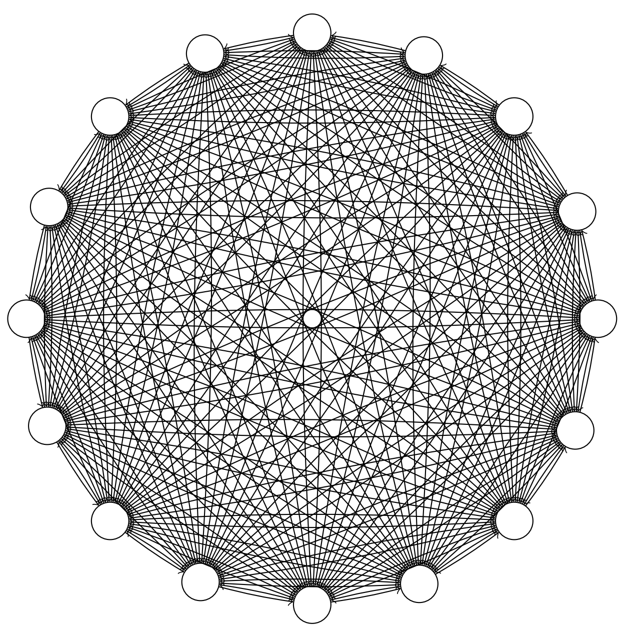
Mathématiques

CLASSICAL MEDLEY

Pour et par la Cité des Taupes

2020



Version du 1er juin 2021.

Table des matières

Introduction

Regardez le code source de cette page (dans `main.tex`) pour voir comment utiliser les macros essentiels.

0.0 Titre de l'encadré

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris.

Démonstration. Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. □

Solution. Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. □

Remarque

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices.

Exemple

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl.

Première partie
Algèbre

1 Théorie des groupes

1.1 Théorème de Lagrange

L'ordre d'un sous groupe H d'un groupe fini G divise l'ordre de ce groupe G.

Remarque

Cette démonstration est très classique et il faut savoir la faire sans hésiter !

Démonstration. On sait que $xRy \iff x^{-1}y \in H$ est une relation d'équivalence sur G et que les classes d'équivalence s'écrivent aH.

Les classes d'équivalence forment une partition de G, on note $a_1H, a_2H, \dots, a_pH$ ces classes.

$$G = \bigcup_{i=1}^{p} \underbrace{a_iH}_{2 \text{ à } 2 \text{ disjoints}} \implies |G| = \sum_{i=1}^{p} |a_iH|$$

Or $\phi_i : x \in H \longmapsto a_ix \in a_iH$ est bijective donc $|H| = |a_iH|$ donc $|G| = p|H|$ d'où la conclusion. $\square$

1.2 Une égalité sur le cardinal du noyau et de l'image d'un morphisme de groupe

On note $(G, \cdot)$ un groupe fini et $f : G \to G'$ un morphisme de groupe.
Montrer que $|G| = |\operatorname{Ker} f| \times |\operatorname{Im} f|$

Démonstration. On pose $\operatorname{Im} f = \{y_1, \cdot, y_p\}$ avec les y_i 2 à 2 distincts. Ainsi,

$$G = f^{-1}(\{y_1\}) \cup \cdots \cup f^{-1}(\{y_n\})$$

On en déduit

$$|G| = \sum_{i=1}^{p} |f^{-1}(y_i)|$$

On fixe un $y \in \operatorname{Im} f$ et un x tel que $y = f(x)$. On pose

$$\begin{aligned} \phi \colon \operatorname{Ker} f &\longrightarrow f^{-1}(\{y\}) \\ t &\longmapsto xt \end{aligned}$$

et qui est un isomorphisme, donc $|f^{-1}(\{y\})| = |\operatorname{Ker} f|$ et ainsi $|G| = p|\operatorname{Ker} f| = |\operatorname{Im} f| \times |\operatorname{Ker} f|$ $\square$

1.3 Sous-groupes d'un groupe cyclique

Soit $(G, \cdot)$ groupe cyclique tel que $G = \langle a \rangle$ et $|G| = n$.
On note H un sous groupe de G. H est cyclique.

Démonstration. Intuitivement, on peut considérer $r = \min\{p \in \mathbf{N}^*/a^p \in H\}$ qui existe car c'est une partie de $\mathbf{N}$ non vide (elle contient n).

On a, puisque H est un groupe, l'inclusion suivante : $\langle a^r \rangle \subset H$, on va montrer l'inclusion réciproque.

Soit $x \in H$, il existe $m \in \mathbf{N}$, $x = a^m$. Posons la division euclidienne de m par r : $m = qr + s$ avec $s \in [\![0, r-1]\!]$ et donc $x = (a^r)^q a^s$.

Comme H est un groupe, cela implique que $a^s \in H$ et $s \in [\![0, r-1]\!]$ donc $s = 0$ et $x \in \langle a^r \rangle$. Ainsi $H = \langle a^r \rangle$ et H est cyclique. □

1.4 Sous-groupes additifs de R

Le but de cet exercice est de classifier les sous-groupes additifs de $\mathbf{R}$. Nous montrerons qu'un tel sous-groupe, noté G est caractérisé de l'une des façons suivantes :

— Ou bien G est de la forme $a\mathbf{Z}$, pour a un réel strictement positif ;
— Ou bien G est dense dans $\mathbf{R}$.

Soit, alors, G un sous-groupe de $(\mathbf{R}, +)$.

1. Montrer que pour tout $a > 0$, $a\mathbf{Z}$ est un sous-groupe de $(\mathbf{R}, +)$.
   Notons $H = G \cap \mathbf{R}_+^*$
2. En supposant G non-vide, montrer que H est non-vide et admet une borne inférieure $\alpha \geqslant 0$. Que vaut α dans le cas $G = \mathbf{Z}$? $G = \mathbf{Q}$?
   On suppose d'abord que $\alpha > 0$.
3. Montrer que $\alpha \in H$.
   On pourra raisonner par l'absurde.
4. Montrer que $G = \alpha\mathbf{Z}$
   On suppose maintenant que $\alpha = 0$.
5. Montrer que G est dense dans $\mathbf{R}$.

1.5 Groupe de cardinal divisible par p

On note p un nombre premier et $(G, \cdot)$ groupe d'ordre divisible par p. Montrer qu'il existe un élément d'ordre p.

Solution. La résolution est astucieuse si on a pas toute la théorie des actions de groupe derrière.

On note $E = \{(x_1, \ldots, x_n)/x_1 \cdot \ldots \cdot x_p = e\}$ et on a que $|E| = |G|^{p-1}$. On remarque en prenant comme permutation circulaire $\sigma = (1, 2, 3, \ldots, p)$ que

$$x_1 \ldots x_p = e \iff x_2 \ldots x_p x_1 = x_{\sigma(1)} \ldots x_{\sigma(p)} = e$$

en multipliant par x_1^{-1} d'un côté puis par x_1 de l'autre.

Pour simplifier, on notera pour $x = (x_1, \dots, x_p)$ et c permutateur, $c.x = x_{\sigma(1)} \dots x_{\sigma(p)}$. On introduit :

$$f \colon \langle \sigma \rangle \times E \longrightarrow E$$
$$(c, x) \longmapsto c.x$$

Pour $x \in E$, on va noter $O(x) = \{c.x / c \in \langle \sigma \rangle\}$. De plus, nous savons que $\langle \sigma \rangle = \{\mathrm{id}, \sigma, \cdots, \sigma^{p-1}\}$ est de cardinal p. On considère aussi :

$$\phi : c \in \langle \sigma \rangle \longmapsto c.x \in O(x)$$

Cette application est surjective par définition et deux cas se présentent :
- si cette application est injective alors $|O(x)| = p$
- si elle ne l'est pas, alors cela nous apporte une contrainte forte. En effet, cela veut dire que il existe deux indices tels que $0 \leqslant i < j \leqslant p - 1$ tel que $\sigma^i.x = \sigma^j.x$ donc $x = \sigma^{j-i}.x$, d'où $(x_1, \dots, x_p) = (x_{1+j-i}, \dots, x_{p+j-i})$
  Cela nous apporte une contrainte forte du fait que p est premier. en effet
  $$x_1 = x_{1+j-i} = x_{1+2(j-i)} = \cdots = x_{1+k(j-i)}$$
  avec $k \in \mathbf{N}$. Mais comme $\sigma^p.x = x$ alors $x_{1+np} = x_1 = x_{1+k(j-i)+np}$
  Or $(j - i, p) = 1$ donc d'après la relation de Bézout, $\exists u, v\mathbf{Z}$ tel que $(j - i)u + pv = 1$ et pour tout $l \in [\![0, p - 1]\!], (j - i)lu + plv = l$.
  Cela nous donne donc que $x_1 = x_{l+1}$ d'où le fait que si ϕ est non injective, $|O(x)| = 1$.

Ensuite, si on note $\mathcal{R}$ la relation d'équivalence sur E donnée par

$$x\mathcal{R}y \iff \exists c \in \langle \sigma \rangle, c.x = y$$

et les classes sont donc les $O(x)$ que l'on nommera orbites. Les orbites forment une partition de E. On note $O(x_1), \dots, O(x_r)$ les orbites de cardinal p et $O(x'_1), \dots, O(x'_s)$ celle de cardinal 1. Ainsi

$$|E| = rp + s = |G|^{p-1}$$

et on sait que $s \geqslant 1$ car $(e, \dots, e)$ a une orbite de cardinal 1.

On a donc comme $p \mid |G|, s \equiv 0 \pmod p$ et $s \geqslant 1$. Ainsi $s \geqslant p \geqslant 2$, il existe $x = (a, \dots, a) \neq (e, \dots, e)$ avec $x \in E$ ie $a^p = e$.

Donc $\mathrm{ord}(a) \mid p$ et $\mathrm{ord}(a) > 1$ car $a \neq e$ et donc $\mathrm{ord}(a) = p$ ce qui nous donne la conclusion. □

1.6 Cyclicité des $(\mathbf{Z}/p\mathbf{Z})^\times$

Pour tout premier p, le groupe multiplicatif des unités $(\mathbf{Z}/p\mathbf{Z})^\star$ de $\mathbf{Z}/p\mathbf{Z}$ est cyclique.

Démonstration. On va d'abord montrer les résultats suivants, vrais dans tous les groupes abéliens finis :
- L'ensemble des ordres est stable par ppcm
- L'exposant d'un groupe est l'ordre d'un élément

On utilisera ensuite la structure de corps de $\mathbf{Z}/p\mathbf{Z}$ (que l'on notera $\mathbf{F}_p$) pour conclure.

Soit $(G, \cdot)$ un groupe abélien fini. On va montrer que l'ensemble des ordres est stable par ppcm. Soient a, b deux éléments d'ordres respectifs m, n. On cherche un élément d'ordre $m \vee n$. On note $d = m \wedge n$ de telle sorte que $m = dm'$, $n = dn'$ et $m \wedge n' = 1$. De cette manière, on a $m \vee n = mn'$

$$\operatorname{ord}(a) = m \qquad \operatorname{ord}\left(b^d\right) = n'$$

et donc $c = ab^d$ est un élément d'ordre $mn' = m \vee n$, ce qui conclut.

On définit l'exposant λ du groupe G comme l'ordre maximal des éléments de G. L'ensemble des ordres étant stable par ppcm, et le ppcm de tous les ordres majorant l'ensemble, le maximum des ordres λ est le ppcm des ordres des éléments. Puis, la stabilité garantit qu'il existe un élément d'ordre λ.

On va maintenant montrer que $\mathbf{F}_p^\star$ est cyclique. $\mathbf{F}_p$ est un corps (c'est un anneau en tant d'anneau quotient et tous les éléments non nuls sont inversibles par le petit théorème de Fermat). Ainsi, un polynôme de $\mathbf{F}_p[X]$ admet au plus autant de racines que son degré. On pose $P = X^\lambda - 1$. Ce polynôme admet au moins $p-1$ racines distinctes (les éléments non nuls du corps) par le petit théorème de Fermat. On a donc $\lambda \geqslant p-1$. Puis, λ est un ordre donc divise $\#\mathbf{F}_p^\star = p-1$ (Lagrange). Ainsi, $\lambda \mid p-1$ et $\lambda = p-1$.

L'exposant du groupe vaut le cardinal du groupe, ce groupe est donc cyclique (un élément d'ordre λ est automatiquement un générateur du groupe). $\square$

1.7 Cyclicité des $(\mathbf{Z}/p^\alpha\mathbf{Z})^\star$

Pour p premier impair, et pour $\alpha > 1$, $(\mathbf{Z}/p^\alpha\mathbf{Z})^\star$ est cyclique.

Démonstration. On va d'abord montrer par récurrence

$$\forall n \in \mathbf{N}, \quad (1+p)^{p^n} \equiv 1 + p^{n+1} \pmod{p^{n+2}}.$$

— Le cas $n = 0$ est direct.

— On suppose le résultat vrai au rang n :

$$(1+p)^{p^n} = 1 + p^{n+1} + p^{n+2}q.$$

On a alors

$$\begin{aligned}(1+p)^{p^{n+1}} &\equiv (1 + p^{n+1} + p^{n+2}q)^p \\ &\equiv 1 + \sum_{k=1}^{p} \binom{p}{k} p^{(n+1)k}(1+pq)^k \\ &\equiv 1 + p^{n+1}(1+pq)p \\ &\equiv 1 + p^{n+2} \pmod{p^{n+3}}.\end{aligned}$$

Donc l'égalité est vraie pour tout entier naturel n.

Il est suffisant de trouver un élément de $(\mathbf{Z}/p^\alpha\mathbf{Z})^\star$ d'ordre $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$, et vu la stabilité des ordres par ppcm vue précédemment, il est suffisant de trouver un élément d'ordre $p-1$ et un élément d'ordre $p^{\alpha-1}$.

On va d'abord exhiber un élément d'ordre $p^{\alpha-1}$. On a

$$(1+p)^{p^{\alpha-2}} \equiv 1+p^{\alpha-1} \pmod{p^\alpha}$$

et

$$(1+p)^{p^{\alpha-1}} \equiv 1 \pmod{p^\alpha}.$$

Donc $\operatorname{ord}(1+p) \mid p^{\alpha-1}$ mais $\operatorname{ord}(1+p) \nmid p^{\alpha-2}$ donc $\operatorname{ord}(1+p) = p^{\alpha-1}$.

Il reste à trouver un élément d'ordre $p-1$. On sait que $\mathbf{F}_p^\star$ est cyclique, on note g un générateur. On a :

$$\forall k < p-1, \quad p \nmid g^k - 1 \quad \text{ie} \quad p^\alpha \nmid g^k - 1$$

et $p \mid g^{p-1} - 1$ donc $\operatorname{ord} g = k(p-1)$ est g^k et d'ordre $p-1$. □

Remarque

La preuve n'est pas constructive, mais on peut faire mieux. On peut en fait montrer que pour un générateur g de $(\mathbf{Z}/p\mathbf{Z})^\star$, l'un des éléments g ou $g+p$ engendre tous les $(\mathbf{Z}/p^\alpha\mathbf{Z})^\star$. On peut alors trouver un générateur de $(\mathbf{Z}/p^\alpha\mathbf{Z})^\star$ avec la même complexité qu'en cherchant un générateur de $(\mathbf{Z}/p\mathbf{Z})^\star$

Remarque

On peut montrer le résultat analogue dans les entiers de Gauss : si p est premier de Gauss de norme impaire, alors $(\mathbf{Z}[i]/p^\alpha\mathbf{Z}[i])^\star$ est cyclique. La preuve est étonnamment proche de celle dans $\mathbf{Z}$.

1.8 Caractérisation des groupes admettant un nombre fini de sous-groupes

Soit $(G,\cdot)$ un groupe admettant un nombre fini de sous-groupes. Alors, G est un groupe fini.

Démonstration. On va montrer que G est fini. Pour cela, procédons par contraposition et raisonnons sur les sous-groupes monogènes.

On suppose que G est infini. Montrons que G admet une infinité de sous-groupes. Supposons que G admette un sous-groupe monogène infini H. H est isomorphe à $\mathbf{Z}$, qui admet une infinité de sous-groupes (pour rappel : les $n\mathbf{Z}$ avec $n \in \mathbf{N}$). Ainsi, H admet une infinité de sous-groupes, qui sont a fortiori des sous-groupes de G.

Tous les sous groupes monogènes de G sont donc finis (cycliques). Par l'absurde, supposons qu'ils soient en nombre fini. Comme G peut s'écrire comme l'union de ses sous groupes monogènes, il vient que G est une union finie d'ensemble finis, ce qui est absurde. Donc G admet une infinité de sous groupes. □

2 Arithmétique

2.9 Formule de Legendre pour les valuation p−adiques

Soit n un entier naturel et p premier. Dans ce cas,

$$v_p(n!) = \sum_{k\geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Démonstration.

$$v_p(n!) = \sum_{m=1}^{n} v_p(m) = \sum_{m=1}^{n} \sum_{k=1}^{v_p(m)} 1 = \sum_{k=1}^{+\infty} \sum_{\substack{1\leqslant m\leqslant n\\ k\leqslant v_p(m)}} 1 = \sum_{k=1}^{+\infty} \sum_{1\leqslant m=p^k u\leqslant n} 1 = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor .$$

□

2.10 Application de la formule de Legendre

Montrer que pour $n, m \in \mathbf{N}$, $\frac{(2m)!(2n)!}{(m+n)!m!n!} \in \mathbf{N}$.

Solution. Il suffit de montrer que pour tout p premier,

$$v_p((n+m)!n!m!) \leqslant v_p((2m)!(2n)!)$$

Notons

$$\Delta_p = v_p((2m)!) + v_p((2m)!) - v_p((n+m)!) - v_p(n!) - v_p(m!)$$

de telle manière que

$$\Delta_p = \sum_{k=1}^{+\infty} \left\lfloor \frac{2m}{p^k} \right\rfloor + \left\lfloor \frac{2n}{p^k} \right\rfloor - \left\lfloor \frac{n+m}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{m}{p^k} \right\rfloor$$

On regarde pour $x, y \in \mathbf{R}^+$,

$$f(x,y) = \lfloor 2x \rfloor + \lfloor 2y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor - \lfloor x+y \rfloor .$$

L'étude de cette fonction est un exercice classique de sup. Tout d'abord $f(x+1,y) = f(x,y)$ et $f(x,y+1) = f(x,y)$. Donc il suffit de traiter le cas $x, y \in [0,1[$. Dans ce cas,

$$f(x,y) = \lfloor 2x \rfloor + \lfloor 2y \rfloor - \lfloor x+y \rfloor .$$

Or si $\lfloor x+y \rfloor = 0$ alors $f(x,y) > 0$, et si $\lfloor x+y \rfloor = 1$ alors $x+y \in [1,2[$ et donc $x \geqslant \frac{1}{2}$ ou $y \geqslant \frac{1}{2}$ et dans ce cas $\lfloor 2x \rfloor \geqslant 1$ ou $\lfloor 2y \rfloor \geqslant 1$ et alors $f(x,y) \geqslant 0$.

Bilan : $f \geqslant 0$ et $\Delta_p \geqslant 0$ pour tout p premier d'où la conclusion. □

2.11 Théorème de Wilson

$p \geqslant 3$ est premier si et seulement si $(p-1)! \equiv -1 \pmod p$.

Démonstration. Si $p = 2$ on a bien $(p-1)! \equiv 1 \pmod p$. Soit p premier impair. Considérons le polynôme $X^{p-1} - 1$. Par le petit théorème de Fermat il s'annule en $1, 2, \ldots, p-1$. Or $\mathbf{Z}/p\mathbf{Z}$ est un corps, donc dans $\mathbf{Z}/p\mathbf{Z}[X]$, on a $X^{p-1} - 1$ et $(X-\overline{1})(X-\overline{2}) \cdot \ldots \cdot (X - \overline{(p-1)})$ qui sont deux polynômes unitaires de même degré $p-1$ qui coïncident sur $p-1$ points. Ils sont donc égaux. En identifiant les termes constants on trouve ainsi $(-1)^{p-1} \cdot (p-1)! \equiv -1 \pmod p$, ce qui constitue la conclusion désirée car $p-1$ est pair.

Réciproquement, si $(p-1)! \equiv -1 \pmod p$ alors p est premier avec $(p-1)!$, c'est-à-dire avec tous les entiers entre 1 et $p-1$, i.e. p est premier.

□

2.12 Résidus quadratiques dans $\mathbf{F}_p$

Si p est un nombre premier, on dit que $x \in \mathbf{F}_p^*$ est un résidu quadratique si il existe y tel que $y^2 = x$. On supposera p impair (le cas p pair est trivial)

1. il y a exactement $\dfrac{p-1}{2}$ résidus quadratiques
2. x est un résidu quadratique si et seulement si $x^{(p-1)/2} = 1$.

Démonstration.

1. Pour le premier point, il suffit de remarquer que l'ensemble des résidus quadratiques est simplement l'image du morphisme de groupe $\varphi : x \mapsto x^2$. Comme $x^2 = 1 \iff x = \pm 1$, le noyau est de cardinal 2, et donc l'image de cardinal $\dfrac{p-1}{2}$.
2. Pour le second point, la clé est de remarquer que si x résidu quadratique, alors $x = y^2$ pour un certain y. Comme $y^{p-1} = 1$ par le petit théorème de Fermat, on a $x^{(p-1)/2} = 1$.
   Ainsi, l'ensemble des résidus quadratiques (de cardinal $(p-1)/2$) est inclus dans l'ensemble des racines de $X^{(p-1)/2} - 1$ qui est de cardinal au plus $(p-1)/2$ ($\mathbf{F}_p$ corps). Ainsi, on a égalité des ensembles.

$\square$

2.13 Méthode de descente infinie

On note p un nombre premier et pour $n \geqslant 3$, on considère l'équation dans $\mathbf{Z}^3$: $x^n + py^n = p^2 z^n$. Résolvez-la.

Solution. On remarque tout d'abord que $(0,0,0)$ est solution.

On aimerait montrer qu'il y en a pas d'autres et pour cela on procède par l'absurde en supposant l'existence d'une solution non nulle et on prendre une solution minimale selon un critère que l'on choisira assez simple.

Par exemple ici, on note $(x,y,z) \in \mathbf{Z}^3 \setminus \{0,0,0\}$ une solution tel que $|x|+|y|+|z|$ est minimale et c'est par cela qu'on cherchera l'absurdité.

$$p \mid p^2 z^n - py^n = x^n$$

donc $p \mid x$ car p est premier donc x s'écrit px' ce qui nous donne :

$$p^n x'^n + py^n = p^2 z^n \text{ donc } p^{n-1} x'^n + y^n = pz^n.$$

On peut recommencer le procédé et obtenir que $p \mid y$. Donc y s'écrit py' et donc

$$p^{n-1} x'^n + p^n y'^n = pz^n \text{ donc } p^{n-2} x'^n + p^{n-1} y'^n = z^n$$

et z peut donc s'écrire pz' et donc

$$p^{n-2} x'^n + p^{n-1} y'^n = p^n z'^n \text{ donc } x'^n + py'^n = p^2 z'^n z$$

et (x',y',z') est une solution non nulle et $|x'|+|y'|+|z'| = \frac{|x|+|y|+|z|}{p}$ ce qui est absurde. $\square$

2.14 Les congruences de Lucas

On note p un nombre premier, $n = \sum_{k=0}^{N} a_k p^k$, $m = \sum_{k=0}^{N} b_k p^k$, les décompositions en base p de n et m ($n \geqslant m$).

Montrer que $\displaystyle\binom{n}{m} \equiv \binom{a_0}{b_0} \times \cdots \times \binom{a_N}{b_N} \pmod p$

Solution. Pour la résolution, nous passerons pas une méthode polynômiale. En effet, nous savons que

$$(1+X)^p = \sum_{k=0}^{p} \binom{p}{k} X^k \equiv 1 + X^p \pmod p$$

car

$$\forall k \in [\![1, p-1]\!], \quad p \mid \binom{p}{k}.$$

Pour le voir,

$$\frac{p}{k}\binom{p-1}{k-1} = \binom{p}{k} \implies p\binom{p-1}{k-1} = k\binom{p}{k} \underset{\substack{\text{Gauß} \\ p \wedge k = 1}}{\implies} p \mid \binom{p}{k}.$$

Nous avons

$$(1+X)^n = \prod_{i=0}^{N} ((1+X)^{p^i})^{a_i}$$

or

$$\begin{aligned}(1+X)^{p^i} &= ((1+X)^p)^{p^{i-1}} \\ &\equiv (1+X^p)^{p^{i-1}} \\ &\equiv (1+X^{p^2})^{p^{i-2}} \\ &\vdots \\ &\equiv 1 + X^{p^i} \pmod p.\end{aligned}$$

Donc

$$(1+X)^n \equiv \prod_{i=0}^{N} (1+X^{p^i})^{a_i} \equiv \prod_{i=0}^{N} \sum_{k=0}^{a_i} \binom{a_i}{k} X^{kp^i} \pmod p.$$

Comme p est premier, $\mathbf{Z}/p\mathbf{Z}$ est un corps et on peut donc identifier le coefficient de X^m, ce qui nous donne :

$$\binom{n}{m} \equiv \binom{a_0}{b_0} \times \cdots \times \binom{a_N}{b_N} \pmod p.$$

En effet, un terme générique du produit est $\binom{a_0}{k_0} \times \cdots \times \binom{a_N}{k_N} \pmod p X^{k_0 p^0 + k_1 p^1 + \cdots + k_N p^N}$ et cela contribue à X^m si et seulement si $k_0 = b_0, \ldots, k_N = b_N$ par unicité de la décomposition en base p car $0 \leqslant k_i < p$. □

Remarque

En particulier, pour $a, b \in \mathbf{N}$, $\binom{pa}{pb} \equiv \binom{a}{b} \pmod p$.

2.15 Périodicité des puissances p^q-ièmes modulo p^q

Soient p premier impair, $q, m > 0$ des entiers. La suite $(k^{mp^q})_{k\in\mathbb{N}}$ est périodique modulo p^q, et admet p comme période.

Démonstration. On commence par montrer

$$\forall i \in [\![1, q-1]\!], \qquad p^{q-i} \;\Big|\; \binom{p^q}{i}$$

Pour ça, on remarque qu'on a toujours $i \geqslant v_p(i!)$ (on peut étudier $(i - v_p(i!))_i$, qui est croissante entre chaque puissance de p qui sont assez rares). On a ainsi toujours

$$q - v_p(i!) \geqslant q - i$$

Puis si on écrit

$$\binom{p^q}{i} = p^q \frac{\overbrace{(p^q-1)\cdots(p^q-i+1)}^{P}}{i!} \in \mathbf{Z}$$

Or

$$\left(\frac{i!}{p^{v_p(i!)}}\right) \wedge \left(p^{q-v_p(i!)}\right) = 1$$

donc (Gauss)

$$\frac{i!}{p^{v_p(i!)}} \;\Big|\; p^{q-v_p(i!)} P \implies p^{q-v_p(i!)} \;\Big|\; \binom{p^q}{i}$$

et le coefficient du binôme est bien divisible par p^{q-i}. On a ainsi

$$\forall k, \qquad (k+p)^{p^q} \equiv k^{p^q} + \sum_{k=1}^{p^q} \binom{p^q}{i} p^i k^{p^q - i} \equiv k^{mp^q} \pmod{p^q}$$

et

$$\forall k, m, \qquad (k+p)^{mp^q} \equiv (k^{p^q} + p^{p^q})^m \equiv k^{mp^q} \pmod{p^q}$$

□

2.16 Somme des puissances $2m+1$-ièmes de $\mathbf{Z}/p\mathbf{Z}$

Soient p premier impair et m un entier naturel.

$$\sum_{k=1}^{p} k^{2m+1} \equiv 0 \pmod p$$

Démonstration.
$$\varphi : (\mathbf{Z}/p\mathbf{Z})^\star \longrightarrow H, \quad k \longmapsto k^{2m+1}$$
est un morphisme de groupes d'image H le sous-groupe des puissances $2m+1$-ièmes. Puis, si $k \in H$ alors $-k \in H$ car $2m+1$ impair puis p impair donne $k \neq -k$. Ainsi, on peut coupler deux à deux les éléments de la somme avec leur inverse (pour l'addition), et la somme est nulle. □

2.17 Résolution de $x^2 + y^2 = 3$ dans $\mathbf{Q}^2$

Résoudre dans $\mathbf{Q}^2$ l'équation
$$x^2 + y^2 = 3$$

Solution. Supposons un couple $(x, y) \in \mathbb{Q}^2$ solution. On écrit $x = \frac{a}{b}$ et $y = \frac{c}{d}$ avec $a, c \in \mathbb{Z}$ et $b, d \in \mathbb{N}^\star$, $a \wedge b = c \wedge d = 1$. L'équation se réécrit
$$\frac{a^2}{b^2} + \frac{c^2}{d^2} = 3 \iff (ad)^2 + (cb)^2 = 3(bd)^2 \implies ad = \pm\sqrt{3(bd)^2 - (cb)^2} = \pm\, b\sqrt{3d^2 - c^2}$$
Donc $3d^2 - c^2$ doit être un carré parfait puisque ab est entier. Les entiers c et d sont premiers entre eux donc au moins l'un des deux est impair. On a
$$3d^2 - c^2 \equiv -d^2 - c^2 \equiv -1 \pmod 4 \quad \text{ou} \quad 3d^2 - c^2 \equiv -2 \pmod 4$$
C'est absurde, car un carré est toujours congru à 0 ou 1 modulo 4 (suivant la parité). Ainsi, l'équation n'admet pas de solution. □

2.18 Théorème de Beatty

Soient $\alpha, \beta \in \mathbf{R}_+^*$. On note S_α (resp. S_β) l'ensemble des entiers strictement positifs qui s'écrivent sous la forme $[n\alpha]$ (resp. $[n\beta]$ pour un certain entier n.
Alors les ensembles $S\alpha$ et S_β forment une partition de $\mathbf{N}^*$ si et seulement si $\alpha, \beta \in \mathbf{R} \setminus \mathbf{Q}$ et sont conjugués.

