soit  $a_1, \dots, a_n \in \mathbb{C}$  et  $k \in \llbracket 0, n \rrbracket$ , la  $k$ -ème fonction symétrique des élémentaire de  $a_1, \dots, a_n$  est

$$\sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} \prod_{j=1}^k a_{i_j}$$

On remarque que  $\sigma_0 = 1$ .

Soit  $P = a_0 + a_1X + \dots + a_nX^n$  scindé, on note  $a_1, \dots, a_n$  ses racines (non distinctes).

Formule de Viete :

$$\forall k \in \llbracket 0, n \rrbracket, \sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$$

# Polynômes de Tchebycheff

Définition et propriétés des polynômes de Tchebycheff.

Le  $n$ -ème polynôme de Tchebycheff est le polynôme tel que

$$\forall \theta \in \mathbb{R}, T_n(\cos \theta) = \cos(n\theta)$$

Propriétés :

1. Formule de récurrence :

$$T_{n+1} + T_{n-1} = 2XT_n$$

2.  $\deg T_n = n$ , coefficient dominant :  $2^{n-1}$ , sauf pour  $n = 0$ ,  $T_0 = 1$ .

3.  $T_n$  est scindé racines simples sur  $\mathbb{R}$  :

$$T_n(X)$$

$$= 2^{n-1} \prod_{k=0}^{n-1} \left( X - \cos \frac{(2k+1)\pi}{2n} \right)$$

4. Orthogonalité : si  $n \neq p$

$$\int_{-1}^1 T_n(x) T_p(x) \frac{dx}{\sqrt{1-x^2}} = 0$$

5. Minimalité en norme :

$$\|P\| = \max_{t \in [-1, 1]} |P(t)|$$

Si  $P$  unitaire de degré  $n$ , alors  $\|P\| \geq \frac{1}{2^{n-1}}$ .

Avec cas d'égalité si  $P(X) = \frac{T_n(X)}{2^{n-1}}$

Preuves :

1. Formules de trigonométrie :

$$\cos((n+1)\theta) + \cos((n-1)\theta) = 2 \cos \theta \cos(n\theta)$$

$$T_{n+1}(\cos \theta) + T_{n-1}(\cos \theta) = 2(\cos \theta)T_n(\cos \theta)$$

Donc ils coïncident en une infinité de valeurs  $[-1, 1]$ , et sont donc égaux.

2. Par récurrence avec la relation de récurrence.

3. On résout  $\cos(n\theta) = 0$ , on fait attention à distinguer les racines.

4. Changement de variable  $x = \cos \theta$ , puis formules de trigonométrie.

5. Par contraposé : On prend  $P$  unitaire de degré  $n$  tel que

$$\|P\| \leq \frac{1}{2^{n-1}}$$

- $P = \frac{1}{2^{n-1}} T_n + Q$ ,  $\deg Q \leq n-1$ .

- On regarde les  $y_k$  quand  $T_n(y_k) = \pm 1$ .

- On en déduit le signe de  $Q$

- Par le TVI  $Q$  à  $n$  racines donc  $Q = 0$ .

- Donc  $P(X) = \frac{T_n(X)}{2^{n-1}}$ .

## Propriétés des fractions rationnelles

Propriétés des fractions rationnelles

---

- Si on dit que  $\frac{P}{Q}$  est scindé, c'est que  $Q$  est scindé.
- Si  $F$  admet une infinité de racines alors  $F = 0$ .
- Si  $F$  et  $G$  coïncident en une infinité de points alors  $F = G$ .

# Décomposition en éléments simples

Formules, propriétés de la décomposition en éléments simples.

Soit  $F \in \mathbb{K}(X)$ ,  $F$  se décompose de façon unique sous la forme

$$F = E + G \text{ avec } E \in \mathbb{K}[X] \text{ et } \deg G < 0$$

On appelle  $E$  la partie entière de  $F$  et  $G$  la partie pôleire.

- Si  $F = \frac{P}{Q}$  scindé racines simples : soit  $a_1, \dots, a_n$  les pôles et  $Q(X) = (X - a_k)R_k(X)$  pour tout  $k \in \llbracket 1, n \rrbracket$  :

$$F = E + \frac{\lambda_1}{X - a_1} + \cdots + \frac{\lambda_n}{X - a_n}$$

Avec

$$\lambda_k = \frac{P(a)}{R_k(a)} = \frac{P(a)}{Q'(a)}$$

- Si  $F$  est scindé pôles multiples, on fait la même chose en retranchant les décompositions à chaque fois.

Décomposition en éléments simples de  $\frac{P'}{P}$  :

$$P(X) = \lambda(X - a_1)^{m_1} \cdots \cdots (X - a_k)^{m_k}$$

$$\frac{P'(X)}{P(X)} = \frac{m_1}{X - a_1} + \cdots + \frac{m_k}{X - a_k}$$

## Axiomes d'un espace vectoriel

Axiomes d'un espace vectoriel.

---

Sois  $\mathbb{K}$  un corps,  $E$  muni de la somme interne  $+$  et du produit externe  $\cdot$  est un  $\mathbb{K}$ -ev si

1.  $(E, +)$  est un groupe abélien.
2.  $\forall x \in E, 1 \cdot x = x.$
3.  $\forall \lambda \in \mathbb{K}, \forall x, y \in E, \lambda(x + y) = \lambda x + \lambda y.$
4.  $\forall \lambda, \mu \in \mathbb{K}, \forall x \in E, (\lambda + \mu)x = \lambda x + \mu x.$
5.  $\forall \lambda, \mu \in \mathbb{K}, \forall x \in E, \lambda(\mu x) = (\lambda\mu)x$

## Théorème de caractérisation du rang

Énoncé du théorème de caractérisation du rang.

Soit  $A \in M_{np}(\mathbb{K})$ ,  $r \in \mathbb{N}$ , les assertions suivantes sont équivalentes

- $A$  équivalente par ligne à une matrice échelonnée avec  $r$  lignes non nulles.
- $\text{rg } \varphi_A = r$
- $\text{rg } (C_1, \dots, C_p) = r$  (avec  $C_i$  la  $i$ -ème colonne de  $A$ )
- $\text{rg } (L_1, \dots, L_n) = r$  (avec  $L_i$  la  $i$ -ème ligne de  $A$ )
- $A \xrightarrow{L,C} J_r$

On dit alors que  $\text{rg } A = r$ .

On a aussi

$$A \xrightarrow{L,C} B \text{ ssi } \text{rg } A = \text{rg } B$$

$$\begin{aligned} \text{rg}(\varphi \circ \psi) &= \text{rg } \psi - \dim(\ker \varphi \cap \text{im } \varphi) \\ &\leq \min(\text{rg } \varphi, \text{rg } \psi) \end{aligned}$$

## Formes linéaires et hyperplans

Formes linéaires et hyperplans.

---

Soit  $E$  un  $\mathbb{K}$ -ev

Un hyperplan de  $E$  est un sev de codimension 1, c'est à dire qui admet un supplémentaire de dimension 1.

- Si  $a \in E^* \setminus \{0\}$ , alors  $\ker a$  est un hyperplan.
- Si  $H$  est un hyperplan de  $E$ , il existe une forme linéaire  $a$  unique à constante multiplicative près tel que  $H = \ker a$ .

Deux hyperplans ont toujours un supplémentaire commun.

### Démonstration

- Si  $H_1$  et  $H_2$  sont des hyperplans,  $H_1 \cup H_2 \neq E$

► Par l'absurde : supposons  $H_1 \cup H_2 = E$  sev de  $E$

Or  $H_1 \cup H_2 = (H_1 \text{ ou } H_2) = E$  (cf unions de sev) qui est absurde.

Donc on dispose de  $x_0 \in E \setminus (H_1 \cup H_2)$

Ainsi  $\text{Vect}(x_0)$  est un supplémentaire de  $H_1$  et  $H_2$

## Matrices semblables

Définition de matrices semblables.

---

Soit  $A, B \in M_{n(\mathbb{K})}$ ,  $A$  est dite semblable à  $B$  si

$$\exists P \in \mathrm{GL}_n(\mathbb{K}), B = P^{-1}AP$$

Invariants :

- $\mathrm{rg} A = \mathrm{rg} B$
- $\mathrm{tr} A = \mathrm{tr} B$
- $\det A = \det B$
- $\chi_A = \chi_B$
- $\mu_A = \mu_B$

# Propriétés élémentaires sur les séries

Propriétés élémentaires sur les séries.

---

- Soit  $(u_n) \in \mathbb{K}^{\mathbb{N}}$  et  $S_n = \sum_{k=0}^n u_k$ , on dit que  $\sum u_n$  converge si  $(S_n)$  converge.
- Si  $\sum u_n$  converge alors

$$(u_n) \xrightarrow{n \rightarrow +\infty} 0$$

- La suite  $(u_n)$  converge ssi la série  $\sum (u_{n+1} - u_n)$  converge.
- L'ensemble  $S$  des séries convergentes est un sev de l'espace des suites, et l'application

$$\begin{aligned}\varphi : \quad S &\rightarrow \mathbb{K} \\ (u_n) &\mapsto \sum_{n=0}^{+\infty} u_n\end{aligned}$$

est linéaire.

- Si  $(u_n) \in \mathbb{R}_+^{\mathbb{N}}$  alors  $\sum u_n$  converge ssi  $(S_n)$  est majoré (théorème de la limite monotone).

# Théorème de comparaison des séries positives

Énoncé et démonstration du théorème de comparaison des séries positives.

---

Soient  $(u_n), (v_n) \in \mathbb{R}_+^{\mathbb{N}}$  alors

1. Si  $\forall n \geq n_0, u_n \leq v_n$  et  $\sum v_n$  converge alors  $\sum u_n$  converge.
2. Si  $u_n = O_{n \rightarrow +\infty}(v_n)$  et  $\sum v_n$  converge alors  $\sum u_n$  converge.
3. Si  $u_n \underset{n \rightarrow +\infty}{\sim} v_n$  alors  $\sum u_n$  converge ssi  $\sum v_n$  converge.

Démonstration :

1.  $(S_n)$  est majoré par  $(\tilde{S}_n)$  qui est fini.
2.  $(S_n)$  est majoré par  $M \cdot \tilde{S}_n$  qui est fini.
3.  $u_n \sim v_n$  implique  $u_n = O(v_n)$  et  $v_n = O(u_n)$ .

## Comparaison série intégrale

Propriétés et méthode de comparaison série intégrale.

Pour  $f \in C_{\text{pm}}^0([a, +\infty[, \mathbb{R}_+)$ , décroissante,  $\forall n \geq \lceil a \rceil + 1 = N_0$

$$f(n) \geq \int_n^{n+1} f(t) dt$$

$$\leq \int_{n-1}^n f(t) dt$$

D'où

$$\sum_{n=N_0}^N f(n) \geq \int_{N_0}^{N+1} f(t) dt$$

$$\leq \int_{N_0-1}^N f(t) dt$$

Ainsi  $\sum f(n)$  converge ssi  $\int_{N_0}^{+\infty} f$  converge.

Et de plus (à redémontrer) :

$$\sum \left( \int_{n-1}^n f(t) dt - f(n) \right)$$

$$\sum \left( f(n) - \int_n^{n+1} f(t) dt \right)$$

sont à terme général positif et convergent car

$$f(n) \leq \int_{n-1}^n f \leq f(n+1)$$

$$0 \leq \int_{n-1}^n f - f(n) \leq f(n+1) - f(n)$$

Et  $\sum f(n+1) - f(n)$  est positive et converge (série télescopique) car  $f$  converge (positive et décroissante).

**Dans le cas  $f$  non monotone :**

Si  $f \in C^1$  et  $\int_n^{+\infty} |f'|$  converge

$$\int_k^{k+1} f = \underbrace{[(t-k-1)f(t)]_k^{k+1}}_{f(k)}$$

$$- \int_k^{k+1} (t-k-1)f'(t) dt$$

$$\int_1^{N+1} f = \sum_{k=1}^N f(k)$$

$$+ \sum_{k=1}^N \int_k^{k+1} (k+1-t)f'(t) dt$$

Or pour tout  $k \geq 1$

$$\left| \int_k^{k+1} (k+1-t)f'(t) dt \right| \leq \int_k^{k+1} |f'|$$

Qui est le terme général d'une série convergente d'où

$$\sum f(n) \text{ converge}$$

$$\text{ssi } \left( \int_1^N f \right)_N \text{ converge}$$

$$\text{ssi } \int_1^{+\infty} f \text{ converge}$$

## Séries de Bertrand

Définitions et propriétés des séries de Bertrand.

---

Soit  $\alpha, \beta \in \mathbb{R}$ , la série  $\sum \frac{1}{n^\alpha (\ln n)^\beta}$  est appelée série de Bertrand.

Cette série converge ssi  $\alpha > 1$  ou  $\alpha = 1$  et  $\beta > 1$ .

Démonstration :

- Cas  $\alpha > 1$  comparaison avec les séries de Riemann, en prenant  $\gamma \in ]1, \alpha[$ .
- Cas  $\alpha < 1$  même chose avec  $\gamma \in ]\alpha, 1]$ .
- Cas  $\alpha = 1$ , comparaison série intégrale avec  $t \mapsto \frac{1}{t(\ln t)^\beta}$ .

# Recherche d'équivalent d'une suite

Méthodes de recherche d'équivalents.

---

Si on cherche un équivalent d'une suite  $(u_n)$

- Étudier la série  $\sum(u_{n+1} - u_n)$  ou  $\sum(u_n - u_{n+1})$ , sommes partielles ou restes (voir théorème de sommation des relations de comparaison).
- Chercher  $a \in \mathbb{R}^*$  tel que  $u_{n+1}^a - u_n^a \xrightarrow[n \rightarrow +\infty]{} l \in \mathbb{R}^*$ , pour avoir

$$u_n^a - u_0^a = \sum_{k=0}^{n-1} u_{k+1}^a - u_k^a \underset{n \rightarrow +\infty}{\sim} nl$$

## Absolue convergence

Définitions et démonstration du théorème de l'absolue convergence d'une série.

---

Une série  $\sum u_n$  (dans  $\mathbb{R}$  ou  $\mathbb{C}$ ) est dite absolument convergente si  $\sum |u_n|$  converge. Si  $\sum u_n$  est absolument convergente, alors elle est convergente.

Démonstration : on étudie  $((u_n)_+)$  et  $((u_n)_-)$  pour le cas réel, puis  $(\text{Re}(u_n))$  et  $(\text{Im}(u_n))$  pour le cas imaginaire, à chaque fois on majore par le module et on applique les théorèmes de comparaison des séries positives.

## Théorème des séries alternées

Énoncer et démonstration du théorème des séries alternées.

---

Si  $(u_n) \in \mathbb{R}_+^{\mathbb{N}}$  décroissante tel que  $u_n \xrightarrow[n \rightarrow +\infty]{} 0$ , alors  $\sum u_n$  converge et  $R_n = \sum_{k=n+1}^{+\infty} = S - S_n$  est du signe du premier terme et  $|R_n| \leq |u_{n+1}|$ .

Démonstration : on montre que les suites  $S_{2n}$  et  $S_{2n+1}$  sont adjacentes et on étudie  $R_{2n}$  et  $R_{2n+1}$ .

# Transformation d'Abel

Définition et applications de la transformation d'Abel.

---

Il s'agit d'une sorte d'IPP sur les séries. Soit  $(a_n)$  et  $(b_n)$  deux suites, la transformation d'Abel est utile si on a des hypothèses sur  $S_n = \sum_{k=0}^n a_k$ . On pose  $S_{-1} = 0$ .

$$\begin{aligned}\sum_{k=0}^n a_k b_k &= \sum_{k=0}^n (S_k - S_{k-1}) b_k \\ &= \sum_{k=0}^n S_k b_k - \sum_{k=0}^n S_{k-1} b_k \\ &= S_n b_n - \sum_{k=0}^{n-1} S_k (b_{k+1} - b_k)\end{aligned}$$

Applications :

$$\sum \frac{\sin(n\theta)}{n^\alpha}$$

$$\sum \frac{\cos(n\theta)}{n^\alpha}$$

$$\sum \frac{e^{in\theta}}{n^\alpha}$$

Remarque : on peut aussi écrire  $a_k = R_{k-1} - R_k$ , qui peut être intéressant si  $\sum a_n$  converge.

# Règle de Raabe-Duhamel

Énoncé et démonstration de la règle de Raab-Duchamel.

Soit  $(a_n) \in (\mathbb{R}_+^*)^\mathbb{N}$ ,  $\frac{a_{n+1}}{a_n} \xrightarrow[n \rightarrow +\infty]{} 1$  et

$$\frac{a_{n+1}}{a_n} = 1 - \frac{a}{n} + O_{n \rightarrow +\infty}\left(\frac{1}{n^{1+h}}\right), \quad h > 0$$

On considère  $n^a a_n = u_n$ , on veut montrer que  $u_n \xrightarrow[n \rightarrow +\infty]{} l \in \mathbb{R}_+^*$ , c'est dire que  $(\ln(u_n))$  a une limite réelle. On étudie  $\sum \ln(u_{n+1}) - \ln(u_n)$ .

$$\begin{aligned} \ln(u_{n+1}) - \ln(u_n) &= \ln\left(\frac{a_{n+1}}{a_n}\right) + a \ln\left(\frac{n+1}{n}\right) \\ &= \ln\left(1 - \frac{a}{n} + O\left(\frac{1}{n^{1+h}}\right)\right) + a \ln\left(1 + \frac{1}{n}\right) \\ &= \frac{a}{n} - \frac{a}{n} + O\left(\frac{1}{n^{1+h}}\right) + O\left(\frac{1}{n^2}\right) \\ &= O\left(\frac{1}{n^{\min(2, 1+h)}}\right) \end{aligned}$$

Donc par le théorème de comparaison des séries à terme positifs (en valeur absolue)  $\sum \ln(u_{n+1}) - \ln(u_n)$  converge, d'où  $(u_n)$  converge.

Ainsi  $n^a a_n \xrightarrow[n \rightarrow +\infty]{} e^l$ , donc  $a_n \sim \frac{e^l}{n^a}$ ,  $\sum a_n$  converge ssi  $a > 1$ .

# Théorème de sommation des relations de comparaison pour les séries

Énoncés des théorèmes de sommation des relations de comparaison pour les séries.

## Pour les restes de séries convergentes :

Si  $(u_n) \in \mathbb{K}^{\mathbb{N}}$ ,  $(a_n) \in \mathbb{R}_+^{\mathbb{N}}$  et  $\sum a_n$  converge.

1. Si  $u_n = O(a_n)$ , alors  $\sum u_n$  converge absolument et

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

2. Si  $u_n = o(a_n)$ , alors  $\sum u_n$  converge absolument et

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

3. Si  $u_n \sim a_n$ , alors

$$\sum_{k=n+1}^{+\infty} u_k \sim \sum_{k=n+1}^{+\infty} a_n$$

Démonstration : on repasse par les définitions de  $o$  et  $O$  :  $\exists N \in \mathbb{N}$ ,  $\forall n \geq N$ ,  $|u_n| \leq K a_n$ , avec  $K > 0$  fixé pour  $O$  et  $K = \varepsilon > 0$  pour  $o$ . Pour  $\sim$ , on a  $u_n - a_n = o(a_n)$ .

## Pour les sommes partielles de séries divergentes :

Si  $(u_n) \in \mathbb{K}^{\mathbb{N}}$ ,  $(a_n) \in \mathbb{R}_+^{\mathbb{N}}$  et  $\sum a_n$  diverge.

1. Si  $u_n = O(a_n)$ , alors  $\sum u_n$  converge absolument et

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

2. Si  $u_n = o(a_n)$ , alors  $\sum u_n$  converge absolument et

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

3. Si  $u_n \sim a_n$ , alors

$$\sum_{k=0}^n u_k \sim \sum_{k=0}^n a_n$$

Démonstration : même que pour l'autre, on a juste à découper la somme entre avant et après un certain rang (pour  $o$  et  $O$ ).

# Équivalents de référence : séries de Riemann

Équivalent des restes ou sommes partielles des séries de Riemann (à redémontrer).

---

Par comparaison série intégrale :

- Pour  $1 \geq a > 0$

$$\int_1^{n+1} \frac{dt}{t^a} \leq 1 + \sum_{k=1}^n \frac{1}{k^a} \leq \int_2^n \frac{dt}{t^a}$$

$$S_n(a) = \sum_{k=1}^n \frac{1}{k^a} \underset{n \rightarrow +\infty}{\sim} \frac{n^{1-a}}{1-a}$$

- Pour  $a > 0$

$$\int_{n+1}^{+\infty} \frac{dt}{t^a} \leq \sum_{k=n+1}^{+\infty} \frac{1}{k^a} \leq \int_n^{+\infty} \frac{dt}{t^a}$$

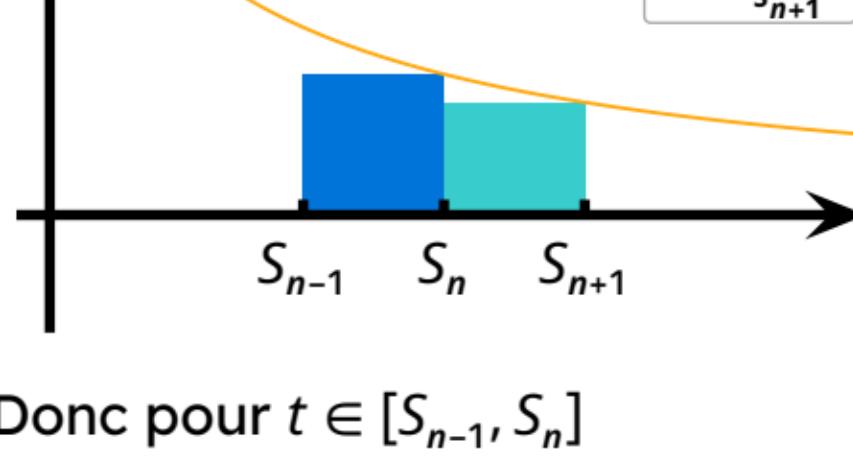
$$R_n(a) = \sum_{k=n+1}^{+\infty} \frac{1}{k^a} \underset{n \rightarrow +\infty}{\sim} \frac{1}{a-1} \cdot \frac{1}{n^{a-1}}$$

## Exercice : Nature de la série terme général sur somme partielle

Démonstration de la CNS sur  $a$  de la convergence de la série  $\sum \frac{u_n}{S_n^a}$  (avec  $\sum u_n$  divergente).

Soit  $(u_n) \in (\mathbb{R}_+^*)^\mathbb{N}$ ,  $\sum u_n$  diverge, et  $a \in \mathbb{R}$ . On note  $S_n = \sum_{k=1}^n u_k$ .

- Si  $a > 1$  :



Donc pour  $t \in [S_{n-1}, S_n]$

$$\frac{1}{t^a} \geq \frac{1}{S_n^a}$$

$$\sum_{k=1}^n \frac{u_k}{S_k^a} \leq \int_{S_0}^{S_n} \frac{dt}{t^a} = \frac{1}{a-1} \left( \frac{1}{S_0^{a-1}} - \frac{1}{S_n^{a-1}} \right)$$

Or  $S_n \xrightarrow[n \rightarrow +\infty]{} 0$  donc

$$\sum_{n=1}^{+\infty} \frac{u_n}{S_n^a} \leq \frac{1}{a-1} \cdot \frac{1}{S_0^a}$$

- Si  $a = 1$  :

Si  $\frac{u_n}{S_n} \xrightarrow[n \rightarrow +\infty]{} 0$ , la série diverge grossièrement, et sinon

$$\frac{u_n}{S_n} \sim -\ln\left(1 - \frac{u_n}{S_n}\right)$$

$$\sim \ln(S_n) - \ln(S_{n-1})$$

Qui est le terme général d'une série télescopique divergente.

- Si  $a \leq 1$ , on compare avec  $a = 1$ , car à partir d'un certain rang  $S_n \geq 1$ .

# Familles sommables

Définition et propriétés élémentaires des familles sommables.

---

Soit  $I$  un ensemble non vide.

Pour  $(u_i) \in \mathbb{R}_+^I$ , on définit

$$\sum_{i \in I} u_i = \sup \left\{ \sum_{j \in J} u_j, J \subseteq I \text{ fini} \right\} \in \mathbb{R}_+ \cup \{+\infty\}$$

Pour une famille  $(u_i) \in \mathbb{K}^I$ , on dit qu'elle est sommable si

$$\sum_{i \in I} |u_i| < +\infty$$

Si  $(u_i)_{i \in I}$  est sommable, alors elle contient un nombre au plus dénombrable d'éléments non nuls (Démonstration : on étudie  $J_n = \{i \in I \mid u_i \geq \frac{1}{n}\}$ )

# Théorème de sommation par paquets

Énoncer et éléments de démonstration du théorème de sommation par paquets.

Soit  $(u_i)_{i \in I} \in \mathbb{R}^I$ , et  $I = \bigcup_{n \in \mathbb{N}} I_n$  une partition. La famille  $(u_i)$  est sommable ssi

$$(*) : \begin{cases} \forall n \in \mathbb{N}, (u_i)_{i \in I_n} \text{ sommable} \\ \sum \left( \sum_{i \in I_n} |u_i| \right) \text{ converge vers } S \end{cases}$$

Dans ce cas

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

Démonstration :

- Cas positif :
  - ▶ On suppose  $(*)$ , on prend une sous famille finie  $J$  de  $I$ , on a donc une famille  $(J_n = I_n \cap J)_n$ , on note  $N = \max(n \in \mathbb{N} \mid J_n \neq \emptyset)$  qui existe car  $J$  fini.

$$\begin{aligned} \sum_{j \in J} u_j &= \sum_{n=0}^N \left( \sum_{j \in J_n} u_j \right) \\ &\leq \sum_{n=0}^{+\infty} \left( \sum_{i \in I_n} u_i \right) = S \end{aligned}$$

- Caractérisation de la borne supérieure, majoration et sous ensembles finis.
- Cas général : D'abord en valeurs absolues, puis parties positives, négatives, réelles et imaginaires.

# Critère de convergence d'intégrales usuelles

Critère de convergence d'intégrales usuelles :

$$\int_1^{+\infty} \frac{dt}{t^a}$$

$$\int_0^1 \frac{dt}{t^a}$$

$$\int_2^{+\infty} \frac{dt}{t^a (\ln t)^\beta}$$

$$\int_0^{\frac{1}{2}} \frac{dt}{t^a (\ln t)^\beta}$$

- $\int_1^{+\infty} \frac{dt}{t^a}$  converge vers  $\frac{1}{a-1}$  ssi  $a > 1$ .
- $\int_0^1 \frac{dt}{t^a}$  converge vers  $\frac{1}{1-a}$  ssi  $a < 1$ .
- $\int_2^{+\infty} \frac{dt}{t^a (\ln t)^\beta}$  converge ssi  $a > 1$  ou  $a = 1$  et  $\beta > 1$
- $\int_0^{\frac{1}{2}} \frac{dt}{t^a (\ln t)^\beta}$  converge ssi  $a < 1$  ou  $a = 1$  et  $\beta > 1$

# Fonction gamma

Définition, convergence et démonstration de la fonction  $\Gamma$ .

---

On définit

$$\Gamma(x) = \int_0^{+\infty} e^{-t} t^{x-1} dt$$

- Qui converge pour  $x > 0$ .
- Pour  $x > 0$

$$\Gamma(x+1) = x\Gamma(x)$$

- $\Gamma(1) = 1$

$t \mapsto e^{-t} t^{x-1}$  est  $C_{\text{pm}}^0$  sur  $]0, +\infty[$ .

- Sur  $[1, +\infty[$

$$e^{-t} t^{x-1} = o_{t \rightarrow +\infty}\left(e^{-\frac{t}{2}}\right)$$

$$= o_{t \rightarrow +\infty}\left(\frac{1}{t^2}\right)$$

Or  $\int_1^{+\infty} e^{-\frac{t}{2}} dt$  converge, donc par le théorème de comparaison d'intégrales de fonctions positives,  $\int_1^{+\infty} e^{-t} t^{x-1} dt$  converge.

- Sur  $]0, 1]$

$$e^{-t} t^{x-1} \underset{t \sim 0_+}{\sim} \frac{1}{t^{1-x}}$$

Or  $\int_0^1 \frac{dt}{t^{1-x}}$  converge ssi  $1 - x < 1$  d'où  $x > 0$ , et on conclut par le même théorème.

$$\begin{aligned} \Gamma(x+1) &= \int_0^{+\infty} e^{-t} t^x dt \\ &= [-e^{-t} t^x]_0^{+\infty} + x \int_0^{+\infty} e^{-t} t^{x-1} dt \\ &= x\Gamma(x) \end{aligned}$$

# Fonctions arithmétiques : Möbius et indicatrice d'Euler

Définition, contexte et démonstration de la fonction de Möbius et la formule d'inversion.

Pour  $A = \mathcal{F}(\mathbb{N}^*, \mathbb{C})$  on définit (\*), pour  $f, g \in A$

$$f * g = \begin{cases} \mathbb{N}^* \rightarrow \mathbb{C} \\ n \mapsto \sum_{d|n} f(d)g\left(\frac{n}{d}\right) \end{cases}$$

Qui est une loi de composition interne sur  $A$ . On montre que

- $\mathbb{1}_{\{1\}}$  est l'élément neutre.
- (\*) est commutatif
- (\*) est associatif

On définit la fonction de Möbius, on note  $\pi(n) = |\{p \in \mathbb{P}, p | n\}|$

$$\mu : \begin{array}{ccc} 1 & \mapsto & 1 \\ n \mid \exists p \in \mathbb{P}, p^2 \mid n & \mapsto & (-1)^{\pi(n)} \\ n \mid \exists p \in \mathbb{P}, p^2 \nmid n & \mapsto & 0 \end{array}$$

On montre de plus

$$\mu * \mathbb{1}_{\mathbb{N}} = \mathbb{1}_{\{1\}}$$

Pour  $n \geq 2$  on écrit  $n = \prod_{j=1}^k p_j^{a_j}$ . Un diviseur  $d$  s'écrit  $\prod_{j=1}^k p_j^{\beta_j}$  avec

$\beta_j \leq a_j$ . Donc

$$\mu(d) \neq 0 \Leftrightarrow \forall j \in \llbracket 1, k \rrbracket, \beta_j \in \{0, 1\}$$

Ainsi

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{\beta_1, \dots, \beta_k \in \{0, 1\}} \mu\left(\prod_{j=1}^k p_j^{\beta_j}\right) \\ &= \sum_{q=0}^k \sum_{I \subset \llbracket 1, q \rrbracket} (-1)^{|I|} \\ &= \sum_{q=0}^k (-1)^q \binom{k}{q} \\ &= 0 \end{aligned}$$

On en déduit la formule d'inversion de Möbius : soit  $f : \mathbb{N}^* \rightarrow \mathbb{C}$ , on pose  $g : n \mapsto \sum_{d|n} f(d)$  ( $g = f * \mathbb{1}_{\mathbb{N}}$ ), on a alors pour tout  $n \in \mathbb{N}$

$$f(n) = \sum_{d|n} \mu(d)g\left(\frac{n}{d}\right)$$

C'est à dire  $f = g * \mu = f * \underbrace{\mathbb{1}_{\mathbb{N}} * \mu}_{\mathbb{1}_{\{1\}}}$ .

De plus  $\mu$  est multiplicative.

# Intégrales de Wallis

Définition, propriétés et démonstration des intégrales de Wallis.

---

On pose pour  $n \in \mathbb{N}$

$$\begin{aligned} W_n &= \int_0^{\frac{\pi}{2}} (\cos t)^n dt \\ &= \int_0^{\frac{\pi}{2}} (\sin \theta)^n d\theta \quad (\theta = \frac{\pi}{2} - t) \end{aligned}$$

## Relation de récurrence

$$\begin{aligned} W_{n+2} &= \int_0^{\frac{\pi}{2}} (\sin t)^{n+2} dt \\ &= \underbrace{\left[ -\cos(t) \sin(t)^{n+1} \right]_0^{\frac{\pi}{2}}}_{0} \\ &\quad + (n+1) \int_0^{\frac{\pi}{2}} (\sin t)^n (\cos t)^2 dt \\ &= (n+1)W_n - (n+1)W_{n+2} \\ &= \frac{n+1}{n+2} W_n \end{aligned}$$

## Formules explicites

$$W_0 = \frac{\pi}{2}$$

$$W_1 = 1$$

$$W_{2n} = \frac{(2n)!}{2^{2n}(n!)^2} \frac{\pi}{2}$$

$$W_{2n+1} = \frac{2^{2n}(n!)^2}{(2n+1)!}$$

D'où

$$W_{n+1} \underset{n \rightarrow +\infty}{\sim} W_n$$

$$W_{2n}^2 \underset{n \rightarrow +\infty}{\sim} W_{2n+1}^2$$

$$\underset{n \rightarrow +\infty}{\sim} W_{2n} W_{2n+1} = \frac{\pi}{4n+2}$$

Ainsi

$$W_{2n+1} \underset{n \rightarrow +\infty}{\sim} \sqrt{\frac{\pi}{4n+2}}$$

$$W_{2n} \underset{n \rightarrow +\infty}{\sim} \sqrt{\frac{\pi}{4n}}$$

# Lemme de Riemann-Lebesgue

Énoncé et démonstration du lemme de Riemann-Lebesgue.

Si  $I$  est un Intervalle de  $\mathbb{R}$ , et  $f \in C_{\text{pm}}^0(I, \mathbb{K})$  intégrable sur  $I$ , alors

$$\int_I f(t) e^{i\lambda t} dt \xrightarrow{\lambda \rightarrow \infty} 0$$

$$\int_I f(t) \cos(\lambda t) dt \xrightarrow{\lambda \rightarrow \infty} 0$$

$$\int_I f(t) \sin(\lambda t) dt \xrightarrow{\lambda \rightarrow \infty} 0$$

## Démonstration

- Si  $f$  est  $C^1$  sur un segment : par IPP, on dérive  $f$ ,  $f'$  étant continue sur un segment elle est uniformément continue sur ce segment (théorème de Heine), et est donc bornée (théorème des bornes atteintes).
- On montre d'abord pour  $I$  segment.
  - On traite le cas  $f$  constante.
  - On généralise à  $f$  en escalier.
  - Par densité des fonctions en escalier on étend aux fonctions continues.
- On étend finalement aux intervalles quelconques.

# Éxistence et unicité des sous groupes de groupe cyclique

Soit  $G$  un groupe cyclique d'ordre  $n$ , et  $d \mid n$ , montrer l'éxistence et l'unicité d'un sous groupe d'ordre  $d$ .

---

Soit  $G$  cyclique d'ordre  $n$ .

Par isomorphisme à  $(\mathbb{Z}/n\mathbb{Z}, +)$ , on se ramène à l'étude de  $(\mathbb{U}_n, \cdot)$ .

Soit  $H$  sous groupe de  $\mathbb{U}_n$ ,  $|H| = d$ .

Pour tout  $x \in H$ ,  $x^d = 1$  donc  $H \subset \mathbb{U}_d$ , par égalité des cardinaux,  $H = \mathbb{U}_d$ .

# Polynômes cyclotomiques

Définitions et propriétés des polynômes cyclotomiques.

Pour  $n \in \mathbb{N}^*$  on note

$$\begin{aligned}\mathbb{V}_n &= \{z \in \mathbb{U}_n \mid \text{ord}(z) = n\} \\ &= \left\{ e^{\frac{2ki\pi}{n}}, k \in (\mathbb{Z}/n\mathbb{Z})^\times \right\}\end{aligned}$$

On définit de  $n$ -ème polynôme cyclotomique

$$\begin{aligned}\Phi_n(X) &= \prod_{\xi \in \mathbb{V}_n} (X - \xi) \\ \deg(\Phi_n) &= \varphi(n)\end{aligned}$$

On montre

$$X^n - 1 = \prod_{d \mid n} \Phi_d$$

$$\Phi_n \in \mathbb{Z}[X]$$

$\Phi_p$  irréductible

## Démonstration

- Pour  $d \mid n$ , on a

$$\mathbb{V}_d = \{z \in \mathbb{U}_n \mid \text{ord}(z) = d\}$$

Car si  $z \in \mathbb{U}_n$  d'ordre  $d$ ,  $z \in \langle z \rangle$  sous groupe de  $\mathbb{U}_n$  de cardinal  $d$ , qui est unique car  $\mathbb{U}_n$  est cyclique. D'où  $z \in \mathbb{U}_d$  et à fortiori  $z \in \mathbb{V}_d$ .