3 Algèbre linéaire

3.1 Résultats généraux

3.19 Technique de l'isolement

Montrer que $(x \mapsto |x - a|)_{a \in \mathbf{R}}$ est libre.

Solution. On se donne une sous-famille finie $(x \mapsto |x - a_1|, \dots, x \mapsto |x - a_p|)$ avec $a_1 < \cdots < a_p$.

Supposons qu'il existe $\lambda_1, \dots, \lambda_p$ tel que
$$\forall x \in \mathbf{R}, \quad \lambda_1 |x - a_1| + \cdots + \lambda_p |x - a_p| = 0.$$

donc

$$\forall x \in \mathbf{R}, \quad \underbrace{\lambda_1|x-a_1|+\cdots+\lambda_{p-1}|x-a_{p-1}|}_{\text{dérivable en } a_p} = \underbrace{-\lambda_p|x-a_p|}_{\text{non dérivable en } a_p \text{ sauf si } \lambda_p=0}.$$

Ainsi $\lambda_p = 0$ et on itère de cette manière jusqu'à obtenir le résultat. □

3.20 Caractérisation des homothéties vectorielles

On se donne $f \in \mathcal{L}(E)$ avec E un K-ev tel que $\forall x \in E, (x, f(x))$ est liée. Montrer qu'il existe $\lambda \in \mathbf{K}, f = \lambda Id_E$

Solution. On a : $\forall x \in E, \exists \lambda_x \in K, f(x) = \lambda_x x$.

On va montrer que λ_x ne dépend pas de x. Soient x, y deux vecteurs non nuls de E.
Supposons (x, y) libre.
Comme $\lambda_{x+y}(x+y) = \lambda_x x + \lambda_y y$, on a : $(\lambda_{x+y} - \lambda_x)x + (\lambda_{x+y} - \lambda_y)y = 0$. La liberté de (x, y) nous donne : $\lambda_x = \lambda_y = \lambda_{x+y}$.
Supposons (x, y) liée. Alors il existe $\mu \in \mathbf{K}^*$ tel que $y = \mu x$. On a : $f(y) = f(\mu x) = \mu\lambda_x x$, puis $\lambda_y y = \lambda_x y$ Or $y \neq 0$ donc $\lambda_x = \lambda_y$. On note donc λ la valeur commune des λ_x pour $x \in E \setminus \{0\}$ et l'on a $\forall x \in E \setminus \{0\}, f(x) = \lambda x$, cela reste vrai si $x = 0$ ie $f = \lambda Id_E$ □

Remarque

Cet exercice est important et à savoir refaire. Il est utile par exemple lorsqu'on chercher le centre de l'anneau $(\mathcal{L}(E), +, \circ)$ noté $Z(\mathcal{L}(E))$.
Si $f \in Z(\mathcal{L}(E))$ alors pour tout $g \in \mathcal{L}(E)$, $f \circ g = g \circ f$.
On fixe $x \in E \setminus \{0\}$ et g un projecteur sur la droite $K_x = \mathrm{Vect}_{\mathbf{K}}(x)$.
On a donc :

$$(f \circ g)(x) = (g \circ f)(x)$$
$$f(x) = \lambda_x x$$

Ainsi : $(x, f(x))$ est liée. Donc il existe $\lambda \in \mathbf{K}$ tel que $f = \lambda Id_E$. Réciproquement, on vérifie que f convient.

3.21 Lemme de factorisation

1. $u \in \mathcal{L}(E, F), v \in \mathcal{L}(E, G)$ et $\mathrm{Ker}\, u \subset \mathrm{Ker}\, v$. Montrer qu'il existe $w \in \mathcal{L}(F, G), v = w \circ u$.
2. $u \in \mathcal{L}(E, G), v \in \mathcal{L}(F, G)$ et $\mathrm{Im}\, u \subset \mathrm{Im}\, v$. Montrer qu'il existe $w \in \mathcal{L}(E, F), u = v \circ w$.

Solution.

1. On note V un supplémentaire de $\mathrm{Ker}\, u$ dans E. On sait d'après le cours que $u_{|V}$ est un isomorphisme de V dans $\mathrm{Im}\, u$.
   Si w convient alors $v_{|V} = w \circ u_{|V}$ donc $w = v_{|V} \circ u_{|V}^{-1}$ sur $\mathrm{Im}\, u$.
   Réciproquement, on note W un supplémentaire de $\mathrm{Im}\, u$ dans F et w l'application linéaire définie par morceau :

$$\begin{cases} w_{|\mathrm{Im}\, u} &= v \circ u_{|V}^{-1} \\ w_{|W} &= 0. \end{cases}$$

On a donc :

$$\begin{cases} v_{|V} & = w \circ u_{|V} \\ v_{|\operatorname{Ker} u} & = 0 = w \circ u_{|\operatorname{Ker} u} \end{cases} \quad \text{car } \operatorname{Ker} u \subset \operatorname{Ker} v.$$

Donc par l'unicité des applications linéaires définies par morceaux : $v = w \circ u$.

2. On procède presque de la même manière :
On note V supplémentaire de $\operatorname{Ker} v$ dans F. Ainsi $v_{|V}$ isomorphisme de V dans $\operatorname{Im} V \supset \operatorname{Im} u$. On note $w = v_{|V}^{-1} \circ u$ et $\operatorname{Im} u \subset \operatorname{Im} v$ donc la composition bien définie et w une application linéaire de E dans $V \subset F$.

$$\forall x \in E, \quad v \circ w(x) = v \circ v_{|V}^{-1} \circ u(x) = u(x) \text{ ie } v \circ w = u.$$

□

3.22 Propriété d'essoufflement des noyaux itérés

On note f un endomorphisme en dimension finie n. La suite

$$\left(\operatorname{Ker}\left(f^k\right)\right)_{k \in \mathbf{N}}.$$

est strictement croissante sur d premiers termes (on peut avoir $d = 0$) puis stationnaire. De plus, la suite $(\delta_k)_{k \in \mathbf{N}}$ définie par

$$\forall k \in \mathbf{N}, \delta_k = \dim\left(\operatorname{Ker}\left(f^{k+1}\right)\right) - \dim\left(\operatorname{Ker}\left(f^k\right)\right)$$

est décroissante (c'est cette monotonie qu'on appelle propriété d'essoufflement).

Démonstration. La croissance simple de la suite des noyaux est directe : si $f^k(x) = 0$ alors $f\left(f^k(x)\right) = f(0) = 0$. On a forcément croissance stricte sur les premiers termes jusqu'à atteindre une égalité (éventuellement la croissance stricte ne concerne aucun termes). Il reste à montrer que dès qu'une égalité est atteinte, la suite devient constante. Supposons

$$\operatorname{Ker}\left(f^k\right) = \operatorname{Ker}\left(f^{k+1}\right)$$

Alors,

$$\operatorname{Ker}\left(f^{k+2}\right) = \left\{x \in E, f\left(f^{k+1}(x)\right) = 0\right\} = \{x \in E, f\left(f^k(x)\right) = 0\} = \operatorname{Ker}\left(f^k\right)$$

La suite est donc bien strictement croissante puis stationnaire. On va maintenant montrer la décroissance de $(\delta_n)_n$. On a, en appliquant le théorème du rang,

$$\begin{aligned} \dim\left(\operatorname{Im}\left(f^k\right)\right) &= \dim\left(\operatorname{Ker}\left(f\,\big|_{\operatorname{Im}(f^k)}\right)\right) + \dim\left(\operatorname{Im}\left(f\,\big|_{\operatorname{Im}(f^k)}\right)\right) \\ &= \dim\left(\operatorname{Ker}\left(f\,\big|_{\operatorname{Im}(f^k)}\right)\right) + \dim\left(\operatorname{Im}\left(f^{k+1}\right)\right) \end{aligned}$$

d'où

$$\delta_k = \dim(\operatorname{Im}(f^k)) - \dim(\operatorname{Im}(f^{k+1})) = \dim\left(\operatorname{Ker}\left(f\,\big|_{\operatorname{Im}(f^k)}\right)\right) = \dim(\operatorname{Im}(f^k) \cap \operatorname{Ker}(f)).$$

Or la suite des images est décroissante donc $(\delta_k)_k$ décroît. □

3.23 Union d'espaces vectoriels

Soient $E_1, \cdots, E_n$ des $\mathbf{K}$-espaces vectoriels, où $\mathbf{K}$ est un corps infini. Si

$$\bigcup_{i=1}^{n} E_i$$

est un espace vectoriel, alors l'un des E_i contient tous les autres.

Démonstration. On suppose que

$$\bigcup_{i=1}^{n} E_i \ \widehat{=}\ E$$

est un espace vectoriel, et qu'aucun des E_i ne contient tous les autres. Quitte à éliminer les redondances et supposer n minimal, on peut faire en sorte (sans modifier l'union) que

$$E_1 \not\subset \bigcup_{j=2}^{n} E_j$$

Ainsi, si $u \in E_1 \setminus \bigcup_{i=2}^{n} E_i$ et $v \in E \setminus E_1$, l'ensemble $v + \mathbf{K}u$ est disjoint de E_1 et contient au plus un vecteur de chaque autre espace vectoriel. Ainsi, $\mathbf{K}$ possède au plus $n-1$ éléments ce qui est absurde. $\square$

Remarque

C'est équivalent au résultat suivant : Si E s'écrit comme une union finie de sous-espaces vectoriels stricts de E, alors $\mathbf{K}$ est un corps fini.

3.24 Théorème de Maschke

Soit $n \in \mathbf{N}^*$. On se donne E un $\mathbf{C}$-espace vectoriel, G un sous-groupe fini de $\mathrm{GL}(\mathcal{L}(E))$, V un sous-espace vectoriel de E stable par tous les éléments de G, et p un projecteur d'image V.
Montrer que $q = \frac{1}{|G|}\sum_{g\in G} gpg^{-1}$ est un projecteur d'image V. En déduire un supplémentaire de V stable par tous les éléments de G.

Démonstration. Calculons q^2. En remarquant que les points fixes de p sont les éléments de V et que les éléments de G stabilisent V, il vient :

$$q^2 = \frac{1}{|G|^2}\sum_{(g,g')\in G^2} gpg^{-1}g'pg'^{-1} = \frac{1}{|G|^2}\sum_{(g,g')\in G^2} gg^{-1}g'p^2g'^{-1} = \frac{1}{|G|^2}\sum_{(g,g')\in G^2} g'pg'^{-1} = q$$

De plus, $\mathcal{L}(E)$ est un anneau, donc $q \in \mathcal{L}(E)$. Ainsi : q est un projecteur.

Montrons que $\mathrm{Im}(q) = V$.
Soit x dans $\mathrm{Im}(q)$. Comme q est un projecteur, on a : $q(x) = x$, donc $\sum_{g\in G}(gpg^{-1})(x) = x$.
Or $\mathrm{Im}(p) = V$ et les éléments de G stabilisent V, donc $\forall g \in G, (gpg^{-1})(x) \in V$, puis : $x \in V$.

Soit x dans V. Montrons que $q(x) = x$, qui suffira à conclure car q est un projecteur.
Pour les mêmes raisons que précédemment :

$$q(x) = \frac{1}{|G|} \sum_{g \in G} (gpg^{-1})(x) = \frac{1}{|G|} \sum_{g \in G} (gg^{-1})(x) = \frac{1}{|G|} \sum_{g \in G} x = x.$$

Donc $x \in \mathrm{Im}(q)$.
Ainsi : $\mathrm{Im}(q) = V$.
Comme q est un projecteur, on a : $E = V \oplus \mathrm{Ker}(q)$.
Montrons que $\mathrm{Ker}(q)$ convient.
Soit $x \in \mathrm{Ker}(q)$ et $g \in G$. On a :

$$\sum_{g' \in G} (g'pg'^{-1})(x) = 0$$

donc

$$\sum_{g' \in G} \left((gg'pg'^{-1}g^{-1}) \circ g\right)(x) = 0$$

puis, par changement de variable : $(q \circ g)(x) = 0$.
$\mathrm{Ker}(q)$ est donc un supplémentaire de V stable par tous les éléments de G. □

3.2 Dualité et formes linéaires

3.25 Base antéduale

On note E un $\mathbf{K}$-ev de dimension n et $(\phi_1, \ldots, \phi_n)$ une base de E^*. Montrer qu'il existe $(x_1, \ldots, x_n) \in E^n$ tels que $\phi_i(x_j) = \delta_{i,j}$.

Solution. On note

$$\begin{aligned} \psi \colon E &\longrightarrow K^n \\ x &\longmapsto (\phi_1(x), \ldots, \phi_n(x)). \end{aligned}$$

Pour une fois, l'injectivité est plus compliqué à montrer que la surjectivité.

Si ψ n'est pas surjective alors $\dim \mathrm{Im}\, \psi < m$ donc $\mathrm{Im}\, \psi$ est inclus dans un hyperplan de $\mathbf{K}^n$. Il existe $(a_1, \ldots, a_n) \in \mathbf{K}^n \setminus \{(0, \ldots, 0)\}$ tel que

$$\forall x \in E, a_1\phi_1(x) + \cdots + a_n\phi_n(x) = 0.$$

donc $(\phi_1, \ldots, \phi_n)$ est liée. Absurde.

Donc ψ est une application linéaire surjective et $\dim E = \dim \mathbf{K}^n = n$ donc ψ est un isomorphisme.

On note $x_1 = \psi^{-1}(1, 0, \ldots, 0)$, $x_2 = \psi^{-1}(0, 1, \ldots, 0)$, . . . , $x_n = \psi^{-1}(0, , \ldots, 1)$ et la famille $(x_1, \ldots, x_n)$ convient.

C'est même une base car c'est l'image par ψ^{-1} de la base canonique de $\mathbf{K}^n$. Cette base s'appelle la base antéduale de $(\phi_1, \ldots, \phi_n)$. □

3.26

Si on note $(e_1, \ldots, e_n)$ une base de E alors pour chaque i, on note e_i^* la forme linéaire donnée par $e_i^*(e_j) = \delta_{i,j}$.
Montrer que $(e_1^*, \ldots, e_n^*)$ est une base de E^*.

Solution. C'est un résultat assez simple à montrer mais l'important est de savoir qu'un tel résultat existe.

Tout d'abord, $(e_1^*, \ldots, e_n^*)$ est une famille de n vecteurs de E^* et $\dim E^* = n$.
Il suffit donc de montrer que cette famille est libre.
Soient $a_1, \ldots, a_n \in KK$ tel que

$$a_1 e_1^* + \cdots + a_n e_n^* = 0.$$

En évaluant cette relation en $e_1, \ldots, e_n$, on obtient que $a_1 = \cdots = a_n = 0$.
Donc $(e_1^*, \ldots, e_n^*)$ est une base appelée base duale de $(e_1, \ldots, e_n)$. □

3.27 Une relation entre les formes linéaires

Soit E un **K**-ev de dimension n. On note $\phi_1, \ldots, \phi_p \in E^*$ $(p \geqslant 1)$.
Montrer que $\phi \in \mathrm{Vect}(\phi_1, \ldots, \phi_p) \iff \mathrm{Ker}\ \phi_1 \cap \cdots \cap \mathrm{Ker}\ \phi_p \subset \mathrm{Ker}\ \phi$

Solution.

— Si $\phi \in \mathrm{Vect}(\phi_1, \ldots, \phi_p)$ alors il existe $a_1, \ldots, a_p \in \mathbf{K}$ tel que :

$$\phi = a_1\phi_1 + \cdots + a_p\phi_p$$

et $\forall x \in \mathrm{Ker}\ \phi_1 \cap \cdots \cap \mathrm{Ker}\ \phi_p$, on a

$$\begin{aligned} \phi(x) &= a_1\phi_1(x) + \cdots + a_p\phi_p(x) \\ &= 0 + \cdots + 0 = 0. \end{aligned}$$

Donc $x \in \mathrm{Ker}\ \phi$ d'où l'inclusion et le sens direct.

— Pour la réciproque, je propose deux manières de la démontrer, l'une avec la base antéduale (qui n'est pas au programme) et l'autre par récurrence :

1. Pour la 1ère méthode, on suppose que $(\phi_1, \ldots, \phi_p)$ est libre pour commencer.
On complète alors en une base $(\phi_1, \ldots, \phi_p, \phi_{p+1}, \ldots, \phi_n)$.
Ainsi, il existe $(a_1, \ldots, a_n) \in K^n$ tel que

$$\phi = a_1\phi_1 + \cdots + a_n\phi_n.$$

On a vu qu'il existe $(x_1, \ldots, x_n)$ la base antéduale (ie $\phi_i(x_j) = \delta_{i,j}$).
Nous avons donc que $x_{p+1} \in \mathrm{Ker}\ \phi_1 \cap \cdots \cap \mathrm{Ker}\ \phi_p$ donc $x_{p+1} \in \mathrm{Ker}(\phi)$ et cela nous donne donc que $\phi(x_{p+1}) = 0 = a_{p+1}$.
Idem pour $x_{p+2}, \ldots, x_n$. On trouve $a_{p+1} = \cdots = a_n = 0$ d'où la conclusion.
Dans le cas général, quitte à renuméroter, on a $(\phi_1, \ldots, \phi_r)$ base de $(\phi_1, \ldots, \phi_p)$ donc $\phi_{r+1}, \ldots, \phi_p \in \mathrm{Vect}(\phi_1, \ldots, \phi_r)$ donc $\mathrm{Ker}\ \phi_1 \cap \cdots \cap \mathrm{Ker}\ \phi_r \subset \mathrm{Ker}\,\phi_{r+1}, \ldots, \mathrm{Ker}\,\phi_p$ (1ère implication).
Cela permet d'obtenir que $\mathrm{Ker}\ \phi_1 \cap \cdots \cap \mathrm{Ker}\ \phi_r \subset \mathrm{Ker}\ \phi_1 \cap \cdots \cap \mathrm{Ker}\ \phi_p \subset \mathrm{Ker}\,\phi$.
Et comme $(\phi_1, \ldots, \phi_r)$ est libre, on peut utiliser le cas précédent et donc $\phi \in \mathrm{Vect}(\phi_1, \ldots, \phi_r) = \mathrm{Vect}(\phi_1, \ldots, \phi_p)$

2. Pour la 2ème méthode, on procède par récurrence.
   On va montrer par récurrence sur p que ϕ est combinaison linéaire de $\phi_1, \dots, \phi_p$.
   Initialisation : cas $p = 1$. C'est le cas simple du cours et c'est ce résultat que l'on veut généraliser ici.
   Si $\operatorname{Ker} \phi_1 \subset \operatorname{Ker} \phi$, montrons alors que $\exists \lambda \in K,\ \phi = \lambda \phi_1$.
   Si $\phi = 0$ alors $\lambda = 0$ convient.
   Si $\phi \neq 0$ alors comme on est avec des formes linéaires, nous avons que $\operatorname{Ker} \phi_1 = \operatorname{Ker} \phi$
   De plus, il existe $a \in K, \operatorname{Ker} \phi \bigoplus Ka = E$.
   Et on peut trouver λ tel que $\phi(a) = \lambda \phi_1(a)$.
   Ainsi $\phi - \lambda \phi_1$ est nulle sur $\ker \phi$ et nulle sur Ka donc nulle sur E d'où le résultat.
   Hérédité : Supposons la propriété vraie au rang p. Et considérons $\phi_1, \dots, \phi_{p+1} \in E^*$ tel que Ker $\phi_1 \cap \dots \cap$ Ker $\phi_{p+1} \subset$ Ker ϕ.
   Premier cas :
   Si Ker $\phi_1 \cap \dots \cap$ Ker $\phi_p = \{0\}$ alors Ker $\phi_1 \cap \dots \cap$ Ker $\phi_p \subset \operatorname{Ker} \phi$ et on conclut par l'hypothèse de récurrence
   Deuxième cas : Si $F =$ Ker $\phi_1 \cap \dots \cap$ Ker $\phi_p \neq \{0\}$. On note ϕ' et ϕ'_{p+1} les restrictions à F de ϕ et ϕ_{p+1}. Ce sont des formes linéaires sur G et $\ker \phi'_{p+1} =$ Ker $\phi_1 \cap \dots \cap$ Ker $\phi_{p+1} \subset$ $\operatorname{Ker} \phi' = \operatorname{Ker} \phi \cap \phi_1 \cap \dots \cap$ Ker ϕ_p
   Ainsi par le cas $p = 1$, il existe λ_{p+1} tel que $\phi' = \lambda_{p+1} \phi'_{p+1}$.
   Ainsi $\phi - \lambda_{p+1} \phi_{p+1}$ est nulle sur F, donc c'est à dire que Ker $\phi_1 \cap \dots \cap$ Ker $\phi_p \subset$ $\operatorname{Ker}(\phi - \lambda_{p+1} \phi_{p+1})$. Et on conclut par l'hypothèse de récurrence.
   Je vous conseille de le reprendre par vous même pour bien voir les choses

□

3.28 Intersection d'hyperplans

On note E un **K**-ev, $\phi_1, \dots, \phi_p \in E^*$ et $H_i = \operatorname{Ker} \phi_i$.
Montrer que $\dim(H_1 \cap \dots \cap H_p) \geqslant n - p$ avec égalité si et seulement si $(\phi_1, \dots, \phi_p)$ est libre.

Solution. $\dim H_1 \geqslant n - 1$.

$\phi_2 \,|_{H_1}$ est une forme linéaire sur H_1 donc

$$\dim \left(\operatorname{Ker} \phi_{2|_{H_1}} \right) = \dim(H_1 \cap H_2) \geqslant \dim(H_1) - 1 \geqslant n - 2.$$

On réitère ce procédé...

$\phi_{p|_{H_1 \cap \dots \cap H_{p-1}}}$ est une forme linéaire donc

$$\dim(\ker \phi_{p|_{H_1 \cap \dots \cap H_{p-1}}} \geqslant \dim(H_1 \cap \dots \cap H_{p-1}) - 1 \geqslant n - p.$$

Et il y a égalité si toutes les inégalités sont des égalités.

On en déduit que $\dim H_1 = n - 1$ donc $\phi_1 \neq 0$ ie (ϕ_1) libre

$\dim(H_1 \cap H_2) = n - 2$ donc $H_1 \not\subset H_2$ donc $\phi_2 \notin \operatorname{Vect}(\phi_1)$ (d'après l'exercice précédent) ie (ϕ_1, ϕ_2) libre

On réitère...

$\dim(H_1 \cap \dots \cap H_p) = n - p$ donc $H_1 \cap \dots \cap H_{p-1} \not\subset H_p$ donc $\phi_p \notin \operatorname{Vect}(\phi_1, \dots, \phi_{p-1})$ donc $(\phi_1, \dots, \phi_p)$ libre.

□

3.29 forme linéaire continue

On note $(E, ||\cdot||)$ un **K**- espace vectoriel normé et $\phi \in \mathcal{L}(E, K)$.
Montrer que ϕ est continue $\iff$ Ker(ϕ) est un fermé.

Solution. $\Longrightarrow$) : $\ker(\phi) = \phi^{-1}(0)$ est un fermé car ϕ continue.

$\Longleftarrow$) : On suppose par l'absurde que ϕ n'est pas continue en 0.

Ainsi
$$\exists \varepsilon_0 > 0, \forall \delta > 0, \exists x \in E, ||x|| \geqslant \delta \text{ et } |\phi(x)| > \varepsilon_0$$
Pour $\delta = \frac{1}{n}$, on obtient $x_n \in E$ tel que $||x|| \geqslant \frac{1}{n}$ et $|\phi(x)| > \varepsilon_0$.

On note $a \notin \operatorname{Ker} \phi$ donc $\operatorname{Ker} \phi \oplus K_a = E$.

Ainsi notre x_n s'écrit $y_n + t_n a$ avec $y_n \in \operatorname{Ker} \phi$ et donc $|\phi(x_n)| = |t_n||\phi(a)| \geqslant \varepsilon_0$.

1er cas : $(t_n)_n$ bornée donc par Bolzano weierstrass, on peut donc extraire $(t_{\psi(n)})_n$ converge vers un $t \in K^*$. On a donc $y_{\psi(n)} = x_{\psi(n)} - t_{\psi(n)} a \xrightarrow[n \to +\infty]{} -ta \in \operatorname{Ker} \phi$ absurde.

2ème cas : $(t_n)_n$ non bornée donc on peut extraire $(t_\psi(n))_n$ tel que $t_\psi(n) \xrightarrow[n \to +\infty]{} +\infty$.

Ainsi
$$\underbrace{\frac{y_{\psi(n)}}{t_{\psi(n)}}} \in \ker \phi = \frac{x_{\psi(n)}}{t_{\psi(n)}} - a \xrightarrow[n \to +\infty]{} -a \notin \ker \phi$$
Absurde.

Bilan : ϕ continue en 0 donc continue sur E (car c'est une forme linéaire).

□

3.3 Matrices

3.30 Similitude sur les matrices réelles

Soit $M, N \in \mathcal{M}_n(\mathbf{R})$ et $P \in \mathrm{GL}_n(\mathbf{C})$ tels que $M = P^{-1}NP$. Montrer qu'il existe $Q \in \mathrm{GL}_n(\mathbf{R})$ tel que $M = Q^{-1}NQ$.

Démonstration. On écrit $P = A + iB$ avec A et B matrices réelles. En identifiant parties réelles et imaginaires, on a $AM = NA$ et $BM = NB$.

Donc pour tout $x \in \mathbf{R}$, $(A + xB)M = (A + xB)N$. On pose $\mathcal{P} = \det(A + XB)$ (qui est un polynôme à coefficient réels non-nul car $\mathcal{P}(i) \neq 0$ puisque $A+iB = P$ est inversible). Par conséquent $\mathcal{P}$ s'annule en un nombre fini de points. D'où l'existence de $x \in \mathbf{R}$ tel que $Q = A + xB \in \mathrm{GL}_n(\mathbf{R})$ vérifie $(A + xB)M = (A + xB)N$, i.e. $M = Q^{-1}NQ$. □

Remarque

Ce résultat est aussi valable pour une extension **L** de corps **K** infini.
On écrit $P = \sum_k P_k \cdot b_k$ où (b_k) est une base de $\mathrm{Vect}(p_{i,j})$ (coefficients de P), et on refait un peu la même démonstration... En faisant attention à l'hypothèse **K** infini.

3.31 Idéaux de $\mathcal{M}_n(\mathbf{K})$

Déterminer les idéaux bilatères et à gauche de $\mathcal{M}_n(\mathbf{K})$.

Solution. On rappelle les définitions.

I est un idéal bilatère de $\mathcal{M}_n(\mathbf{K})$ si :

— $(I,+)$ sous-groupe de $\mathcal{M}_n(\mathbf{K})$

— $\forall M \in I, \forall A \in \mathcal{M}_n(\mathbf{K}), AM, MA \in I$.

I est un idéal à gauche de $\mathcal{M}_n(\mathbf{K})$ si :

— $(I,+)$ sous-groupe de $\mathcal{M}_n(\mathbf{K})$

— $\forall M \in I, \forall A \in \mathcal{M}_n(\mathbf{K}), MA \in I$.

Pour les idéaux bilatères :

$I = \{0\}$ en est un, on suppose désormais que $I \neq \{0\}$.

Il existe donc $A \in I$ tel que $\mathrm{rg}(A) = r > 0$ donc il existe $P, Q \in GL_n(K)$ tel que

$$A = P \underbrace{\left(\begin{array}{ccc|ccc} 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & & \vdots \\ \vdots & \ddots & 1 & \ddots & & \vdots \\ \hline \vdots & & \ddots & 0 & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ \multicolumn{3}{c|}{\underbrace{0 \quad \cdots \quad \cdots}_{r}} & \cdots & 0 & 0 \end{array}\right)}_{J_r} Q \text{ donc } J_r = P^{-1}AQ^{-1} \in I.$$

Puis $J_1 = J_r J_1 \in I$. Les matrices de rang 1 sont donc équivalentes à J_1 donc sont dans I, ce qui est le cas des matrices canoniques $E_{i,j}$.

Puis pour $M \in \mathcal{M}_n(\mathbf{K})$,

$$M = \sum_{1 \leqslant i,j \leqslant n} m_{i,j} E_{i,j} = \sum_{1 \leqslant i,j \leqslant n} (m_{i,j} I_n) \underbrace{E_{i,j}}_{\in I} \in I.$$

Donc $\mathcal{M}_n(\mathbf{K}) \subset I$ ce qui nous donne $I = \mathcal{M}_n(\mathbf{K})$.

Bilan : les idéaux bilatères de $\mathcal{M}_n(\mathbf{K})$ sont $\{0\}$ et $\mathcal{M}_n(\mathbf{K})$.