- On a donc

$$\mathbb{U}_n = \bigcup_{d \mid n} \mathbb{V}_d$$

$$X^n - 1 = \prod_{\xi \in \mathbb{U}_n} (X - \xi)$$

$$= \prod_{d \mid n} \left( \prod_{\xi \in \mathbb{V}_d} (X - \xi) \right)$$

$$= \prod_{d \mid n} \Phi_d$$

- On montre que la division euclidienne dans  $\mathbb{Z}[X]$  par un polynôme unitaire donnent un polynôme dans  $\mathbb{Z}[X]$ . On refait la démonstration de la division euclidienne (récurrence).

- Référence forte sur  $n$  pour montrer que  $\Phi_n \in \mathbb{Z}[X]$

$$\begin{aligned}X^n - 1 &= \Phi_n \cdot \left( \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d \right)\end{aligned}$$

- Soit  $p \in \mathbb{P}$

$$\Phi_p = \prod_{\substack{\omega \in \mathbb{U}_p \\ \text{ord}(\omega) = p}} (X - \omega)$$

$$= \frac{X^p - 1}{X - 1} = \sum_{k=0}^{p-1} X^k$$

$$= X^{p-1} + \sum_{k=1}^{p-1} \underbrace{\binom{k}{p}}_{\text{divisible par } p} X^{k-1}$$

et le coefficient constant est  $\binom{p}{1}$  qui n'est pas divisible par  $p^2$ ,

d'où par le critère d'Eisenstein,  $\Phi_p$  irréductible dans  $\mathbb{Q}[X]$ .

Démonstration de  $n = \sum_{d \mid n} \varphi(d)$  :

$$n = |\mathbb{U}_n|$$

$$= \sum_{d \mid n} |\mathbb{V}_d|$$

$$= \sum_{d \mid n} \varphi(d)$$

# Groupes quotientés

Définitions et propriétés des groupes quotientés.

Soit  $G$  un groupe,  $H$  sous-groupe.

On définit la relation d'équivalence

$$\forall (x, y) \in G^2, x \sim y \text{ ssi } y \in xH$$

On obtient ainsi les classes à gauche  $gH$  pour tout  $g \in G$ , dont l'ensemble est noté  $G/H$ .

$H$  est dit distingué si

$$\forall g \in G, gHg^{-1} = H$$

Et dans ce cas  $G/H$  à une structure de groupe muni de la multiplication sur les classes

$$\bar{x} \cdot \bar{y} = \overline{x \cdot y}$$

Et on pose

$$\begin{aligned} f : & G \rightarrow G/H \\ & g \mapsto gH \end{aligned}$$

qui est un morphisme de groupe surjectif appelé projection canonique de  $G$  sur  $G/H$  dont le noyau est  $H$ .

## Cas particuliers

- Tous noyau de morphisme est un sous-groupe distingué.
- Tous sous-groupe d'indice 2 ( $\frac{|G|}{|H|} = 2$ ) est distingué.

## Idéaux maximaux, anneaux quotientés

Définitions d'idéal maximale, anneau quotienté, propriétés.

Soit  $(A, +, \cdot)$  un anneau et  $I$  idéal de  $A$ .

### Idéal maximale

Un idéal  $I$  de  $A$  est dit maximale si pour tout  $J$  idéal de  $A$

$$I \subsetneq J \Rightarrow J = A$$

### Anneau quotienté

On définit sur  $A$  la relation d'équivalence

$$\forall (x, y) \in A^2, x \sim y \text{ ssi } x - y \in I$$

On note  $A/I$  l'ensemble des classes d'équivalences par cette relation qu'on muni d'une structure de groupe en définissant les loi suivantes

$$\bar{x} + \bar{y} = \overline{x + y}$$

$$\bar{x} \cdot \bar{y} = \overline{x \cdot y}$$

Qui ne dépend pas du représentant choisis.

### Propriétés

- $I$  est maximale ssi tous les éléments non nuls de  $A/I$  sont inversibles.

- Si  $A$  commutatif,  $I$  maximale, alors  $I$  est premier ( $A/I$  est intègre).

Démonstration :

- On suppose  $I$  maximale. Soit  $x \in A \setminus I$  c'est à dire  $x \notin \overline{0_A}$ , montrons que  $\bar{x}$  est inversible.

$I \subseteq xA + I = J$  est un idéal, or  $I$  maximale d'où  $1_A \in A = J$ , d'où l'existence de  $y \in A$  et  $z \in I$  tel que

$$xy + z = 1_A$$

$$\bar{x}\bar{y} = \overline{xy} = \overline{1_A}$$

$$\exists z \in I, \underbrace{xy + z}_{\in J} = 1_A$$

$1_A \in J$  donc  $J = A$ ,  $I$  est maximale.

- Soit  $x, y \in A$  tels que  $xy \in I$ , supposons que  $x \notin I$ . Donc  $\bar{x}$  inversible : on dispose de  $x' \in A$

et  $z \in I$  tels que

$$xx' + z = 1_A$$

$$\underbrace{xyx' + zy}_{\in I} = y \in I$$

# Signature d'une permutation

Définitions et propriétés de la signature dans  $\mathfrak{S}_n$ .

---

Plusieurs définitions alternatives.

- $\varepsilon : (\mathfrak{S}_n, \circ) \rightarrow (\mathbb{Z}^\times, \cdot)$  est l'unique morphisme non triviale.

Pour  $\sigma \in \mathfrak{S}_n$  :

$$\begin{aligned}\varepsilon(\sigma) &= \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} \\ &= (-1)^{N_\sigma} \\ &= (-1)^{n - |\text{Orb}(\sigma)|}\end{aligned}$$

Où  $N_\sigma = |\{(i, j) \mid i < j \text{ et } \sigma(i) > \sigma(j)\}|$ .

# Hölder

Inégalité de Hölder et démonstration.

Soit  $p, q \in \mathbb{R}_+^*$  tels que  $\frac{1}{p} + \frac{1}{q} = 1$ .

Pour  $x_1, \dots, x_n, y_1, \dots, y_n \in \mathbb{R}_+$

$$\sum_{i=1}^n x_i y_i \leq \left( \sum_{i=1}^n x_i^p \right)^{\frac{1}{p}} \left( \sum_{i=1}^n y_i^q \right)^{\frac{1}{q}}$$

## Démonstration

- Pour tout  $x, y \in \mathbb{R}_+$ ,

$$xy \leq \frac{1}{p}x^p + \frac{1}{q}y^q$$

Le cas nul se traite facilement, puis on utilise la concavité de  $\ln$  sur  $\mathbb{R}_+^*$  :

$$\ln\left(\frac{1}{p}x^p + \frac{1}{q}y^q\right) \geq \frac{1}{p}\ln(x^p) + \frac{1}{q}\ln(y^q)$$

$$= \ln(xy)$$

$$\frac{1}{p}x^p + \frac{1}{q}y^q \geq xy$$

- On traite d'abord le cas où l'un des vecteurs ( $X$  ou  $Y$ ) est nul.
- On traite ensuite le cas où

$$\sum_{i=1}^n x_i^p = 1 \quad \text{et} \quad \sum_{j=1}^n y_j^q = 1$$

Pour tout  $i \in \llbracket 1, n \rrbracket$

$$x_i y_i \leq \frac{1}{p}x_i^p + \frac{1}{q}y_i^q$$

$$\sum_{i=1}^n x_i y_i \leq \underbrace{\frac{1}{p} \sum_{i=1}^n x_i^p}_{1} + \underbrace{\frac{1}{q} \sum_{i=1}^n y_i^q}_{1}$$

$$\leq 1 = \left( \sum_{i=1}^n x_i^p \right)^{\frac{1}{p}} \left( \sum_{i=1}^n y_i^q \right)^{\frac{1}{q}}$$

- Enfin dans le cas général, on pose pour  $i \in \llbracket 1, n \rrbracket$

$$\tilde{x}_i = \frac{x_i}{\sum_{i=1}^n x_i} \quad \tilde{y}_i = \frac{y_i}{\sum_{i=1}^n y_i}$$

Et ça marche.

## Actions de groupe

Définitions et exemples usuels, propriétés des actions de groupes.

Soit  $G$  un groupe,  $X$  un ensemble. Une action de groupe est la donnée d'un morphisme de groupe

$$\varphi : \begin{cases} G \rightarrow \mathfrak{S}(X) \\ g \mapsto \rho_g : \begin{cases} X \rightarrow X \\ x \mapsto \rho_g(x) = g.x \end{cases} \end{cases}$$

Ainsi tout groupe fini de cardinal  $n \in \mathbb{N}$  est isomorphe à un sous groupe de  $\mathfrak{S}_n$ .

### Démonstration

Grâce à l'action de groupe  $\varphi$

$$\varphi : \begin{cases} G \rightarrow \mathfrak{S}(G) \simeq \mathfrak{S}_n \\ a \mapsto \rho_a : \begin{cases} G \rightarrow G \\ g \mapsto ag \end{cases} \end{cases}$$

Qui est un morphisme de groupe (car  $\rho_a \circ \rho_b = \rho_{a,b}$ ), injectif (car  $\ker \varphi = e_G$ ), d'où  $\varphi|_{\varphi(G)}$  isomorphisme de  $G \rightarrow \varphi(G)$ , avec  $\varphi(G)$  sous groupe de  $\mathfrak{S}(G) \simeq \mathfrak{S}_n$ .

### Autre action classique

On peut aussi considérer l'action de conjugaison

$$\theta : \begin{cases} G \rightarrow \mathfrak{S}(G) \\ g \mapsto \rho_g : \begin{cases} G \rightarrow G \\ x \mapsto gxg^{-1} \end{cases} \end{cases}$$

On a

$$\begin{aligned} \ker \theta &= \{g \in G \mid \theta(g) = \text{id}\} \\ &= \{g \in G \mid \forall x \in G, gxg^{-1} = x\} \\ &= \{g \in G \mid \forall x \in G, gx = xg\} \\ &= Z(G) \end{aligned}$$

## Formule des classes

Énoncé, démonstration et définitions de la formule des classes.

Soit  $G$  un groupe et  $\varphi$  une action de  $G$  sur un ensemble  $X$ . On définit pour tout  $x \in X$

$$\text{Stab}(x) = \{g \in G \mid g.x = x\}$$

C'est un sous groupe de  $G$  :

- $e.x = x$  d'où  $e \in \text{Stab}(x)$
- $\forall g \in \text{Stab}(x), g^{-1}.x = g^{-1}.g.x = x$
- $\forall g, h \in \text{Stab}(x), (gh).x = g.h.x = x$

On définit également

$$\text{Orb}(x) = \{g.x, g \in G\}$$

Qui est la classe d'équivalence de  $x$  pour la relation d'équivalence

$$x \sim y \text{ si } \exists g \in G, y = g.x$$

Donc les orbites forment une partition de  $X$ .

## Formule des classes

Pour tout  $x \in X$  fini et  $G$  fini

$$|\text{Orb}(x)| \cdot |\text{Stab}(x)| = |G|$$

### Démonstration

Soit  $x \in X$ , pour  $y \in \text{Orb}(x)$ , on dispose de  $g_0 \in G$  tel que  $g_0.x = y$ .

Étudions  $\{g \in G \mid g.x = y\}$  :

$$\begin{aligned} g.x = y &\Leftrightarrow g.x = g_0.x \\ &\Leftrightarrow (g_0^{-1}g).x = x \\ &\Leftrightarrow g_0^{-1}g \in \text{Stab}(x) \\ &\Leftrightarrow g \in g_0 \text{ Stab }(x) \end{aligned}$$

D'où

$$G = \bigcup_{y \in \text{Orb}(x)} \{g \in G \mid g.x = y\}$$

$$|G| = \sum_{y \in \text{Orb}(x)} |g_0 \text{ Stab }(x)|$$

$$= \sum_{y \in \text{Orb}(x)} |\text{Stab}(x)|$$

$$= |\text{Orb}(x)| \cdot |\text{Stab}(x)|$$

## Exercice : Les p-groupes

Définitions d'un  $p$ -groupe, et démonstration de

1. Pour  $G$   $p$ -groupe,  $|Z(G)| = p^a$  avec  $a \in \mathbb{N}^*$ .
2. Tout groupe  $G$  d'ordre  $p^2$  est abélien

---

Un  $p$ -groupe est un groupe dont tout les éléments sont d'ordre  $p^r$  avec  $r \in \mathbb{P}$ . A fortiori, il s'agit d'un groupe de cardinal  $p^a$ .

1. On étudie l'action de groupe

$$\varphi : \begin{cases} G \rightarrow \mathfrak{S}(G) \\ g \mapsto \rho_g : \begin{cases} G \rightarrow G \\ x \mapsto gxg^{-1} \end{cases} \end{cases}$$

On montre que

$$x \in Z(G) \text{ ssi } \text{Orb}(x) = \{e_G\}$$

Et par la formule des classes on a pour tout  $x \in G$  :

$$p^a = |G| = |\text{Orb}(x)| \cdot |\text{Stab}(x)|$$

Donc  $|\text{Orb}(x)| \mid p^a$  d'où si  $|\text{Orb}(x)| > 0$ ,  $p \mid |\text{Orb}(x)|$ .

Or les  $\text{Orb}(x)$  forment une partition de  $G$  donc

$$p^a = |G| = \sum_{x \in G} |\text{Orb}(x)|$$

$$= |Z(G)| + \underbrace{\sum_{\substack{x \in G / \sim \\ |\text{Orb}(x)| > 1}} |\text{Orb}(x)|}_{\text{divisible par } p}$$

Donc  $p \mid |Z(G)|$  mais  $e_G \in Z(G)$

donc  $|Z(G)| > 0$  d'où  $|Z(G)| \geq p$ .

2. Par l'exercice ci dessus

$$Z(G) \in \{p, p^2\}$$

Supposons qu'il existe  $x \in G \setminus Z(G)$ , alors

$$Z(G) \subset \text{Stab}(x) \text{ et } x \in \text{Stab}(x)$$

Donc  $|\text{Stab}(x)| \geq p + 1$  sous-groupe de  $G$  donc

$$\text{Stab}(x) = G$$

D'où  $x \in Z(G)$ , absurde.

## Exercice : élément d'ordre $p$ dans un groupe d'ordre divisé par $p$

Soit  $G$  un groupe d'ordre  $pq$  avec  $p \in \mathbb{P}$  et  $q \in \mathbb{N}^*$ , démonstration de l'existence d'un élément d'ordre  $p$ .

Soit  $G$  d'ordre  $n = pq$  avec  $(p, q) \in \mathbb{P} \times \mathbb{N}^*$ .

On pose

$$\Gamma = \{(x_1, \dots, x_p) \in G^p \mid x_1 \cdots x_p = e_G\}$$
$$\sigma = (1 \ 2 \ \cdots \ p) \in \mathfrak{S}_p$$

On considère  $H = \langle \sigma \rangle$  qui agit sur  $\Gamma$  via

$$\varphi : \begin{cases} H & \rightarrow \mathfrak{S}(\Gamma) \\ \sigma^k & \mapsto \rho_{\sigma^k} \end{cases}$$

Où

$$\rho_{\sigma^k} : \begin{cases} \Gamma & \rightarrow \Gamma \\ (x_1, \dots, x_p) & \mapsto (x_{\sigma^k(1)}, \dots, x_{\sigma^k(p)}) \end{cases}$$

(On montre par récurrence sur  $k$  que  $\rho_{\sigma^k}$  à bien valeur dans  $\Gamma$ ).

On remarque que  $|H| = p$  et

$$\forall X = (x_1, \dots, x_p) \in G^p,$$

$$X \in \Gamma \Leftrightarrow x_p^{-1} = x_1 \cdots x_{p-1}$$

$$\Gamma \simeq G^{p-1} \text{ donc } |\Gamma| = n^{p-1}$$

Pour tout  $x \in \Gamma$  (par la formule des classes)

$$p = |H| = |\text{Orb}(x)| \cdot |\text{Stab}(x)|$$

$$\text{donc } |\text{Orb}(x)| \in \{1, p\}$$

$$\text{Orb}(x) = \{x\} \Leftrightarrow x_1 = x_2 = \cdots = x_p$$

$$\Leftrightarrow x_1^p = e_G$$

Et

$$n^{p-1} = |\Gamma| = \sum_{x \in \Gamma/\sim} |\text{Orb}(x)|$$

$$= \sum_{\substack{x \in \Gamma/\sim \\ |\text{Orb}(x)| = 1}} 1 + \sum_{\substack{x \in \Gamma/\sim \\ |\text{Orb}(x)| > 1}} p$$

$$= |\{x \in G \mid x^p = e_G\}| + kp$$

Avec  $k \in \mathbb{N}$ . Or  $p \mid n$  donc

$$p \mid |\{x \in G \mid x^p = e_G\}| \geq 1$$

Donc il existe au moins  $p - 1$  éléments d'ordre  $p$ .

**Cas  $n = 2$  :**  
On regroupe les éléments avec leurs inverse, ce qui montre par la parité du cardinal l'existence d'un élément d'ordre 2.

# Théorème de Burnside

Énoncer et démonstration du théorème de Burnside.

Soit  $G$  un groupe fini qui agit sur un ensemble  $X$  fini par  $\varphi$ .

On définit pour  $g \in G$

$$\text{Fix}(g) = \{x \in X, g.x = x\}$$

Notons  $N$  le nombre d'orbites :

$$N = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

## Démonstration

On étudie

$$\begin{aligned} \Gamma &= \{(g, x) \in G \times X \mid g.x = x\} \\ &= \bigcup_{x \in X} \{(g, x), g \in \text{Stab}(x)\} \\ &= \bigcup_{g \in G} \{(g, x), x \in \text{Fix}(g)\} \end{aligned}$$

Or par la formule des classes

$$|\text{Stab}(x)| = \frac{|G|}{|\text{Orb}(x)|}$$

D'où (en notant  $x_i$  représentant du  $i$ -ème orbite)

$$\begin{aligned} |\Gamma| &= \sum_{x \in X} |\text{Stab}(x)| \\ &= \sum_{j=1}^N \sum_{x \in \bar{x}_j} |\text{Stab}(x)| \\ &= \sum_{j=1}^N \sum_{x \in \bar{x}_j} \frac{|G|}{|\text{Orb}(x_j)|} \\ &= N |G| \end{aligned}$$

Or

$$|\Gamma| = \sum_{g \in G} |\text{Fix}(g)|$$

D'où

$$N = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

## Exercice : Groupe d'éléments d'ordre inférieur à deux

Propriétés du groupe  $G$  tel que  
 $\forall x \in G, x^2 = 1$

---

On a immédiatement

$$\forall x \in G, x = x^{-1}$$

- $G$  est abélien, soit  $x, y \in G$  :

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

- Si  $G$  fini,  $G \simeq (\mathbb{Z}/2\mathbb{Z})^n$  et  $|G| = 2^n$  pour un  $n \in \mathbb{N}$ .

Passons en notation additive pour plus de clarté :

Faisons de  $G$  un  $\mathbb{F}_2$ -ev :

$$\begin{aligned}\mathbb{F}_2 \times G &\rightarrow G \\ (\bar{k}, g) &\mapsto kg\end{aligned}$$

Qui ne dépend pas du représentant car  $2G = \{0\}$ .

$G$  un  $\mathbb{F}_2$ -ev de dimension finie, donc isomorphe à  $\mathbb{F}_2^n$  en tant qu'espace vectoriel, et à fortiori en tant que groupe.

## Irréductibles d'un anneau

Définition, propriétés élémentaires sur les irréductibles dans un anneau principal.

Soit  $(A, +, \cdot)$  un anneau principal.

- Dans un anneau principal on a un PGCD

Pour tout  $a, b \in A$ , il existe  $d \in A$  tel que  $aA + bA = dA$ , unique (à associés près), qu'on appelle PGCD de  $a$  et  $b$  ( $a \wedge b = d$ ).

On a aussi Bézout car  $d \in dA = aA + bA$  d'où  $\exists (u, v) \in A^2, d = au + bv$ .

- Un élément de  $A$  est dit irréductible si ses seuls diviseurs sont ses associés et les inversibles.
- Pour tout  $a \in A$ , il existe une unique (à permutation et multiplication par des inversibles près) décomposition de  $a$  en irréductibles.

### Démonstration de la décomposition

- Toute suite croissante d'idéaux est stationnaire.

$(I_i)_{i \in \mathbb{N}}$  suite d'idéaux de  $A$  croissante au sens de l'inclusion.

$$K = \bigcup_{i \in \mathbb{N}} I_i$$

Est encore un idéal car union croissante d'idéaux

Par principauté de  $A$ ,  $K = zA$  avec  $z \in K$  donc on dispose de  $k \in \mathbb{N}$  tel que  $z \in I_k$  d'où

$$K = zA \subseteq I_k \subseteq K$$

- Tout élément de  $A$  admet au moins un diviseur irréductible dans  $A$ .

Soit  $x \in A$ , on construit la suite  $(x_n)$  par récurrence :  $x_0 = x$  et pour  $n \in \mathbb{N}$

- Si  $x_n$  irréductible,  $x_{n+1} = x_n$
- Sinon on prend  $x_{n+1}$  diviseur de  $x_n$  non associés et non inversible.

Par définition de la divisibilité,  $(x_n A)_n$  est une suite croissante d'idéaux, et est donc stationnaire.

Soit  $k$  le rang à partir duquel c'est le cas,  $x_k$  est donc un diviseur irréductible de  $x$ .

- Existence de la décomposition : récurrence avec la propriété ci dessus.

- Unicité de la décomposition : on prend deux décomposition on montre que chaque irréductible est présent à la même puissance dans les deux.

# Polynômes en caractéristique strictement positive

Remarques et mises en gardes à propos de  $\mathbb{K}[X]$  quand  $\text{car}(\mathbb{K}) > 0$

Soit  $\mathbb{K}$  un corps tel que  $\text{car}(\mathbb{K}) > 0$

- Le morphisme d'évaluation  $\theta : \mathbb{K}[X] \rightarrow \mathcal{F}(\mathbb{K}, \mathbb{K})$  n'est pas forcément injectif.

Dans  $\mathbb{F}_p$ ,  $\theta(X^p - X) = \theta(0) = 0_{\mathcal{F}(\mathbb{F}_p, \mathbb{F}_p)}$  or  $X^p - 1 \neq 0$ .

- Il n'y a pas équivalence entre multiplicité d'une racine et les valeurs des dérivées successives.

Pour  $\text{car}(\mathbb{K}) = p \in \mathbb{P}$

Pour  $k \in \llbracket 1, p-1 \rrbracket$

$$\binom{k}{p} = \frac{\overbrace{p(p-1) \cdots (p-k+1)}^{p \text{ divise}}}{\underbrace{k!}_{p \text{ ne divise pas}}}$$

D'où  $\binom{k}{p}$  nul dans  $\mathbb{K}$ .

Ainsi pour tout  $a, b \in \mathbb{K}$

$$(a+b)^p = a^p + b^p + \sum_{k=1}^{p-1} \binom{k}{p} a^k b^{p-k}$$

$$= a^p + b^p$$

Et on peut définir le morphisme de corps de Frobenius

$$\sigma : \begin{cases} \mathbb{K} \rightarrow \mathbb{K} \\ x \mapsto x^p \end{cases}$$

Donc dans  $\mathbb{F}_p[X]$

$$Q = (X-1)^p = X^p - 1$$

1 est racine de multiplicité  $p$  de  $Q$  or  $Q' = 0$  d'où pour tout  $k \in \mathbb{N}$ ,  $Q^{(k)}(1) = 0$ .

# Théorème de Wilson

Énoncer et démonstration du théorème de Wilson.

Pour tout  $p \in \mathbb{N}^*$ ,  $p$  est premier si  $(p - 1)! \equiv -1[p]$ .

## Démonstration

- Soit  $n \in \mathbb{N}^*$  non premier.
  - ▶ Si  $3 \leq n = m^2$  avec  $m \in \mathbb{N}^*$ .  $2m \cdot m \mid (n - 1)!$  d'où  $(n - 1)! \equiv 0[n]$
  - ▶ Sinon on dispose de  $1 \leq p, q < n$  tels que  $n = pq$  d'où  $n = pq \mid (n - 1)!$  et  $(n - 1)! \equiv 0[n]$ .
- Soit  $p \in \mathbb{P}$ , étudions  $(p - 1)!$  dans  $(\mathbb{Z}/p\mathbb{Z})^\times$

Soit  $x \in (\mathbb{Z}/p\mathbb{Z})^\times$  tel que  $x^2 = 1$

$$(x + 1)(x - 1) = 0$$

Donc  $x = \{1, -1\}$ .

On peut donc regrouper les éléments du produit  $(p - 1)!$  avec leurs inverses (qui sont dans le produit), à l'exception de 1 et -1 d'où

$$(p - 1)! = (p - 1)(p - 2) \cdots \cdot 1 = -1 \cdot 1 = 1$$

Dans  $\mathbb{Z}/p\mathbb{Z}$ .

## Autre démonstration horrible pour le deuxième sens

Soit  $p \in \mathbb{P}$ , on étudie  $R = X^p - X$  dans  $\mathbb{F}_p[X]$ .

Pour tout  $x \in \mathbb{F}_p$ ,  $R(x) = 0$  donc  $(X - x) \mid R$  et premiers entre eux deux à deux d'où

$$\prod_{x \in \mathbb{F}_p} (X - x) \mid R$$

Et par égalité des degrés on a égalité des polynômes.

Considérons maintenant le morphisme d'anneau suivant :

$$\pi : \begin{cases} \mathbb{Z}[X] & \rightarrow \mathbb{F}_p[X] \\ \sum_{k=0}^n a_k X^k & \mapsto \sum_{k=0}^n \bar{a}_k X^k \end{cases}$$

$$Q = \prod_{k=0}^{p-1} (X - k) = X^p + \sum_{k=0}^{p-1} a_k X^k$$

$$\pi(Q) = \prod_{k=0}^{p-1} (X - \bar{k}) = R$$

$$a_1 = (-1)^{p-1} \sum_{\substack{I \subset [0, p-1] \\ |I| = p-1}} \prod_{i \in I} i$$

$$= (p - 1)!$$

$$\bar{a}_1 = \overline{(p - 1)!} = -1$$

# Formule de Taylor-Lagrange formelle

Formule de Taylor-Lagrange formelle sur  $\mathbb{K}[X]$ , démonstration.

Soit  $\mathbb{K}$  un corps tel que  $\text{car}(\mathbb{K}) = 0$ ,  $P \in \mathbb{K}[X]$ ,  $N \geq \deg P$  et  $a \in \mathbb{K}$ .

$$P = \sum_{k=0}^N P^{(k)}(a) \frac{(X - a)^k}{k!}$$

## Démonstration

Notons  $E = \mathbb{K}_N[X]$  qui est un  $\mathbb{K}$ -ev de dimension  $N + 1$ .

La famille  $((X - a)^k)_{k \in \llbracket 0, N \rrbracket}$  est libre car échelonné en degré, c'est donc une base de  $E$ , et comme  $P \in E$ , et comme  $P \in E$

$$P = \sum_{k=0}^N \lambda_k (X - a)^k$$

Pour  $j \in \llbracket 0, N \rrbracket$

$$\begin{aligned} P^{(j)}(a) &= \sum_{k=j}^N \frac{\lambda_k k!}{(k - j)!} (a - a)^{k-j} \\ &= \lambda_j j! \end{aligned}$$

$$\lambda_j = \frac{P^{(j)}(a)}{j!}$$

# Contenus d'un polynôme à coefficients entiers

Définitions, propriétés, et démonstrations à propos du contenu dans  $\mathbb{Z}[X]$ .

Soit  $P = \sum_{k=0}^d a_k X^k \in \mathbb{Z}[X]$ , on définit le contenu de  $P$  comme

$$c(P) = \bigwedge_{k=0}^d a_k$$

Et on dit qu'un polynôme  $P$  est primitif si  $c(P) = 1$ .

- Soient  $P, Q \in \mathbb{Z}[X]$  tels que  $c(P) = c(Q) = 1$ , alors  $c(PQ) = 1$ . A
- Pour tout  $P, Q \in \mathbb{Z}[X]$ ,  $c(PQ) = c(P)c(Q)$ .

## Démonstration

- Soit  $p \in \mathbb{P}$ , posons le morphisme d'anneau

$$\pi : \begin{cases} \mathbb{Z}[X] & \rightarrow \mathbb{F}_p[X] \\ \sum_{k=0}^d a_k X^k & \mapsto \sum_{k=0}^d \overline{a_k} X^k \end{cases}$$

$c(P) = 1$  donc  $P$  admet au moins un coefficient non divisible par  $p$  et de même pour  $Q$ .

$$\pi(P) \neq 0 \text{ et } \pi(Q) \neq 0$$

$$\pi(PQ) = \pi(P)\pi(Q) \neq 0$$

Donc  $p$  ne divise pas tous les

coefficients de  $PQ$  pour tout

$p \in \mathbb{P}$ , d'où  $c(PQ) = 1$ .

- On remarque que pour  $P \in \mathbb{Z}[X]$

et  $k \in \mathbb{Z}$ ,  $c(kP) = kc(P)$  et on

étudie  $\tilde{P} = \frac{P}{c(P)}$  et  $\tilde{Q} = \frac{Q}{c(Q)}$ .

# Exercice : Produit de polynômes de rationnels unitaire entier

Soient  $P, Q \in \mathbb{Q}[X]$  unitaires, montrer que si  $PQ \in \mathbb{Z}[X]$  alors  $P, Q \in \mathbb{Z}[X]$ .

---

$P, Q \in \mathbb{Q}[X]$  unitaires,  $PQ \in \mathbb{Z}[X]$ .

Comme  $PQ$  unitaire  $c(PQ) = 1$ . On trouve  $a, b \in \mathbb{Z}$  tels que  $aP, bQ \in \mathbb{Z}[X]$ .

$$c(aP)c(bQ) = abc(PQ) = ab$$

Or  $P$  et  $Q$  étant unitaires

$$\begin{cases} c(aP) \mid a \\ c(bQ) \mid b \end{cases} \text{ donc } \begin{cases} a = k_a c(aP) \\ b = k_b c(bQ) \end{cases}$$

$$c(aP)c(bQ) = ab = k_a k_b c(aP)c(bQ)$$

$$\text{d'où } k_a = k_b = 1 \text{ et } \begin{cases} a = c(aP) \\ b = c(bQ) \end{cases}$$

Ainsi

$$\begin{cases} P = a \frac{P}{a} \in \mathbb{Z}[X] \\ Q = b \frac{Q}{b} \in \mathbb{Z}[X] \end{cases}$$

# Exercice :

## Irréductibilité dans les rationnels

Soit  $P \in \mathbb{Z}[X]$  dont les seuls diviseurs dans  $\mathbb{Z}[X]$  sont de degré 0 ou  $\deg P$ , montrer que  $P$  est irréductible dans  $\mathbb{Q}[X]$ .

On suppose par contraposé que  $P$  n'est pas irréductible dans  $\mathbb{Q}$ .

$$P = QR$$

$$1 \leq \deg Q, \deg R \leq \deg P - 1$$

On introduit  $a, b \in \mathbb{Z}$  tels que  $aQ, bR \in \mathbb{Z}[X]$ .

$$\begin{aligned} abc(P) &= c(aQbR) \\ &= c(aQ)c(bR) \end{aligned}$$

$$\begin{aligned} P &= \frac{aQbR}{ab} \\ &= \frac{(aQ)(bR)}{\frac{c(aQ)c(bR)}{c(P)}} \\ &= c(P) \cdot \underbrace{\frac{aQ}{c(aQ)}}_{Q_0} \cdot \underbrace{\frac{bR}{c(bR)}}_{R_0} \in \mathbb{Z}[X] \end{aligned}$$

Avec  $Q_0$  et  $R_0$  diviseurs de  $P$  dans  $\mathbb{Z}[X]$  de degrés compris dans  $\llbracket 1, \deg P - 1 \rrbracket$ .

# Entiers algébriques

Définition d'entier algébrique.

Soit  $a \in \mathbb{C}$ , on dit que  $a$  est un entier algébrique s'il existe  $Q \in \mathbb{Z}[X]$  unitaire tel que  $Q(a) = 0$ .

- $a$  est donc aussi algébrique dans  $\mathbb{Q}$ , et son polynôme minimal est aussi dans  $\mathbb{Z}[X]$ .

## Entiers algébriques de degré 2

- $a \in \mathbb{C}$  entier algébrique de degré 2 : on dispose de  $\pi_a \in \mathbb{Z}[X]$  unitaire de degré 2 qui annule  $a$ .  $\mathbb{Z}[a] = \text{im } \theta_a$  est un sous-anneau de  $\mathbb{R}$  (et donc de  $\mathbb{C}$ ).
- $\mathbb{Z}[a] = \{x + ay, (x, y) \in \mathbb{Z}^2\}$  et tout élément s'écrit de manière unique sous cette forme.
- On peut écrire  

$$\pi_a = (X - a)(X - \beta)$$

On remarque que  $\beta \in \mathbb{Z}[a]$  car  $a + \beta = a \in \mathbb{Z}$  d'où  $\beta = a - a \in \mathbb{Z}[a]$ .

On définit

$$\tau : \begin{cases} \mathbb{Z}[a] & \rightarrow \mathbb{Z}[a] \\ x + ay & \mapsto x + \beta y \end{cases}$$

On a alors

$$\forall z, z' \in \mathbb{Z}[a], \tau(zz') = \tau(z)\tau(z')$$

- Et on peut alors définir

$$N : \begin{cases} \mathbb{Z}[a] & \rightarrow \mathbb{Z} \\ z = x + ay & \mapsto z\tau(z) \end{cases}$$

Qui est aussi multiplicatif.

- $z \in \mathbb{Z}[a]$  est inversible ssi  $N(z) = |1|$ .

## Démonstration

- Notons  $P_a$  ce polynôme, comme  $Q(a) = 0, P_a \mid Q$  dans  $\mathbb{Q}[X]$ , d'où

$$\mathbb{Z}[X] \ni Q = P_a R \in \mathbb{Q}[X]$$

Et donc  $P_a, R \in \mathbb{Z}[X]$  car  $Q$  unitaire (cf. exercices sur le contenu).

- $a$  de degré 2 donc

$$\pi_a(X) = X^2 + aX + b$$

- On a déjà  $\{x + ay, (x, y) \in \mathbb{Z}^2\} \subseteq \mathbb{Z}[a]$ .
- Soit  $x = P(a) \in \mathbb{Z}[a]$ ,  $P = Q\pi_a + R$  avec  $Q \in \mathbb{K}[X], R \in \mathbb{K}_1[X]$ .

Donc

$$R = yX + x \in \mathbb{Z}[X]$$

$$P(a) = \underbrace{Q(a)\pi_{a(a)}}_0 + ya + x$$

- Soit  $x_1 + ay_1 = x_2 + ay_2$  avec  $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ .

$$x_1 - x_2 = (y_2 - y_1)a$$

Par l'absurde, si  $y_1 \neq y_2$  :

$$a = \frac{x_1 - x_2}{y_2 - y_1} \in \mathbb{Q}[X]$$

Qui est absurde car  $\pi_a$  serait de degré 1.