Pour les idéaux à gauche :

On peut remarquer la chose suivante : Si I est un idéal à gauche et si $A \in I$ alors pour $\lambda \in \mathbf{K}, \lambda A = A \times \lambda I_n \in I$ donc I est un sous espace vectoriel de $\mathcal{M}_n(\mathbf{K})$.

On note $(A_1, \dots, A_r)$ une base de I et $M \in I$ de rang maximal.

Nous avons $M\mathcal{M}_n(\mathbf{K}) \subset I$.

Soit $A \in I$, si $\operatorname{Im} A \subset \operatorname{Im} M$ alors il existe B tel que $A = MB$ (lemme de factorisation) donc $A \in M\mathcal{M}_n(\mathbf{K})$.

Soit $A \in I$. Par l'absurde si $\operatorname{Im} A \not\subset \operatorname{Im} M$ alors M non inversible et il existe X colonne tel que $AX \notin \operatorname{Im} M$. On note $(X_1, \dots, X_n)$ une base d'un supplémentaire de $\operatorname{Ker} M$.

On note $(X_{r+1}, \dots, X_n)$ une base de $\operatorname{Ker} M$ et on note B telle que.

$$\begin{cases} BX_1 = \dots & = BX_r & = 0 \\ BX_{r+1} & = & X \\ BX_{r+2} = \dots & = BX_n & = 0 \end{cases}$$

La matrice $M + AB \in I$ et son image contient $(\underbrace{MX_1, \dots, MX_r}_{\text{Base } \operatorname{Im} M}, AX)$ donc $rg(M + AB) \geqslant r + 1 > r$ absurde donc $\operatorname{Im} A \not\subset \operatorname{Im} M$.

Bilan : Les idéaux à gauche de $\mathcal{M}_n(\mathbf{K})$ sont les ensembles du type $A\mathcal{M}_n(\mathbf{K})$ avec $A \in \mathcal{M}_n(\mathbf{K})$. □

3.32 Un résultat sur le crochet de Lie

Pour $A, B \in M_n(K)$, on note le crochet de Lie $[A, B] = AB - BA$.
Montrer que si A et $[A, B]$ commutent alors

$$\forall k \in \mathbf{N}^*, A^k B - BA^k = k[A, B]A^{k-1}$$

Solution. La preuve n'est pas difficile mais il existe des sujets (X/ENS) qui utilise cette relation pour une question sans la demander, il faut donc savoir qu'il existe une telle relation.

On procède par récrurrence sur$k$.

Initialisation ; Au cas $k = 1$: clair

Hérédité :On suppose la propriété vraie au rang $k \geqslant 1$.

Par hypothèse :

$$A^k B - BA^k = k[A, B]A^{k-1}$$

En multipliant par A à gauche :

$$A^{k+1}B - ABA^k = kA[A, B]A^{k-1} = k[A, B]A^k$$

Or $AB = [A, B] + BA$.

$$A^{k+1}B - ABA^{k+1} - [A, B]A^k = k[A, B]A^k$$

Ce qui nous donne :

$$A^{k+1}B - BA^{k+1} = (k + 1)[A, B]A^k$$

Ce qui achève la récurrence □

Remarque

Il existe une autre relation avec le crochet de Lie qui est l'identité de Jacobi :

$$[A, [B, C]] + [B, [C, A]] + [C, [B, A]] = 0$$

. Il suffit de tout exprimer pour s'en convaincre.

3.33 Quelques résultats avec le crochet de Lie

1. On note $A \in M_n(K)$ nilpotente et $\phi : B \in M_N(K) \mapsto [A, B]$. Montrer que ϕ est nilpotente
2. On suppose que $A = Diag(\lambda_1, \dots, \lambda_n)$. Montrer que ϕ est diagonalisable. Etablir le même résultat lorsque A est diagonalisable

Démonstration. 1. On aura besoin de calculer ϕ^n pour cela, au lieu de trouver une formule par récurrence, adoptons le raisonnement suivant :
On introduit $\tau_G : B \mapsto AB$ et $\tau_D : B \mapsto BA$. Ainsi $\tau_G, \tau_D \in \mathcal{L}(M_n(K))$ et ils commutent. Ainsi, comme $\phi = \tau_G - \tau_D$, on peut utiliser le binôme de Newton et obtenit :

$$\forall n \in \mathbf{N}, \quad \phi^n = \sum_{k=0}^{n} \binom{n}{k} \tau_G^k \tau_D^{n-k} (-1)^{n-k}$$

Or τ_G et τ_d sont nilpotentes par hypothèse, en notant n l'indice de nilpotence, on a que $\phi^{2n-1} = 0$ et donc ϕ nilpotente.

2. Il faut remarquer que si on note les matrices canoniques $E_{i,j}$. On a ce résultat :

$$\phi(E_{i,j}) = AE_{i,j} - E_{i,j}A = \lambda_i E_{i,j} - \lambda_j E_{i,j} = (\lambda_i - \lambda_j)E_{i,j}$$

Donc $E_{i,j}$ valeur propre pour $\lambda_i - \lambda_j$ et $(E_{i,j})_{1 \leqslant i,j \leqslant n}$ est une base de vecteurs propre de ϕ donc ϕ est diagonalisable.
Dans le cas A diagonalisable, il existe $P \in GL_n(K)$ tel que $P^{-1}AP = D$ est diagonale. De plus

$$\phi(B) = AB - BA \implies P^{-1}\phi(B)P = P^{-1}APP^{-1}BP - P^{-1}BPP^{-1}AP = [P^{-1}AP, P^{-1}BP]$$

On note $\psi : B \mapsto PBP^{-1}$ qui est un isomorphisme.

□

3.34 Commutant d'un endomorphisme diagonalisable

On note $u \in \mathcal{L}(E)$, avec E un K-ev de dimension n et on suppose que u est diagonalisable.
On note $\mathcal{C}(u) = v \in \mathcal{L}(E), u \circ v = v \circ u$.
Donner la dimension de $\mathcal{C}(u)$

Solution. On vérifie aisément que $\mathcal{C}(u)$ est un sev de $\mathcal{L}(E)$
Comme u est diagonalisable alors

$$E = E_{\lambda_1}(u) \oplus \cdots \oplus E_{\lambda_p}(u)$$

avec $\lambda_1, \dots, \lambda_p$ les valeurs propres 2 à 2 distinctes de u.
Soit $v \in \mathcal{C}(u)$ alors on sait que chaque $E_{\lambda_k}(u)$ est stable par v. Cela nous incite à regarder l'application suivante :

$$\begin{aligned}\Psi : \quad & \mathcal{C}(u) \to \mathcal{L}(E_{\lambda_1}(u)) \times \cdots \times \mathcal{L}(E_{\lambda_p}(u)) \\ & v \mapsto (v_{|E_{\lambda_1}(u)}, \dots, v_{|E_{\lambda_p}(u)})\end{aligned}$$

Ψ est bien sûr linéaire. regardons son noyau :

Soit $v \in \mathrm{Ker}(\Psi)$, alors $\forall i \in [\![1, p]\!], v_{|E_{\lambda_i}(u)} = 0$. Donc $v = 0$ sur E car elle est nulle sur une décomposition ce qui nous donne l'injectivité de Ψ.

Pour la surjectivité : Soit $(v_1, \dots, v_p) \in \mathcal{L}(E_{\lambda_1}(u)) \times \cdots \times \mathcal{L}(E_{\lambda_p}(u))$.

Il existe un unique $v \in \mathcal{L}(E)$ tel que $v_{|E_{\lambda_i}(u)} = v_i$ pour tout i(Al définie par morceau).

Or,

$$(v \circ u)_{|E_{\lambda_i}(u)} = \lambda_i v \text{ et } (u \circ v)_{|E_{\lambda_i}(u)} = \lambda_i v$$

et ce quelque soit i donc $v \circ u = u \circ v$ et donc $v \in \mathcal{C}(u)$. D'où la surjectivité.

Ainsi Ψ est un isomorphisme et donc

$$\dim(\mathcal{C}(u) = \sum_{i=1}^{p} (\dim E_{\lambda_i}(u))^2$$

□

3.35 Matrices de trace nulle

Montrer qu'une matrice de trace nulle est semblable à une matrice de diagonale nulle

Solution. Montrons le résultat par récurrence sur la taille de la matrice notée n.

Initialisation : cas n=1 : clair

Hérédité : Supposons la propriété vraie au rang $n \geqslant 1$ et on note $A \in M_{n+1}(\mathbf{C}), Tr(A) = 0$.

1er cas : $\forall X \in M_{n+1}(\mathbf{C}), (X, AX)$ liée alors (caractérisation des homothéties vectorielles), il existe $\lambda \in \mathbf{C}, A = \lambda I_{n+1}$ et $Tr(A) = 0$ donc $A = 0$ qui convient.

2ème cas : $\exists X \in M_{n+1}(\mathbf{C}), (X, AX)$ libre (donc $X \neq 0$).

On complète en une base $B = (X, AX, X_3, \dots, X_{n+1}$ et ainsi

$$Mat_B(A) = \left(\begin{array}{c|ccc} 0 & \dots & \dots & \dots \\ \hline 1 & & & \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right)$$

Comme $Tr(A) = Tr(A') = 0$ alors par hypothèse de récurrence, il existe $P \in GL_n(\mathbf{C})$ tel que $P^{-1}AP = D$ avec D de diagonale nulle. Or

$$\left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & P \end{array}\right) \text{ et } \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & P^{-1} \end{array}\right)$$

sont toutes les 2 inversibles et

$$\left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & P \end{array}\right) Mat_B(A) \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & P^{-1} \end{array}\right) = \left(\begin{array}{c|c} 0 & \dots \\ \hline \vdots & D \end{array}\right)$$

Donc A est bien semblable à une matrice de diagonale nulle ce qui achève la récurrence. □

Remarque

Avec cette remarque, on peut par exemple, résoudre l'exercice suivant :
Soit $A \in M_n(\mathbf{C})$ de trace nulle. Montrer qu'il existe $B, C \in M_n(\mathbf{C}), A = BC - CB = [B, C]$.
On peut donc se ramener au cas où la diagonale de A est nulle et on note

$$B = \begin{pmatrix} 1 & & & \\ & 2 & 0 & \\ & 0 & \ddots & \\ & & & n \end{pmatrix}$$

Soit $C \in M_n(\mathbf{C})$. On a :

$$\begin{aligned} A = [B, C] &\iff \forall (i,j) \in [\![1,n]\!], A_{i,j} = (BC - CB)_{i,j} = \sum_{k=1}^{n} B_{i,k}C_{k,j} - C_{i,k}B_{k,j} \\ &\iff \forall (i,j) \in [\![1,n]\!] A_{i,j} = (i-j)C_{i,j} \\ &\underbrace{\iff}_{A_{i,i}=0} \forall (i,j) \in [\![1,n]\!] C_{i,j} = \frac{A_{i,j}}{i-j} \end{aligned}$$

3.36 Caractérisation des matrices nilpotentes

Montrer que A nilpotente dans $\mathcal{M}_n(\mathbf{C})$ ssi $\mathrm{Tr}(A) = \mathrm{Tr}(A^2) = \cdots = \mathrm{Tr}(A^n) = 0$

Solution. Si A est nilpotente alors A est semblable à T triangulaire supérieure stricte et donc $\mathrm{Tr}(A) = \mathrm{Tr}(T) = 0$ et comme $A^2, \ldots, A^n$ nilpotentes, on a aussi $\mathrm{Tr}(A^2) = \cdots = \mathrm{Tr}(A^n) = 0$.

Réciproquement, on note $\lambda_1, \ldots, \lambda_n$ les valeurs propres de A éventuellement répétées. On suppose par l'absurde qu'il y en a différent de 0.

Quitte à renuméroter, on considère $\lambda_1, \ldots, \lambda_p$ les valeurs propres distinctes entre elle et de 0 de A.

Il existe des entiers $n_1, \ldots, n_p \geqslant 1$ (n_i le nombre de fois où λ_i apparaît).

$$\left\{ \begin{array}{l} n_1\lambda_1 + \cdots + n_p\lambda_p = \mathrm{Tr}(A) = 0 \\ n_1\lambda_1^2 + \cdots + n_p\lambda_p^2 = \mathrm{Tr}(A^2) = 0 \\ \ldots \\ n_1\lambda_1^n + \cdots + n_p\lambda_p^n = \mathrm{Tr}(A^n) = 0 \end{array} \right. \iff \begin{pmatrix} \lambda_1 & \lambda_2 & \ldots & \lambda_p \\ \lambda_1^2 & \lambda_2^2 & \ldots & \lambda_p^2 \\ \vdots & \vdots & & \vdots \\ \lambda_1^p & \lambda_2^p & \ldots & \lambda_p^p \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_p \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\iff \begin{pmatrix} n_1 \\ \vdots \\ n_p \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

car la matrice est inversible, c'est absurde car les $n_i \geqslant 1$.
Donc 0 est la seule valeur propre de A et $\chi_A(X)$ scindé donc A nilpotente. □

3.4 Déterminants

3.37 Déterminant tridiagonal

Calcul de $D_n = \begin{vmatrix} a & c & 0 & \dots & 0 \\ b & a & c & \ddots & 0 \\ 0 & b & a & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a \end{vmatrix} \in \mathcal{M}_n(\mathbf{C})$ pour $n \geqslant 3$.

Démonstration. On développe par rapport à la 1ère colonne : pour $n \geqslant 3$

$$D_n = aD_{n-1} - b \begin{vmatrix} c & 0 & 0 & \dots & 0 \\ b & a & c & \dots & 0 \\ 0 & b & a & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & c \\ 0 & 0 & \dots & b & 0 \end{vmatrix} = aD_{n-1} - bcD_{n-2}.$$

Nous avons $D_1 = a$ et $D_2 = a^2 - bc$. On peut prendre pour convention $D_0 = 1$ pour garder la formule vraie pour $n \geqslant 2$.

Ainsi D_n est une suite récurrente linéaire d'ordre 2 que l'on peut résoudre.

Son équation caractéristique est $r^2 - ar + bc = 0 \implies r_\pm = \dfrac{a \pm \sqrt{a^2 - 4bc}}{2}$ et donc $D_n = Ar_+^n + Br_-^n$ où A et B sont déterminés par les conditions initiales pour $n = 0, 1$. □

Remarque

Il est souvent judicieux d'étendre une relation de récurrence à des valeurs négatives (ici on a défini D_0 par exemple mais on aurait pu aussi définir $D_{-1} = 0$) lorsque les deux valeurs choisies risquent d'alourdir le calcul de A et B.

Exemple

Prenons par exemple $a = \cos(\theta)$ et $b = c = 1$ avec $\theta \notin \pi\mathbf{Z}$.

L'équation caractéristique est donc $r^2 - 2\cos(\theta)r + 1 = 0$ dont les racines sont $r_\pm = e^{\pm i\theta}$.

Ainsi $D_n = Ae^{in\theta} + Be^{-int}$, déterminons A et B avec les conditions initiales.

$$\begin{cases} A + B &= 1 \\ Ae^{i\theta} + Be^{-i\theta} &= 2\cos(\theta) \end{cases} \implies A = \frac{\begin{vmatrix} 1 & 1 \\ 2\cos(\theta) & e^{i\theta} \end{vmatrix}}{e^{-i\theta} - e^{i\theta}} \text{ et } B = \frac{\begin{vmatrix} 1 & 1 \\ e^{i\theta} & 2\cos(\theta) \end{vmatrix}}{e^{-i\theta} - e^{i\theta}}$$

Ainsi $A = \frac{e^{i\theta}}{2i\sin(\theta)}$ et $B = \frac{e^{-i\theta}}{-2i\sin(\theta)}$. (On a utilisé ici les formules de Cramer pour éviter des cas particuliers avec le pivot de Gauss.)

$$D_n = \frac{1}{2i\sin(\theta)}e^{i(n+1)\theta} - \frac{1}{2i\sin(\theta)}e^{-i(n+1)\theta} = \frac{\sin((n+1)\theta)}{\sin(\theta)}.$$

3.38 Déterminant de Vandermonde

Soit $\lambda_1, \dots, \lambda_n \in \mathbf{K}$.
Déterminer :

$$V(\lambda_1, \dots, \lambda_n) = \begin{vmatrix} 1 & \lambda_1 & \dots & \lambda_1^{n-1} \\ 1 & \lambda_2 & \dots & \lambda_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \lambda_n & \dots & \lambda_n^{n-1} \end{vmatrix}$$

Solution. On va montrer par récurrence sur $n \in \mathbf{N}$ que

$$V(\lambda_1, \dots, \lambda_n) = \prod_{1 \leqslant i < j \leqslant n} (\lambda_j - \lambda_i)$$

Initialisation : le cas $n = 1$ est clair
Hérédité : Supposons la propriété vraie au rang n et soient $\lambda_1, \dots, \lambda_{n+1} \in K$
1er cas : il existe $i \neq j$ tel que $\lambda_i = \lambda_j$ et donc on a bien :

$$V(\lambda_1, \dots, \lambda_{n+1}) = 0 = \prod_{1 \leqslant i < j \leqslant n+1} (\lambda_j - \lambda_i)$$

2ème cas : les λ_i 2 à 2 distincts. Adoptons une méthode polynômiale

$$V(\lambda_1, \dots, \lambda_n, x) = \begin{vmatrix} 1 & \lambda_1 & \dots & \lambda_1^{n} \\ 1 & \lambda_2 & \dots & \lambda_2^{n} \\ \vdots & \vdots & & \vdots \\ 1 & \lambda_n & \dots & \lambda_n^{n-1} \\ 1 & x & \dots & x^n \end{vmatrix}$$

C'est un polynôme en x de degré $\leqslant n$ (développer par rapport à la dernière colonne pour voir) et ce polynôme s'annule en $x = \lambda_1, \dots, \lambda_n$ donc en n racines distinctes.

On en déduit que :

$$V(\lambda_1, \dots, \lambda_n, x) = A(x - \lambda_1) \dots (x - \lambda_n)$$

On obtient le coefficient dominant A en développant par rapport à la dernière colonne et on trouve ainsi que $A = V(\lambda_1, \dots, \lambda_n)$

Ainsi :

$$\begin{aligned} V(\lambda_1, \dots, \lambda_n, \lambda_{n+1}) &= V(\lambda_1, \dots, \lambda_n) \times (x - \lambda_1) \dots (x - \lambda_n) \\ &= \prod_{1 \leqslant i < j \leqslant n+1} (\lambda_j - \lambda_i) \end{aligned}$$

Ce qui achève la récurrence. □

3.39 Déterminant circulant droit

On appelle **déterminant circulant droit** le déterminant de la matrice D définie comme suit :

$$D = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}.$$

Montrer que :

$$\det D = \prod_{k=0}^{n-1} P(\omega^k).$$

Où $\omega = e^{\frac{2i\pi}{n}}$ racine primitive de l'unité et P le polynôme défini par $P = \sum_{k=0}^{n-1} a_k X^k$.

Démonstration. Posons pour $i \in [\![0, n-1]\!]$

$$V_i = \begin{pmatrix} 1 \\ \omega^i \\ \vdots \\ \omega^{i(n-1)} \end{pmatrix}.$$

Remarquons alors que $DV_i = P(\omega^i)V_i$. En posant la matrice $Q = \Big(V_0, V_1, \ldots, V_{n-1}\Big)$ il vient $DQ = Q \times \operatorname{diag}\Big(P(1), P(\omega), \ldots, P(\omega^{n-1})\Big)$ donc nous avons

$$\det(D)\det(Q) = \det(Q) \prod_{i=0}^{n-1} P(\omega^i).$$

Et le détermiant de Q est non nul ($\det Q = V(1, \omega, \ldots, \omega^{n-1})$ avec V le déterminant de Vandermonde et les ω^i sont deux à deux distincts) ce qui conclut la preuve. $\square$

3.40 Déterminant de Cauchy

Soient $(\alpha_1, \ldots, \alpha_n) \in \mathbf{C}^n$ et $(\beta_1, \ldots, \beta_n) \in \mathbf{C}^n$ tels que pour tout $i, j \in \{1, \ldots, n\}$, $\alpha_i + \beta_j \neq 0$. Alors :

$$\det \left(\frac{1}{\alpha_i + \beta_j}\right)_{1 \leqslant i,j \leqslant n} = \frac{\prod\limits_{1 \leqslant i,j \leqslant n} (\alpha_j - \alpha_i)(\beta_j - \beta_i)}{\prod\limits_{1 \leqslant i,j \leqslant n} (\alpha_i + \beta_j)}.$$

3.5 Réduction

3.41 Réduction d'une matrice compagnon

Soient $a_0, \dots, a_{n-1} \in \mathbf{K}$ et

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ & \ddots & \ddots & 0 & \vdots \\ & & \ddots & 0 & a_{n-2} \\ & & & 1 & a_{n-1} \end{pmatrix}.$$

On dit que A est la **matrice compagnon du polynôme** P, où

$$P = X^n - a_{n-1}X^{n-1} - \cdots - a_1 X - a_0 \in \mathbf{C}[X]$$

1. On cherche à étudier dans cette question à quelle condition sur P la matrice A est diagonalisable.
   (a) Montrer que les valeurs propres de A sont exactement les racines dans $\mathbf{K}$ du polynôme P.
   (b) En déduire que si le polynôme P a exactement n racines deux à deux distinctes dans $\mathbf{K}$, alors A est diagonalisable. Déterminer dans ce cas une base de $\mathbf{K}^n$ formée de vecteurs propres de A.
   (c) Réciproquement, montrer que si A est diagonalisable, alors le polynôme P est scindé et à racines simples dans $\mathbf{K}$.
2. Calculer le polynôme caractéristique de A.

Exemple

On peut démontrer que la matrice

$$A = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & -1 \end{pmatrix}$$

est diagonalisable dans $\mathcal{M}_3(\mathbf{C})$ mais pas dans $\mathcal{M}_3(\mathbf{R})$ en étudiant la fonction polynômiale $x \to x^3 + x^2 + 1$.

3.42 Diagonalisation à ε près

Soit $\varepsilon > 0$ et $M \in \mathcal{M}_n(\mathbf{C})$. On note $\mathcal{B}_0$ la base canonique de $\mathbb{R}^n$. Montrer qu'il existe $\mathcal{B}_\varepsilon$ une base de $\mathbf{R}^n$ telle que $M' = P^{-1}_{\mathcal{B}_0,\mathcal{B}_\varepsilon} M P_{\mathcal{B}_0,\mathcal{B}_\varepsilon}$ s'écrive

$$M' = \begin{pmatrix} \lambda_1 & & a_{i,j} \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

avec $|a_{i,j}| < \varepsilon$ pour tout $j > i$.

Solution. On trigonalise M. Soit $\mathcal{B} = (e_1, ..., e_n)$ une base de trigonalisation de M. On écrit

$$P_{\mathcal{B}_0,\mathcal{B}}^{-1} M P_{\mathcal{B}_0,\mathcal{B}} = \begin{pmatrix} \lambda_1 & & m_{i,j} \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

On pose pour $k > 0$, $\mathcal{B}'_k = (e_1, \frac{e_2}{k}, ..., \frac{e_n}{k^{n-1}})$ et $P_k = P_{\mathcal{B}_0,\mathcal{B}'_k}$.
On a alors

$$P_k^{-1} M P_k = \begin{pmatrix} \lambda_1 & & \frac{a_{i,j}}{k^{j-i}} \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

On a pour tout $i, j \in [\![1, n]\!]$ tels que $j > i$, $\frac{a_{i,j}}{k} \underset{k\to+\infty}{\longrightarrow} 0$. Donc il existe $k_0 \in \mathbb{N}$ tel que pour tout $i, j \in [\![1, n]\!]$ tels que $i < j$, $\frac{a_{i,j}}{k_0^{j-i}} < \varepsilon$. P_{k_0} convient : on a diagonalisé M à ε près. □

3.43 Relation sur le polynôme caractéristique

On note $A, B \in M_n(\mathbf{K})$. Montrer que $\chi_{AB}(X) = \chi_{BA}(X)$

Solution. On va en donner 2 preuves relativement différentes.

1ère preuve :

Remarquons que :

$$\begin{pmatrix} A & -XI_n \\ I_n & 0 \end{pmatrix} \begin{pmatrix} B & -XI_n \\ I_n & -A \end{pmatrix} = \begin{pmatrix} AB - XI_n & 0 \\ B & -XI_n \end{pmatrix}$$

et

$$\begin{pmatrix} B & -XI_n \\ I_n & -A \end{pmatrix} \begin{pmatrix} A & -XI_n \\ I_n & 0 \end{pmatrix} = \begin{pmatrix} BA - XI_n & -XB \\ 0 & -XI_n \end{pmatrix}$$

Comme $\det(AB) = \det(BA)$, on prend le déterminant et on obtient :

$$\chi_{AB}(X) \times \det(-XI_n) = \chi_{BA}(X) \det(-XI_n) \implies \chi_{AB}(X) = \chi_{BA}(X)$$

2ème preuve :

Remarquons que si A est inversible alors comme $AB = A(BA)A^{-1}$ et donc

$$\chi_{AB}(X) = \det(XI_n - AB) = \det(A(XI_n - BA)A^{-1}) = \det(XI_n - BA) = \chi_{BA}(X)$$

Si A ne l'est pas, on sait que comme $\det(A - TI_n)$ est polynomiale en T et s'annule en un nombre fini de points. Considérons un T tel que $A - TI_n$ est inversible et donc on a la relation suivante vraie sur une infinité de valeurs.

$$\chi_{(A-TI_n)B}(X) = \chi_{B(A-TI_n)}(X)$$

et on évalue en $T = 0$.

□

3.44 Un résultat classique de réduction de matrices complexes

On note $A \in GL_n(\mathbf{C})$. Montrer que A^2 diagonalisable $\iff$ A diagonalisable. Que dire si $A \notin GL_n(\mathbf{C})$?

Solution. Si A diagonalisable alors il existe $P \in GL_n(\mathbf{C})$ tel que $P^{-1}AP = D$ est diagonale donc $P^{-1}A^2P = D^2$ ce qui implique que A^2 est diagonalisable

Si A^2 est diagonalisable alors on note $\lambda_1, \ldots, \lambda_p$ les valeurs propres de A^2, on a $\lambda_i \neq 0$ car $A^2 \in GL_n(\mathbf{C})$.

Nous avons donc que :

$$M_{n,1}(\mathbf{C}) = \bigoplus_{i=1}^{p} \ker(A^2 - \lambda_i I_n)$$

On sait qu'il existe (on est dans $\mathbf{C}$) $\delta_i \neq 0$ tel que $\lambda_i = \delta_i^2$ donc $X^2 - \lambda_i = \underbrace{(X - \delta_i)(X + \delta_i)}_{\text{Premiers entre eux car } \delta_i \neq 0}$

Ainsi par le Théorème de décomposition des noyaux :

$$Ker(A^2 - \lambda_i I_n) = Ker(A - \delta_i I_n) \oplus Ker(A + \delta_i I_n)$$

$$M_{n,1}(\mathbf{C}) = \bigoplus_{i=1}^{p} \ker(A - \delta_i I_n) \oplus Ker(A + \delta_i I_n)$$

Qui est une somme directe de sev propres de A une fois enlevé les termes $= \{0\}$. Donc A est diagonalisable.

Si $A \notin GL_n(\mathbf{C})$:

$$A = \begin{pmatrix} & & 1 \\ & (0) & \\ & & \end{pmatrix}$$

est un contre-exemple ☐

3.45 Décomposition de Dunford

Soit $f \in \mathcal{L}(E)$.
On suppose que χ_f est scindé sur $\mathbf{K}$. Montrer qu'il existe un unique couple $(d, n) \in \mathcal{L}(E)^2$ tel que :

- $f = d + n$
- d est un endomorphisme diagonalisable,
- n est un endomorphisme nilpotent,
- $d \circ n = n \circ d$.

De plus, montrer que d et n sont des polynômes en f et $\chi_d = \chi_f$.
La relation $f = d + n$ s'appelle la **décomposition de Dunford** de f.