- Soit  $z = x + ay \in \mathbb{Z}[a]$

$$N(z) = z\tau(z) = (x + ay)(x + \beta y) = x^2 + (a + \beta)xy + a\beta y^2$$

$$= x^2 + axy + a\beta y^2 \in \mathbb{Z}$$

- Soit  $z \in \mathbb{Z}[a]$  inversible, on dispose de  $z' \in \mathbb{Z}[a]$  tel que  $zz' = 1$ .

$$N(zz') = N(1) = 1 = N(z)N(z')$$

Donc  $|N(z)| = 1$

- Soit  $z \in \mathbb{Z}[a]$  tel que  $N(z) = \varepsilon \in \{1, -1\}$

$$(x + ay)(x + \beta y) = \varepsilon$$

$$z(\varepsilon x + \varepsilon \beta y) = 1 = \varepsilon$$

$$z^{-1} = \varepsilon(x + \beta y)$$

# Exercice : Polynômes à coefficients entiers

1. Soit  $P = \sum_{k=0}^d a_k X^k \in \mathbb{Z}[X]$ , montrer que si  $P$  admet une racine rationnelle  $\frac{p}{q}$  avec  $p \wedge q = 1$ , alors  $q \mid a_d$  et  $p \mid a_0$ .
- 

1.

$$0 = P\left(\frac{p}{q}\right) = \sum_{k=0}^d a_k p^k q^{d-k}$$

$$-\underbrace{\sum_{k=0}^{d-1} a_k p^k q^{d-k}}_{\text{divisible par } q} = a_d p^d$$

$$-\underbrace{\sum_{k=1}^d a_k p^k q^{d-k}}_{\text{divisible par } p} = a_0 q^d$$

D'où  $\begin{cases} q \mid a_d p^d \\ p \mid a_0 q^d \end{cases}$  or  $q \wedge p = 1$  donc par le théorème de Gauss,

$$\begin{cases} q \mid a_d \\ p \mid a_0 \end{cases}$$

On en déduit que si  $P \in \mathbb{Z}[X]$  est unitaire et admet une racine rationnelle, alors elle est entière.

## Critère d'Eisenstein

Énoncé et démonstration du critère d'Eisenstein.

Soit  $P = \sum_{k=0}^d a_k X^k \in \mathbb{Z}[X]$  tel qu'il existe  $p \in \mathbb{P}$  et

$$\begin{cases} \forall k \in \llbracket 0, d-1 \rrbracket, p \mid a_k \\ p \nmid a_d \\ p^2 \nmid a_0 \end{cases}$$

Alors  $P$  n'a pas de diviseurs dans  $\mathbb{Z}[X]$  de degré compris dans  $\llbracket 1, d-1 \rrbracket$ , et est donc irréductible dans  $\mathbb{Q}[X]$  (cf. exercices sur le contenu).

### Démonstration

On considère le morphisme d'anneau suivant

$$\pi : \begin{cases} \mathbb{Z}[X] & \rightarrow \mathbb{F}_p[X] \\ \sum_{k=0}^d a_k X^k & \mapsto \sum_{k=0}^d \overline{a_k} X^k \end{cases}$$

Supposons par l'absurde que  $P = QR$  avec  $Q, R \in \mathbb{Z}[X]$

$$\overline{0} \neq \overline{a_d} X^d = \pi(P) = \pi(Q)\pi(R)$$

Par unicité de la décomposition en irréductibles dans  $\mathbb{F}_p[X]$

$$\pi(Q) = aX^k \quad \pi(R) = \beta X^l$$

$$k + l = d \quad \deg Q \geq k \quad \deg R \geq l$$

Or  $\deg Q + \deg R = d$  d'où

$$Q = \sum_{i=0}^k b_i X^i \text{ avec } \begin{cases} \overline{b_k} = a \neq 0 \\ \overline{b_0} = 0 \end{cases}$$

$$R = \sum_{i=0}^l c_i X^i \text{ avec } \begin{cases} \overline{c_l} = \beta \neq 0 \\ \overline{c_0} = 0 \end{cases}$$

D'où  $a_0 = b_0 c_0$  est divisible par  $p^2$ , absurde.

# Exercice : rationalité d'une racine de haute multiplicité

Soit  $P \in \mathbb{Q}[X]$  de degré  $n$  et  $a$  racine de  $P$  de multiplicité  $m_a > \frac{n}{2}$ , montrer que  $a \in \mathbb{Q}$ .

---

Soit  $P \in \mathbb{Q}[X]$  de degré  $n$  et  $a$  racine de  $P$  de multiplicité  $m_a > \frac{n}{2}$ .

$$P = \prod_{k=0}^N Q_k^{p_k}$$

Décomposition en irréductibles de  $P$  dans  $\mathbb{Q}[X]$ . Pour tout  $i \neq j$ ,  $P_i \wedge P_j = 1$  dans  $\mathbb{Q}[X]$  et donc dans  $\mathbb{C}[X]$ .

Ainsi  $a$  n'est racine que d'un des  $P_i$ , notons  $P_1(a) = 0$ .

C'est une racine simple car  $P_1$  irréductible, d'où

$$p_1 \geq m_a > \frac{n}{2}$$

$$2p_1 > n \geq p_1 \deg(P_1)$$

$$2 > \deg(P_1) = 1$$

Donc  $P_1 = \lambda(X - a) \in \mathbb{Q}[X]$  d'où  $a \in \mathbb{Q}$ .

# Algèbres

Définition d'une  $\mathbb{K}$ -Algèbre avec  $\mathbb{K}$  un corps.

Une  $\mathbb{K}$ -Algèbre est un ensemble  $A$  muni de deux lois de composition internes  $(+)$ ,  $(\times)$  et d'une loi de composition externe  $(\cdot)$  tel que

- $(A, +, \times)$  est un anneau
- $(A, +, \cdot)$  est un  $\mathbb{K}$ -ev
- $\forall(a, x, y) \in \mathbb{K} \times A^2$

$$a(x \times y) = (ax) \times y = x \times (ay)$$

## Exemples

- $\mathbb{K}$  est une  $\mathbb{K}$ -Algèbre
- $(\mathbb{K}[X], +, \times, \cdot)$  est une  $\mathbb{K}$ -Algèbre
- Pour  $E$  un  $\mathbb{K}$ -ev,  $(\mathcal{L}(E), +, \circ, \cdot)$  est une  $\mathbb{K}$ -Algèbre.

## Exercice : existence d'un élément d'ordre du ppcm de deux autres

1. Soit  $G$  un groupe abélien fini, montrer que pour tout  $x, y \in G$ , il existe un élément  $z \in G$  tel que  $\text{ord}(z) = \text{ord}(x) \vee \text{ord}(y)$ .
2. En déduire que

$$\max_{g \in G} \text{ord}(g) = \bigvee_{g \in G} \text{ord}(g)$$

- 
1. Soit  $G$  un groupe abélien,  $x, y \in G$  qui admettent un ordre.

$$\text{ord}(x) = \prod_{i=1}^N p_i^{a_i}$$

$$\text{ord}(y) = \prod_{i=1}^N p_i^{\beta_i}$$

Pour tout  $k \in \llbracket 1, N \rrbracket$

$$\text{ord}\left(x^{\prod_{i \neq k} p_i^{a_i}}\right) = p_k^{a_k}$$

$$\text{ord}\left(y^{\prod_{i \neq k} p_i^{\beta_i}}\right) = p_k^{\beta_k}$$

On pose alors

$$z_k = \begin{cases} x^{\prod_{i \neq k} p_i^{a_i}} & \text{si } a_k \geq \beta_k \\ y^{\prod_{i \neq k} p_i^{\beta_i}} & \text{sinon} \end{cases}$$

D'où  $\text{ord}(z_k) = p_k^{\max(a_k, \beta_k)}$

Ainsi en posant  $z = \prod_{k=1}^N z_k$  :

$$\text{ord}(z) = \prod_{k=1}^N p_k^{\max(a_k, \beta_k)}$$

$$= \text{ord}(x) \vee \text{ord}(y)$$

(Car  $G$  est abélien).

2. Par récurrence (car  $G$  fini) on dispose de  $h \in G$  tel que

$$\text{ord}(h) = \bigvee_{g \in G} \text{ord}(g) = m$$

Posons  $g_0 \in G$  d'ordre  $\max_{g \in G} \text{ord}(g)$ .

On a donc

$$m \leq \text{ord}(g_0) \mid m$$

$$m = \text{ord}(g_0)$$

## Exercice : Cyclicité des sous-groupes finis des inversibles d'un corps

Soit  $\mathbb{K}$  un corps, et  $G \leq \mathbb{K}^*$  fini.  
Montrer que  $G$  est cyclique.

### Première méthode

On utilise la propriété suivante (à redémontrer) : si  $G$  abélien fini

$$\max_{g \in G} \text{ord}(g) = \bigvee_{g \in G} \text{ord}(g)$$

Or pour tout  $g \in G$ ,  $g^m = 1$  d'où  
 $G \subset \{\text{racines de } X^m - 1 \text{ dans } \mathbb{K}[X]\}$

D'où  $|G| \leq m$  car  $\mathbb{K}$  est un corps et ainsi l'élément d'ordre maximale est d'ordre supérieure ou égal au cardinal de  $G$ , d'où  $G$  cyclique.

### Deuxième méthode

Pour  $d \mid n = |G|$  on pose

$$\Gamma_d = \{g \in G \mid \text{ord}(g) = d\}$$

$$G = \bigcup_{d \mid n} \Gamma_d$$

$$n = \sum_{d \mid n} |\Gamma_d|$$

On pose aussi

$$A_d = \{g \in G \mid g^d = 1\} \\ = \{\text{racines de } X^d - 1\} \cap G$$

$$|A_d| \leq d$$

Pour  $d \mid n$  on a

- $\Gamma_d = \emptyset$  et  $|\Gamma_d| = 0$
- Ou il existe  $x \in \Gamma_d$ , d'où  $\langle x \rangle \subset A_d$  et  $d \leq |A_d| \leq d$ .

Ainsi

$$\Gamma_d = \{g \in A_d = \langle x \rangle \mid \text{ord}(g) = d\}$$

$$|\Gamma_d| = \varphi(d)$$

Finalelement

$$\sum_{d \mid n} \varphi(d) = n = \sum_{d \mid n} \underbrace{|\Gamma_d|}_{\in \{0, \varphi(d)\}}$$

D'où nécessairement  $|\Gamma_d| = \varphi(d)$  pour tout  $d \mid n$ , en particulier pour  $|\Gamma_n| = \varphi(n) > 0$  : il existe  $\varphi(n)$  éléments d'ordre  $n$ .

## Exercice : Les carrés de $\mathbb{F}_p$

Notons  $\mathbb{F}_p^2 = \{x^2, x \in \mathbb{F}_p\}$  et  $\mathbb{F}_p^{*2} = \{x^2, x \in \mathbb{F}_p^*\}$ .

- Montrer que  $|\mathbb{F}_p^2| = \frac{p+1}{2}$  et  $|\mathbb{F}_p^{*2}| = \frac{p-1}{2}$ .
- Montrer que pour  $x \in \mathbb{F}_p^*$ ,  $x \in \mathbb{F}_p^{*2}$  ssi  $x^{\frac{p-1}{2}} = 1$ .
- En déduire que pour  $p \geq 3$ ,  $-1$  est un carré ssi  $p \equiv 1[4]$ .
- On suppose  $p \equiv 3[4]$ , pour  $x \in \mathbb{F}_p^*$  montrer que  $x$  est un carré ssi  $-x$  n'en est pas un.
- Soit  $p \in \mathbb{P}$  |  $p \equiv -1[4]$ , pour tout  $r \in \mathbb{F}_p^*$  montrer que  $\Gamma_r = \{(x, y) \in (\mathbb{F}_p^*)^2 \mid x^2 - y^2 = r\}$  est de cardinal  $p - 3$ .

- On étudie le morphisme de groupe

$$\theta : \begin{cases} \mathbb{F}_p^* \rightarrow \mathbb{F}_p^{*2} \\ x \mapsto x^2 \end{cases}$$

$$\begin{aligned} \ker \theta &= \{x \in \mathbb{F}_p^*, x^2 = 1\} \\ &= \{x \in \mathbb{F}_p^*, (x-1)(x+1) = 0\} \\ &= \{-1, 1\} \end{aligned}$$

$$\underbrace{|\ker \theta|}_{2} \cdot \underbrace{|\text{im } \theta|}_{|\mathbb{F}_p^{*2}|} = p - 1$$

$$\text{D'où } |\mathbb{F}_p^{*2}| = \frac{p-1}{2}.$$

Et  $\mathbb{F}_p = \mathbb{F}_p^* \cup \{0\}$  d'où

$$|\mathbb{F}_p^2| = |\mathbb{F}_p^{*2}| + 1 = \frac{p+1}{2}$$

- Soit  $x \in \mathbb{F}_p^{*2}$ , on écrit  $x = y^2$  avec  $y \in \mathbb{F}_p^*$ .

$$\begin{aligned} x^{\frac{p-1}{2}} &= y^{p-1} = 1 \\ \Leftrightarrow (-x)^{\frac{p-1}{2}} &= -1 \\ \Leftrightarrow -x &\notin \mathbb{F}_p^* \end{aligned}$$

D'où

$$\underbrace{\mathbb{F}_p^{*2}}_{\frac{p-1}{2}} \subset \underbrace{\{\text{racines de } X^{\frac{p-1}{2}} - 1\}}_{\leq \frac{p-1}{2}}$$

D'où l'égalité des ensembles.

- $\overline{-1} \in \mathbb{F}_p^2 \Leftrightarrow (-1)^{\frac{p-1}{2}} = \overline{1}$   
 $\Leftrightarrow \frac{p-1}{2} \in 2\mathbb{Z}$   
 $\Leftrightarrow p \equiv 1[4]$

- On suppose  $p \equiv 3[4]$

$$(-1) \notin \mathbb{F}_p^2 \text{ car } (-1)^{\frac{p-1}{2}} = -1$$

$$x \in \mathbb{F}_p^2 \Leftrightarrow x^{\frac{p-1}{2}} = 1$$

$$\Leftrightarrow (-x)^{\frac{p-1}{2}} = -1$$

$$\Leftrightarrow -x \notin \mathbb{F}_p^*$$

- Si  $r$  est un carré,  $r = a^2$  avec  $a \in \mathbb{F}_p^*$

$$(x, y) \in \Gamma_r \Leftrightarrow x^2 - y^2 = a^2$$

$$\Leftrightarrow (xa^{-1})^2 - (ya^{-1})^2 = 1$$

$$\Leftrightarrow (xa^{-1}, ya^{-1}) \in \Gamma_1$$

D'où  $|\Gamma_r| = |\Gamma_1|$

$$\underbrace{|\Gamma_r|}_{\frac{p-1}{2}} = \underbrace{|\Gamma_1|}_{\leq \frac{p-1}{2}}$$

- Si  $r$  n'est pas un carré,  $-r$  en est un.

$$(x, y) \in \Gamma_r \Leftrightarrow y^2 - x^2 = -r$$

Et on se ramène au cas précédent.

$$|\Gamma_r| = |\Gamma_1|$$

Dénombrons  $\Gamma_1$ .

$$(x, y) \in \Gamma_1 \Leftrightarrow x^2 - y^2 = 1$$

$$\Leftrightarrow (x-y)(x+y) = 1$$

Posons  $a = x+y$ ,  $b = x-y$  ( $p$  impair d'où  $2 \in \mathbb{F}_p^*$ )

$$\begin{aligned} x &= a + \frac{b}{2} \\ y &= a - \frac{b}{2} \end{aligned}$$

$$(x, y) \in \Gamma_1 \Leftrightarrow b = a^{-1}$$

On a  $(p-1)$  choix pour  $a$ , et  $b$  déterminé par  $a$ , d'où au plus  $(p-1)$  couples.

Il faut exclure les cas où notre choix de  $a$  permet  $x, y \notin \mathbb{F}_p^*$ :

$$x = \overline{0} \Leftrightarrow a = -a^{-1}$$

$$\Leftrightarrow a^2 = -1$$

$$y = \overline{0} \Leftrightarrow a = a^{-1}$$

$$\Leftrightarrow a^2 = 1$$

Ainsi  $|\Gamma_r| = |\Gamma_1| = p - 3$ .

## Sous algèbres

Définition, propriétés des sous-algèbres.

---

Soit  $(A, +, \times, \cdot)$  une  $\mathbb{K}$ -algèbre,  $B \subset A$  est une sous-algèbre de  $A$  si c'est un sous-anneau et un  $\mathbb{K}$ -espace vectoriel de  $A$ .

De plus si  $B$  est de dimension finie

$$B^\times = B \cap A^\times$$

### Démonstration

On a évidemment  $B^\times \subset B \cap A^\times$ .

On suppose  $b \in B \cap A^\times$ , on dispose de  $a \in A$ ,  $ab = ba = 1$ .

On pose

$$\varphi_b = \begin{cases} B & \rightarrow B \\ x & \mapsto bx \end{cases} \in \mathcal{L}(B)$$

Soit  $x \in \ker \varphi_b$ , on a  $bx = 0$  donc  $(ab)x = x = 0$ .

Donc  $\varphi_b$  bijectif (argument dimensionnel), et  $\varphi_b^{-1}(1) = a$  existe et  $a \in B$ .

# Algèbres commutatives intègres de dimension finie

Que peut-on dire d'une algèbre  $(A, +, \times, \cdot)$  commutative et intègre de dimension finie ?

---

Si  $(A, +, \times, \cdot)$  est commutative, intègre et de dimension finie, alors c'est un corps.

## Démonstration

Soit  $a \in A \setminus \{0\}$ , étudions

$$\varphi_a : \begin{cases} A & \rightarrow A \\ x & \mapsto ax \end{cases} \in \mathcal{L}(A)$$

$$\begin{aligned} \ker \varphi_a &= \{x \in A \mid ax = 0\} \\ &= \{x \in A \mid x = 0\} \quad (\text{par intégrité}) \\ &= \{0\} \end{aligned}$$

Et par argument dimensionnel,  $\varphi_a$  bijectif, d'où  $\varphi_a^{-1}(a) = a^{-1}$  existe.

## Morphisme d'algèbre

Définition, propriétés des morphismes d'algèbres.

---

Pour  $A, B$  deux  $\mathbb{K}$ -algèbre, une application  $\varphi : A \rightarrow B$  est un morphisme d'algèbre si c'est un morphisme d'anneau linéaire.

Et dans ce cas  $\text{im } \varphi$  est une sous-algèbre de  $B$  et  $\ker \varphi$  est un idéal et un sev de  $A$ .

## Dévissage de groupes

Propriétés, outils du dévissage de groupes.

1. Soient  $G$  et  $H$  deux groupes cycliques de cardinaux  $n$  et  $p$ ,  $G \times H$  est cyclique ssi  $n \wedge p = 1$ .

2.

### Démonstration

1. • Par contraposé, supposons que  $n \wedge p = d > 1$ , ainsi  $m = n \vee p < np$ .

Pour tout  $(x, y) \in G \times H$ ,

$$(x, y)^m = (x^m, y^m) = (e_G, e_H)$$

donc  $\text{ord}((x, y)) \mid m < |G \times H|$  qui ne peut être cyclique.

• Soit  $x \in G$  d'ordre  $n$  et  $y \in H$  d'ordre  $p$ . Pour  $k \in \mathbb{N}^*$

$$(x, y)^k \Leftrightarrow (x^k, y^k) = (e_G, e_H)$$

$$\Leftrightarrow \begin{cases} n \mid k \\ p \mid k \end{cases} \Leftrightarrow np \mid k$$

$\Leftrightarrow G \times H$  cyclique

• Autre méthode :

$$G \simeq \mathbb{Z}/n\mathbb{Z}$$

$$H \simeq \mathbb{Z}/p\mathbb{Z}$$

$$G \times H \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

$$\simeq \mathbb{Z}/(np)\mathbb{Z} \text{ cyclique}$$

2. Soient  $H, K$  sous-groupes de  $G$  et  $\varphi$  (qui n'est pas forcément un morphisme) tel que

$$\varphi : \begin{cases} H \times K \rightarrow G \\ (h, k) \mapsto hk \end{cases}$$

On note  $HK = \varphi(H \times K)$ . Soient  $(h, k), (h_0, k_0) \in H \times K$

$$\varphi(h, k) = \varphi(h_0, k_0)$$

$$\Leftrightarrow hk = h_0k_0$$

$$\Leftrightarrow h_0^{-1}h = k_0k_0^{-1} = t \in H \cap K$$

$$\Leftrightarrow \exists t \in H \cap K, \begin{cases} h = k_0t \\ k = t^{-1}h_0 \end{cases}$$

$\varphi$  est injectif ssi  $H \cap K = \{e_G\}$ , c'est automatique si  $|H| \wedge |K| = 1$  (en étudiant les ordres et les divisibilités de ceux-ci).

Dans ce cas  $|HK| = |\text{im } \varphi| = |H| \cdot |K|$

Dans le cas général

$$|\varphi^{-1}\{\varphi(h_0, k_0)\}| = |H \cap K|$$

# Groupe Diédral

Construction et propriétés du groupe diédral.

## Construction

Soient  $n \geq 2$  et  $A_0, \dots, A_{n-1}$  des points de  $\mathbb{R}^2$  d'afixes

$$\forall i \in \llbracket 0, n-1 \rrbracket, A_i : e^{\frac{2ik\pi}{n}}$$

On considère  $\Gamma$  l'ensemble des isométries qui préservent le polygone  $A_0, \dots, A_{n-1}$ .

Comme une transformation affine préserve les barycentres, tout élément de  $\Gamma$  préserve l'isobarycentre (l'origine).

On a alors

$$\Gamma \in O(\mathbb{R}^2)$$

Et donc tout  $\gamma \in \Gamma$ , est soit une rotation ou une réflexion.

- Si  $\gamma$  est une rotation :  $\gamma(A_0) \in \{A_0, \dots, A_{n-1}\}$  d'où  $\gamma = \text{rot}\left(\frac{2k\pi}{n}\right)$  pour un  $k \in \llbracket 0, n-1 \rrbracket$ .

On note  $r$  la rotation d'angle  $\frac{2\pi}{n}$

$$\gamma = r^k$$

- Si  $\gamma$  est une réflexion

Soit  $s$  la réflexion à l'axe des abscisses,  $s \in \Gamma$ .

$s \circ \gamma \in \Gamma$  est une rotation car

$$\det(s \circ \gamma) = (-1)^2 = 1$$

Ainsi  $\exists k \in \llbracket 0, n-1 \rrbracket$  tel que

$$s \circ \gamma = r^k \Leftrightarrow \gamma = s \circ r^k$$

Donc

$$\Gamma = \bigcup_{k=0}^{n-1} \{r^k, sr^k\}$$

## Groupe

$\Gamma$  est un sous-groupe de  $O(\mathbb{R}^2)$ .

- $|\Gamma| = 2n$
- $\Gamma = \langle s, r \rangle$

## Algèbre engendrée

Pour  $(A, +, \times, \cdot)$  une  $\mathbb{K}$ -algèbre et  $a \in A$ , définition et propriétés de  $\mathbb{K}[a]$ .

Soit  $(A, +, \times, \cdot)$  une  $\mathbb{K}$ -algèbre et  $a \in A$ . Si on pose le morphisme d'algèbre

$$\theta_a : \begin{cases} \mathbb{K}[X] & \rightarrow A \\ P = \sum_{k=0}^d a_k X^k & \mapsto \sum_{k=0}^d a_k a^k \end{cases}$$

On note  $\mathbb{K}[a] = \text{im } \theta_a$  qui est la plus petite sous-algèbre de  $A$  contenant  $a$ .

De plus  $\ker \theta_a$  est un idéal de  $\mathbb{K}[X]$ .

- Si  $\theta_a$  est injectif et  $\mathbb{K}[a] \simeq \mathbb{K}[X]$  qui est donc de dimension infinie.
- Sinon on dispose d'un unique polynôme  $\pi_a$  unitaire tel que  $\ker \theta_a = \pi_a \mathbb{K}[X]$  (par principauté).  
 $\pi_a$  est appelé polynôme minimal de  $a$ ,  $\mathbb{K}[a]$  est de dimension  $d = \deg \pi_a$  et  $(1, a, \dots, a^{d-1})$  en est une base.

### Démonstration

- Soit  $B \in \mathbb{K}[X] \setminus \{0\}$  et  $d = \deg B$ , par l'éxistence et l'unicité de la division euclidienne on a

$$\mathbb{K}[X] = B\mathbb{K}[X] \oplus \mathbb{K}_{d-1}[X]$$

- Soit  $u \in L(E, F)$  et  $G$  un supplémentaire de  $\ker u$ , montrons que  $u|_G$  est un isomorphisme de  $G \rightarrow \text{im } u$ .  
 $\ker u|_G = \ker u \cap G = \{0\}$  par supplémentarité.

Soit  $y \in \text{im } u$ ,  $y = u(x)$ ,  $x = a + b$  avec  $(a, b) \in \ker u \times G$ .

$$u(x) = \underbrace{(a)}_0 + u(b)$$

$$y = u|_G(b)$$

Soit  $y \in \text{im } u|_G$ ,  $y = u|_G(x) = u(x)$ .

D'où  $\text{im } u = \text{im } u|_G$ .

- Si  $\theta_a$  est injectif, c'est un isomorphisme de  $\mathbb{K}[X]$  sur  $\text{im } \theta_a = \mathbb{K}[a]$ .

- Sinon on a  $\pi_a$  de degré  $d$  et

$$\mathbb{K}[X] = \pi_a \mathbb{K}[X] \oplus \mathbb{K}_{d-1}[X]$$

$\mathbb{K}_{d-1}$  est un supplémentaire de  $\ker \theta_a$ , ainsi  $\theta_a|_{\mathbb{K}_{d-1}[X]}$  est un isomorphisme de  $\mathbb{K}_{d-1}[X] \rightarrow \mathbb{K}[a]$ , d'où

$$\dim \mathbb{K}[a] = d$$

Et l'image de la base canonique de  $\mathbb{K}_{d-1}[X]$  par  $\theta|_{\mathbb{K}_{d-1}[X]}$  est

$$(1, a, \dots, a^{d-1})$$

Qui est donc une base de  $\mathbb{K}[a]$ .

# Condition d'intégrité d'une sous-algèbre engendrée

Pour  $A$  une  $\mathbb{K}$ -algèbre et  $a \in A$  tel que  $\theta_a$  n'est pas injectif, sous quelle condition  $\mathbb{K}[a]$  est-elle intègre ?

Soit  $A$  une  $\mathbb{K}$ -algèbre et  $a \in A$  tel que  $\theta_a$  n'est pas injectif.

$\mathbb{K}[a]$  est intègre ssi  $\pi_a$  est irréductible.

## Démonstration

- Si  $\pi_a$  irréductible, soit  $x = P(a), y = Q(a) \in \mathbb{K}[a]$  tels que  $xy = 0$ .

$$PQ(a) = 0$$

$$\pi_a \mid PQ$$

Donc par le lemme d'Euclide,

$$\text{ou } \begin{array}{l} \pi_a \mid P \Leftrightarrow x = 0 \\ \pi_a \mid Q \Leftrightarrow y = 0 \end{array}$$

- Par contraposé, si  $\pi_a$  non irréductible,  $\pi_a = PQ$  avec  $P, Q \in \mathbb{K}[X]$  non inversible ou associé à  $\pi_a$ .

$$\underbrace{P(a)}_{\neq 0} \underbrace{Q(a)}_{\neq 0} = \pi_a(a) = 0$$

D'où  $\mathbb{K}[a]$  non intègre.

# inversibilité des éléments d'une sous-algèbre engendrée

Soit  $\mathbb{K}[a]$  une sous-algèbre de  $A$  de dimension finie pour  $a \in A$ , sous quelle condition  $x \in \mathbb{K}[a]$  est-il inversible ?

Soit  $\mathbb{K}[a]$  une sous-algèbre de  $A$  de dimension finie pour  $a \in A$ . Soit  $x = P(a) \in \mathbb{K}[a]$ .

$$x \in \mathbb{K}[a]^* \text{ ssi } P \wedge \pi_a = 1$$

On en déduit que  $\mathbb{K}[a]$  est un corps ssi  $\pi_a$  est irréductible.

## Démonstration

Par propriété de sous-algèbre

$$\mathbb{K}[a]^* = A^* \cap \mathbb{K}[a]$$

Ainsi

$$\begin{aligned} x \in \mathbb{K}[a]^* &\Leftrightarrow \exists y \in \mathbb{K}[a], xy = 1 \\ &\Leftrightarrow \exists Q \in \mathbb{K}[X], PQ(a) = 1 \\ &\Leftrightarrow \exists Q \in \mathbb{K}[X], \pi_a \mid (PQ - 1) \\ &\Leftrightarrow \exists Q, V \in \mathbb{K}[X], PQ - 1 = \pi_a V \\ &\Leftrightarrow \exists Q, V \in \mathbb{K}[X], PQ - \pi_a V = 1 \\ &\Leftrightarrow P \wedge \pi_a = 1 \end{aligned}$$

Ainsi si  $\pi_a$  irréductible, pour tout  $x = P(a) \in \mathbb{K}[a] \setminus \{0\}$ ,  $P \wedge \pi_a = 1$  d'où  $x$  inversible et  $\mathbb{K}[a]$  est un corps.

Et si  $\mathbb{K}[a]$  est un corps, alors il est intègre et  $\pi_a$  irréductible.

# Algèbres et extensions de corps

Propriétés des algèbres en lien avec les extensions de corps.

---

Soient  $\mathbb{K} \subseteq \mathbb{L}$  deux corps. On remarque que  $\mathbb{L}$  est une  $\mathbb{K}$ -algèbre.

1. Soit  $a \in \mathbb{L}$  qui admet un polynôme annulateur dans  $\mathbb{K}[X]$  et  $\pi_a$  son polynôme minimal.

$\pi_a$  est irréductible dans  $\mathbb{K}[X]$  et  $\mathbb{K}[a]$  est un corps.

## Démonstration

1.  $P, Q \in \mathbb{K}[X]$  tels que  $\pi_a = PQ$ .

Dans  $\mathbb{L}$

$$P(a)Q(a) = \pi_a(a) = 0$$

Donc  $P(a) = 0 \Leftrightarrow \pi_a \mid P$  ou  $Q(a) = 0 \Leftrightarrow \pi_a \mid Q$  donc  $\pi_a$  irréductible.

Ainsi  $\mathbb{K}[a]$  est un corps.

# Nombres algébriques

Définitions et propriétés des nombres algébriques sur un corps  $\mathbb{K}$ .

---

Soit  $a \in A$  une  $\mathbb{K}$ -algèbre, on dit que  $a$  est algébrique sur  $\mathbb{K}$  s'il admet un polynôme annulateur dans  $\mathbb{K}[X]$ .

Par défaut  $a$  algébrique veut dire algébrique sur  $\mathbb{Q}$ , quitte à les échangers prenons  $P(a) = 0, P \in \ker \theta_a = \pi_a \mathbb{K}[X]$ .

## Propriété

1. Soit  $a \in \mathbb{L}$  une extension de corps de  $\mathbb{K}$ ,  $a$  algébrique sur  $\mathbb{K}$ .

Pour tout  $P \in \mathbb{K}[X]$  unitaire,  $P = \pi_a$  ssi  $P(a) = 0$  et  $P$  irréductible sur  $\mathbb{K}[X]$ .

## Démonstration

1. Sens directe connus. Soit  $P \in \mathbb{K}[X]$  unitaire, irréductible et annulateur de  $a$ .

On a  $\pi_a \mid P$ , or  $P$  irréductible donc  $P$  et  $\pi_a$  sont associé, or tout deux unitaires donc  $P = \pi_a$ .

## Théorème de la base télescopique

Énoncer et démonstration du théorème de la base télescopique.

Soit  $\mathbb{K} \subseteq \mathbb{L}$  deux corps tel que  $\mathbb{L}$  est de dimension finie sur  $\mathbb{K}$ .

Soient

- $E$  un  $\mathbb{L}$ -ev, (et donc un  $\mathbb{K}$ -ev).
- $e = (e_1, \dots, e_n)$  base de  $E$  sur  $\mathbb{L}$ .
- $z = (z_1, \dots, z_p)$  base de  $\mathbb{L}$  sur  $\mathbb{K}$ .

Alors  $F = (z_i e_j)_{\substack{i \in [1, p] \\ j \in [1, n]}}$  est une base de  $E$  sur  $\mathbb{K}$

Ainsi  $\dim_{\mathbb{K}} E = \dim_{\mathbb{L}} E \cdot \dim_{\mathbb{K}} \mathbb{L}$ .

### Démonstration

- Soit  $\omega \in E$ , on dispose de  $\lambda_1, \dots, \lambda_n \in \mathbb{L}$  tels que

$$\omega = \sum_{j=1}^n \lambda_j e_j$$

On dispose de  $(a_{ij})_{ij} \in \mathbb{K}^{[1, p] \times [1, n]}$

$$\forall j \in [1, n], \lambda_j = \sum_{i=1}^p a_{ij} z_i$$

Ainsi

$$\omega = \sum_{j=1}^n \sum_{i=1}^p a_{ij} z_i e_j$$

- Soit  $(a_{ij})_{ij} \in \mathbb{K}^{[1, p] \times [1, n]}$  tel que

$$\underbrace{\sum_{j=1}^n \sum_{i=1}^p a_{ij} z_i e_j}_{\lambda_j \in \mathbb{L}} = 0$$

$$\sum_{j=1}^n \lambda_j e_j = 0$$

Donc pour tout  $j \in [1, n]$ ,  $\lambda_j = 0$ .

$$\lambda_j = \sum_{i=1}^p a_{ij} z_i = 0$$

Donc par liberté de  $z$ ,  $a_{ij} = 0$  pour tout  $i, j$ .

# Clôture algébrique des rationnels

Propriétés de la clôture algébrique de  $\mathbb{Q}$ .

Notons  $\mathbb{K}$  l'ensemble des  $a \in \mathbb{C}$  algébriques sur  $\mathbb{Q}$ .

$\mathbb{K}$  est un corps algébriquement clos.

## Démonstration : corps

- Soit  $a, \beta \in \mathbb{K}$ , montrons que  $a\beta, a + \beta \in \mathbb{K}$ .

On utilise le fait que  $z$  algébrique dans  $\mathbb{L}$  ssi  $\mathbb{L}[z]$  de dimension finie sur  $\mathbb{L}$  (car  $z$  admet un polynôme annulateur dans  $\mathbb{L}[X]$ ).

- Donc  $\mathbb{Q}[a]$  est de dimension finie sur  $\mathbb{Q}$ ,
- $\beta$  algébrique sur  $\mathbb{Q} \subset \mathbb{Q}[a]$  donc algébrique sur  $\mathbb{Q}[a]$ .
- Donc  $\mathbb{Q}[a][\beta]$  est de dimension finie sur  $\mathbb{Q}[a]$ , et donc par le théorème de la base télescopique, sur  $\mathbb{Q}$ .
- Or  $\mathbb{Q}[a + \beta], \mathbb{Q}[a\beta] \subseteq \mathbb{Q}[a][\beta]$ , donc  $\mathbb{Q}[a + \beta]$  et  $\mathbb{Q}[a\beta]$  sont de dimension finie sur  $\mathbb{Q}$ .
- Soit  $a \in \mathbb{K} \setminus \{0\}$ , soit  $\pi_a$  son polynôme minimal et  $d = \deg \pi_a$ .

$$\underbrace{\pi_a(X)}_{\in \mathbb{Q}[X]} \left( \frac{1}{X} \right) \text{ annule } \frac{1}{a}$$

Donc  $\frac{1}{a} \in \mathbb{K}$

- $1 \in \mathbb{K}$  car  $\mathbb{Q} \subseteq \mathbb{K}$ .

## Démonstration : clôture

Soit  $P = \sum_{k=0}^d a_k X^k \in \mathbb{K}[X]$ . Soit  $a \in \mathbb{C}$  racine de  $P$ , montrons que  $a \in \mathbb{K}$ .

Pour tout  $k \in \llbracket 0, d \rrbracket$ ,  $a_k \in \mathbb{K}$  donc  $\mathbb{Q}[a_k]$  de dimension finie sur  $\mathbb{Q}$ .

Par récurrence on a

$$\mathbb{L} = \mathbb{Q}[a_0][a_1] \cdots [a_d]$$

De dimension finie sur  $\mathbb{Q}$ .

Comme  $P \in \mathbb{L}[X]$  annule  $a$ ,  $\mathbb{L}[a]$  est de dimension finie sur  $\mathbb{L}$  et donc sur  $\mathbb{Q}$ , id est  $a \in \mathbb{K}$ .

## Exercice : Gauss-Lucas

Soit  $P \in \mathbb{C}[X]$ , montrer que les racines de  $P'$  sont dans l'enveloppe convexe des racines de  $P$ .