Solution. Comme on suppose que $\chi_f(X)$ est scindé sur K, on peut l'écrire :

$$\chi_f(X) = (X-\lambda_1)^{\alpha_1}\dots(X-\lambda_r)^{\alpha_r}$$

tels que les λ_i sont 2 à 2 distincts et les $\alpha_i \geqslant 1$.
On se fixe une base B et on note $A = \mathrm{Mat}_B(f)$.
Par le Théorème de décomposition des noyaux, nous avons :

$$M_{n,1}(K) = \ker((A-\lambda_1 I_n)^{\alpha_1}) \oplus \dots \oplus \ker((A-\lambda_r I_n)^{\alpha_r})$$

On va noter $\Gamma_i(A) = ker((A-\lambda_r I_n)^{\alpha_r}$ pour alléger les notations.
Comme A et $(A-\lambda_i I_n)^{\alpha_i}$ commutent, on sait donc que les $\Gamma_i(A)$ sont stables par A.
De plus,

$$(A-\lambda_i I_n)^{\alpha_i}_{|\Gamma_i(A)} = 0 = (A_{|\Gamma_i(A)} - \lambda_i I_{n_{|\Gamma_i(A)}})^{\alpha_i}$$

Ce qui nous donne la nilpotence de $A_{|\Gamma_i(A)} - \lambda_i I_{n_{|\Gamma_i(A)}}$
Or,

$$A_{|\Gamma_i(A)} = \underbrace{\lambda_i I_{n_{|\Gamma_i(A)}}}_{diagonale} + \underbrace{(A_{|\Gamma_i(A)} - \lambda_i I_{n_{|\Gamma_i(A)}})}_{nilpotent}$$

Ainsi dans une base B_1 adaptée à la décomposition donnée par le théorème de décomposition des noyaux, nous avons.

$$\mathrm{Mat}_{B_1}(A) = \begin{pmatrix} \lambda_1 I_{r_1} + N_1 & & \\ (0) & \ddots & (0) \\ & & \lambda_r I_{r_r} + N_r \end{pmatrix}$$

Avec les N_i nilpotents et les r_i sont les dimensions de chaque $\Gamma_i(A)$.
Ainsi avec cette écriture, nous avons :

$$\chi_A(X) = \chi_{\lambda_1 I_{r_1}+N_1} \times \dots \times \chi_{\lambda_r I_{r_r}+N_r}$$

Or $\chi_{\lambda_i I_{r_i}+N_i} = \det((X-\lambda_i)I_{r_i} - N_i) = (X-\lambda_i)^{r_i}$
Ainsi

$$\chi_A(X) = (X-\lambda_1)^{r_1} \times \dots \times (X-\lambda_r)^{r_r}$$

or nous avions déjà que :

$$\chi_A(X) = (X-\lambda_1)^{\alpha_1}\dots(X-\lambda_r)^{\alpha_r}$$

Par unicité de la décomposition en facteur irréductibles, $a_i = r_i$ et donc $dim\Gamma_i(A) = \alpha_i$
On note :

$$D = \begin{pmatrix} \lambda_1 I_{\alpha_1} & & \\ (0) & \ddots & (0) \\ & & \lambda_r I_{\alpha_r} \end{pmatrix} \text{ et } N = \begin{pmatrix} N_1 & & \\ (0) & \ddots & (0) \\ & & N_r \end{pmatrix}$$

D est bien diagonale, N nilpotente, $ND = DN$ et $A = D + N$ et cela conclut sur l'existence.

Si on note Π_i le projecteur sur $\Gamma_i(f)$ associé à la décomposition du théorème de décomposition des noyaux, alors on sait que Π_i est un polynôme en f (revenir à la démonstration).

Ainsi comme $d = \lambda_1\Pi_1 + \cdots + \lambda_r\Pi_r$ alors d est un polynôme en f. De plus, $n = f - d$ donc n est un polynôme en f aussi

Traitons maintenant l'unicité :

Supposons qu'il existe 2 couples (d, n) et (d', n') qui conviennent.

Alors nous avons $f = d + n = d' + n'$ donc $d - d' = n' - n$. Comme ce sont tous des polynômes en f,n et n' commutent ce qui implique que $n' - n$ est nilpotente. De même, d' commute avec d et donc $d - d'$ est diagonalisable et nilpotente donc nulle (si ce point demande plus d'éclaircissement, nous contacter). Ainsi $d = d'$ et $n = n'$. D'où l'unicité. □

3.46 Diagonalisation simultanée

Soit $(f_i)_{i\in I}$ une famille de $\mathcal{L}(E)$ d'endomorphismes diagonalisables tels que les f_i commutent 2 à 2, montrer qu'il existe une base B telle que $\forall i \in I, M_B(f_i)$ diagonale

Solution. La preuve se fait par récurrence sur $\dim(E) = n$

Initialisation : $n = 1$ clair.

Hérédité : Supposons la propriété vraie jusqu'au rang $n \geqslant 1$ et on prend $\dim(E) = n + 1$.

L'idée est de penser à la décomposition en sev propre :

$$E = \bigoplus_{\lambda\in Sp_K(f_i)} E_\lambda(f_i)$$

Or pour appliquer l'hypothèse de récurrence, il va falloir faire une disjonction de cas.

Cas 1 : Tous les f_i sont des homothéties, dans ce cas, toutes les bases conviennent

Cas 2 : il existe f_{i_0} telle que f_{i_0} n'est pas une homothétie. Alors, nous avons :

$$E = \bigoplus_{\lambda\in Sp_K(f_{i_0})} \underbrace{E_\lambda(f_{i_0})}_{\dim\leqslant 1}$$

De plus, les $E_\lambda(f_{i_0})$ sont stables par tous les f_i car ils commutent et les $f_{i\,|E_\lambda(f_{i_0})}$ sont aussi diagonalisables et commutent 2 à 2.

En appliquant donc l'hypothèses de récurrence à chaque famille de restrictions à un sev propre, il existe une base B_λ de $E_\lambda(f_{i_0})$ qui les diagonalise simultanément et donc si on note B la concaténation de toutes ses bases, B convient.

Ce qui achève la récurrence □

3.47

Soit $(A_i)_{i\in I}$ des matrices tridiagonalisables de $\mathcal{M}_n(K)$ qui commutent 2 à 2.
Montrer qu'il existe $P \in \mathrm{GL}_n(\mathbf{K})$ telle que $\forall i \in I, P^{-1}A_iP$ triangulaire supérieure.

Là aussi on procède par récurrence sur n.

Initialisation : $n = 1$ clair

Hérédité : Supposons l'hypothèses vraie jusqu'au rang n. On note $(A_i)_{i\in I}$ famille de $M_{n+1}(K)$ vérifiant les hypothèses.

1er cas : Tous les A_i sont des matrices scalaires. $P = I_{n+1}$ convient.

2ème cas : il existe i_0 tel que A_{i_0} non scalaire.

On fixe $\lambda \in Sp_{\mathbf{K}}(A_{i_0})$, on a $1 \leqslant \dim(E_\lambda(A_{i_0})) \leqslant n$

De plus, $E_\lambda(A_{i_0})$ stable par tous les A_i

On note $({}_1, \dots, e_r)$ une base de $E_\lambda(A_{i_0})$ complétée en une base B de $M_{n+1}(\mathbf{K})$

Pour tout $i \in I$, on peut écrire

$$\begin{pmatrix} X_i & Y_i \\ (0) & Z_i \end{pmatrix}$$

avec $Z_i, Y_i \in \mathcal{M}_{n+1-r}(\mathbf{K}), X_i \in \mathcal{M}_r(\mathbf{K})$.

On a $\chi_{A_i} = \chi_{X_i} \times \chi_{Z_i}$ donc χ_{X_i}, χ_{Z_i} scindé.

et comme $M_B(A_i)M_B(a_j) = M_B(a_j)M_B(a_i)$ ce qui nous indique que X_i et X_j commutent ainsi que Z_i et Z_j.

Ainsi $(X_i)_{i\in I}$ famille vérifiant les hypothèses dans $\mathcal{M}_r(\mathbf{K})$ avec $1 \leqslant r \leqslant n$ et pareil pour $(Z_i)_{i\in I}$ dans $\mathcal{M}_{n+1-r}(\mathbf{K})$.

Ainsi par hypothèse de récurrence, il existe $P \in \mathrm{GL}_r(\mathbf{K}), Q \in \mathrm{GL}_{n+1-r}(\mathbf{K})$ tel que les $P^{-1}X_iP, Q^{-1}X_iQ$ sont triangulaires supérieures pour tout i.

$$\underbrace{\begin{pmatrix} P^{-1} & 0 \\ 0 & Q^{-1} \end{pmatrix}}_{M^-1} M_B(A_i) \underbrace{\begin{pmatrix} P & 0 \\ 0 & Q \end{pmatrix}}_{M} = \begin{pmatrix} P^{-1}X_iP & *** \\ (0) & Q^{-1}Z_iQ \end{pmatrix}$$

qui est triangulaire supérieure ce qui achève la récurrence

4 Algèbre commutative

4.48 Construction d'un corps fini à p^α éléments

On note p premier, α entier naturel non nul. Construire un corps de cardinal p^α.

Solution. On introduit d'abord la notion d'anneau quotient. Soit A un anneau commutatif, et I un idéal de A. On appelle anneau quotient A/I l'anneau constitué des classes d'équivalences de la relation d'équivalence

$$a \equiv b \iff a - b \in I.$$

On admet l'existence d'un polynôme irréductible [1] P_α de degré α dans $\mathbf{F}_p[X] = (\mathbf{Z}/p\mathbf{Z})[X]$. On considère l'idéal engendré par P_α, qu'on note (P_α). On se place dans l'anneau quotient $K = \mathbf{F}_p[X]/(P_\alpha)$, et on note la relation d'équivalence associée au quotient $\equiv$.

On note P, Q dans $\mathbf{F}_p[X]$ et on va montrer $\overline{PQ} = \overline{P} \times \overline{Q}$ et $\overline{P+Q} = \overline{P} + \overline{Q}$ (c'est vrai en général dans un anneau quotient, la démonstration est la même dans le cas général). On note $P_1, P_2 \in \overline{P}$, $Q_1, Q_2 \in \overline{Q}$ et on remarque $(P_1 + Q_1) - (P_2 + Q_2) = (P_1 - P_2) - (Q_2 - Q_1) \equiv 0$ donc $P_1 + Q_1 \equiv P_2 + Q_2$ et la classe de $P + Q$ ne dépend pas du choix de représentant. De même pour le produit, $P_1Q_1 - P_2Q_2 = P_1(Q_1 - Q_2) + (P_1 - P_2)Q_2 \equiv 0$, ce qui conclut.

K est un anneau (là encore c'est un résultat général sur les anneaux quotients) en tant qu'image de l'anneau $\mathbf{F}_p[X]$ par le morphisme d'anneaux

1. C'est non-trivial, et on demande en général de traiter des cas particuliers

$$\varphi : \begin{array}{ccc} \mathbf{F}_p[X] & \longrightarrow & K \\ P & \longmapsto & \overline{P}. \end{array}$$

Si $\overline{P} \neq 0$, alors P_α ne divise pas P, et comme il est irréductible il est premier avec P. Ainsi, il existe une relation de Bézout du type $UP_\alpha + VP = 1$ et donc $\overline{VP} = \overline{1}$ de sorte que $\overline{P}$ est inversible. Donc K est un corps.

Il reste à montrer que $\#K = p^\alpha$. Chaque classe de K possède un représentant de degré $< \alpha$, et ce représentant est unique (c'est une propriété de la division euclidienne). Ainsi, il y a exactement autant d'éléments dans K que de polynômes de $\mathbf{F}_p[X]$ de degré $< \alpha$, c'est à dire p^α □

Exemple

L'exemple le plus courant est la construction d'un corps à 9 éléments. On peut prendre $P_\alpha = X^2 + 1$ et $K = \mathbf{F}_3[X]/(X^2+1)\mathbf{F}_3[X]$.

4.49 Lien entre anneau euclidien et principal

Soit A un anneau commutatif. On dira que A est euclidien s'il existe une application $v : A \setminus \{0\} \to \mathbf{N}$ (qu'on appellera *stathme euclidien*) qui vérifie :

$$\forall (a,b) \in A \times A \setminus \{0\}, \exists! q, r \in A, \quad a = bq + r \quad \text{et} \quad v(r) < v(b) \text{ ou } r = 0$$

et

$$\forall a, b \in A \setminus \{0\}, v(b) \leqslant v(ab).$$

On dira alors que $a = bq + r$ est la division euclidienne de a par b.
On dira que A est principal si tous ses idéaux sont principaux, c'est à dire si tous les idéaux de A sont engendrés par un seul élément (qui dépend de l'idéal).
Les anneaux euclidiens sont principaux.

Démonstration. On note A euclidien (commutatif donc) et v son stathme, et on va montrer que A est principal. Soit I un idéal de A (bilatère par commutativité). On cherche à trouver d tel que $(d) = I = dA$. Si I est trivial, alors $d = 0$ convient. Sinon, on note $g \in I$ tel que $v(g)$ soit minimal. On va montrer que g engendre I.

On a bien $gA \subseteq I$ car I est un groupe. Soit $x \in I$. On écrit la division euclidienne de x par g :

$$x = gq + r \qquad r = 0 \text{ ou } v(r) < v(g)$$

or $r = x - gq \in I$ et $v(r) < v(g)$ absurde donc $r = 0$ et $x = gq$ et $I \subseteq gA$.

□

Remarque

On n'a pas utilisé la seconde propriété vérifiée par le stathme. Une application qui ne vérifie que la première propriété est appelée préstathme euclidien, et il suffit en fait d'avoir l'existence d'un préstathme euclidien pour montrer qu'un anneau est principal. On peut en fait encore affaiblir les hypothèses en montrant l'existence d'une norme de Dedekind-Hasse (ces normes généralisent la notion de préstathme euclidien)

4.50 Polynôme minimal d'un nombre algébrique

On appelle nombres algébriques les éléments de

$$\mathcal{A} = \{\alpha \in \mathbf{C}, \exists P \in \mathbf{Q}[X] \setminus \{0\}, P(\alpha) = 0\}.$$

Pour α algébrique, l'ensemble des polynômes annulant α possède un unique polynôme unitaire minimal pour le degré, appelé polynôme minimal et noté Π_α. C'est un polynôme irréductible de $\mathbf{Q}[X]$.

Démonstration. On note I_α l'ensemble des polynômes annulateurs de $\alpha \in \mathcal{A}$. C'est un sous-groupe de $(\mathbf{Q}[X], +)$ (car $0+0 = 0-0 = 0$), et pour tout polynôme à coefficients rationnels Q, pour $P \in I_\alpha$ on a $QP(\alpha) = Q(\alpha) \times 0 = 0$ donc $QP \in I_\alpha$ et I_α est un idéal bilatère (l'anneau est commutatif). L'anneau $\mathbf{Q}[X]$ est euclidien donc principal (Cf. Lien entre anneau euclidien et principal), donc I_α est de la forme $I_\alpha = P\mathbf{Q}[X]$, et $\Pi_\alpha = \frac{P}{\operatorname{dom} P}$ convient. Il est bien unique car si Π'_α convient, on a $\Pi_\alpha | \Pi'_\alpha$ et $\Pi'_\alpha | \Pi_\alpha$ et $\operatorname{dom}(\Pi_\alpha) = \operatorname{dom}(\Pi'_\alpha) = 1$ donc $\Pi_\alpha = \Pi'_\alpha$

Supposons Π_α réductible. Alors il existe P, Q non constants à coefficients rationnels tels que $\Pi_\alpha = PQ$ et l'un d'eux admet α pour racine, ce qui contredit la minimalité de Π_α. □

4.51 Structure de corps des algébriques

L'ensemble $\mathcal{A}$ des nombres algébriques est un corps.

Démonstration.
- $\mathcal{A} \subset \mathbf{C}$
- $1 \in \mathcal{A}$ en tant que racine de $X - 1$
- Soient $x, y \in A$, $p = \deg \Pi_x, q = \deg \Pi_y$. Pour tout $n \in \mathbf{N}$,

$$\begin{cases} x^n \in \mathrm{Vect}_{\mathbf{Q}}(1, x, \cdots, x^{p-1}) \\ y^n \in \mathrm{Vect}_{\mathbf{Q}}(1, y, \cdots, y^{q-1}) \end{cases} \qquad \text{donc} \qquad x^n y^n, (x+y)^n \in \mathrm{Vect}_{\mathbf{Q}}(x^i y^j, i < q, j < q)$$

  Les familles $((x-y)^n)_n$ et $((xy)^n)_n$ sont liées donc (on traite le cas de $x - y$, le cas de xy se traite de la même manière) il existe un polynôme P en $x - y$ à coefficients non tous nuls (et dans le corps de l'espace vectoriel, donc rationnels) tel que $P(x - y) = 0$. Les coefficients de P étant non tous nuls, $x - y$ est algébrique et $x - y, xy \in \mathcal{A}$.
- Si $x \in \mathcal{A}$ non nul et si on note $E = \mathrm{Vect}_{\mathbf{Q}}(1, x, \cdots, x^{p-1})$ alors

$$\varphi : z \in E \longmapsto xz \in E$$

  est un endomorphisme injectif en dimension finie donc c'est un isomorphisme et $\varphi^{-1}(1)$ donne $x^{-1} \in E \subset \mathcal{A}$.

□

4.52 Lemme de Gauss

Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbf{Z}[X] \setminus \{0\}$. On appelle contenu de P la quantité $c(P) = \mathrm{pgcd}(a_0, ..., a_d)$, le pgcd des coefficients du polynôme. On dit que P est primitif si $c(P) = 1$. On rappelle qu'un polynôme à coefficients entiers est dit irréductible s'il ne s'écrit pas comme produit de deux éléments non-inversibles dans $\mathbf{Z}[X]$.

1. Montrer que si P et Q sont deux polynômes primitifs, alors leur produit est primitif.
2. Montrer que si P et Q sont deux polynôme, alors $c(PQ) = c(P)c(Q)$. C'est le lemme de Gauss.
3. Soit P et Q deux polynômes de $\mathbf{Q}[X]$ unitaires tels que $PQ \in \mathbf{Z}[X]$. Montrer que P et Q sont à coefficients entiers.
   alors P est irréductible dans $\mathbf{Q}[X]$.

Démonstration. 1. On procède par l'absurde. On suppose $c(PQ) \neq 1$. Il existe p premier qui divise $c(PQ)$. Donc p divise tous les coefficients de PQ. En projetant dans $\mathbf{Z}/p\mathbf{Z}[X]$, il vient $\overline{PQ} = 0$. Or $\mathbf{Z}/p\mathbf{Z}$ est un corps donc $\mathbf{Z}/p\mathbf{Z}[X]$ est intègre. Donc $\overline{P} = 0$ ou $\overline{Q} = 0$, i.e. p divise tous les coefficients de P, ou tous ceux de Q. Ceci est exclu par hypothèse. On en conclut le résultat.

2. Par définition et homogénéité du pgcd, $\tilde{P} = \dfrac{P}{c(P)}$ et $\tilde{Q} = \dfrac{Q}{c(Q)}$ sont primitifs. Une fois de plus par homogénéité, il vient $c(PQ) = c(c(P)c(Q)\tilde{P}\tilde{Q}) = c(P)c(Q)c(\tilde{P}\tilde{Q})$. La question précédente appliquée à $\tilde{P}$ et $\tilde{Q}$ donne le résultat.

3. Il existe des entiers positifs minimaux a et b tels que aP et bQ soient à coefficients entiers : ce sont les ppcm des dénominateurs des coefficients de, respectivement, P et Q.
   En particulier $c(aP) = c(bQ) = 1$. En effet, si p premier divise $c(aP)$, p divise tous les coefficients de aP, en particulier le coefficient dominant qui est a car P unitaire. Donc $\frac{a}{p}P$ est à coefficients entiers, avec $\frac{a}{p}$ entier, ce qui contredit l'hypothèse de minimalité.
   Or, on a $c((aP)(bQ)) = abc(PQ) = c(aP)c(bQ) = 1$. Donc a et b divisent 1. Donc $a = b = 1$ c'est-à-dire $P, Q \in \mathbf{Z}[X]$.

□

4.53 Petit théorème de Fermat pour la trace

Soit $n \in \mathbf{N}^*$, $A \in \mathcal{M}_n(\mathbf{Z})$ et p un nombre premier. Montrer que :

$$\operatorname{Tr}(A^p) \equiv \operatorname{Tr}(A) \mod p$$

Démonstration. On plonge $\mathcal{M}_n(\mathbf{Z})$ dans $\mathcal{M}_n(\mathbf{Z}/p\mathbf{Z})$ via l'injection canonique $\iota : (a_{i,j})_{1\leqslant i,j\leqslant n} \in \mathcal{M}_n(\mathbf{Z}) \longmapsto (\overline{a_{i,j}})_{1\leqslant i,j\leqslant n} \in \mathcal{M}_n(\mathbf{Z}/p\mathbf{Z})$.
On vérifie facilement que ι est un morphisme d'anneau. □

Deuxième partie
Analyse

1 Suites

1.54 Lemme sous additif (Fekete)

On dit qu'une suite réelle $(u_n)_{n\in\mathbf{N}^*}$ est sous additive si :

$$\forall (n,m) \in \mathbf{N}^2 \setminus \{(0,0)\}, u_{n+m} \leqslant u_n + u_m.$$

On pose $\ell = \inf\left\{\frac{u_k}{k}, k \geqslant 1\right\}$. Montrer que $\lim\limits_{n\to+\infty} \frac{u_n}{n} = \ell$.

Démonstration. On pose artificiellement $u_0 = 0$.
Soit $\varepsilon > 0$ et $n, p \in \mathbf{N}^*$. On pose la division euclidienne de n par p de sorte que $n = pq_n + r_n$ avec $r_n \in [\![0, p-1]\!]$ et $q_n \in \mathbf{Z}$. On remarque que $q_n \geqslant 0$. Ainsi,

$$u_n \leqslant u_{pq_n} + u_{r_n} \leqslant u_{p(q_n-1)} + u_p + u_{r_n} \leqslant \cdots \leqslant q_n \cdot u_p + u_{r_n}$$

Donc,

$$\begin{aligned}\frac{u_n}{n} &\leqslant \frac{q_n}{n} \cdot u_p + \frac{u_{r_n}}{n}\\ &\leqslant \frac{n-r_n}{n} \cdot \frac{u_p}{p} + \frac{u_{r_n}}{n}\\ &\leqslant \frac{n-r_n}{n} \cdot \frac{u_p}{p} + \frac{\max\limits_{0\leqslant k\leqslant p-1}(u_k)}{n}\end{aligned}$$

Or $\frac{n-r_n}{n} \xrightarrow[n\to\infty]{} 1$, donc :

$$\exists N \in \mathbf{N}^*, \forall n \geqslant N, \frac{n-r_n}{n} \cdot \frac{u_p}{p} \leqslant \frac{u_p}{p} + \frac{\varepsilon}{2}$$

Fixons-le. Ainsi :

$$\forall n \geqslant N, \frac{u_n}{n} \leqslant \frac{u_p}{p} + \frac{\varepsilon}{2} + \frac{\max\limits_{0\leqslant k\leqslant p-1}(u_k)}{n}$$

Or $\frac{\max\limits_{0\leqslant k\leqslant p-1}(u_k)}{n} \xrightarrow[n\to+\infty]{} 0$, donc :

$$\exists N' \geqslant N, \forall n \geqslant N', \frac{u_n}{n} \leqslant \frac{u_p}{p} + \varepsilon$$

Fixons-le. Ainsi :

$$\forall n \geqslant N', \ell \leqslant \frac{u_n}{n} \leqslant \frac{u_p}{p} + \varepsilon$$

Fixons p une suite d'entiers naturels non nuls telle que $\frac{u_{p_k}}{p_k} \xrightarrow[k\to+\infty]{} \ell$.
Supposons que $\ell \in \mathbf{R}$.

Alors, par passage à la limite dans les inégalités larges : $\forall n \leqslant N', \ell \leqslant \dfrac{u_n}{n} \leqslant \ell + \varepsilon$.
On en déduit :

$$\lim_{n \to +\infty} \frac{u_n}{n} = \ell$$

Supposons que $\ell = -\infty$. Par comparaison, on retrouve le résultat escompté. □

1.55 Développement asymptotique d'une suite implicite

Montrer qu'il existe un unique $u_n \in [0, 1]$ tel que $u_n^5 + nu_n - 1 = 0$.
Donner un développement asymptotique à 2 termes de u_n.

Démonstration. Pour $n \in \mathbf{N}^*$, on note $f_n : x \mapsto x^5 + nx - 1$. f_n est dérivable sur [0,1] et

$$\forall x \in [0, 1], f_n'(x) = 5x^4 + n > 0.$$

Donc f_n est continue strictement croissante de $[0, 1]$ dans $[-1, n]$ donc f_n induit une bijection de $[0, 1]$ dans $[-1, n]$. D'où l'existence et l'unicité de u_n.

Puis

$$u_n = \frac{1}{n} - \frac{u_n^5}{n} \xrightarrow[n \to +\infty]{} 0 \text{ car } (u_n) \text{ est bornée.}$$

Ainsi comme $\frac{u_n^5}{n} = o(u_n)$ alors $u_n \underset{\infty}{\sim} 1/n$ Donc $u_n = 1/n + o(1/n)$ et alors :

$$\begin{aligned} u_n &= \frac{1}{n} - \frac{u_n^5}{n} \\ &= \frac{1}{n} - \frac{1}{n} \cdot \left(\frac{1}{n} + o\left(\frac{1}{n} \right) \right)^5 \\ &= \frac{1}{n} - \frac{1}{n^6} \cdot (1 + o(1))^5 \\ &= \frac{1}{n} - \frac{1}{n^6} + o\left(\frac{1}{n^6} \right). \end{aligned}$$

□

Remarque

On peut injecter à l'infini pour avoir tous les termes du développement asymptotique et le raisonnement est le même pour les suites vérifiant $u_n^\alpha + nu_n - 1 = 0$ avec $\alpha \in \mathbf{Z}$. Cette méthode permet de trouver le développement asymptotique de la majorité des suites implicites de ce type.

1.56 Approximation des irrationnels par des rationnels

Soit $\alpha > 0$ et $(p_n), (q_n)$ des suites d'entiers positifs tels que $\frac{p_n}{q_n} \to \alpha$. Montrez que $p_n \to +\infty$ et $q_n \to +\infty$.

Démonstration. Supposons par l'absurde que (q_n) ne diverge pas vers $+\infty$, alors quitte à extraire une sous-suite, on peut supposer qu'elle est bornée. Ainsi, (q_n) prend un nombre fini de valeurs, donc par le principe des tiroirs, (q_n) prend une valeur une infinité de fois. Si bien que quitte à

extraire une sous-suite, on peut supposer (q_n) constante égale à $q \geqslant 1$. Si bien que $p_n \to \alpha q$. $\mathbb{Z}$ étant fermé, ceci implique $\alpha q \in \mathbb{Z}$. Donc $\alpha \in \mathbb{Q}$ $(q \neq 0)$: absurde.
D'où $q_n \to \infty$, comme $p_n \sim \alpha q_n$, on a $|p_n| \to +\infty$ □

1.57 Lemme de Dirichlet

Soit $\alpha \notin \mathbb{Q}$. Montrer que :

1. Pour tout entier $N \geqslant 1$, il existe $p \in \mathbb{N}$, et $1 \leqslant q \leqslant N$ tels que :
$$0 \leqslant \left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{Nq}$$
2. Il existe deux suites $(p_n)_{n\geqslant 0}$ et $(q_n)_{n\geqslant 0}$ d'entiers avec $q_n \geqslant 1$ pour tout n telles que (q_n) injective et :
$$\forall n \geqslant 0, \left|\alpha - \frac{p_n}{q_n}\right| \leqslant \frac{1}{q_n^2}$$

Démonstration.

1. C'est essentiellement le principe des tiroirs. En effet, si on considère les réels $(\alpha \cdot q - E(\alpha \cdot q))_{1\leqslant q\leqslant N+1}$ de $[0, 1[$, il en existe 2 $q_1 < q_2$ tels que :
$$|q_1\alpha - E(q_1\alpha) - q_2\alpha + E(q_2\alpha)| \leqslant \frac{1}{N}$$
En effet, il suffit de prendre comme tiroirs les intervalles $[k/N, (k + 1)/n[$, $(0 \leqslant k < N)$ et remarquer qu'il y en a 2 dans le même tiroir. Pour conclure, on prend $q = q_2 - q_1$, $p = E(q_2\alpha) - E(q_1\alpha)$ qui vérifient clairement l'inégalité de droite. Par ailleurs, on ne peut pas avoir $\alpha = \dfrac{p}{q}$ car $\alpha \notin \mathbb{Q}$ donc on a l'inégalité de gauche aussi.
2. C'est un corollaire de ce qui précède, en effet, si on note pour tout $N \geqslant 1$, p_N, q_N des entiers comme en 1, alors $\dfrac{p_N}{q_N} \to \alpha$ donc par l'exercice précédent, $q_n \to +\infty$ donc on peut en extraire une sous-suite injective, ensuite, on remarque que comme $q_N \leqslant N$, on a l'inégalité attendue.

□

Remarque

On retiendra le fait suivant : Si on prend un réel α, alors on peut l'approcher par des rationnels avec une vitesse de convergence quadratique en le dénominateur. Ce qui peut être utile dans certains exercices. Par exemple, on peut démontrer la non convergence de $u_n = \dfrac{\tan(n)}{n}$ en utilisant le résultat ci-dessus, qui permet de trouver des n tels que n est très proche de $\pi/2$ modulo π (Exercice).

1.58 Les nombres algébriques sont difficiles à approcher

Soit α un réel algébrique de degré $d \geqslant 2$, alors on dispose d'une constante $A > 0$ telle que pour tout entiers $p \in \mathbb{Z}$ et $q \geqslant 1$:
$$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{A}{q^d}$$

Démonstration. α est un réel algébrique de degré $d \geqslant 2$, donc on dispose d'un polynôme P à coefficients entiers (pas forcément unitaire !) tel que $P(\alpha) = 0$.
Comme P est un polynôme, et que $\alpha \notin \mathbb{Q}$ ($d \geqslant 2$!), on dispose de $r > 0$ tel que si $\left|\alpha - \dfrac{p}{q}\right| \leqslant r$, alors $P(p/q) \neq 0$.
On utilise alors le fait que comme $P \in \mathbb{Z}[X]$, si $\frac{p}{q} \in [\alpha - r, \alpha + r] \cap \mathbb{Q}$, $q \geqslant 1$ on a $q^d P(p/q) \in \mathbb{Z}^*$ donc :

$$|P(p/q)| \geqslant \frac{1}{q^d}$$

Comme $P(\alpha) = 0$, ceci s'écrit :

$$\frac{1}{q^d} \leqslant |P(p/q) - P(\alpha)| \leqslant C \cdot |p/q - \alpha|$$

Où on a posé $C = \sup\limits_{x \in [r-\alpha, r+\alpha]} |P'(x)|$.
Pour conclure, on prend $A = \min(r, C)$. Si $|p/q - \alpha| \leqslant r$ on a l'inégalité attendue par ce qui précède. Sinon, on minore q^d par 1. Ce qui achève la preuve. □

Remarque

Le résultat de cet exercice est l'opposé de celui qui précède, il permet de montrer qu'on ne peut pas approcher trop rapidement un nombre algébrique par des rationnels. Il servira donc à démontrer des résultats comme le suivant :
Soit α un nombre algébrique, montrer que le rayon de convergence de $f(z) = \sum_{n \geqslant 1} \dfrac{z^n}{\sin(n\pi\alpha)}$ est non nul.