Soit  $P \in \mathbb{C}[X]$ , montrer que les racines de  $P'$  sont dans l'enveloppe convexe des racines de  $P$ .

On écrit

$$P = c \prod_{k=1}^N (X - a_k)^{m_k}$$

Soit  $b$  une racine de  $P'$ .

Si  $b \in \{a_1, \dots, a_N\}$ ,  $b$  est nécessairement dans leur enveloppe convexe.

Sinon

$$\frac{P'}{P} = \sum_{k=1}^n \frac{m_k}{X - a_k}$$

$$0 = \frac{P'}{P}(b) = \sum_{k=1}^N \frac{m_k}{b - a_k} = \sum_{k=1}^N \frac{m_k}{|b - a_k|^2}$$

$$= \sum_{k=1}^N \frac{m_k}{|b - a_k|^2} (b - a_k)$$

$$b = \frac{\sum_{k=1}^N \frac{a_k m_k}{|b - a_k|^2}}{\sum_{k=1}^N \frac{m_k}{|b - a_k|^2}}$$

$$= \sum_{k=1}^N \lambda_k a_k$$

Où  $\lambda_k = \frac{\frac{a_k m_k}{|b - a_k|^2}}{\sum_{i=1}^N \frac{m_i}{|b - a_i|^2}}$  (on a alors

$$\sum_{k=1}^N \lambda_k = 1).$$

$b$  est donc un barycentre à

coefficients positifs des  $a_1, \dots, a_n$

et est donc dans leur enveloppe convexe.

## Exercice : Dénombrément de morphismes

1. Dénombrer les morphismes de  $G_1$  vers  $G_2$ , avec  $|G_1| \wedge |G_2| = 1$ .
2. Dénombrer les morphismes de  $G_1$  vers  $G_2$  où  $G_1$  et  $G_2$  sont cyclique.
3. Même chose avec les injections et les surjections.

### Remarque générale

Soit  $\varphi : G_1 \rightarrow G_2$  morphisme de groupe,  $x \in G_1$

$$\varphi(x)^{\text{ord}(x)} = e_{G_2}$$

$$\text{donc } \text{ord}(\varphi(x)) \mid |G_2|$$

$$\text{et } \text{ord}(\varphi(x)) \mid |G_1|$$

Ainsi  $\text{ord}(\varphi(x)) \mid |G_1| \wedge |G_2|$ .

### Exercices

1. Soit  $\varphi : G_1 \rightarrow G_2$  morphisme,  $x \in G_1$ . Par la remarque ci dessus  $\text{ord}(\varphi(x)) \mid p \wedge q = 1$  donc  $\varphi(x) = 0$ , il n'y a donc que morphisme le morphisme triviale.
2. Notons  $G_1 = \langle a \rangle$ , posons

$$\theta : \begin{cases} \text{hom}(G_1, G_2) \rightarrow G_2 \\ \varphi \mapsto \varphi(a) \end{cases}$$

Qui est injectif car tout morphisme est uniquement déterminé par son image du générateur  $a$ .

Pour tout  $\varphi \in \text{hom}(G_1, G_2)$  on a

$$\varphi(a)^{|G_1|} = \varphi(a^{|G_1|}) = \varphi(e_{G_1}) = e_{G_2}$$

D'où

$$\text{im } \theta \subset \{y \in G_2 \mid y^{|G_1|} = e_{G_2}\}$$

Soit  $y \in \text{im } \theta$  posons

$$\varphi : \begin{cases} G_1 \rightarrow G_2 \\ x = a^k \mapsto y^k \end{cases}$$

Qui ne dépend pas du  $k$  choisi, soit  $x = a^k = a'$  :

$$a^{k-l} = e_{G_1}$$

$$\text{donc } |G_1| \mid k - l$$

$$\text{et } y^{k-l} = e_{G_2}$$

$$\text{d'où } y^k = y^l$$

Donc  $\theta(\varphi) = y$ .

$$|\text{hom}(G_1, G_2)| = |\text{im } \theta|$$

$$= |\{y \in G_2 \mid y^{|G_1|} = e_{G_2}\}|$$

$$= |\{y \in G_2 \mid \text{ord}(y) \mid |G_1|\}|$$

$$= \bigcup_{d \mid |G_1| \wedge |G_2|} \{y \in G_2 \mid \text{ord}(y) = d\}$$

$$= \sum_{d \mid |G_1| \wedge |G_2|} \varphi(d)$$

$$= |G_1| \wedge |G_2|$$

3. • Pour les injections on veut  $\varphi \in \text{hom}(G_1, G_2)$  tels que  $\ker \varphi = \{e_{G_1}\}$ .

Pour  $k \in \llbracket 1, |G_1| - 1 \rrbracket$ ,

$$\varphi(a)^k = \varphi(a^k) \neq 0$$

$$\text{ord } \varphi(a) = |G_1|$$

Si  $|G_1| \nmid |G_2|$ ,  $G_2$  ne contient

pas éléments d'ordre  $|G_1|$  donc

aucune injection.

Si  $|G_1| \mid |G_2|$ , il y a  $\varphi(|G_1|)$

éléments d'ordre  $|G_1|$ , donc autant d'injections.

- Pour les surjections on veut

$\text{ord } \varphi(a) = |G_2|$ , donc

$$\begin{cases} 0 & \text{si } |G_2| \nmid |G_1| \\ \varphi(|G_2|) & \text{sinon} \end{cases}$$

## Exercice : Union de sous espaces vectoriels

$E$  un  $\mathbb{K}$  espace vectoriel.

1. Soit  $F, G$  deux sev de  $E$ , montrer que  $F \cup G$  sev ssi  $F \subseteq G$  ou  $G \subseteq F$ .
2. Supposons  $\mathbb{K}$  infini, soit  $F_1, \dots, F_n$   $n$  sevs, montrer que si  $\bigcup_{k=1}^n F_k$  est un sev, alors il existe  $i \in \llbracket 1, n \rrbracket$  tel que

$$\bigcup_{k=1}^n F_k = F_i$$

- 
1. Soit  $F, G$  sevs de  $E$  un  $\mathbb{K}$ -ev tel que  $F \cup G$  est un sev.

Si  $F \not\subseteq G$ , on pose  $z \in F \setminus G$ , soit  $x \in G$ .

$$x + z \in F \cup G$$

$x + z \notin G$  car sinon

$$F \setminus G \ni z = \underbrace{(x + z)}_{\in G} - \underbrace{x}_{\in G} \in G$$

Donc  $x + z \in F$  d'où

$$x = (x + z) - z \in F$$

Et  $G \subseteq F$ .

2. Soient  $F_1, \dots, F_n$  sevs de  $E$  tels que  $\bigcup_{k=1}^n F_k$  est un sev.

Notons  $U_m = \bigcup_{k=1}^m F_k$  pour  $m \in \mathbb{N}$ .

On a déjà fait le cas  $n = 2$  et le cas  $n = 1$  est trivial.

Supposons la propriété vraie pour un  $n \in \mathbb{N}$ .

Si  $U_n \subseteq F_{n+1}$  alors on a fini.

Si  $F_{n+1} \subseteq U_n$  alors par hypothèse de récurrence, on dispose de  $i \in \llbracket 1, n \rrbracket$

$$U_{n+1} = U_n = F_i$$

Sinon, on dispose de

$$x \in F_{n+1} \setminus U_n \subseteq U_{n+1}$$

$$y \in U_n \setminus F_{n+1} \subseteq U_{n+1}$$

Soient  $\lambda_0, \dots, \lambda_{n+1} \in \mathbb{K}$  deux à deux distincts.

$$z_k = x + \lambda_k y$$

Par le lemme des tiroirs, on dispose de  $k \neq l$  et  $j$  tel que  $z_k, z_l \in F_j$

Si  $j = n + 1$

$$z_k - z_l = \underbrace{(\lambda_k - \lambda_l)}_{\neq 0} y \in F_{n+1}$$

Et  $y \in F_{n+1}$  impossible.

Si  $j \in \llbracket 1, n \rrbracket$

$$\lambda_l z_k - \lambda_k z_l = \underbrace{(\lambda_l - \lambda_k)}_{\neq 0} x \in F_j$$

Et  $x \in F_j$  impossible.

## Somme directe de sous espaces vectoriels

Définition et propriétés de somme directe de sev.

Soient  $F_1, \dots, F_n$  sev de  $E$  un  $\mathbb{K}$ -ev. On dit qu'ils sont en somme directe si pour tout  $x \in \sum_{k=1}^n F_k$

$$\exists!(x_1, \dots, x_n) \in \prod_{k=1}^n F_k, \quad x = \sum_{k=1}^n x_k$$

Il y a équivalence entre  $F_1, \dots, F_n$  en somme directe et

1.  $\forall(x_1, \dots, x_n) \in \prod_{k=1}^n F_k, \quad \sum_{k=1}^n x_k = 0 \Rightarrow \forall k \in \llbracket 1, n \rrbracket, \quad x_k = 0.$
2.  $\forall i \in \llbracket 1, n \rrbracket, \quad F_i \cap \left( \sum_{i \neq k}^n F_k \right) = \{0\}$
3.  $F_n \cap \bigoplus_{k=1}^{n-1} F_k = \{0\}$

### En dimension finie

4.  $\dim \sum_{k=1}^n F_k \leq \sum_{k=1}^n \dim F_k$  avec égalité ssi les  $F_1, \dots, F_n$  sont en somme directe.

### Démonstration

1.  $\Rightarrow$  il s'agit d'un cas particulier pour  $x = 0$ .

$\Leftarrow$  Supposons  $\sum_{k=1}^n x_k = \sum_{k=1}^n x'_k$

Alors  $\sum_{k=1}^n (x_k - x'_k) = 0$  donc  $x_k = x'_k$  pour tout  $k \in \llbracket 1, n \rrbracket$ .

3.  $\Rightarrow$  Soit  $x \in F_n \cap \bigoplus_{k=1}^n F_k$

$$x = \sum_{k=1}^{n-1} 0 + x = \sum_{k=1}^{n-1} x_k + 0 \quad \text{car } x \in \bigoplus_{k=1}^{n-1} F_k$$

Donc par unicité de la décomposition  $x = \sum_{k=1}^n 0 = 0$ .

$\Leftarrow$  Soit  $x_1, \dots, x_n \in E$  tels que

$$\sum_{k=1}^n x_k = 0$$

$$-x_n = \sum_{k=1}^{n-1} x_k \in F_n \cap \bigoplus_{k=1}^{n-1} F_k$$

Donc  $x_n = 0$  et  $\sum_{k=1}^{n-1} x_k = 0$  donc

$x_1 = x_2 = \dots = x_n = 0$ .

## Espaces supplémentaires

Définition, propriétés des espaces supplémentaires.

---

Soient  $F_1, \dots, F_n$  sevs de  $E$  un  $\mathbb{K}$ -ev.  
On dit qu'ils sont supplémentaires si

$$E = \bigoplus_{k=1}^n F_k$$

Et on a

$$E = \bigoplus_{k=1}^n F_k$$

$$\Leftrightarrow \begin{cases} E = \sum_{k=1}^n F_k \\ \dim(E) = \sum_{k=1}^n \dim(F_k) \end{cases}$$

$$\Leftrightarrow \begin{cases} \sum_{k=1}^n F_k = \bigoplus_{k=1}^n F_k \\ \dim(E) = \sum_{k=1}^n \dim(F_k) \end{cases}$$

## Notations de matrices

Notations de matrices :  
changements de bases, matrices d'un endomorphisme, ...

Soit  $u \in \mathcal{L}(E, F)$ ,  $e = (e_1, \dots, e_n)$ ,  $e' = (e'_1, \dots, e'_n)$  bases de  $E$  et  $f = (f_1, \dots, f_p)$  base de  $F$ .

### Applications linéaires

$$\mathcal{M}_{e,f}(u) = \mathcal{M}_{e \leftarrow f}(u) = \mathcal{M}_e^f(u) \in \mathcal{M}_{pn}(\mathbb{K})$$

Et la matrice est alors

$$\mathcal{M}_{f \leftarrow e}(u) = f_1 \begin{pmatrix} u(e_1) & u(e_2) & \cdots & u(e_n) \\ a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{p1} & a_{p2} & \cdots & a_{pn} \end{pmatrix}$$

Où pour  $j \in \llbracket 1, n \rrbracket$

$$u(e_j) = \sum_{k=1}^p a_{kj} f_k$$

### Endomorphismes

$$\mathcal{M}_e(u) = \mathcal{M}_{e \leftarrow e}(u) = \mathcal{M}_e^e(u)$$

$$u(e_j) = \sum_{k=1}^p a_{kj} f_k$$

### Changement de base

$$P_{e \rightarrow e'} = \mathcal{M}_e(e') = \mathcal{M}_{e \leftarrow e'}(\text{id})$$

## Exercice : Noyaux et images itérées

Soit  $u \in \mathcal{L}(E)$  avec  $E$  un  $\mathbb{K}$ -ev. Que peut-on dire des suites  $(\ker u^k)_k$  et  $(\text{im } u^k)_k$  ?

Soit  $u \in \mathcal{L}(E)$  avec  $E$  un  $\mathbb{K}$ -ev.

### Dimension quelconque

- Si  $\ker u^k = \ker u^{k+1}$  pour un  $k \in \mathbb{N}$  alors pour tout  $n \geq k$ ,  $\ker u^k = \ker u^n$ .
- De même pour les images.

### Dimension finie

En notant  $n = \dim E$  on a

$$d_k = \dim \ker u^k \in \llbracket 0, n \rrbracket \nearrow$$
$$r_k = \text{rg } u^k \in \llbracket 0, n \rrbracket \searrow$$

Ces deux suites sont donc stationnaires, on peut poser

$$m_K = \min\{k \in \mathbb{N} \mid \ker u^k = \ker u^{k+1}\}$$
$$m_I = \min\{k \in \mathbb{N} \mid \text{im } u^k = \text{im } u^{k+1}\}$$

On a de plus  $m_K = m_I = m$ .

Et en notant

$$K = \bigcup_{k \in \mathbb{N}} \ker u^k = \ker u^m$$
$$I = \bigcap_{k \in \mathbb{N}} \text{im } u^k = \text{im } u^m$$

Qui sont les valeurs auquelles les suites stationnent, on a

- $K \oplus I = E$
- $K, I$  stables par  $u$
- $u|_K^k$  est nilpotent
- $u|_I^I$  est inversible.

On dispose de  $d \in \mathbb{N}^*$  tel que

$$u^d(K) = u^d(I) = \{0\}$$
$$K \subseteq \ker u^d \subset K = \bigcup_{k \in \mathbb{N}} \ker u^k$$

Et on a

$$u(I') = I'$$
$$u^m(I') = I'$$
$$I' \subseteq \text{im } u^m = I$$

Donc

$$\dim K' \leq \dim K$$
$$\dim I' \leq \dim I$$

Et on obtient l'égalité par complémentarité, d'où  $K' = K$  et  $I' = I$ .

## Développement du déterminant par ligne ou par colonne

Formules et définitions du développement du déterminant par ligne ou par colonne.

Soit  $A \in \mathcal{M}_n(\mathbb{K})$

- pour tout  $j \in \llbracket 1, n \rrbracket$  :

$$\det(A) = \sum_{i=1}^n (-1)^{i+j} a_{ij} \det(\tilde{A}_{ij})$$

- pour tout  $i \in \llbracket 1, n \rrbracket$  :

$$\det(A) = \sum_{j=1}^n (-1)^{i+j} a_{ij} \det(\tilde{A}_{ij})$$

Où  $\tilde{A}_{ij} \in \mathcal{M}_{n-1}(\mathbb{K})$  est la matrice  $A$  privée de sa  $i^{\text{ème}}$  ligne et  $j^{\text{ème}}$  colonne.

On appelle  $\hat{A}_{ij} = (-1)^{i+j} \det(\tilde{A}_{ij})$  cofacteur.

On appelle  $\text{com}(A)$  la matrice des cofacteurs.

Et on a

$$A \cdot \text{com}(A)^T = \det(A)I_n,$$

## Exercice : rang d'une comatrice

Soit  $A \in \mathcal{M}_n(\mathbb{K})$  ( $n \geq 3$ ), calculer  $\text{rg com}(A)$  en fonction de  $\text{rg } A$ .

Soit  $A \in \mathcal{M}_n(\mathbb{K})$  avec  $n \geq 3$ .

- Si  $\text{rg } A = n$ ,  $A \in \text{GL}_n(\mathbb{K})$  donc  $\text{com } A \in \text{GL}_n(\mathbb{K})$  et  $\text{rg com}(A) = n$ .
- Si  $\text{rg } A \leq n - 2$ , pour tout  $i, j \in \llbracket 1, n \rrbracket$  la matrice  $\tilde{A}_{ij}$  extraite de  $A$  privée de sa  $i^{\text{ème}}$  ligne et  $j^{\text{ème}}$  colonne est de rang inférieur à  $n - 2$  et n'est donc pas inversible,  $\text{com } A = 0$  et  $\text{rg com}(A) = 0$ .
- Si  $\text{rg } A = n - 1$ , on dispose d'une matrice extraite de taille  $n - 1$  inversible, donc au moins un des cofacteur est non nul d'où  $\text{rg com}(A) \geq 1$ .

De plus

$$A^T \text{com}(A) = \det(A)I_n = 0$$

Donc  $\text{im com}(A) \subseteq \ker A^T$  et  $\dim \ker A^T = 1$  d'où  $\text{rg com}(A) \leq 1$ .

## Algorithme du pivot de Gauss

Déscription de l'algorithme du pivot de Gauss, et propriétés qui en découlent.

### Opérations, représentation matricielle

Notons  $(E_{ij})_{ij}$  la base canonique de  $\mathcal{M}_n(\mathbb{K})$ . On a

$$E_{ik} E_{lj} = \delta_{kl} E_{ij}$$

Pour  $A \in \mathcal{M}_{np}(\mathbb{K})$

$$E_{kl}^{(n)} A = \begin{pmatrix} & | & 1 \\ L_I & | & k \\ & | & \vdots \\ & | & n \end{pmatrix}$$

$$AE_{kl}^{(p)} = \left( \frac{C_k}{1 \dots I \dots n} \right)$$

Ainsi on peut définir

- $T_{kl}(\lambda) = I_n + \lambda E_{kl}^{(n)}$  la transvection sur les lignes ( $L_k \leftarrow L_k + \lambda L_l$ )
- $T'_{kl}(\lambda) = I_p + \lambda E_{kl}^{(p)}$  la transvection sur les colonnes ( $C_l \leftarrow C_l + \lambda C_k$ )
- $P_{kl} = I_n - E_{kk}^{(n)} - E_{ll}^{(n)} + E_{kl}^{(n)} + E_{lk}^{(n)}$  la transposition de lignes ( $L_l \leftrightarrow L_k$ )
- $P_{kl} = I_p - E_{kk}^{(p)} - E_{ll}^{(p)} + E_{kl}^{(p)} + E_{lk}^{(p)}$  la transposition de colonnes ( $C_l \leftrightarrow C_k$ )

### Algorithme

Prenons  $A = (c_1 \dots c_n) \in \mathcal{M}_n(\mathbb{K})$

- Si  $A = 0$  fini.

- Soit  $j = \min\{k \in \llbracket 1, n \rrbracket \mid C_k \neq 0\}$

$$A^{(1)} : C_j \leftrightarrow C_1$$

- Soit  $i = \min\{k \in \llbracket 1, n \rrbracket \mid a_{i1} \neq 0\}$

► Si  $i = 1$  on effectue  $L_2 \leftarrow L_2 + L_1$  et on prend  $i = 2$ .

$$A^{(2)} : L_1 \leftarrow L_1 + \left(1 - \frac{a_{11}}{a_{i1}}\right) L_i$$

$$A^{(2)} = \left( \begin{array}{c|cccc} 1 & * & \dots & * \\ \hline * & & & & \\ \vdots & & & * & \\ * & & & & \end{array} \right)$$

- Pour tout  $i \in \llbracket 2, n \rrbracket$  on effectue

$$A^{(i+1)} : L_i \leftarrow L_i - a_{i1} L_1$$

Ainsi

$$A^{(n+1)} = \left( \begin{array}{c|cccc} 1 & * & \dots & * \\ \hline 0 & & & & \\ \vdots & & & \tilde{A} & \\ 0 & & & & \end{array} \right)$$

On repète l'algorithme sur  $\tilde{A}$ , on obtient alors

$$\tilde{\tilde{A}} = \left( \begin{array}{ccccc} 1 & \ddots & (*) & * & (*) \\ & \ddots & & \vdots & (*) \\ & & 1 & * & \\ \hline & & & \mu & * \dots * \\ & & & & 0 \\ & & & & \ddots \\ & & & & 0 \end{array} \right)$$

Avec  $\mu \neq 1$ ssi le blocs de zéros à la fin est de taille nulles (on ne dispose pas des lignes nécessaires pour se ramener à  $\mu = 1$ ).

On peut alors finalement effectuer pour tout  $i \in \llbracket 1, \text{rg } A \rrbracket$ , puis pour  $j \in \llbracket i+1, n \rrbracket$

$$\tilde{\tilde{A}} : C_j \leftarrow C_j - \frac{\tilde{\tilde{A}}_{ij}}{\tilde{\tilde{A}}_{ii}} C_i$$

$$\tilde{\tilde{A}} = \left( \begin{array}{ccccc} 1 & & & & \\ \ddots & & & & \\ & 1 & & & \\ & & \mu & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & 0 \end{array} \right)$$

On remarque que si  $A$  est inversible, les transpositions sont inutiles car il n'existe pas de colonnes nulles.

### Propriétés

- Les transvections engendrent  $\text{SL}_n(\mathbb{K})$ .
- Les transvections et une dilatation (pour atteindre n'importe quel déterminant) suffisent à engendrer  $\text{GL}_n(\mathbb{K})$ .

## Intersection d'hyperplans

Propriétés sur les intersections d'hyperplans.

Soient  $(\varphi_1, \dots, \varphi_p) \in \mathcal{L}(E, \mathbb{K})^p$

$$\dim \bigcap_{k=1}^p \ker \varphi_k = n - \operatorname{rg}(\varphi_1, \dots, \varphi_p) \geq n - p$$

### Démonstration

On montre l'inégalité par récurrence sur  $p$ .

Montrons l'égalité.

Quitte à extraire et renommer,  $(\varphi_1, \dots, \varphi_r)$  est libre.

Or pour tout  $k \in \llbracket r+1, p \rrbracket$ ,

$$\varphi_k \in \operatorname{Vect}(\varphi_1, \dots, \varphi_r)$$

$$\text{Donc } \bigcap_{i=1}^r \ker \varphi_i \subseteq \ker \varphi_k$$

$$\text{D'où } \bigcap_{k=1}^p \ker \varphi_k = \bigcap_{k=1}^r \ker \varphi_k$$

Donc (cf. lemme sur la liberté d'une famille de formes linéaires)

$$\theta : \begin{cases} E \rightarrow \mathbb{K}^r \\ x \mapsto \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_r(x) \end{pmatrix} \end{cases} \text{ surjective}$$

$$\ker \theta = \bigcap_{k=1}^r \ker \varphi_k$$

Donc par le théorème du rang

$$\dim \left( \bigcap_{k=1}^p \ker \varphi_k \right) = n - \operatorname{rg}(\varphi_1, \dots, \varphi_p)$$

## Liberté d'une famille de l'espace dual

Démonstration d'une CNS pour la liberté d'une famille de  $\mathcal{L}(E, \mathbb{K})$  où  $E$  est un  $\mathbb{K}$ -ev.

Soient  $\varphi_1, \dots, \varphi_p \in \mathcal{L}(E, \mathbb{K})$ .

La famille  $(\varphi_1, \dots, \varphi_p)$  est libre ssi

$$\theta : \begin{cases} E \rightarrow \mathbb{K}^p \\ x \mapsto \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_p(x) \end{pmatrix} \end{cases} \text{ surjective}$$

### Démonstration

- Supposons  $\theta$  surjective, on considère  $\lambda_1, \dots, \lambda_p \in \mathbb{K}$  tels que

$$\sum_{k=1}^p \lambda_k \varphi_k = 0$$

Soit  $i \in \llbracket 1, p \rrbracket$ , on dispose de  $x \in E$  tel que

$$\theta(x) = \begin{pmatrix} 1 \\ \vdots \\ i \\ \vdots \\ p \end{pmatrix} = \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_i(x) \\ \vdots \\ \varphi_p(x) \end{pmatrix}$$

Ainsi

$$\left( \sum_{k=1}^p \lambda_k \varphi_k \right)(x) = 0 = \lambda_i$$

- Par contraposé supposons  $\theta$  non surjective :  $\text{rg } \theta \leq p - 1$ .

On dispose de  $H$  hyperplan tel que  $\text{im } \theta \subseteq H$ . Donc on dispose de  $(a_1, \dots, a_p) \in \mathbb{K}^p \setminus \{0\}$  tels que

$$H = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \in \mathbb{K}^p \mid \sum_{k=1}^p a_k x_k = 0 \right\}$$

Donc pour tout  $x \in E$ ,

$$\theta(x) = \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_p(x) \end{pmatrix} \in \text{im } \theta \subseteq H$$

$$\sum_{k=1}^p a_k \varphi_k(x) = 0$$

Donc  $\sum_{k=1}^p a_k \varphi_k = 0$  et la famille est liée

## Condition de liberté d'une forme linéaire à une famille

Soit  $\varphi_1, \dots, \varphi_p, \psi \in \mathcal{L}(E, \mathbb{K})$ .

Démonstration d'une CNS pour que  $\psi \in \text{Vect}(\varphi_1, \dots, \varphi_p)$ .

Soit  $\varphi_1, \dots, \varphi_p, \psi \in \mathcal{L}(E, \mathbb{K})$ .

Pour tout  $\psi \in \mathcal{L}(E, \mathbb{K})$

$$\varphi \in \text{Vect}(\varphi_1, \dots, \varphi_p)$$

$$\text{ssi } \bigcap_{k=1}^p \ker \varphi_k \subseteq \ker \psi$$

### Démonstration

- Si  $\varphi \in \text{Vect}(\varphi_1, \dots, \varphi_p)$ , on dispose de  $\lambda_1, \dots, \lambda_p \in \mathbb{K}$  tels que

$$\psi = \sum_{k=1}^p \lambda_k \varphi_k$$

D'où

$$\begin{aligned} \psi \left( \bigcap_{k=1}^p \ker \varphi_k \right) &= \sum_{k=1}^p \lambda_k \varphi_k \left( \bigcap_{i=1}^p \ker \varphi_i \right) \\ &= \{0\} \end{aligned}$$

Et donc  $\bigcap_{k=1}^p \ker \varphi_k \subseteq \ker \psi$ .

- Supposons  $\bigcap_{k=1}^p \ker \varphi_k \subseteq \ker \psi$ .

Quitte à extraire et renommer,  $(\varphi_1, \dots, \varphi_r)$  est libre.

Or pour tout  $k \in \llbracket r+1, p \rrbracket$ ,

$$\varphi_k \in \text{Vect}(\varphi_1, \dots, \varphi_r)$$

$$\text{Donc } \bigcap_{i=1}^r \ker \varphi_i \subseteq \ker \varphi_k$$

$$\text{D'où } \bigcap_{k=1}^p \ker \varphi_k = \bigcap_{k=1}^r \ker \varphi_k$$

Donc

$$\theta : \begin{cases} E \rightarrow \mathbb{K}^r \\ x \mapsto \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_r(x) \end{pmatrix} \end{cases} \text{ surjective}$$

Posons alors

$$\theta' : \begin{cases} E \rightarrow \mathbb{K}^{r+1} \\ x \mapsto \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_r(x) \\ \psi(x) \end{pmatrix} \end{cases}$$

Or

$$\bigcap_{k=1}^r \ker \varphi_k = \bigcap_{k=1}^p \ker \varphi_k \subseteq \ker \psi$$

$$\text{Donc } \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \notin \text{im } \theta'$$

La famille  $(\varphi_1, \dots, \varphi_r, \psi)$  est liée d'où  $\psi \in \text{Vect}(\varphi_1, \dots, \varphi_p)$ .

## Base duale, antéduale

Définitions, propriétés, démonstrations autours des bases duals.

### Base duale

Soit  $E$  un  $\mathbb{K}$ -ev de dimension finie,  $e = (e_1, \dots, e_n)$  une base de  $E$ .

Il existe une unique famille  $(\varphi_1, \dots, \varphi_n) \in \mathcal{L}(E, \mathbb{K})^n$  tel que

$$\forall i, j \in \llbracket 1, n \rrbracket, \varphi_i(e_j) = \delta_{ij}$$

Cette famille est appelée base duale de  $e$  et est une base de  $\mathcal{L}(E, \mathbb{K})$ .

Dans ce cas

$$\forall x \in E, x = \sum_{k=1}^n \varphi_k(x) e_k$$

$$\forall \psi \in \mathcal{L}(E, \mathbb{K}), \psi = \sum_{k=1}^n \psi(e_k) \varphi_k$$

### Base antéduale

Pour toute base  $(\varphi_1, \dots, \varphi_n)$  de  $\mathcal{L}(E, \mathbb{K})$ , il existe une unique base  $(e_1, \dots, e_n)$  de  $E$  tel que  $(\varphi_1, \dots, \varphi_n)$  en est la base duale.

### Démonstration

- Existence / Unicité : car les formes linéaire sont uniquement déterminés par leurs image d'une base.

- Génératrice : Soit  $\psi \in \mathcal{L}(E, \mathbb{K})$  pour tout  $i \in \llbracket 1, n \rrbracket$

$$\left( \sum_{k=1}^n \psi(e_k) \varphi_k \right)(e_i) = \sum_{k=1}^n \psi(e_k) \varphi_k(e_i) = \psi(e_i)$$

$$\text{Donc } \psi = \sum_{k=1}^n \psi(e_k) \varphi_k$$

Donc  $(\varphi_1, \dots, \varphi_n)$  est une base.

- Soit  $x = \sum_{k=1}^n x_k e_k \in E, i \in \llbracket 1, n \rrbracket$

$$\varphi_i(x) = \varphi_i \left( \sum_{k=1}^n x_k e_k \right)$$

$$= \sum_{k=1}^n x_k \delta_{ik} = x_i$$

- Soit  $(\varphi_1, \dots, \varphi_n)$  base de  $\mathcal{L}(E, \mathbb{K})$

$$\theta : \begin{cases} E \rightarrow \mathbb{K}^n \\ x \mapsto \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_n(x) \end{pmatrix} \end{cases} \text{ surjective}$$

Par liberté de la famille, donc bijective par argument dimensionnel.

Notons  $(b_1, \dots, b_n)$  la base

canonique de  $\mathbb{K}^n$ .

La famille  $(e_k = \theta^{-1}(b_k))_{k \in \llbracket 1, n \rrbracket}$  est

l'unique base de  $E$  tel que

$$\forall i, j \in \llbracket 1, n \rrbracket, \varphi_i(e_j) = \delta_{ij}$$

## Lemme de factorisation

Énoncé et démonstration du lemme de factorisation en algèbre linéaire.

Soient  $E, F, G$  trois  $\mathbb{K}$ -ev

1. Soient  $u \in \mathcal{L}(E, F)$ ,  $v \in \mathcal{L}(E, G)$ , dans ce cas

$$\ker u \subseteq \ker v$$

$$\Leftrightarrow \exists w \in \mathcal{L}(F, G), v = w \circ u$$

(Si  $u$  est inversible  $w = v \circ u^{-1}$ ).

2. Soient  $u \in \mathcal{L}(E, F)$ ,  $v \in \mathcal{L}(G, F)$ , dans ce cas

$$\text{im } v \subseteq \text{im } u$$

$$\Leftrightarrow \exists w \in \mathcal{L}(G, E), v = u \circ w$$

### Démonstration

1. • Supposons qu'il existe  $w \in \mathcal{L}(F, G)$  tel que  $v = w \circ u$ .

$$\begin{aligned} v(\ker u) &= w(u(\ker u)) \\ &= w(\{0\}) = 0 \end{aligned}$$

D'où  $\ker u \subseteq \ker v$ .

- Supposons que  $\ker u \subseteq \ker v$ .

Soient  $H, K$  tels que

$$\ker u \oplus H = E$$

$$\text{im } u \oplus K = F$$

Posons

$$\tilde{u} : \begin{cases} H \rightarrow \text{im } u \\ x \mapsto u(x) \end{cases}$$

$$\ker \tilde{u} = \ker u \cap H = \{0\}$$

$$\dim H = \text{rg } u$$

Donc  $\tilde{u}$  inversible.

On peut donc écrire

$$w : \begin{cases} F = \text{im } u \oplus K \rightarrow G \\ x = y + z \mapsto v \circ \tilde{u}^{-1}(y) \end{cases}$$

Soit  $x = y + z \in E = \ker u \oplus H$ .

$$\begin{aligned} w \circ u(x) &= v(\tilde{u}^{-1}(u(z))) \\ &= v(z) \end{aligned}$$

$$v(x) = \underbrace{v(y)}_0 + v(z)$$

On a bien pour  $x \in E$

$$u \circ w(x) = \tilde{u}(\tilde{u}^{-1}(v(x))) = v(x)$$

## Vandermonde, interpolation de Lagrange

Définitions, propriétés et démonstrations de l'interpolation de Lagrange et des matrices des Vandermonde.

Soit  $\mathbb{K}$  un corps,  $n \in \mathbb{N}$ ,  $a_0, \dots, a_n \in \mathbb{K}$  deux à deux distincts.

$$\theta : \begin{cases} \mathbb{K}_n[X] \rightarrow \mathbb{K}^{n+1} \\ P \mapsto \begin{pmatrix} P(a_0) \\ \vdots \\ P(a_n) \end{pmatrix} \in \mathcal{L}(\mathbb{K}_n[X], \mathbb{K}^{n+1}) \end{cases}$$

Pour tout  $P \in \ker \theta$ ,

$$P(a_0) = P(a_1) = \dots = P(a_n) = 0$$

Donc  $P$  est de degré  $n$  avec  $n + 1$  racines distinctes, d'où  $P = 0$ .

Donc  $\theta$  est un isomorphisme.

Notons

$$e = (e_0, \dots, e_n)$$

$$c = (1, X, \dots, X^n)$$

Les bases canoniques de  $\mathbb{K}^{n+1}$  et  $\mathbb{K}_n[X]$ .

$$\forall k \in \llbracket 0, n \rrbracket, \theta^{-1}(e_k) = \prod_{\substack{i=0 \\ i \neq k}}^n \frac{X - a_i}{a_k - a_i} = L_k(X)$$

$$\mathcal{M}_{e \leftarrow c}(\theta) = \begin{pmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^n \end{pmatrix}$$

Sont déterminant vaut

$$V(a_0, \dots, a_n) = \det(\mathcal{M}_{e \leftarrow c}(\theta)) = \prod_{0 \leq i < j \leq n} (a_j - a_i)$$

Démonstration

Par récurrence sur  $n$ , initialisée aisément pour  $n = 1$ .

On suppose la formule pour un  $n \in \mathbb{N}$ .

$$P(X) = V(a_0, \dots, a_n, X)$$

$$= \begin{vmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n+1} \\ 1 & X & X^2 & \cdots & X^{n+1} \end{vmatrix}$$

$$= \sum_{j=0}^{n+1} (-1)^{n+j} X^j V_j$$

Où  $V_j$  est le déterminant mineur en  $(n + 2, j + 1)$ . De plus

$$\deg P \leq n + 1$$

$$\text{cd } P = V(a_0, \dots, a_n) \neq 0$$

De plus pour tout  $k \in \llbracket 0, n \rrbracket$ ,  $P(a_k) = 0$  donc

$$P = V(a_0, \dots, a_n) \prod_{k=0}^n (X - a_k)$$

$$= \prod_{0 \leq i < j \leq n} (a_j - a_i) \prod_{k=0}^n (X - a_k)$$

Ainsi on peut calculer

$$P(a_{n+1}) = V(a_0, \dots, a_{n+1})$$

$$= \prod_{0 \leq i < j \leq n} (a_j - a_i) \prod_{k=0}^n (a_{n+1} - a_k)$$

$$= \prod_{0 \leq i < j \leq n+1} (a_j - a_i)$$