2 Séries

2.59 Transformation d'Abel

On part de deux suites (a_n) (b_n) et d'une somme $S = \sum\limits_{k=0}^{n} a_k b_k$. On pose $S_n = \sum\limits_{k=0}^{n} a_k$ avec la convention $S_{-1} = 0$. Montrer que

$$S = S_n b_n + \sum_{k=0}^{n} S_k (b_k - b_{k+1})$$

Démonstration.

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

□

Remarque

Cela permet donc de montrer que si (S_n) est bornée et si (b_n) est décroissante et tend vers 0 alors $\sum a_k b_k$ converge. Par exemple : $\sum \frac{\sin(n)}{n}$ converge.

2.60 Utilisation de paquets

Commençons pas une remarque : Si $\sum a_n$ converge alors pour toute suite $(u_n) \in \mathbf{N}^{\mathbf{N}}$, $u_n \geqslant n$ pour tout n, on a : $\sum_{n}^{u_n} a_n \xrightarrow[n \to +\infty]{} 0$.

En particulier, si $\lim\limits_{n \to +\infty} \sum_{n}^{u_n} a_n \neq 0$ alors la série diverge.

Avec cette remarque, montrer que $\sum \frac{\cos(\ln(n))}{n}$ diverge.

Solution. Il faut remarquer que ln est une fonction "lente" et donc les termes du cos ne vont pas bien se compenser. Regardons par exemple :

$$\begin{aligned}
\sum_{-\frac{\pi}{3}+2n\pi \leqslant \ln(n) \leqslant \frac{\pi}{3}+2n\pi} \frac{\cos(\ln(n))}{n} &= \sum_{e^{-\frac{\pi}{3}} e^{2n\pi} \leqslant n \leqslant e^{\frac{\pi}{3}} e^{2n\pi}} \frac{\cos(\ln(n))}{n} \\
&\geqslant \frac{1}{2} \sum_{e^{-\frac{\pi}{3}} e^{2n\pi} \leqslant n \leqslant e^{\frac{\pi}{3}} e^{2n\pi}} \frac{1}{n} \\
&\geqslant \frac{1}{2e^{\frac{\pi}{3}} e^{2n\pi}} \cdot \left(\left\lfloor e^{\frac{\pi}{3}} e^{2n\pi} \right\rfloor - \left\lfloor e^{-\frac{\pi}{3}} e^{2n\pi} \right\rfloor \right) \\
&\xrightarrow[n \to +\infty]{} \frac{e^{\frac{\pi}{3}} - e^{-\frac{\pi}{3}}}{e^{\frac{\pi}{3}}} > 0.
\end{aligned}$$

Ce qui conclut. □

2.61 Somme des inverses des sommes des carrés

Calculer
$$S = \sum_{n=1}^{\infty} \frac{1}{1^2 + 2^2 + ... + n^2}.$$

Solution. On veut calculer
$$S = \sum_{n=1}^{\infty} \frac{1}{1^2 + 2^2 + ... + n^2}$$
On sait que ceci est égal à
$$S = 6\sum_{n=1}^{\infty} \frac{1}{n(n+1)(2n+1)}$$
On effectue une décomposition en éléments simples,
$$\frac{1}{n(n+1)(2n+1)} = \frac{1}{n} + \frac{1}{n+1} - \frac{2}{n+\frac{1}{2}}$$
puis on regroupe pour faire apparaître, idéalement, des sommes télescopiques. Mais ici, on a des séparations demi-entières :
$$\frac{1}{n(n+1)(2n+1)} = \left(\frac{1}{n} - \frac{1}{n+\frac{1}{2}}\right) + \left(\frac{1}{n+1} - \frac{1}{n+\frac{1}{2}}\right)$$
Cependant, le truc dans ces cas là est d'utiliser l'égalité $\ln 2 = -\sum_{n=1}^{\infty} \frac{(-1)^n}{n}$. On a en effet
$$\sum_{n=1}^{\infty} \left(\frac{1}{n} - \frac{1}{n+\frac{1}{2}}\right) = 2\sum_{n=1}^{\infty} \left(\frac{1}{2n} - \frac{1}{2n+1}\right) = 2 - 2\ln 2$$
De même,
$$\sum_{n=1}^{\infty} \left(\frac{1}{n+1} - \frac{1}{n+\frac{1}{2}}\right) = 1 - 2\ln 2$$
En rassemblant, on trouve
$$S = 6(3 - 4\ln 2).$$
□

2.62 Equivalent de séries particulières

On veut étudier $\sum\limits_{k=n}^{+\infty} f(k)$ (on suppose donc la série convergente) avec f décroissante, intégrable sur $\mathbf{R}^+$ et $f(n) \underset{+\infty}{\sim} f(n+1)$.

Montrer que
$$\sum_{k=n}^{+\infty} f(k) \underset{+\infty}{\sim} \int_n^{+\infty} f.$$

Démonstration. On pose $F(x) = \int_0^x f$ une primitive de f. $\forall n \in \mathbf{N}$, F est continue sur $[n, n+1]$, dérivable sur $]n, n+1[$ donc par application du théorème des accroissements finis :

$$\exists c_n \in]n, n+1[, f(n+1) \leqslant F(n+1) - F(n) = f(cn) \leqslant f(n).$$

Donc $F(n+1) - F(n) \underset{+\infty}{\sim} f(n)$ qui est le terme général d'une série convergente et de signe constant donc, par équivalence des restes :

$$\sum_{k=n}^{+\infty} f(k) \underset{+\infty}{\sim} \sum_{k=n}^{+\infty} F(k+1) - F(k) = \lim_{k \to +\infty} F(k) - F(n) = \int_n^{+\infty} f.$$

□

Remarque

Cet exercice est important car il peut être adapté selon les situations (si f est croissante ou qu'on veut un équivalent des sommes partielles par exemple) et permet d'expliquer pourquoi lorsqu'on recherche un équivalent du terme général de façon à trouver une série télescopique, on regarde une primitive du terme général.

Par exemple, trouvons un équivalent de $H_n = \sum_{k=1}^{n} \frac{1}{k}$. ln est une primitive de $x \mapsto \frac{1}{x}$ et

$$\ln(n+1) - \ln(n) = \ln\left(1 + \frac{1}{n}\right) \underset{+\infty}{\sim} \frac{1}{n}$$

et donc par équivalence des sommes partielles (car H_n est divergente de terme général positif) :

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

2.63 Règle de Raabe-Duhamel

On note (u_n) une suite jamais nulle réelle tel que $\frac{u_{n+1}}{u_n} = 1 - \frac{\lambda}{n} + o(\frac{1}{n})$ avec $\lambda > 0$

Quelle est la nature de $\sum u_n$ en fonction de λ ?

Démonstration. On a $\dfrac{u_{n+1}}{u_n} \sim 1$ donc u_n de signe constant à partir d'un certain rang, quitte à changer u_n en $-u_n$, on suppose $u_n > 0$ à partir d'un certain rang.

Ainsi :

$$\ln(u_{n+1}) - \ln(u_n) = \ln\left(1 - \frac{\lambda}{n} + o\left(\frac{1}{n}\right)\right) \underset{+\infty}{\sim} -\frac{\lambda}{n}$$

$-\frac{\lambda}{n}$ est le terme général d'une série divergente de signe constant donc pas équivalence des sommes partielles :

$$\ln(u_n) \underset{+\infty}{\sim} -\lambda H_n \underset{+\infty}{\sim} -\lambda \ln(n).$$

Donc $\ln(u_n) = -\lambda \ln(n) + o(\ln(n))$ ce qui implique que $u_n = n^{-\lambda + o(1)}$.

Si $\lambda > 1$ alors $\sum u_n$ converge.

Si $\lambda < 1$ alors $\sum u_n$ diverge.

On ne peut pas conclure dans le cas $\lambda = 1$ (regarder pour $u_n = \dfrac{1}{n}$ et $v_n = \dfrac{1}{n\ln(n)^2}$). □

Remarque

Cette règle permet de résoudre le cas litigieux de la règle de d'ALEMBERT, ie lorsque $\dfrac{u_{n+1}}{u_n} \xrightarrow[n\to+\infty]{} 1$.
Malheureusement elle possède encore un cas litigieux lorsque $\lambda = 1$ mais cette règle peut être affinée si on sait que le $o\left(\dfrac{1}{n}\right)$ est le terme d'une série convergente.
On peut aussi déterminer l'équivalent suivant : $\dfrac{u_{n+1}}{u_n} \sim 1 - \dfrac{\alpha}{n} + O\left(\dfrac{1}{n^2}\right)$ alors il existe $K \in \mathbb{R}^{+*}$ tel que $u_n \sim \dfrac{K}{n^\alpha}$.

2.64 Comparaison série-intégrale généralisée

Soit $f : \mathbf{R}_+ \to \mathbf{R}$ de classe $\mathcal{C}^1$ telle que f' intégrable, alors $\sum_{n\geqslant 0} f(n)$ et $\int_0^\infty f$ sont de même natures.

Démonstration. C'est une généralisation de la comparaison série intégrale usuelle. Car si f positive décroissante, alors f' de signe constant négatif et f étant minorée, f' est intégrable et le théorème s'applique.
Pour le cas général, le caractère $\mathcal{C}^1$ de f incite à faire une IPP, mais qu'on ne peut pas faire n'importe comment. Si $n \geqslant 0$ on a :

$$\int_n^{n+1} f(t)\mathrm{d}t = [(t-(n+1))f(t)]_n^{n+1} - \int_n^{n+1} (t-n-1)f'(t)\mathrm{d}t$$

$$\int_n^{n+1} f(t)\mathrm{d}t - f(n) = \int_n^{n+1} ((n+1)-t)f'(t)\mathrm{d}t$$

En sommant cette inégalité, il vient alors que pour tout $N \geqslant 0$:

$$\int_0^{N+1} f - \sum_{n=0}^{N} f(n) = \sum_{n=0}^{N} \int_n^{n+1} ((n+1)-t)f'(t)\mathrm{d}t$$

On remarque alors que la série de droite est absolument convergente, en effet, comme $0 \leqslant (n+1)-t \leqslant 1$ on a :

$$\sum_{n=0}^{N} \left| \int_n^{n+1} ((n+1)-t)f'(t)\mathrm{d}t \right| \leqslant \int_0^{N+1} |f'| \leqslant \int_0^\infty |f'| < +\infty$$

Ainsi, ceci montre que $\left(\int_0^N f\right)_{N\geqslant 0}$ converge si et seulement si $\left(\sum_{n=0}^{N} f(n)\right)_{N\geqslant 0}$ converge. Pour conclure, on remarque que comme f' intégrable, f a une limite finie en $+\infty$. Si elle est non nulle, alors f est ni intégrable, ni sommable donc c'est facile. Sinon, on a équivalence entre convergence de $\int_0^N f$ et de $\int_0^\infty f$ et on obtient alors le résultat attendu. □

3 Intégration

3.65 Intégrale de Wallis

On note, pour tout n dans $\mathbf{N}$, $W_n = \int_0^{\frac{\pi}{2}} \cos(t)^n \mathrm{d}t = \int_0^{\frac{\pi}{2}} \sin(t)^n \mathrm{d}t$. Trouver une expression de W_n en fonction de la parité de n. Puis donner la monotonie de (W_n) et en donner un équivalent.

Solution. Tout d'abord, nous avons $W_0 = \frac{\pi}{2}$ et $W_1 = 1$. Pour $n \geqslant 2$,

$$\begin{aligned}
W_n &= \int_0^{\frac{\pi}{2}} \underbrace{\cos(t)^{n-1}}_{v'} \underbrace{\cos(t)}_{u} \\
&= [\sin(t)\cos(t)^{n-1}]_0^{\frac{\pi}{2}} + \int_0^{\frac{\pi}{2}} \sin(t)^2 (n-1)\cos(t)^{n-2} \\
&= 0 + \int_0^{\frac{\pi}{2}} (1-\cos(t)^2)(n-1)\cos(t)^{n-2} \\
&= (n-1)W_{n-2} - (n-1)W_{n-1}
\end{aligned}$$

Ainsi $W_n = \frac{n-1}{n} W_{n-2}$. Donc,

$$\forall p \in \mathbf{N}, \quad W_{2p} = \frac{2p-1}{2p} W_{2p-2} = \frac{(2p-1)(2p-3)\cdot \ldots \cdot 1}{2p \cdot 2(p-1) \cdot \ldots \cdot 2} W_0 = \frac{(2p)!}{2^{2p} p!^2} \frac{\pi}{2}$$

et

$$W_{2p+1} = \frac{2p \cdot \ldots \cdot 2}{(2p+1) \cdot \ldots \cdot 3} W_1 = \frac{2^{2p} p!^2}{(2p+1)!}$$

Pour la monotonie :

$$\forall t \in \left[0, \frac{\pi}{2}\right], \forall n \in \mathbf{N}, \quad \cos(t)^{n+1} \leqslant \cos(t)^n$$

donc en intégrant, $W_{n+1} \leqslant W_n$. Puis :

$$\frac{n+1}{n+2} W_n = W_{n+2} \leqslant W_{n+1} \leqslant W_n$$

ce qui donne que $W_{n+1} \sim W_n$. Remarquons que comme $(n+2)W_{n+2} = (n+1)W_{n+1}$ alors

$$\underbrace{(n+2)W_{n+1}W_{n+2}}_{u_{n+1}} = \underbrace{(n+1)W_n W_{n+1}}_{u_n} = \cdots = u_0 = \frac{\pi}{2}$$

Donc $\frac{\pi}{2} = (n+1)W_{n+1}W_n \sim nW_n^2$ ainsi $W_n \sim \sqrt{\frac{\pi}{2n}}$. □

3.66 Semi-convergence d'une intégrale classique

Établir la semi-convergence de l'intégrale suivante : $\int_0^{+\infty} \frac{\sin(t)}{t} dt$.

Solution. $t \mapsto \frac{\sin(t)}{t}$ est continue sur $]0, +\infty[$ et prolongeable par continuité en 0 car $\frac{\sin(t)}{t} \xrightarrow[t\to 0]{} 1$.

Il reste l'étude en $+\infty$, pour $x \in \mathbf{R}^+$,

$$\begin{aligned}\int_1^x \frac{\sin(t)}{t}\mathrm{d}t &= \left[-\frac{\cos(t)}{t}\right]_1^x + \int_1^x \frac{-\cos(t)}{t^2}\mathrm{d}t \\ &= -\frac{\cos(x)}{x} + \cos(1) - \int_1^x \underbrace{\frac{\cos(t)}{t^2}}_{\substack{|\cdot|\leqslant \frac{1}{t^2} \\ \text{intégrable en } +\infty}}\end{aligned}$$

Donc il y a une limite finie en $+\infty$ donc l'intégrale converge.

Pour $t > 0$,

$$\left|\frac{\sin(t)}{t}\right| \geqslant \frac{\sin(t)^2}{t} = \frac{1-\cos(t)}{2t}$$

donc pour $x \geqslant 1$,

$$\int_1^x \left|\frac{\sin(t)}{t}\right| \mathrm{d}t \geqslant \frac{1}{2} \underbrace{\int_1^x \frac{\mathrm{d}t}{t}}_{\ln(x) \xrightarrow[x\to+\infty]{} +\infty} - \underbrace{\int_1^x \frac{\cos(2t)}{2t}}_{\substack{\text{limite finie} \\ \text{en } +\infty}}.$$

Donc $\int_1^x \left|\frac{\sin(t)}{t}\right| \mathrm{d}t \xrightarrow[x\to+\infty]{} +\infty$ et l'intégrale n'est pas absolument convergente, d'où la semi-convergence.

□

3.67 Les intégrales de Bertrand

Déterminer la nature de

$$\int_0^{\frac{1}{2}} \frac{1}{t^\alpha |\ln(t)|^\beta}\mathrm{d}t.$$

Solution. $t \mapsto \frac{1}{t^\alpha|\ln(t)|^\beta}$ est continue sur $\left]0, \frac{1}{2}\right]$.

Si $\alpha < 0$ alors la fonction se prolonge par continuité en 0 donc est intégrable en 0.

Si $\alpha < 1$ alors

$$\frac{t^{\frac{1+\alpha}{2}}}{t^\alpha |\ln(t)|^\beta} = \frac{t^{\frac{1-\alpha}{2}}}{|\ln(t)|^\beta} \xrightarrow[t\to 0^+]{} 0$$

donc $\frac{1}{t^\alpha|\ln(t)|^\beta} = o_{0^+}\left(\frac{1}{t^{\frac{1+\alpha}{2}}}\right)$ et $\frac{1+\alpha}{2} < 1$ donc il y a intégrabilité.

Si $\alpha \geqslant 1$ alors pour $x > 0$:

$$\begin{aligned}\int_x^{\frac{1}{2}} \frac{1}{t^\alpha |\ln(t)|^\beta}\mathrm{d}t \underbrace{=}_{u=-\ln(t)} &\int_{-\ln(x)}^{-\ln(\frac{1}{2})} \frac{-e^{-u}}{(e^{-u})^\alpha u^\beta}\mathrm{d}u \\ &= \int_{-\ln(x)}^{-\ln(\frac{1}{2})} \frac{-e^{-(\alpha-1)u}}{u^\beta}\mathrm{d}u\end{aligned}$$

Si $\alpha > 1$ alors $\frac{e^{u(\alpha-1)}}{u^\beta} \xrightarrow[u\to+\infty]{} +\infty$ donc non intégrable en $+\infty$

et si $\alpha = 1$ alors $u \mapsto \frac{1}{u^\beta}$ intégrable si et seulement si $\beta > 1$.
Bilan : $\int_0^{\frac{1}{2}} \frac{1}{t^\alpha |\ln(t)|^\beta} dt$ converge si et seulement si $\alpha < 1$ ou $\alpha = 1$ et $\beta > 1$. □

Remarque

On aura de même $\int\limits_2^{+\infty} \dfrac{1}{t^\alpha\,|\ln(t)|^\beta} dt$ converge si et seulement si $\alpha > 1$ ou $\alpha = 1$ et $\beta > 1$.

3.68 La totale sur le lemme de Riemann-Lebesgue

1. Soit $f \in \mathcal{C}^1([a,b],\mathbf{C})$ alors montrer que $\int_a^b f(t)e^{int}\mathrm{d}t \xrightarrow[n\to+\infty]{} 0$. Montrer le résultat lorsque $f \in \mathcal{C}^0_{PM}([a,b],\mathbf{C})$.
2. Soit $f \in \mathcal{C}^1(\mathbf{R},\mathbf{C})$ intégrable sur $\mathbf{R}$ alors montrer $\int_{-\infty}^{+\infty} f(t)e^{int}\mathrm{d}t \xrightarrow[n\to+\infty]{} 0$. Montrer le résultat lorsque f est seulement continue et intégrable sur $\mathbf{R}$.

Solution. 1. Si $f \in \mathcal{C}^1([a,b],\mathbf{C})$, on va faire une IPP afin de sortir le n qui va tendre vers $+\infty$

$$\begin{aligned}\int_a^b \underbrace{f(t)}_{v}\underbrace{e^{int}}_{u'}\mathrm{d}t &= \left[\frac{f(t)}{in}e^{int}\right]_a^b - \frac{1}{in}\int_a^b f'(t)e^{int}\mathrm{d}t \\ &= \underbrace{\frac{f(b)e^{inb} - f(a)e^{ina}}{in}}_{\xrightarrow[n\to+\infty]{} 0} - \underbrace{\frac{1}{in}\int_a^b f'(t)e^{int}\mathrm{d}t}_{|\ |\leqslant \frac{1}{n}\int_a^b |f'(t)| \xrightarrow[n\to+\infty]{} 0}.\end{aligned}$$

D'où la conclusion.
Lorsque f est continue par morceau, la méthode est un peu plus subtile et repose sur 2 points importants :
On note $E = \left\{ f \in \mathcal{C}^0_{PM}([a,b],\mathbf{C}),\ \int\limits_a^b f(t)e^{int}\mathrm{d}t \xrightarrow[n\to+\infty]{} 0 \right\}$
le premier point est que E est un sous-espace vectoriel de $\mathcal{C}^0_{PM}([a,b],\mathbf{C})$ (grâce à la linéarité de l'intégrale et de la limite).
Le 2ème point est que l'ensemble des fonctions en escalier est dense dans l'ensemble des fonctions continues par morceaux, montrons alors que l'ensemble des fonctions en escalier appartient à E.
Pour cela, on va montrer que les fonctions indicatrices du type $\mathbb{1}_{[\alpha,\beta]}, \mathbb{1}_{]\alpha,\beta],\dots}$ sont dans E avec $\alpha, \beta \in [a,b]$

$$\int_a^b \mathbb{1}_{[\alpha,\beta]}(t)e^{int}\mathrm{d}t = \int_\alpha^\beta e^{int}\mathrm{d}t = \frac{e^{inb} - e^{ina}}{in} \xrightarrow[n\to+\infty]{} 0$$

même chose pour les autres cas.
Les fonctions en escalier étant des combinaisons linéaires des fonctions indicatrices précédentes, on en déduit que E contient toutes les fonctions en escalier de $[a,b]$.

Soit $f \in \mathcal{C}^0_{PM}([a,b],\mathbf{C})$ et soit $\varepsilon > 0$, il existe ϕ en escalier tel que $\forall t \in [a,b], |f(t)-\phi(t)| \leqslant \varepsilon'$.

$$\int_a^b f(t)e^{int}\mathrm{d}t = \underbrace{\int_a^b (f(t)-\phi(t))e^{int}\mathrm{d}t}_{|\ |\leqslant (b-a)\varepsilon'} + \underbrace{\int_a^b \phi(t)e^{int}\mathrm{d}t}_{\xrightarrow[n\to+\infty]{} 0}.$$

Donc $\exists N \in \mathbf{N}, \forall n \geqslant N$,

$$\left|\int_a^b f(t)e^{int}\mathrm{d}t\right| \leqslant (b-a)\varepsilon' + \varepsilon' = \varepsilon$$

en choisissant $\varepsilon' = \frac{\varepsilon}{b-a+1}$. Donc $f \in E$ d'où la conclusion.

2. Le cas $\mathcal{C}^1$ est légèrement plus compliqué. En effet, on peut pas appliquer l'intégration par partie sur cette intégrale impropre. Considérons $a > 0$ fixé,

$$\int_{-a}^a f(t)e^{int}\mathrm{d}t = \left[\frac{f(t)}{in}e^{int}\right]_{-a}^a - \int_{-a}^a \frac{f'(t)}{in}e^{int}\mathrm{d}t$$

Ainsi

$$\left|\int_{-a}^a f(t)e^{int}\mathrm{d}t\right| \leqslant \frac{|f(a)|}{n} + \frac{|f(-a)|}{n} + \frac{2a \sup\limits_{[-a,a]} |f'|}{n} \xrightarrow[n\to+\infty]{} 0$$

Soit $\varepsilon > 0$, par intégrabilité de f, il existe $a > 0$ tel que $\int_a^{+\infty} |f| \leqslant \varepsilon'$ et $\int_{-\infty}^{-a} |f| \leqslant \varepsilon'$.
Pour a ainsi fixé, il existe $M \in \mathbf{N}$, $\forall n \geqslant M$, $\left|\int_{-a}^a f(t)e^{int}\mathrm{d}t\right| \leqslant \varepsilon'$
Ainsi

$$\begin{aligned}\left|\int_{-\infty}^{+\infty} f(t)e^{int}\mathrm{d}t\right| &\leqslant \left|\int_a^{+\infty}\right| + \left|\int_{-\infty}^{-a}\right| + \left|\int_{-a}^{a}\right| \\ &\leqslant 3\varepsilon' = \varepsilon\end{aligned}$$

en choisissant $\varepsilon' = \frac{\varepsilon}{3}$. On a donc le résultat.
Pour f seulement continue, on a pas besoin de refaire le même raisonnement avec les fonctions continues par morceau mais utilisé le théorème de Weierstraß (densité des polynômes dans l'ensemble des fonctions continues sur un segment) sur un segment $[-a,a]$ pour a fixé.
Soit $\varepsilon > 0$.On va effectuer le même découpage que précédemment et on définit de même un tel $a > 0$. On sait qu'il existe un polynôme P tel que $\sup\limits_{[-a,a]} |f-P| \leqslant \varepsilon'$.

On a :

$$\int_{-a}^a f(x)e^{int}\mathrm{d}t = \underbrace{\int_{-a}^a (f(x)-P(x))e^{int}\mathrm{d}t}_{|\ |\leqslant 2a\varepsilon'} + \underbrace{\int_{-a}^a P(x)e^{int}\mathrm{d}t}_{\xrightarrow[n\to+\infty]{} 0}.$$

N'oublions pas que P est un polynôme donc le fait que la 2ème intégrale tend vers 0 vient du cas précédent.
donc :

$$\left|\int_{-a}^a f(x)e^{int}\mathrm{d}t\right| \leqslant (2a+1)\varepsilon' = \varepsilon.$$

en choisissant $\varepsilon' = \frac{\varepsilon}{2a+1}$.

On a donc pour tout $a > 0$, $\int_{-a}^{a} f(x)e^{int}\mathrm{d}t \xrightarrow[n\to+\infty]{} 0$ et on obtient la conclusion avec le découpage précédent.

□

Remarque

On a essayé ici de couvrir toutes les types de démonstrations possibles, notamment pour les 3 cas C^1, C^0 et C_{PM} et pour les intégrales propres et impropres. Ce lemme a plusieurs formes mais les démonstrations restent quasiment les mêmes.

3.69 Calcul par compensation

Soit f continue sur $\mathbf{R}^+$ telle que $\lim\limits_{x\to+\infty} f(x) = l \in \mathbf{R}$ et soit $0 < a < b$.

Montrer que $\displaystyle\int_0^{+\infty} \frac{f(ax) - f(bx)}{x}\mathrm{d}x$ converge et calculer l'intégrale.

Solution. Pour $0 < \varepsilon < R$

$$\begin{aligned}
\int_\varepsilon^R \frac{f(ax) - f(bx)}{x}\mathrm{d}x &= \int_\varepsilon^R \frac{f(ax)}{x}\mathrm{d}x - \int_\varepsilon^R \frac{f(bx)}{x}\mathrm{d}x \\
&\underbrace{=}_{t=ax} \int_{a\varepsilon}^{aR} \frac{f(t)}{t}\mathrm{d}t - \int_{b\varepsilon}^{bR} \frac{f(t)}{t}\mathrm{d}t \\
&= \int_{a\varepsilon}^{1} + \int_1^{aR} - \int_{b\varepsilon}^{1} - \int_1^{bR} \\
&= \int_{a\varepsilon}^{b\varepsilon} \frac{f(t)}{t}\mathrm{d}t - \int_{aR}^{bR} \frac{f(t)}{t}.
\end{aligned}$$

Or, intuitivement $\int_{a\varepsilon}^{b\varepsilon} \frac{f(t)}{t}$ risque de se comporter lorsque ε tend vers 0 comme $f(0)\int_{a\varepsilon}^{b\varepsilon} \frac{1}{t}\mathrm{d}t$. Montrons-le :

$$\begin{aligned}
\left|\int_{a\varepsilon}^{b\varepsilon} \frac{f(t)}{t}\mathrm{d}t - f(0)\ln(\frac{b}{a})\right| &= \left|\int_{a\varepsilon}^{b\varepsilon} \frac{f(t) - f(0)}{t}\mathrm{d}t\right| \\
&\leqslant \underbrace{\sup_{[a\varepsilon, b\varepsilon]} |f(u) - f(0)|}_{\xrightarrow[\varepsilon\to 0^+]{} 0} \times \underbrace{\left|\int_{a\varepsilon}^{b\varepsilon} \frac{\mathrm{d}t}{t}\right|}_{\ln(\frac{b}{a})}.
\end{aligned}$$

On aura de même $\displaystyle\left|\int_{aR}^{bR} \frac{f(t)}{t}\mathrm{d}t - l\ln\left(\frac{b}{a}\right)\right| \xrightarrow[R\to+\infty]{} 0.$

Donc $\displaystyle\int_\varepsilon^R \frac{f(ax) - f(bx)}{x}\mathrm{d}x$ a une limite si $\varepsilon \to 0^+, R \to +\infty$ donc $\displaystyle\int_0^{+\infty} \frac{f(ax) - f(bx)}{x}\mathrm{d}x$ converge et vaut $(f(0) - l)\ln\left(\frac{b}{a}\right)$.

□

Exemple

Par exemple : $\displaystyle\int_0^{+\infty} \frac{\arctan(x)-\arctan(2x)}{x}\mathrm{d}x = -\frac{\pi}{2}\ln(2).$

3.70 Sommes de Riemann généralisées

Soit f continue par morceau décroissante et intégrable sur $\mathbf{R}^+$ et $S(h) = h\displaystyle\sum_{k=1}^{+\infty} f(hk)$ avec $h>0$.
Montrer que $S(h) \xrightarrow[h\to 0^+]{} \int_0^{+\infty} f$.

Solution.

$$0 \leqslant \underbrace{hf(h(k+1))}_{\text{donc terme général série convergente}} \leqslant \underbrace{\int_{hk}^{(k+1)h} f}_{\text{terme général série convergente car f intégrable}} \leqslant hf(hk).$$

Ainsi en sommant ces inégalités :

$$S(h) - hf(0) \leqslant \int_0^{+\infty} f \leqslant S(h)$$

et donc :

$$\int_0^{+\infty} f \leqslant S(h) \leqslant hf(0) + \int_0^{+\infty} f.$$

Ce qui nous donne la conclusion en tendant h vers 0 □

Exemple

On pose $\phi(x) = \displaystyle\sum_{k=0}^{+\infty} e^{-k^2x^2}$ pour $x>0$.

Ainsi $x\phi(x) = x\displaystyle\sum_{k=0}^{+\infty} f(kx)$ avec $f : t \mapsto e^{-t^2}$ continue décroissante et intégrable sur $\mathbf{R}^+$.

Donc $x\phi(x) \xrightarrow[x\to 0^+]{} \displaystyle\int_0^{+\infty} e^{-t^2}\mathrm{d}t = \frac{\sqrt{\pi}}{2}$.

On en déduit que $\displaystyle\sum_{k=0}^{+\infty} e^{-k^2x^2} \underset{0^+}{\sim} \frac{\sqrt{\pi}}{2x}$.

3.71 Étude de $I(\alpha) = \left(\int_0^1 f^\alpha\right)^{\frac{1}{\alpha}}$

Soit $f : [0,1] \to \mathbf{R}_*^+$ et on pose $I(\alpha) = \left(\displaystyle\int_0^1 f^\alpha\right)^{\frac{1}{\alpha}}$. Étudier $I(\alpha)$ en 0^+ et en $+\infty$.

Solution. **Étude en 0^+ :**

Pour $x \in [0,1]$ fixé,

$$f^\alpha(x) = e^{\alpha \ln(f(x))} = 1 + \alpha \ln(f(x)) + \varepsilon(\alpha, x)$$

avec $\varepsilon(\alpha, x) \xrightarrow[\alpha \to 0^+]{} 0$. Ainsi,

$$\int_0^1 f^\alpha = 1 + \alpha \int_0^1 \ln(f) + \int_0^1 \varepsilon(\alpha, x)\mathrm{d}x$$

et donc :

$$I(\alpha) = e^{\frac{1}{\alpha}\ln(1+\alpha\int_0^1 \ln(f) + \int_0^1 \varepsilon(\alpha,x)\mathrm{d}x)}.$$

Le tout est de contrôler le terme négligeable, l'inégalité de Taylor-Lagrange devrait nous y aider.

$$\left| e^{\alpha \ln(f(x))} - 1 - \alpha \ln(f(x)) \right| \leqslant \frac{(\alpha \ln(f(x)))^2}{2} \sup_{x \in [0, \alpha \ln(f(x))]} |e^x|$$

f est continue sur $[0,1]$ donc est bornée, on peut donc déduire que pour α assez petit :

$$\forall x \in [0,1], \quad [\alpha \ln(f(x)), 0] \subset [-2, 2]$$

D'où

$$\underbrace{\left| e^{\alpha \ln(f(x))} - 1 - \alpha \ln(f(x)) \right|}_{|\varepsilon(\alpha,x)|} \leqslant \frac{(\alpha \ln(f(x)))^2}{2} \cdot e^2.$$

Donc

$$\begin{aligned} \left| \int_0^1 \varepsilon(\alpha, x)\mathrm{d}x \right| &\leqslant \int_0^1 |\varepsilon(\alpha, x)|\,\mathrm{d}x \\ &\leqslant \frac{e^2}{2}\alpha^2 \int_0^1 \ln(f(x))^2 \mathrm{d}x = \underset{0^+}{o}(\alpha). \end{aligned}$$

En effet, f est à valeurs dans $\mathbf{R}^{+*}$, donc $\displaystyle\int_0^1 \ln(f(x))^2\mathrm{d}x$ est bien définie.

Par suite,

$$I(\alpha) = e^{\frac{1}{\alpha}(\alpha \int_0^1 \ln(f) + o(\alpha))} \xrightarrow[\alpha \to 0^+]{} e^{\alpha \int_0^1 \ln(f)}$$

Étude en $+\infty$:

On note $M = \sup\limits_{[0,1]} |f|$, et on sait qu'il existe $x_0 \in [0,1]$ tel que $M = f(x_0)$. Quitte à faire un raisonnement similaire, on peut supposer que $x_0 \in]0,1[$.

Soit $\varepsilon > 0$,

$$\exists \delta > 0, \forall x \in [x_0 - \delta, x_0 + \delta, M - \varepsilon' \leqslant f(x) \leqslant M.$$

Puis

$$(M - \varepsilon')^\alpha 2\delta \leqslant \int_{x_0 - \delta}^{x^0 + \delta} f^\alpha \leqslant \int_0^1 f^\alpha \leqslant M^\alpha.$$

Ainsi

$$\underbrace{(M - \varepsilon') \cdot (2\delta^{\frac{1}{\alpha}})}_{\xrightarrow[\alpha \to +\infty]{} M - \varepsilon'} \leqslant I(\alpha) \leqslant M.$$

Donc il existe $A > 0$ tel que pour $\alpha \geqslant A$, $M - 2\varepsilon' \leqslant I(\alpha) \leqslant M$ et en choisissant $\varepsilon' = \frac{\varepsilon}{2}$,on obtient que $I(\alpha) \xrightarrow[\alpha \to +\infty]{} M$.

Cela explique en partie la notation de la norme infinie pour désigner le max d'une fonction. □

4 Suites et séries de fonctions

4.72 Calcul d'une intégrale grâce aux résultats sur les séries de fonction

Calculer $\displaystyle\int_0^{+\infty} \frac{t}{e^t - 1} \mathrm{d}t$.

Solution. Pour $t > 0$,

$$\frac{t}{e^t - 1} = \frac{t}{e^t(1 - e^{-t})} = \frac{t}{e^t} \sum_{k \geqslant 0} (e^{-t})^k = \sum_{k \geqslant 0} \underbrace{te^{-(k+1)t}}_{f_k(t)}.$$

Les f_k sont continues, intégrable ($= o(\frac{1}{t^2})$) sur $\mathbf{R}^+$ et $\sum f_k$ converge simplement sur $\mathbf{R}^+$ (calcul fait juste au dessus) et sa somme $t \mapsto \frac{t}{e^t-1}0$ est continue sur $\mathbf{R}^+$

De plus, pour$k \geqslant 0$,

$$\begin{aligned}
\int_0^{+\infty} |f_k(t)| \mathrm{d}t &= \int_0^{+\infty} te^{-(k+1)t} \mathrm{d}t \\
&\underbrace{=}_{IPP} \left[\frac{te^{-(k+1)t}}{-(k+1)} \right]_0^{+\infty} + \int_0^{+\infty} \frac{e^{-(k+1)t}}{k+1} \\
&= \frac{1}{(k+1)^2} \text{ terme général d'une série convergente}
\end{aligned}$$

Donc d'après le théorème d'interversion série-intégrale, nous avons :

$$\int_0^{+\infty} \frac{t}{e^t - 1} \mathrm{d}t = \sum_{k \geqslant 0} \int_0^{+\infty} te^{-(k+1)t} \mathrm{d}t = \sum_{k \geqslant 0} \frac{1}{(k+1)^2} = \frac{\pi^2}{6}.$$

□

Remarque

Il s'agit d'un exemple parmi tant d'autres de calculs d'intégrale de ce type. On en verra d'autres notamment dans la partie sur les intégrales à paramètres.

4.73 Quelques résultats sur la fonction ζ

On note : $\displaystyle\zeta(x) = \sum_{n \geqslant 1} \frac{1}{n^x}$ pour $x > 1$, $\displaystyle\phi(x) = \sum_{n \geqslant 1} \frac{(-1)^{n-1}}{n^x}$ ainsi que $u_n : x \in \mathbf{R}^{+*} \mapsto \frac{1}{n^x}$.

1. Montrer que ζ est C^∞.
2. Montrer que ζ est convexe.
3. Donner le développement asymptotique de ζ à 2 termes en 1^+.

4. Donner le développement asymptotique entier de ζ.
5. Donner une relation entre ϕ et ζ et en déduire un prolongement de ζ sur $]0,1[$.

Solution. 1. Montrons que ζ est $\mathcal{C}^n$ sur $]1,+\infty[$ pour tout $n \in \mathbf{N}$.
Pour tout $k \in \mathbf{N}^*$, les fonctions u_k sont $\mathcal{C}^\infty$ sur $]1,+\infty[$ et

$$\forall i \in [\![0,n]\!],\ \forall x \in]1,+\infty[, \qquad u_k^{(i)}(x) = \frac{(-1)^i \ln(k)^i}{k^x}.$$

Ainsi pour $x > 1$,

$$u_k^{(i)}(x) = o\left(\frac{1}{k^{\frac{1+x}{2}}}\right)$$

qui est le terme général d'une série convergente ce qui implique la convergence simple de $\sum_{k\geqslant 1} u_k^{(i)}$ sur $]1,+\infty[$.

Soit $[a,b] \subset]1,+\infty[$,

$$\forall x \in [a,b],\ \forall k \geqslant 1, \left|u_k^{(n)}(x)\right| \leqslant \frac{\ln(k)^n}{k^a} = o\left(\frac{1}{k^{\frac{1+a}{2}}}\right)$$

terme général d'une série convergente ne dépendant pas de x. Cela nous donne la convergence sur tout segment de $\sum u_k^{(n)}$ sur $]1,+\infty[$.
Le théorème de dérivation terme à terme itéré nous donne que ζ est $\mathcal{C}^n$ sur $]1,+\infty[$ et

$$\forall n \geqslant 1, \forall x > 1, \zeta^{(n)}(x) = \sum_{k\geqslant 1} \frac{(-1)^n \ln(k)^n}{k^x}.$$

ζ est donc bien $\mathcal{C}^\infty$ sur $]1,+\infty[$.

2. On a $\zeta''(x) > 0$ sur $]1,+\infty[$ donc ζ est convexe.
3. Pour $x > 1$ et $n \geqslant 1$, par comparaison série-intégrale :

$$\frac{1}{(n+1)^x} \leqslant \int_n^{n+1} \frac{\mathrm{d}t}{t^x} \leqslant \frac{1}{n^x}$$

et donc en sommant,

$$\zeta(x) - 1 \leqslant \int_1^{+\infty} \frac{\mathrm{d}t}{t^x} = \left[\frac{t^{1-x}}{1-x}\right]_0^{+\infty} = \frac{1}{x-1} \leqslant \zeta(x)$$

ce qui nous donne l'équivalence suivante : $\zeta(x) \underset{1^+}{\sim} \frac{1}{x-1}$.

Étudions $\zeta(x) - \frac{1}{x-1}$.

$$\zeta(x) - \frac{1}{x-1} = \sum_{k\geqslant 1} \left(\frac{1}{n^x} - \int_n^{n+1} \frac{\mathrm{d}t}{t^x}\right)$$

On pose donc $f_n(x) = \frac{1}{n^x} - \int_n^{n+1} \frac{\mathrm{d}t}{t^x}$ pour $x \in [1,+\infty[$.

Nous avons $\forall x \geqslant 1, \forall n \geqslant 0$:

$$0 \leqslant f_n(x) \leqslant \frac{1}{n^x} - \frac{1}{(n+1)^x}$$

qui est le terme général d'une série convergente, ce qui implique la convergence simple de $\sum f_n(x)$ sur $[1, +\infty[$.
Pour $x \geqslant 1, n \geqslant 1$,

$$\begin{aligned} 0 \leqslant \sum_{k=n+1}^{+\infty} f_k(x) &\leqslant \sum_{k=n+1}^{+\infty} \frac{1}{k^x} - \frac{1}{(k+1)^x} \\ &= \frac{1}{(n+1)^x} \\ &\leqslant \frac{1}{n+1} \xrightarrow[n\to+\infty]{} 0 \text{ et ne dépend pas de x} \end{aligned}$$

D'où la convergence uniforme de $\sum f_n$ sur $[1, +\infty[$.
Or les f_n sont continues sur $[1, +\infty[$, donc $x \mapsto \sum_{n\leqslant 1} f_n(x)$ est continue sur le même intervalle.
Or pour $x \geqslant 1$,

$$\begin{aligned} \sum_{n\leqslant 1} f_n(x) &= \sum_{n\geqslant 1} \frac{1}{n^x} - \int_n^{n+1} \frac{\mathrm{d}t}{t^x} \\ &= \zeta(x) - \frac{1}{x-1} \xrightarrow[x\to+1^+]{} \sum_{n\leqslant 1} f_n(1). \end{aligned}$$

Or,

$$\begin{aligned} \sum_{n\leqslant 1} f_n(1) &= \sum_{n\leqslant 1} \frac{1}{n} - \int_n^{n+1} \frac{\mathrm{d}t}{t} \\ &= \lim_{n\to+\infty} H_n - \sum_{k=1}^{n}(ln(k+1) - ln(k)) \\ &= \lim_{n\to+\infty} H_n - ln(n) \\ &= \gamma \text{ en utilisant que} H_n = \ln(n) + \gamma + o(1) \end{aligned}$$

Ainsi $\zeta(x) = \frac{1}{x-1} + \gamma + o(1)$.

4. Maintenant faisons l'étude de ζ en $+\infty$. On va montrer que les sommes partielles de $\zeta(x)$ est son propre développement asymptotique. Chaque terme contribue de plus en plus faiblement à ζ
Pour $n \geqslant 1$,

$$n^x(\zeta(x) - \sum_{k=1}^{n} \frac{1}{k^x} = \sum_{k=n+1}^{+\infty} \frac{n^x}{k^x}.$$

Or

$$\forall x \geqslant 2, \forall k \geqslant (n+1), \frac{n^x}{k^x} \leqslant \frac{n^2}{k^2}$$

qui est le terme général d'une série convergente ne dépendant pas de x.

Ainsi $\sum \frac{n^x}{k^x}$ converge uniformément sur $[2,+\infty[$. On peut donc appliquer le théorème d'interversion des limites et obtenir :

$$\lim_{x\to+\infty} \sum_{k=n+1}^{+\infty} \frac{n^x}{k^x} = \sum_{k=n+1}^{+\infty} \lim_{x\to+\infty} \frac{n^x}{k^x} = 0.$$

Cela nous donne directement que :

$$\zeta(x) = \sum_{k=1}^{n} \frac{1}{k^x} + \underset{+\infty}{o}(\frac{1}{n^x}).$$

5. Déterminons le lien entre ϕ et ζ.
   Pour $x > 1$,

$$\begin{aligned}\zeta(x) - \phi(x) &= \sum_{n\geqslant 1} \frac{1-(-1)^n-1}{n^x} \\ &= 2\sum_{n\geqslant} \frac{1}{(2n)^x} \\ &= \frac{2}{2^x}\zeta(x).\end{aligned}$$

   Cela nous donne $\phi(x) = (1-\frac{1}{2^{x-1}})\zeta(x)$ ou $\zeta(x) = \frac{1}{1-\frac{1}{2^{x-1}}}\phi(x)$.
   Cette égalité nous donner directement un prolongement de ζ sur $]0,1[$.

□

Remarque

La dernière égalité nous donne d'ailleurs un résultat classique, en effet

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

Donc

$$\zeta(x) \underset{1^+}{\sim} \frac{1}{\ln(2)(x-1)}\phi(1)$$

et d'après le point 3, $\phi(1) = \sum_{n\geqslant 1} \frac{(-1)^{n-1}}{n} = \ln(2)$.

4.74 Théorèmes de Dini

Soient $a < b$ dans $\mathbf{R}$, $f_n : [a,b] \to \mathbf{R}$ une suite de fonctions continues qui converge simplement vers une fonction continue f.

1. Si chaque f_n est croissante, alors la convergence est uniforme.
2. Si la suite (f_n) est croissante, alors la convergence est uniforme.

Démonstration. 1. L'idée est que l'on peut utiliser la convergence simple pour un nombre fini de points, puis utiliser la croissance et la continuité uniforme de f pour contrôler le reste. Soit $\varepsilon > 0$, f étant continue sur un compact, elle est uniformément continue. Soit donc $\delta > 0$

un module de continuité uniforme pour ε, et $a = x_0 < \ldots < x_k = b$ une subdivision de pas $\leqslant \delta$.
Par utilisation de la convergence simple sur un nombre fini de points, on dispose de $N \geqslant 0$ tel que pour tout $n \geqslant N$, et $i \in \{0, \ldots, k\}$, on ait $|f_n(x_i) - f(x_i)| \leqslant \varepsilon$.
Soit alors $n \geqslant N$ et $x \in [a, b]$. On dispose de i tel que $x \in [x_i, x_i + 1]$ par notre choix de subdivision.
En utilisant la croissance des f_n on obtient :

$$f(x) - 2\varepsilon \leqslant f(x_i) - \varepsilon \leqslant f_n(x_i) \leqslant f_n(x) \leqslant f_n(x_{i+1}) \leqslant f(x_{i+1}) + \varepsilon \leqslant f(x) + 2\varepsilon.$$

Ainsi, $|f_n(x) - f(x)| \leqslant 2\varepsilon$, donc (f_n) converge uniformément vers f sur $[a, b]$.

2. Il y a une preuve naturelle qui utilise la même idée que la question 1 mais qui a le mauvais goût d'utiliser Borel-Lebesgue (voir 1 page 73). Voici une preuve un peu plus astucieuse mais expéditive :
Soit $\varepsilon > 0$, et $K_n = \{x \in [a, b] \mid f_n(x) \leqslant f(x) - \varepsilon\}$. K_n est fermé par continuité de f_n et f, dans un compact donc K_n compact. De plus, par croissance de la suite (f_n), on a $K_{n+1} \subseteq K_n$. Enfin, par convergence simple, on a $\cap_{n\geqslant 0} K_n = \emptyset$. Si bien qu'il existe N tel que $K_N = \emptyset$. Donc pour tout $x \in [a, b]$, et $n \geqslant N$, on a $f(x) - \varepsilon < f_n(x) \leqslant f(x)$. Ce qui montre la convergence uniforme.

□

4.75 Séries de primitives

On note $f_0 : [a, b] \to \mathbf{R}$ continue et pour $n \geqslant 1,\ f_n : x \in [a, b] \mapsto \displaystyle\int_a^x f_{n-1}(t)\mathrm{d}t$.
Que dire de $S = \sum_{n\geqslant 1} f_n$? On essaiera de trouver son expression

Solution. On pose $M = \sup\limits_{[a,b]} |f|$.

L'inégalité suivante assez intuitive sera notre élément moteur. Montrons par récurrence sur n que $\forall x \in [a, b], |f_n(x)| \leqslant M\dfrac{(x-a)^n}{n!}$

Initialisation : au rang n=0

Hérédite : Soit $n \geqslant 0$, on suppose la propriété vraie au rang n.

$$\forall x \in [a, b] \quad , |f_{n+1}(x)| \leqslant \int_a^x |f_n(t)|\mathrm{d}t \qquad \underset{HR}{\leqslant} M \int_a^x \frac{(t-a)^n}{n!}\mathrm{d}t \leqslant M\frac{(x-a)^{n+1}}{(n+1)!}$$

Ce qui achève la récurrence.

Ainsi en utilisant cette inégalité, nous avons que :

$$\forall n \in \mathbf{N},\ \forall x \in [a, b], \quad |f_n(x)| \leqslant M\frac{(b-a)^n}{n!} \text{ qui est le tg d'une série convergente,dépend pas de x}$$

cela nous donne la convergence normale de $\sum f_n$ sur $[a, b]$.

Au vu de la tête de S, il serait raisonnable de la dériver. Montrons que S est C^1.

- Les f_n pour $n \geqslant 1$ sont C^1 que $[a, b]$
- S converge simplement sur $[a, b]$ car converge normalement

— $\sum_{n\geqslant 1} f_n' = \sum_{n\geqslant 1} f_{n-1} = f_0 + \sum_{n\geqslant 1} f_n$ qui converge normalement donc uniformément sur $[a,b]$

Par le théorème de dérivation terme à terme, S est C^1 sur $[a,b]$ et

$$\forall x \in [a,b], \quad S'(x) = f_0(x) + S(x) \text{et} S(a) = 0$$

□

5 Séries entières

5.76 Utilisation d'une équation différentielle pour obtenir un DSE

Soit $f(x) = \frac{\arcsin x}{\sqrt{1-x^2}}$ définie pour $x \in]-1,1[$. Déterminer si f est DSE et dans ce cas, donner son DSE.

Solution. Tout d'abord, arcsin est dérivable et $\forall x \in]-1,1[, \arcsin'(x) = \frac{1}{sqrt(1-x^2)} = (1-x^2)^{\frac{-1}{2}}$ est DSE avec un rayon égal à 1.

Donc f est DSE en tant que produit de DSE de rayon 1. Son rayon est donc $\geqslant 1$ mais la fonction n'est pas définie au-delà donc son rayon est 1.

f est dérivable sur $]-1,1[$ et

$$\begin{aligned}
\forall x \in]-1,1[, \quad f'(x) &= \frac{1}{1-x^2} + \arcsin x \times \frac{\frac{1}{2}2x}{(1-x^2)\sqrt{1-x^2}} \\
&= \frac{1}{1-x^2} + \frac{x}{1-x^2} f(x).
\end{aligned}$$

Ainsi, $(1-x^2)f'(x) = 1 + xf(x)$.

Donc en posant pour $x \in]-1,1[$, $f(x) = \sum\limits_{n\geqslant 0} a_n x^n$, cherchons grâce à cette équation différentielle la suite (a_n).

En injectant on trouve :

$$(1-x^2)\sum_{n\geqslant 0} n a_n x^n = 1 + x \sum_{n\geqslant 0} a_n x^n$$

Donc :

$$\sum_{n\geqslant 1} n a_n x^{n-1} - \sum_{n\geqslant 1} n a_n x^{n+1} = 1 + \sum_{n\geqslant 0} a_n x^{n+1}$$

On déduit par l'unicité des coefficients d'un DSE au voisinage de 0 que :

$$\begin{cases} a_1 = 1 \\ (n+2)a_{n+2} - n a_n \quad = a_n \end{cases} \iff \begin{cases} a_1 = 1 \\ a_{n+2} = \frac{n+1}{n+2} a_n \end{cases}$$

et comme $a_0 = f(0) = 0$ par itération les a_{2p} sont nuls.

et par itération et manipulation avec des factorielles.

$$a_{2p+1} = \frac{(2^p p!)^2}{(2p+1)!}$$

Par suite,

$$\frac{arcsin(x)}{\sqrt(1-x^2)} = \sum_{p\geqslant 0} \frac{2^{2p}p!^2}{(2p+1)!}x^{2p+1}$$

□

5.77 Continuité radiale d'Abel

On note $f(z) = \sum_{n\geqslant 0} a_n z^n$ avec $R = R(f) > 0$ et on suppose qu'il existe z_0 tel que $\sum_{n\geqslant 0} a_n z_0^n$ converge et $|z_0| = R$.
Montrer que $\lim_{t\to 1-} f(tz_0) = f(z_0)$

Solution. On note $R_q = \sum_{k=q+1}^{+\infty} a_k z_0^k \xrightarrow[q\to+\infty]{} 0$.

On va essayer d'évaluer la quantité : $|f(tz_0) - f(t)|$ lorsque t s'approche de 1.
Soit $\varepsilon > 0$ et $\varepsilon' > 0$

$$|f(tz_0) - f(t)| = \left| \sum_{k=0}^{n-1} a_k t^k z_0^k - \sum_{k=0}^{n-1} a_k z_0^k + \sum_{k=n}^{+\infty} a_k t^k z_0^k - \sum_{k=n}^{+\infty} a_k z_0^k \right|$$

la quantité $\sum_{k=n}^{+\infty} a_k t^k z_0^k$ est la plus compliqué à manier.
Regardons-la : Pour $m > n > 0$

$$\begin{aligned}
\sum_{k=n}^{m} a_k t^k z_0^k &= \sum_{k=n}^{+\infty} t^k (R_{k-1} - R_k) \\
&= t^n(R_{n-1} - R_n) + t^{n+1}(R_n - R_{n+1}) + \cdots + t^(R_{m-1} - R_m) \\
&= R_{n-1}t^n + R_n(t^{n+1} - t^n) + \cdots + R_{m-1}(t^m - t^{m-1}) - R_m t^m
\end{aligned}$$

Or $\exists N \in N, \forall n \geqslant N, |R_n| \leqslant \varepsilon'$, donc pour $m > n \geqslant N, t \in [0, 1[$,

$$\begin{aligned}
\left| \sum_{k=n}^{m} a_k t^k z_0^k \right| &\leqslant |R_{n-1}| + |R_n||t^n - t^{n+1}| + \cdots + |R_{m-1}||t^m - t^{m-1}| + |R_m| \\
&\geqslant 2\varepsilon' + \varepsilon'(t^n - t^{n+1} + \cdots + t^{m-1} - t^m) \\
&\geqslant 2\varepsilon' + \varepsilon'(t^n - t^m) \\
&\geqslant 3\varepsilon'
\end{aligned}$$

Donc en tendant m vers $+\infty$

$$\left| \sum_{k=n}^{+\infty} a_k t^k z_0^k \right| \geqslant 3\varepsilon'$$

Ainsi

$$\begin{aligned}|f(tz_0)-f(t)| &= \left|\sum_{k=0}^{N-1} a_k t^k z_0^k - \sum_{k=0}^{N-1} a_k z_0^k + \sum_{k=N}^{+\infty} a_k t^k z_0^k - \sum_{k=N}^{+\infty} a_k z_0^k\right| \\ &\geqslant \underbrace{\left|\sum_{k=0}^{N-1} a_k t^k z_0^k - \sum_{k=0}^{N-1} a_k z_0^k\right|}_{\xrightarrow[t\to 1^-]{}0} + 3\varepsilon' + \varepsilon'\end{aligned}$$

Ainsi $\exists \delta > 0, \forall t \in [1-\delta, 1[$,

$$|f(tz_0)-f(t)| \geqslant 5\varepsilon' \geqslant \varepsilon$$

D'où le résultat en prenant $\varepsilon' = \varepsilon/5$

□

Remarque

Si la série $\sum a_n z_0^n$ est ACV alors il n'y a pas besoin de ce raisonnement car on a la convergence normale sur $D_f(0,R)$

5.78 Quelques formules utiles

Soit $f(t) = \sum_{n\geqslant 0} a_n t^n$ de rayon $R \geqslant 1$

1. Montrer que pour $|t|<1$, $\dfrac{f(t)}{1-t} = \sum_{n\geqslant 0} S_n t^n$ avec $S_n = \sum_{n\geqslant 0} a_k$
2. Si $f(1)$ converge alors $\dfrac{f(t)-f(1)}{t-1} = \sum_{n\geqslant 0} R_n t^n$ avec $R_n = \sum_{k\geqslant n+1} a_k$

Solution. 1. Pour $|t|<1$,

$$\begin{aligned}\frac{f(t)}{1-t} &= \left(\sum_{k\geqslant 0} a_k t^k\right)\left(\sum_{l\geqslant 0} t^l\right) \\ &\underbrace{=}_{Cauchy} \sum_{n\geqslant 0}\Big(\sum_{k+l=n} a_k \times 1\Big)t^n \\ &= \sum_{n\geqslant 0} S_n t^n\end{aligned}$$

2. On suppose que $f(1)$ converge c'est à dire que $\sum_{k=0}^{+\infty} a_k$ converge.

Calculons

$$\begin{aligned}(t-1)\sum_{n\geqslant 0} R_n t^n &= \sum_{n\geqslant 0} R_n t^{n+1} - \sum_{n\geqslant 0} R_n t^n \\ &= -R_0 + \sum_{n\geqslant 0} \underbrace{(R_n - R_{n+1})}_{a_{n+1}} t^{n+1} \\ &= -R_0 + f(t) - a_0\end{aligned}$$

Or $R_0 = \sum_{k=1}^{+\infty} a_k = f(1) - a_0$

Donc $-R_0 + f(t) - a_0 = f(t) - f(1)$ ce qui permet de conclure

□

5.79 Inverse d'une fonction développable en série entière

Soit $\sum a_n z^n$ une série entière de rayon de convergence $R > 0$ et S sa somme (définie sur $D(0,R)$).

1. Montrer qu'il existe $p > 0$ tel que : $\forall n \in \mathbf{N}^*,\ |a_n| \leqslant p^n$
2. Montrez que si $S(0) \neq 0$, alors $\frac{1}{S}$ est développable en série entière au voisinage de zéro.

Démonstration.

1. Soit $r \in]0,R[$. Nous savons d'après le lemme d'Abel que $|a_n| r^n \to 0$. Il existe donc $n_0 \in \mathbf{N}^*$ tel que $\forall n \geqslant n_0,\ |a_n| r^n \leqslant 1$. Ainsi $p = \max\left(|a_1|, \ldots, |a_{n_0-1}|, \frac{1}{r}\right)$ convient.
2. *Analyse :* Supposons qu'il existe : $(b_n)_{n\in\mathbf{N}} \in \mathbf{C}^{\mathbf{N}}$ et $R' > 0$ tels que

$$\forall z \in D(0,R'),\ \frac{1}{S(z)} = \sum_{n=0}^{+\infty} b_n z^n$$

Nous avons alors :

$$\forall z \in D(0,\min(R,R')),\ S(z)\frac{1}{S(z)} = \sum_{n=0}^{+\infty}\left(\sum_{k=0}^{n} a_{n-k} b_k\right) z^n = 1$$

Ce qui nous donne :

$$b_0 = \frac{1}{a_0} \quad \text{et} \quad \forall n \in \mathbf{N}^*,\ b_n = -\frac{1}{a_0}\sum_{k=0}^{n-1} a_{n-k} b_k$$

Synthèse : Vu que $a_0 \neq 0$, on peut poser

$$b_0 = \frac{1}{a_0} \quad \text{et} \quad \forall n \in \mathbf{N}^*,\ b_n = -\frac{1}{a_0}\sum_{k=0}^{n-1} a_{n-k} b_k$$

L'analyse nous donne directement que $(a*b)_0 = 1$ et $\forall n \in \mathbf{N}^*,\ (a*b)_n = 0$ (avec $*$ le produit de Cauchy).

Il nous suffit donc de montrer que $\sum b_n z^n$ a un rayon de convergence strictement positif pour conclure. Soit $p > 0$ tel que $\forall n \in \mathbf{N}^*,\ |a_n| \leqslant p^n$. Définissons $(c_n)_{n\in\mathbf{N}} \in \mathbf{C}^{\mathbf{N}}$:

$$c_0 = 1 \text{ et } \quad \forall n \in \mathbf{N}^*,\ c_n = \sum_{k=0}^{n-1} p^{n-k} c_k$$

On a par récurrence immédiate que $\forall n \in \mathbf{N}, |b_n| \leqslant \frac{c_n}{|a_0|}$ Montrons par récurrence forte pour $n \in \mathbf{N}^*$ que $c_n = 2^{n-1}p^n$.

— $c_1 = p = 2^0 p$

— Supposons la propriété vraie pour $k \in [\![1, n]\!]$, montrons la au rang $n+1$.

$$\begin{aligned} c_{n+1} &= \sum_{k=0}^{n} p^{n+1-k} c_k \\ &= p^{n+1}\left(1 + \sum_{k=1}^{n} 2^{k-1}\right) \\ &= p^{n+1}\left(1 + \sum_{k=0}^{n-1} 2^{k}\right) \\ &= p^{n+1}\left(1 + \frac{2^n - 1}{2-1}\right) \\ &= 2^n p^{n+1} \end{aligned}$$

$\sum c_n z^n$ a un rayon de convergence égal à $\frac{1}{2p}$ ce qui conclut la preuve.

□

5.80 Analycité dans le disque ouvert de convergence

Soit $f(z) = \sum_{n\geqslant 0} a_n z^n$ une série entière de rayon $R > 0$, alors si $|z_0| < R$, f est DSE en z_0 de rayon au moins $R - |z_0| > 0$.

Démonstration. Soit $z_0 \in D(0, R)$, $R' = R - |z_0| > 0$, et $h \in D(0, R')$.
On remarque que $|z_0 + h| < |z_0| + R - |z_0| = R$ donc on peut écrire :

$$f(z_0 + h) = \sum_{n\geqslant 0} a_n (z_0 + h)^n$$

$$= \sum_{n\geqslant 0} \sum_{k=0}^{n} \binom{n}{k} a_n h^k z_0^{n-k}$$

On veut intervertir les deux sommes. Pour cela, on pose $(b_{n,k})_{0\leqslant k\leqslant n} = \left(\binom{n}{k} a_n h^k z_0^{n-k}\right)$. On remarque que :

$$\sum_{n\geqslant 0} \sum_{k=0}^{n} |b_{n,k}| = \sum_{n\geqslant 0} |a_n|(|z_0| + |h|)^n.$$

On utilise ensuite le fait que $\sum a_n z^n$ et $\sum |a_n| z^n$ ont même rayon de convergence, et le fait que $|z_0| + |h| < R$ pour obtenir la sommabilité de $(b_{n,k})$. Ainsi, le théorème de sommation par paquets permet d'écrire :

$$f(z_0+h) = \sum_{k\geqslant 0} h^k \left(\sum_{n\geqslant k} a_n \binom{n}{k} z_0^{n-k} \right) = \sum_{n\geqslant 0} h^k c_k$$

Comme c_k ne dépend pas de h, et que cette expression est valable pour $h \in D(0,R')$, on a le résultat attendu ! □

5.81 Principe des zéros isolés pour une série entière

Soit $f(z) = \sum_{n\geqslant 0} a_n z^n$ une série entière de rayon $R > 0$ non nulle, alors les zéros de f sur $D(0,R)$ sont isolés.

Démonstration. Pour le montrer, considérons Z l'ensemble des zéros non isolés de f dans $D(0,R)$. Montrons que Z est à la fois ouvert et fermé dans $D(0,R)$.
Z est ouvert : Soit $z \in Z$, alors comme $|z| < R$, f est DSE en z, et si $|h|$ assez petit, on peut écrire :

$$f(z+h) = \sum_{n\geqslant 0} b_n h^n$$

On prend alors $(h_n)_{n\geqslant 0}$ une suite injective qui tend vers 0 telle que pour tout n, $f(z+h_n) = 0$ (existe car z zéro non isolé).
Supposons par l'absurde qu'il existe n_0 tel que $b_{n_0} \neq 0$, et prenons n_0 minimal. Alors on montre sans peine que :

$$f(z+h_n) \sim b_{n_0} h^{n_0}$$

Et donc $f(z+h_n)$ non nul pour n assez grand : contradiction.
Ainsi, tous les coefficients sont nuls. Donc f est identiquement nulle au voisinage de z, d'où Z ouvert.

Z est fermé : On remarque que si on prend une suite (z_n) de zéros qui converge vers $z \in D(0,R)$, alors en utilisant la même technique que ci-dessus, on montre que f identiquement nulle au voisinage de z et donc $z \in Z$.

Ainsi, Z est ouvert/fermé dans $D(0,R)$ qui est connexe. Donc $Z = \emptyset$ ou $Z = D(0,R)$. f étant non nulle, on a $Z = \emptyset$. □

5.82 Principe du maximum pour une série entière

Soit f une série entière de rayon $R > 0$, et $r < R$, alors $\sup_{|z|\leqslant r} |f(z)| = \sup_{|z|=r} |f(z)|$.

Démonstration. Si f est constante, alors c'est trivial. On supposera donc f non constante. Soit $r < R$, comme $\overline{D(0,r)}$ est compact, et f continue, le sup est bien défini et même atteint. On va montrer qu'il n'est pas atteint en un point intérieur (ce qui est légèrement plus fort).
Soit $z_0 \in D(0,r)$, si $f(z_0) = 0$ il n'y a rien à faire (f non nulle). Sinon développe $f - f(z_0)$ en série entière au voisinage de z_0. Prenons $0 < \delta < R - r$ On dispose d'une suite $(a_n)n \geqslant 1$ telle que si $|h| < r - |z_0| + \delta$,

$$f(z_0+h) = f(z_0) + \sum_{n\geqslant 0} a_n z^n$$

Comme f non nulle, les zéros de f sont isolés, donc il existe n tel que $a_n \neq 0$. Prenons n_0 minimal. Alors si $|h| \leqslant r - |z_0|$ on a :

$$f(z_0+h) = a_{n_0}h^{n_0} + h^{n_0+1}\sum_{n\geqslant 0} a_{n+n_0+1}h^n$$

Notons que $\sum_{n\geqslant 0} a_{n+n_0+1}h^n$ est de rayon au moins $r-|z_0|+\delta$. Donc est bornée sur $\overline{D(r-|z_0|)}$ (compact du disque ouvert de convergence). Ainsi :

$$f(z_0+h) = f(z_0) + a_{n_0}h^{n_0} + O(h^{n_0+1}).$$

On écrit à présent $f(z_0) = re^{i\theta}$ avec $r>0$. On a alors :

$$\left|\frac{f(z_0+h)}{f(z_0)}\right| = \left|1 + a_{n_0}h^{n_0}e^{-i\theta}/r + O(h^{n_0+1})\right|$$

Pour conclure, on prend $h = te^{i\theta/n_0}/a_{n_0}^{1/n_0}$ (on prend une racine n_0-eme quelconque) et on obtient pour $t>0$ au voisinage de 0 :

$$\left|\frac{f(z_0+h)}{f(z_0)}\right|^2 = \left|1 + t^{n_0}/r + O(t^{n_0+1})\right| = 1 + t^{n_0}/r + O(t^{n_0+1})$$

Et cette quantité est strictement plus grande pour t assez petit. Donc f n'admet pas de maximum local sur $D(0,r)$. $\square$

5.83 Formule de Cauchy

Soit $\sum_n a_n z^n$ une série entière de rayon de convergence $R>0$ et f la somme de cette série entière sur son rayon de convergence.

1. Montrer que pour tout $r\in]0,R[$ et $n\in\mathbf{N}$, $2\pi r^n a_n = \int_0^{2\pi} f(re^{i\theta})e^{-in\theta}$.
2. Montrer que pour tout $r\in]0,R[$, la série $\sum |a_n|^2 r^{2n}$ converge et on a $\sum_{n\geqslant 0}|a_n|^2 r^2 n = \frac{1}{2\pi}\int_0^{2\pi}|f(re^{i\theta})|^2 \mathrm{d}\theta$.

Solution. C'est essentiellement de l'interversion série-intégrale :

1. Soit $r\in]0,R[$ et $n\in\mathbf{N}$, on a :

$$\int_0^{2\pi} f(re^{i\theta})e^{-in\theta}\mathrm{d}\theta = \int_0^{2\pi}\sum_{k\geqslant 0} a_n r^n e^{i(k-n)\theta}\mathrm{d}\theta$$

Toutes les fonctions sont continues et intégrables sur $[0,2\pi]$, et on a :

$$\sum_{m\geqslant 0}\int_0^{2\pi}\left|a_m r^m e^{i(m-n)\theta}\right| = \sum_{m\geqslant 0} 2\pi r^m |a_m| < \infty$$

En effet, $\sum |a_n| z^n$ a même rayon que $\sum a_n z^n$ donc la série converge.
Ainsi, le théorème d'interversion séries-intégrales s'applique et on a :

$$\int_0^{2\pi} f(re^{i\theta})e^{-in\theta}\mathrm{d}\theta = \sum_{m\geqslant 0}\int_0^{2\pi} a_m r^m e^{i(m-n)\theta}\mathrm{d}\theta$$

Or, $\displaystyle\int_0^{2\pi} e^{i(m-n)\theta}\mathrm{d}\theta = 2\pi\delta_{n,m}$ donc :

$$\int_0^{2\pi} f(re^{i\theta})e^{-in\theta}\mathrm{d}\theta = 2\pi r^n a_n$$

2. C'est plus ou moins la même chose, en écrivant :

$$\frac{1}{2\pi}\int_0^{2\pi}|f(re^{i\theta})|^2\mathrm{d}\theta = \frac{1}{2\pi}\int_0^{2\pi} f(re^{i\theta})\overline{f(re^{i\theta})}\mathrm{d}\theta$$

On utilise ensuite la continuité de la conjugaison :

$$= \frac{1}{2\pi}\int_0^{2\pi}\sum_{n\geqslant 0} f(re^{i\theta})\overline{a_n}r^n e^{-in\theta}\mathrm{d}\theta$$

L'interversion se justifie de la même facon qu'en 1, car f est borné sur $S(0,r)$ (continue sur compact) :

$$= \frac{1}{2\pi}\sum_{n\geqslant 0}\overline{a_n}r^n\int_0^{2\pi} f(re^{i\theta})e^{-in\theta}\mathrm{d}\theta$$

Il reste plus qu'à utiliser la formule de Cauchy

$$= \sum_{n\geqslant 0}|a_n|^2 r^{2n}$$

□

5.84 Théorème de Liouville

On suppose f DSE de rayon $R = +\infty$ et f bornée. Montrer que f est constante.

Solution. On utilise la formule de Cauchy.

$$\forall n\in\mathbf{N}, \forall r>0 \quad , \frac{1}{2\pi r^n}\int_0^{2\pi} f(re^{it})e^{-int}\mathrm{d}t$$

Donc,

$$\begin{aligned}\forall n\geqslant 1, \quad |a_n| &\leqslant \frac{1}{2\pi r^n}\int_0^{2\pi}|f(re^{it}e^{-int}|\mathrm{d}t\\ &\leqslant \frac{sup|f|}{r^n}\xrightarrow[r\to+\infty]{} 0\end{aligned}$$

Donc $a_n = 0$ et f constante □

5.85 O

n note $f(z) = \sum a_n z^n$ de rayon $R = +\infty$ tel qu'il existe $a, b > 0, \forall z\in\mathbf{C}, |f(z)| \leqslant a|z|^N + b$. Montrer que f est polynomiale.

Solution. Pour $n \geqslant N+1$ et $r > 0$,

$$a_n = \frac{1}{2\pi r^n}\int_0^{2\pi} f(re^{it})e^{-int}\mathrm{d}t$$

$$\begin{aligned}\implies |a_n| &\leqslant \frac{1}{2\pi r^n}\int_0^{2\pi} \underbrace{|f(re^{it}|}_{\leqslant a|r|^N+b} \\ &\leqslant \frac{a|r|^N+b}{r^n} \xrightarrow[r\to+\infty]{} 0\end{aligned}$$

Donc $a_n = 0$ et f est polynomiale de degré $\leqslant N$ □

5.86 Théorème de Bernstein

Soient $a > 0$ et $f :]-a, a[\to \mathbf{R}$ une fonction de classe $\mathcal{C}^\infty$.
On suppose que

$$\forall k \in \mathbf{N}, \forall x \in]-a, a[,\ f^{(2k)}(x) \geqslant 0$$

Alors f est développable en série entière sur $]-a, a[$.

Démonstration. Lemme : $F : x \mapsto f(x) + f(-x)$ développable en série entière sur $]-a, a[$. Preuve : On va montrer que F est développable en série entière en 0 de rayon $\geqslant a$.
Pour cela, soit $0 < b < a$ fixé, et $0 < x \leqslant b$.
Contrôlons le reste de Taylor, en remarquant que les dérivées impaires de F en 0 sont toutes nulles.
Si $n \geqslant 0$ on a :

$$R_n(x) = F(x) - \sum_{k=0}^{n} \frac{x^{2k}}{(2k)!}F^{(2k)}(0) = \int_0^x \frac{(x-t)^{2n+1}}{(2n+1)!}F^{(2n+2)}(t)\mathrm{d}t$$

On va exprimer $R_n(x)$ en fonction de $R_n(b)$. Pour cela, il faut changer les bornes par un changement de variable : $u = \frac{b}{x}t$. Ce qui donne :

$$\begin{aligned}R_n(x) &= \int_0^b \frac{(x - xu/b)^{2n+1}}{(2n+1)!}F^{(2n+2)}(\frac{xu}{b})\frac{x}{b}\mathrm{d}u \\ &= \left(\frac{x}{b}\right)^{2n+2}\int_0^b \frac{(b-u)^{2n+1}}{(2n+1)!}F^{(2n+2)}(\frac{xu}{b})\mathrm{d}u\end{aligned}$$

Ainsi, comme $F^{(2n+2)}$ est positive par hypothèse, on a montré :

$$0 \leqslant R_n(x) \leqslant \left(\frac{x}{b}\right)^{2n+2} R_n(b)$$

Mais d'après la formule de $R_n(b)$, on a $R_n(b) \leqslant F(b)$ donc on a $R_n(x) \to 0$. Ce qui veut dire :

$$\forall x \in]0, a[, F(x) = \sum_{n\geqslant 0} \frac{x^{2n}}{(2n)!}F^{(2n)}(0)$$

Par parité de F, on a le résultat sur $]-a, a[$ ce qui achève la preuve du lemme.

Pour conclure, on remarque que $f^{(2n)}(x) = \frac{1}{2}F^{(2n)}(x)$. Ainsi, on peut dominer les restes d'ordres pairs de f par ceux de F, et donc montrer que :

$$\forall x \in]-a, a[, f(x) = \lim_{n \to +\infty} \sum_{k=0}^{2n+1} \frac{x^k}{k!} f^{(k)}(0)$$

On obtient le résultat final en remarquant que si $x \in]-a, a[$, alors :

$$\left| \frac{x^{2n}}{(2n)!} f^{(2n)}(0) \right| = \left| \frac{x^{2n}}{(2n)!} \frac{1}{2} F^{(2n)}(0) \right| \to 0$$

Donc f est développable en série entière sur $]-a, a[$! □

6 Analyse réelle

6.87 Résultats sur les points fixes

1. On note $f : [a, b] \to \mathbf{R}$ continue. Montrer que si $f([a, b]) \subset [a, b]$ ou si $[a, b] \subset f([a, b])$ alors f possède un point fixe
2. On note $f : [0, 1] \to \mathbf{R}$ continue tel que $f(0) = f(1)$. Montrer que si $n \geqslant 2, \exists \alpha \in [0, 1 - \frac{1}{n}], f(\alpha + \frac{1}{n}) = f(\alpha)$

Solution. 1. Si $f([a, b]) \subset [a, b]$ alors la fonction $g : t \mapsto f(t) - t$ vérifie $g(a) \geqslant 0$ et $g(b) \leqslant 0$ et comme g est continue, le théorème des valeurs intermédiaires nous donne l'existence de $\alpha \in [a, b]$ tel que $g(\alpha) = 0$ ie $f(\alpha) = \alpha$.
Si $[a, b] \subset f([a, b])$ alors il existe $u, v \in [a, b], a = f(u), b = f(v)$ et $g(u) = f(u) - u = a - u \leqslant 0$ et $g(v) = f(v) - v = b - v \geqslant 0$.
Donc il existe $\alpha \in [u, v]$ ou $[v, u]$ tel que $g(\alpha) = 0$ ie $f(\alpha) = \alpha$

2. Cette fois-ci, on note $g : x \in [0, 1 - \frac{1}{n}] \mapsto f(x + \frac{1}{n}) - f(x)$
L'astuce est de voir que :

$$g(0) + g(\frac{1}{n}) + \cdots + g(1 - \frac{1}{n}) = f(1) - f(0) = 0$$

Ainsi les $g(\frac{k}{n})$ ne sont pas tous > 0 ni tous < 0 donc il existe 2 indices k, l tel que $g(\frac{k}{n}) \leqslant 0$ et $g(\frac{l}{n}) \geqslant 0$. Ainsi il existe α tel que $g(\alpha) = 0$ et α convient .

□

6.88 Théorème de Rolle généralisé

On suppose que $f :]a, b[\to \mathbf{R}$ dérivable ($a, b \in \overline{\mathbf{R}}$) et $\lim_{x \to a} f = \lim_{x \to b} f \in \overline{\mathbf{R}}$. Montrer qu'il existe $\alpha \in]a, b[$ tel que $f'(\alpha) = 0$

Solution. On suppose que f' ne s'annule pas sur $]a, b[$.

On a tout d'abord l'injectivité de f car si il existe $x, y \in]a, b[, f(x) = f(y)$ on pourrait conclure avec le théorème Rolle simple. Or f est continue donc vu qu'elle est injective, f est strictement monotone ce qui contredit $\lim_{x \to a} f = \lim_{x \to b} f$. Absurde □

6.89 L'opérateur Δ

On note pour f la fonction numérique : $\Delta_h(f)(x) = f(x+h) - f(x)$ lorsque cela a un sens (selon le domaine de définition de f)

1. Soit $f \in \mathcal{C}^n([[x_0, x_0+nh], \mathbf{R})$. Montrer qu'il existe $\theta \in]0,1[$ tq $\Delta_h(f)(x_0) = h^n f^{(n)}(x_0+n\theta h)$.
2. Montrer que si $f \in \mathcal{C}^2([0,1], \mathbf{R})$ et si $|f"| \leqslant 1$ alors $|f(1) - 2f(\frac{1}{2}) + f(0)| \leqslant \frac{1}{4}$

Solution. 1. On le fait par récurrence sur $n \in \mathbf{N}^*$:
Initialisation : pour n=1, soit $f \in \mathcal{C}^1([[x_0, x_0+h], \mathbf{R})$..
Par application du théorème des accroissements finis,

$$\exists c \in]x_0, x_0+h[, f(x_0+h) - f(x_0) = hf'(c)$$

et c s'écrit $x_0 + \theta h$ avec $\theta \in]0,1[$
Hérédite : Supposons la propriété vraie au rang n. Soit $f \in \mathcal{C}^{n+1}([[x_0, x_0+(n+1)h], \mathbf{R})$..
Nous avons $\Delta_h(f)^{n+1}(x_0) = \Delta_h(f)^n \circ \Delta_h(f)(x_0)$.
On va appliquer l'hypothèse de récurrence à $\Delta_h(f)$ et non à f.
En effet, $\Delta_h(f)$ est $\mathcal{C}^n$ sur $[x_0, x_0+nh]$ donc par hypothèse de récurrence donc il existe $\theta \in]0,1[$ tel que

$$\Delta_h(f)^n \circ \Delta_h(f)(x_0) = h^n \Delta_h(f)^{(n)}(x_0+n\theta h) = h^n \Delta_h(f^{(n)})(x_0+n\theta h)$$

On réapplique le Théorème des accroissement finis, cette fois-ci à f^n ce qui nous donne l'existence de $\theta' \in]0,1[$ tel que $\Delta_h(f)^{n+1}(x_0) = h^{n+1}f^{(n+1)}(x_0+n\theta h+\theta' h)$
et $n\theta + \theta' \in]0, n+1[$ donc on peut poser $\theta_1 = \frac{n\theta+\theta'}{n+1}$ pour avoir le résultat.

2. Il s'agit d'une application simple de ce qu'on a fait précédemment. En effet,

$$f(1) - 2f(\frac{1}{2}) + f(0) = \Delta_{\frac{1}{2}}(f)(0)$$

donc $\exists \theta \in]0,1[, \Delta_{\frac{1}{2}}(f)(0) = \frac{1}{4}f"(\theta) \leqslant \frac{1}{4}$ d'où la conclusion.

□

6.90 Inégalités (Young et Hölder)

On considère p, q des réels strictement positifs tels que $\frac{1}{p} + \frac{1}{q} = 1$. Alors,

$$\forall a, b \geqslant 0, \quad ab \leqslant \frac{a^p}{p} + \frac{b^q}{q} \qquad \text{(Young)}$$

et

$$\forall x, y \in \mathbb{R}^n, \quad \sum_{i=1}^n |x_i y_i| \leqslant \|x\|_p \|y\|_q \qquad \text{(Hölder)}$$

où $\|\cdot\|_p$ correspond à

$$\|x\|_p = \sum_{i=1}^n |x_i|^p.$$

Remarque

Avec $p = q = 2$, on retrouve respectivement les inégalités arithmético-géométriques et de Cauchy-Schwarz.

Démonstration. La fonction $-\ln$ est convexe donc pour $a, b > 0$

$$-\ln\left(\frac{a^p}{p} + \frac{b^q}{q}\right) \leqslant -\frac{1}{p}\ln(a^p) - \frac{1}{q}\ln(b^q) = -\ln(ab)$$

d'où l'inégalité de Young, qui est toujours vraie si a ou b est nul.
On note $a, b \in \left(\mathbf{R}^+\right)^n$, et on applique l'inégalité de Young :

$$\sum_{i=1}^n a_i b_i \leqslant \frac{1}{p}\sum_{i=1}^n a_i^p + \frac{1}{q}\sum_{i=1}^n b_i^q.$$

On change a en λa et on obtient :

$$\sum_{i=1}^n a_i b_i \leqslant \frac{\lambda^{p-1}}{p}\sum_{i=1}^n a_i^p + \frac{1}{\lambda q}\sum_{i=1}^n b_i^q$$

et en prenant

$$\lambda = \frac{\left(\sum_{i=1}^n b_i^q\right)^{\frac{1}{p}}}{\left(\sum_{i=1}^n a_i^p\right)^{\frac{1}{p}}}$$

on obtient

$$\sum_{i=1}^n a_i b_i \leqslant \left(\sum_{i=1}^n a_i^p\right)^{\frac{1}{p}} \left(\sum_{i=1}^n b_i^q\right)^{\frac{1}{q}}.$$

Dans le cas général, on a

$$\left|\sum_{i=1}^n x_i y_i\right| \leqslant \sum_{i=1}^n |x_i y_i| \leqslant \|x\|_p \|y\|_q.$$

□

6.91 Une preuve d'irrationalité grâce aux formule de Taylor

Montrer que $\cos(1)$ est irrationnel.

Démonstration. Supposons que $cos(1) = \frac{p}{q} \in \mathbf{Q}$, on a donc par la formule de Taylor-Lagrange :

$$cos(1) = \sum_{k=0}^q \frac{\cos^{(k)}(0)}{k!} + \int_0^1 \frac{(1-t)^q}{q!}\cos^{(q+1)}(t)\mathrm{d}t$$

$$q!\left|\cos(1) - \sum_{k=0}^q \frac{\cos^{(k)}(0)}{k!}\right| \leqslant \int_0^1 (1-t)^q \mathrm{d}t = \frac{1}{q+1} < 1$$

Or la quantité de gauche est entière donc on en déduit que $\cos(1) = \sum_{k=0}^{q} \frac{\cos^{(k)}(0)}{k!}$ donc

$$\int_0^1 \underbrace{\frac{(1-t)^q}{q!}\cos^{(q+1)}(t)}_{\text{continue et de signe constante}} \, dt = 0$$

$$\implies \forall t \in [0,1], (1-t)^q \underbrace{\cos^{(q+1)}(t)}_{\pm\cos(t) \text{ ou } \sin(t)} = 0 \text{ ce qui est absurde.}$$ □

7 Dénombrabilité

7.92 Dénombrabilité de l'ensemble des nombres algébriques

$a \in \mathbf{C}$ est algébrique si a est racine d'un polynôme non constant de $\mathbf{Z}[X]$. Montrer que l'ensemble $\mathcal{A}$ des nombres algébriques est dénombrable.

Démonstration. Pour $n \in \mathbf{N}^*$, on pose P_n les polynômes de $\mathbf{Z}[X]$ de degré n.

Pour $P \in \mathbf{Z}[X]$, On note $\mathbf{Z}_{\mathbf{C}}(P)$ les racines complexes de P.

De plus :

$$f \quad : \quad \begin{array}{ccc} \mathbf{Z}^n \times \mathbf{Z}^n & \to & P_n \\ (a_0, \dots, a_n) & \mapsto & a_0 + a_1 X + \cdots + a_n X^n \end{array}$$

est bijective donc surjective, $\mathbf{Z}^n \times \mathbf{Z}^n$ est dénombrable donc P_n dénombrable.

L'ensemble $\mathcal{A}$ des nombres algébriques est $\mathcal{A} = \bigcup_{n \in \mathbf{N}^*} \bigcup_{P \in P_n} \mathbf{Z}_{\mathbf{C}}(P)$ ce qui implique que $\mathcal{A}$ est dénombrable.

□

7.93 Cercles et points à coordonnées rationnelles

Montrer que pour tout $a \in \mathbf{R}^2$, il existe des cercles centrés en a qui n'ont aucun point à coordonnées rationnelles.

Démonstration. $\mathbf{R}$ est indénombrable donc l'ensemble de ces cercles est indénombrable (surjection entre l'ensemble des cercles et leur rayon), or $\mathbf{Q}^2$ est dénombrable et les cercles sont distincts, si ils rencontraient tous $\mathbf{Q}^2$ alors on aurait une bijection entre les 2 et $\mathbf{R}$ serait dénombrable d'où l'existence. □

Exemple

Le cercle de rayon $\sqrt{3}$ et de centre 0 en est un. On peut démontrer ceci par l'absurde et le principe de la descente infinie.

Remarque

On peut montrer qu'un cercle a 0 ou une infinité de points rationnels.

7.94 Théorème de Cantor

Soit E un ensemble, il n'existe pas de surjection de E vers $\mathcal{P}(E)$

Démonstration. Supposons par l'absurde l'existence d'une telle surjection $f : E \to \mathcal{P}(E)$. On pose alors $A = \{x \in E, x \notin f(x)\}$. Par hypothèse, A admet un antécédent x par f. On arrive alors à une contradiction.
En effet, ou bien $x \in A$, et donc $x \notin f(x) = A$: absurde. Ou bien $x \notin A = f(x)$ et donc $x \in A$: absurde aussi.

□

Remarque

On utilise ici un procédé diagonal, technique assez courante quand on veut montrer qu'un ensemble B est plus gros qu'un autre ensemble A : On prend une surjection de A vers B, et on construit un élément de B en faisant en sorte qu'il soit différent de toutes les images, en modifiant un peu toutes les images.

7.95 Théorème de Cantor-Bernstein

Soit E, F deux ensembles, si on dispose d'une injection de E vers F et d'une injection de F vers E, alors on dispose d'une bijection de E vers F

Démonstration. On a besoin d'un lemme pour cet exercice, dont la preuve est malheureusement assez astucieuse :
Lemme : Si E ensemble, et $f : \mathcal{P}(E) \to \mathcal{P}(E)$ croissante pour l'inclusion, alors f admet un point fixe.
Preuve : Soit $C = \{A \subseteq E \mid A \subseteq f(A)\}$, et $H = \cup_{A \in C} A$, on va montrer que H convient par double inclusion :
si $A \in C$, alors $A \subseteq H$ donc $f(A) \subseteq f(H)$ (croissance de f), d'où $A \subseteq f(H)$ par hypothèse. En prenant l'union sur $A \in C$, on obtient $H \subseteq f(H)$. En utilisant encore la croissance de f, on a $f(H) \subseteq f(f(H))$ donc $f(H) \in C$, par définition de H, ceci implique $f(H) \subseteq H$. D'où $H = f(H)$.

Revenons à l'exercice initial. Par hypothèse, on dispose de $f : E \to F$ injective, et $g : E \to F$ injective.
Si $H \subseteq E$, f fournit une bijection de $H \to f(H)$, donc on aimerait utiliser g pour obtenir une bijection de $E \setminus H \to F \setminus f(H)$.
mais H ne convient pas toujours, par exemple si on prend naivement $H = E$, $E \setminus H = \emptyset$ tandis que $F \setminus f(H)$ n'est pas vide.
Pour que H convienne, il faudrait pouvoir poser $\varphi(x) = g^{-1}(x)$ si $x \in E \setminus H$. Et donc avoir :

$$E \setminus H = g(F \setminus f(H))$$

En passant au complémentaire, ceci s'écrit :

$$H = E \setminus g(F \setminus f(H))$$

On remarque alors que H doit être point fixe de l'application $A \mapsto E \setminus g(F \setminus f(A))$, qui a le bon goût d'être croissante pour l'inclusion (composée d'applications croissantes (les images directes) et

d'un nombre pair d'applications décroissantes (les complémentaires). Si bien qu'on peut appliquer le lemme pour obtenir H vérifiant l'égalité.
On définit enfin :

$$\varphi : x \in E \mapsto \begin{cases} f(x) & x \in H \\ g^{-1}(x) & x \in E \setminus H \end{cases}$$

φ est bien définie car si $x \in E \setminus H$, alors $x \in g(F)$, elle est injective car ses restrictions à H, et $E \setminus H$ sont injectives, et les images de ces deux restrictions sont disjointes. Enfin, elle est surjective car $\varphi(E \setminus H) = g^{-1}(E \setminus H) = F \setminus \varphi(E)$. □

7.96 Cardinal des fonctions continues

$C^0(\mathbf{R}, \mathbf{R})$ est équipotent à $\mathbf{R}$

Démonstration. La clé est de remarquer qu'une fonction f continue est uniquement déterminée par sa restriction à $\mathbf{Q}$ par densité de $\mathbf{Q}$ et continuité de f. Ainsi, on peut injecter $C^0(\mathbf{R}, \mathbf{R})$ dans $\mathbf{R}^{\mathbf{Q}}$ qui est équipotent à $\mathbf{R}^{\mathbf{N}} \sim (2^{\mathbf{N}})^{\mathbf{N}} \sim 2^{\mathbf{N} \times \mathbf{N}} \sim 2^{\mathbf{N}} \sim \mathbf{R}$.
Ainsi, on peut injecter $C^0(\mathbf{R}, \mathbf{R})$ dans $\mathbf{R}$. Et on a une injection dans l'autre sens en associant à tout réel c la fonction constante égale à c. Cantor-Bernstein permet alors de conclure. □

Troisième partie
Topologie

1 Compacité

1.97 suite décroissante de fermés dans un compact

Soit A une partie compacte de E et $(F_n)_n$ une suite décroissante de fermés non vide et inclus dans A. Montrer que $\bigcap\limits_{n\in\mathbf{N}} F_n \neq \emptyset$

Solution.

$$\forall n \in \mathbf{N}, \exists x_n \in F_n$$

On forme ainsi une suite $(x_n)_n \in A^{\mathbf{N}}$ donc $\exists\phi$ extractrice, $a \in A, x_{\phi(n)} \xrightarrow[n\to+\infty]{} a$.

$\forall i \in \mathbf{N}$, on a, à partir d'un certain rang n, $x_{\phi(n)} \in F_i$ donc comme F_i est fermé, $a \in \bigcap_{n\in\mathbf{N}} F_n$ d'où la conclusion

□

1.98 La propriété de Borel-Lebesgue

Soit $(E, \|.\|)$ un espace vectoriel normé. $K \subset E$ vérifie la propriété de Borel-Lebesgue si de tout recouvrement de K par des ouverts on peut en extraire un recouvrement fini, soit si :

$$K \subset \bigcup_{i\in I} O_i$$

avec les O_i des ouverts, alors il existe $J \subset I$ fini tel que

$$K \subset \bigcup_{i\in J} O_i$$

Le but est de montrer qu'un espace vérifie la propriété de Borel-Lebesgue si et seulement si il est compact.

— *Sens direct :*
  1. Montrez que pour toute suite décroissante de fermés (F_n) telle que $\forall n \in \mathbf{N}, F_n \cap K \neq \varnothing$,
  $$\bigcap_{n\in\mathbf{N}} F_n \neq \varnothing$$
  2. Montrez que de toute suite $(x_n)_{n\in\mathbf{N}}$ de K on peut en extraire une sous-suite convergente.
  On pourra s'intéresser aux ensembles $A_k = \{x_n,\ n \geqslant k\}$

— *Sens réciproque :*
  3. **Lemme de précompacité** :
  K est dit précompact si pour tout $\varepsilon > 0$, il existe un recouvrement fini de K par des boules ouvertes de rayon ε
  Montrez qu'un compact K est précompact.

4. Un autre lemme :
   Soit K un compact et $(O_i)_{i\in I}$ un recouvrement de K par des ouverts. Montrez alors que :
   $$\exists\alpha > 0,\ \forall x \in K,\ \exists i \in I,\ B(x,\alpha) \subset O_i$$
5. Conclure.

Solution. 1. Supposons par l'absurde que
$$\bigcap_{n\in\mathbf{N}} F_n = \varnothing$$
Nous avons alors :
$$E = E \setminus \bigcap_{n\in\mathbf{N}} F_n = \bigcup_{n\in\mathbf{N}} E \setminus F_n$$
Donc : $K \subset \bigcup_{n\in\mathbf{N}} E\setminus F_n$. Les $E\setminus F_n$ étant ouverts, il existe $J \subset \mathbf{N}$ fini tel que $K \subset \bigcup_{n\in J} E\setminus F_n$. Or $F_{n+1} \subset F_n$ donc $E \setminus F_n \subset E \setminus F_{n+1}$, ainsi avec $j = \max J$ on a $K \subset E \setminus F_j$ ce qui est absurde car F_j est d'intersection non vide avec K.

2. On sait que x est valeur d'adhérence de (x_n) si :
$$\forall\varepsilon > 0, \forall n \in \mathbf{N}, \exists p \geqslant n,\ \|x_p - x\| \leqslant \varepsilon$$
Donc x est valeur d'adhérence si et seulement si :
$$x \in \bigcap_{n\in\mathbf{N}} \overline{A_n}$$
Les $\overline{A_n}$ (définis par l'énoncé) sont une suite décroissantes de fermés d'intersection avec K non vide, avec la question précédente :
$$\bigcap_{n\in\mathbf{N}} \overline{A_n} \neq \emptyset$$
Donc (x_n) admet une valeur d'adhérence. K est compact.

3. Raisonnons par contraposition, soit K un ensemble ne vérifiant pas cette propriété.
Soit $\varepsilon > 0$. Prenons $x_0 \in K$ et construisons par récurrence la suite x_n à valeur dans K telle que :
$$\forall n \in \mathbf{N},\ x_{n+1} \notin \bigcup_{k\leqslant n} B(x_k,\varepsilon)$$
ce qui est possible par hypothèse (K n'est jamais recouvert par les $\bigcup_{k\leqslant n} B(x_k,\varepsilon)$). Nous avons :
$$\forall p,q \in \mathbf{N},\ p \neq q \Longrightarrow \|x_p - x_q\| \geqslant \varepsilon$$
Donc toutes les suites extraites de $(x_n)_{n\in\mathbf{N}}$ sont non convergentes : K n'est pas compact.

4. Raisonnons par l'absurde :

$$\forall n \in \mathbf{N}^*,\ \exists x_n \in K,\ \forall i \in I,\ B\left(x_n, \frac{1}{n}\right) \not\subset O_i$$

Soit x une valeur d'adhérence (qui existe car nous sommes dans un compact) de $(x_n)_{n\in\mathbf{N}^*}$. Soit $i \in I$ tel que $x \in O_i$. Vu que c'est un ouvert, il existe $\eta > 0$ tel que :

$$B(x, \eta) \subset O_i$$

x étant une valeur d'adhérence :

$$\exists n \in \mathbf{N}^*,\ \|x_n - x\| < \frac{\eta}{2} \quad \text{et} \quad n > \frac{2}{\eta}$$

Et :

$$\forall y \in B\left(x_n, \frac{1}{n}\right),\ \|x - y\| \leqslant \|x - x_n\| + \|x_n - y\| < \eta$$

Donc :

$$B\left(x_n, \frac{1}{n}\right) \subset B(x, \eta) \subset O_i$$

Ce qui est absurde.

5. Soit K un compact et $(O_i)_{i\in I}$ une famille d'ouverts tels que

$$K \subset \bigcup_{i\in I} O_i$$

Soit α donné par le second lemme. D'après le lemme de précompacité, il existe $n \in \mathbf{N}$ et $x_0, \dots, x_n$ dans K tels que :

$$K \subset \bigcup_{k=0}^{n} B(x_k, \alpha)$$

Et le second lemme nous donne que :

$$\forall k \in [\![0, n]\!],\ \exists i_k \in I,\ B(x_k, \alpha) \subset O_{i_k}$$

Donc :

$$K \subset \bigcup_{k=0}^{n} O_{i_k}$$

Ce qui conclut la preuve.

□

Remarque

On peut se demander à quoi sert le second lemme. Lorsque E est complet, un ensemble précompact est compact.

1.99 Théorème de Riesz

Un espace vectoriel normé est de dimension finie si et seulement si la sa boule unité est compacte.

Le sens directe relève du cours, on veut montrer le sens réciproque. Raisonnons par contraposition, soit $(E, \|.\|)$ un evn de dimension infinie :

1. Soit F sous espace de dimension finie de E et $a \in E$: montrez qu'il existe $b \in F$ tel que
$$d(a, F) = \|a - b\|$$
En déduire l'existence d'un $c \in E$ tel que $\|c\| = 1 = d(c, F)$.
2. Conclure.

Solution. 1. F étant de dimension finie, il est fermé. Soit x quelconque dans F. Par définition de la distance :
$$d(a, F) \leqslant \|x - a\|$$
Si cette distance est atteinte, elle l'est sur le sous ensemble de F : $\{y \in F,\ \|y - a\| \leqslant \|x - a\|\}$ qui est fermé et borné donc est un compact car inclus dans F de dimension finie. L'application $y \in F \mapsto \|y - a\|$ étant continue, elle admet un minimum sur ce compact.
Soit $a \in E \setminus F$ (qui existe car F est strictement inclus dans E car de dimension finie) Soit $b \in F$ tel que $d(a, F) = \|a - b\|$. F étant fermé, $\|a - b\| > 0$ (on rappelle que $d(x, A) = 0 \iff x \in \overline{A}$). Posons $c = \frac{b-a}{\|b-a\|}$.
Clairement $\|c\| = 1$, montrons que sa distance à F aussi. F étant un espace vectoriel, nous avons :
$$\begin{aligned} d(c, F) &= \inf_{x \in F}\left(\left\| \frac{b-a}{\|b-a\|} - x \right\|\right) \\ &= \inf_{x \in F}\left(\left\| \frac{b-a}{\|b-a\|} - \frac{b-x}{\|b-a\|} \right\|\right) \\ &= \frac{1}{\|b-a\|} \inf_{x \in F}(\|x - a\|) \\ &= 1 \end{aligned}$$

2. On prend un espace vectoriel F quelconque et on construit une suite $(c_n)_{n \in \mathbf{N}} \in B(0,1)^{\mathbf{N}}$ telle que :
$$d(c_n, F_n) = 1$$
avec
$$F_n = F \oplus \bigoplus_{k=0}^{n-1} c_k \mathbf{K}$$
Ainsi construite, $\forall i \neq j, \|c_i - c_j\| \geqslant 1$ donc on ne peut pas en extraire une sous-suite convergente.

□

2 Complétude

2.100 Suites de Cauchy et espaces complets

Soit $(E, \|.\|)$ un espace vectoriel normé. On dit qu'une suite $(x_n)_{n\in\mathbf{N}} \in E^{\mathbf{N}}$ est de Cauchy si :

$$\forall \varepsilon > 0,\ \exists n \in \mathbf{N},\ \forall p, q \geqslant n,\ \|x_p - x_q\| \leqslant \varepsilon$$

1. Montrez que toute suite convergente est une suite de Cauchy.
2. Montrez qu'une suite de Cauchy possédant une valeur d'adhérence converge.

E est dit complet si toute les suites de Cauchy sont convergentes.

3. Supposons pour cette question que E soit de dimension finie. Montrez que E est complet.
4. Montrez que E est complet si et seulement si toute série absolument convergente est convergente.
5. Montrez que $(l^\infty, \|.\|_\infty)$ (espace des suites réelles bornées) est complet.
6. Supposons E complet. Montrez la **propriété de Baire** : si $(\Omega_n)_{n\in\mathbf{N}}$ est une famille d'ouverts denses de E, alors $\bigcap_{n\in\mathbf{N}} \Omega_n$ est dense dans E. Que dire des fermés ?
7. Montrez que $\mathbf{R}[X]$ n'est complet pour aucune norme.

Solution.

1. Soit $(x_n)_{n\in\mathbf{N}} \in E^{\mathbf{N}}$ une suite convergente vers $x \in E$.

$$\forall \varepsilon > 0,\ \exists n \in \mathbf{N},\ \forall p \geqslant n,\ \|x_p - x\| \leqslant \frac{\varepsilon}{2}$$

Donc :

$$\forall p, q \geqslant n,\ \|x_p - x_q\| \leqslant \|x_p - x\| + \|x - x_q\| \leqslant \varepsilon$$

$(x_n)_{n\in\mathbf{N}}$ est bien de Cauchy.

2. Soit $(x_n)_{n\in\mathbf{N}} \in E^{\mathbf{N}}$ une suite de Cauchy possédant $x \in E$ comme valeur d'adhérence.

$$\forall \varepsilon > 0,\ \exists n \in \mathbf{N},\ \forall p, q \geqslant n,\ \|x_p - x_q\| \leqslant \frac{\varepsilon}{2}$$

Or x étant valeur d'adhérence :

$$\exists p \geqslant n,\ \|x - x_p\| \leqslant \frac{\varepsilon}{2}$$

D'où :

$$\forall q \geqslant n,\ \|x_q - x\| \leqslant \|x_q - x_p\| + \|x_p - x\| \leqslant \varepsilon$$

Ainsi $(x_n)_{n\in\mathbf{N}}$ converge vers x.

3. Soit $(x_n)_{n\in\mathbf{N}} \in E^{\mathbf{N}}$ une suite de Cauchy.

$$\exists n \in \mathbf{N},\ \forall p, q \geqslant n,\ \|x_p - x_q\| \leqslant 1$$

Donc en particulier :

$$\forall p \geqslant n,\ \|x_p\| \leqslant \|x_n\| + \|x_p - x_n\| \leqslant \|x_n\| + 1$$

Ainsi la suite $(x_n)_{n\in\mathbf{N}}$ est bornée, nous sommes en dimension finie donc d'après le théorème de BOLZANO-WEIERSTRASS elle admet une valeur d'adhérence donc converge d'après le résultat précédent. E est complet.

4. *Sens direct.* Soit $(x_n)_{n\in\mathbf{N}} \in E^{\mathbf{N}}$ le terme général d'une suite absolument convergente. $\sum \|x_n\|$ étant convergente, elle est de CAUCHY (question 1). Ainsi :

$$\forall\varepsilon > 0,\ \exists n \in \mathbf{N},\ \forall p > q \geqslant n, \left|\sum_{k=0}^{p} \|x_k\| - \sum_{k=0}^{q} \|x_k\|\right| = \sum_{k=q+1}^{p} \|x_k\| \leqslant \varepsilon$$

Mais alors :

$$\left\|\sum_{k=0}^{p} x_k - \sum_{k=0}^{q} x_k\right\| \leqslant \sum_{k=q+1}^{p} \|x_k\| \leqslant \varepsilon$$

Donc $\left(\sum_{k=0}^{n} x_k\right)_{n\in\mathbf{N}}$ est de **Cauchy** donc converge car E est complet, ce qui établit le résultat.

Sens réciproque. Soit $(x_n)_{n\in\mathbf{N}}$ une suite de **Cauchy**. Montrons qu'elle admet une valeur d'adhérence pour conclure avec la question 2. On sait que :

$$\forall k \in \mathbf{N},\ \exists n_k \in \mathbf{N},\ \forall p, q \geqslant n_k,\ \|x_p - x_q\| \leqslant \frac{1}{2^k}$$

Quitte à augmenter les n_k, on peut supposer que $(n_k)_{k\in\mathbf{N}}$ est strictement croissante. Mais alors : $\forall k \in \mathbf{N},\ \|x_{n_{k+1}} - x_{n_k}\| \leqslant \frac{1}{2^k}$

La série de terme général $(x_{n_{k+1}} - x_{n_k})_{k\in\mathbf{N}}$ est convergente car absolument convergente donc $(x_{n_k})_{k\in\mathbf{N}}$ est convergente, ce qui termine la preuve.

5. Soit $((x_{n,m})_{m\in\mathbf{N}})_{n\in\mathbf{N}}$ une suite de CAUCHY de l^∞. Elle est donc bornée, notons M un majorant. Nous avons :

$$\forall\varepsilon > 0,\ \exists n \in \mathbf{N},\ \forall p, q \geqslant n,\ \|x_p - x_q\|_\infty \leqslant \varepsilon$$

Donc :

$$\forall m \in \mathbf{N},\ |x_{p,m} - x_{q,m}| \leqslant \|x_p - x_q\|_\infty \leqslant \varepsilon$$

Ainsi les suites $(x_{n,m})_{n\in\mathbf{N}}$ sont de CAUCHY et à valeur dans $\mathbf{R}$ donc convergentes. Posons $a_m = \lim\limits_{n\to\infty} x_{n,m}$.

Nous avons : $\forall m \in \mathbf{N},\ \forall n \in \mathbf{N},\ |x_{n,m}| \leqslant M$. Donc en faisant tendre n vers $+\infty$: $\forall m \in \mathbf{N},\ |a_m| \leqslant M$. La suite $(a_m)_{m\in\mathbf{N}}$ est donc dans l^∞. Il suffit de montrer que la suite $((x_{n,m})_{m\in\mathbf{N}})_{n\in\mathbf{N}}$ converge vers la suite $(a_m)_{m\in\mathbf{N}}$ au sens de la norme infini pour conclure. Nous savons que :

$$\forall\varepsilon > 0,\ \exists n \in \mathbf{N},\ \forall p, q \geqslant n,\ \forall m \in \mathbf{N},\ |x_{p,m} - x_{q,m}| \leqslant \varepsilon$$

En faisant tendre q vers $+\infty$ il vient :

$$\forall\varepsilon > 0,\ \exists n \in \mathbf{N},\ \forall p \geqslant n,\ \forall m \in \mathbf{N},\ |x_{p,m} - a_m| \leqslant \varepsilon$$

Soit :

$$\forall\varepsilon > 0,\ \exists n \in \mathbf{N},\ \forall p \geqslant n,\ \|x_p - a\|_\infty \leqslant \varepsilon$$

Ce qui est bien ce que l'on voulait.

6. Soit x dans E et $\varepsilon > 0$. Par densité de Ω_0

$$\exists x_0 \in \Omega_0,\ x_0 \in B\left(x, \frac{\varepsilon}{2}\right)$$

Puis $\Omega_0 \cap B\left(x, \frac{\varepsilon}{2}\right)$ étant un ouvert :

$$\exists \rho_0 < 1,\ B(x_0, \rho_0) \subset \Omega_0 \cap B\left(x, \frac{\varepsilon}{2}\right) \subset \Omega_0 \cap \overline{B}\left(x, \frac{\varepsilon}{2}\right)$$

Et quitte à diminuer ρ_0, on peut même supposer que $\overline{B}(x_0, \rho_0) \subset \Omega_0 \cap \overline{B}\left(x, \frac{\varepsilon}{2}\right)$
Par densité de Ω_1 :

$$\exists x_1 \in \Omega_1,\ x_1 \in B(x_0, \rho_0)$$

$\Omega_1 \cap B(x_0, \rho_0)$ étant un ouvert :

$$\exists \rho_1 < \frac{1}{2},\ \overline{B}(x_1, \rho_1) \subset \Omega_1 \cap \overline{B}(x_0, \rho_0)$$

On construit ainsi une suite $(x_n)_{n\in\mathbf{N}}$ telle que $\forall n \in \mathbf{N}^*,\ \|x_n - x_{n-1}\| < \frac{1}{2^n}$, nous sommes dans un espace complet, $\sum x_n - x_{n-1}$ étant absolument convergente est convergente donc $(x_n)_{n\in\mathbf{N}}$ converge vers une limite $x_\infty \in E$. De plus :

$$\forall n \in \mathbf{N},\ \forall k \geqslant n,\ x_k \in \overline{B}(x_n, \rho_n)$$

Donc par passage à la limite (les ensembles considérés sont des fermés)

$$\forall n \in \mathbf{N},\ x_\infty \in \overline{B}(x_n, \rho_n)$$

Et vu que $\overline{B}(x_n, \rho_n) \subset \Omega_n$, $x_\infty \in \bigcap\limits_{n\in\mathbf{N}} \Omega_n$.
De plus, $\forall n \in \mathbf{N},\ x_n \in \overline{B}\left(x, \frac{\varepsilon}{2}\right)$ donc $x_\infty \in B(x, \varepsilon)$ ce qui conclut la preuve.
On déduit de cela en passant au complémentaire que la réunion de fermés d'intérieur vide est d'intérieur vide.

7. Soit $\|.\|$ une norme quelconque pour $\mathbf{R}[X]$. Les $\mathbf{R}_n[X]$ sont des fermés (sous espaces vectoriels de dimension finie). Soit $P \in \mathbf{R}_n[X]$. Nous avons :

$$\forall \varepsilon > 0,\ \forall Q \in \mathbf{R}[X] \setminus \{0\},\ P + \frac{\varepsilon Q}{2\|Q\|} \in B(P, \varepsilon)$$

Il suffit de prendre Q de degré strictement supérieur à n pour conclure que les $\mathbf{R}_n[X]$ sont d'intérieur vide. Mais $\bigcup\limits_{n\in\mathbf{N}} \mathbf{R}_n[X] = \mathbf{R}[X]$ qui n'est pas d'intérieur vide donc $(\mathbf{R}[X], \|.\|)$ n'est pas complet.

Remarque

Plus généralement, on peut montrer que les espaces normés à base dénombrable ne sont jamais complets. (C'est pas très dur, mais Pandou flemme).

□

3 Convexité

3.101 Le théorème de Carathéodory

Soit E un $\mathbf{R}$-espace vectoriel normé de dimension n et A une partie de E non vide.

1. Montrez l'existence d'un plus petit convexe contenant A, que l'on notera par la suite $C(A)$ (appelé enveloppe convexe de A).
2. Montrez que si A est convexe alors A est stable par passage aux barycentres à poids positifs. On rappel qu'un barycentre à poids positifs de $x_1, \dots, x_n$ est un vecteur de la forme
$$\sum_{i=1}^{n} \lambda_i x_i$$
où les λ_i sont des réels positifs de somme égale à 1.
3. Montrez que $C(A)$ est l'ensemble des barycentres à poids positifs des points de A.
4. Soit $x_1, \dots, x_p$ éléments de E avec $p \geqslant n+2$. Montrez qu'il existe $\mu_1, \dots, \mu_p$ réels non tous nuls tels que :
$$\sum_{i=1}^{p} \mu_i x_i = 0 \text{ et } \sum_{i=1}^{p} \mu_i = 0$$
on pourra considérer la famille $(x_1 - x_p, \dots, x_{p-1} - x_p)$
5. Montrez que $C(A)$ est l'ensemble des barycentres à poids positifs d'au plus $n+1$ points de A. (c'est ce résultat qui est nommé théorème de Carathéodory)
6. Montrez que l'enveloppe convexe d'un compact non vide de E est compacte

Solution. 1. Posons $C_A = \{C \subset E,\ C \text{ convexe et } A \subset C\}$ l'ensemble des convexes contenant A. Cet ensemble est non vide, en effet il contient E. On s'intéresse donc à
$$B = \bigcap_{C \in C_A} C$$
Il est non vide car il contient A et est inclus dans tout convexe contenant A. Soit $x, y \in B$. Par définition de B, pour tout $C \in C_A$, $x, y \in C$ et par convexité de C : $\forall \lambda \in [0,1],\ \lambda x + (1-\lambda) y \in C$. Cette propriété étant vraie pour tout $C \in C_A$, nous avons $\lambda x + (1-\lambda)y \in B$. B est donc le plus petit convexe contenant A.

2. Montrons par récurrence sur $n \in \mathbf{N}^*$ que tout barycentre à poids positifs de n points de A est dans A.
   - Pour $n = 1$ c'est évident.
   - Pour $n = 2$ cela résulte de la convexité de A. (on remarque bien sur qu'un barycentre à poids positifs $\lambda_1 x + \lambda_2 y$ peut s'écrire $\lambda_1 x + (1 - \lambda_1) y$)
   - Soit $n > 1$ tel que la propriété soit vraie. Montrons la au rang $n+1$. Soit $\lambda_1, \dots, \lambda_{n+1}$ réels positifs de somme 1 et $x_1, \dots, x_{n+1}$ éléments de A.
     Si $\lambda_{n+1} = 1$ le résultat est clair (nécessairement tout les autres λ_i sont nuls)
     Supposons $\lambda_{n+1} \neq 1$. On a :
$$\sum_{i=1}^{n+1} \lambda_i x_i = (1 - \lambda_{n+1}) \sum_{i=1}^{n} \frac{\lambda_i}{1 - \lambda_{n+1}} x_i + \lambda_{n+1} x_{n+1}$$

On remarque que $\forall i \in [\![1, n]\!],\ \frac{\lambda_i}{1-\lambda_{n+1}} \geqslant 0$ et

$$\begin{aligned}\sum_{i=1}^{n} \frac{\lambda_i}{1-\lambda_{n+1}} &= \frac{\sum_{i=1}^{n} \lambda_i}{1-\lambda_{n+1}} \\ &= \frac{1-\lambda_{n+1}}{1-\lambda_{n+1}} \\ &= 1\end{aligned}$$

Par application de l'hypothèse de récurrence on obtient que $(1-\lambda_{n+1}) \sum_{i=1}^{n} \frac{\lambda_i}{1-\lambda_{n+1}} x_i \in A$ et la convexité de A nous permet de conclure.

3. Notons $B(A)$ l'ensemble des barycentres à poids positifs des éléments de A. Avec la question précédente on a $B(A) \subset C(A)$ ($A \subset C(A)$ et $C(A)$ est stable par passage aux barycentres à poids positifs)
   Pour montrer l'inclusion réciproque il suffit de montrer que $B(A)$ est convexe ce qui est pratiquement évident (le lecteur vérifiera facilement qu'un barycentre de barycentres est un barycentre).
4. la famille $(x_1 - x_p, \ldots, x_{p-1} - x_p)$ est liée car comporte $p-1 \geqslant n+1$ vecteurs. Il existe donc $\mu_1, \ldots, \mu_{p-1}$ réels non tous nuls tels que :
$$\sum_{i=1}^{p-1} \mu_i (x_i - x_p) = 0$$
   On pose $\mu_p = -\sum_{i=1}^{p-1} \mu_i$, on a donc :
$$\sum_{i=1}^{p} \mu_i x_i = 0$$
   et :
$$\sum_{i=1}^{p} \mu_i = 0$$
5. Montrons par récurrence sur $p \geqslant n+1$ que d'un barycentre à poids positifs de p points de A on peut se ramener à un barycentre à poids positifs de $n+1$ points de A.
   — C'est évident pour $p = n+1$
   — Soit $p \geqslant n+2$ tel que la propriété soit vraie au rang $p-1$. Soit $x_1, \ldots, x_p$ points de A et $\lambda_1, \ldots, \lambda_p$ réels positifs de somme 1. Soit $\mu_1, \ldots, \mu_p$ réels vérifiant les hypothèses de la question précédente.
   Soit $j \in [\![1, p]\!]$ tel que $\frac{\lambda_j}{\mu_j} = \min\left\{\frac{\lambda_i}{\mu_i},\ \mu_i > 0\right\}$ (qui existe car cet ensemble est minoré par 0 et non vide car la somme des μ_i est nulle et ils sont non tous nuls donc l'un d'entre eux est strictement positif)
   Nous avons :
$$x_j = -\sum_{i \neq j} \frac{\mu_i}{\mu_j} x_i$$

et

$$\sum_{i=1}^{p} \lambda_i x_i = \sum_{i \neq j} \left(\lambda_i - \lambda_j \frac{\mu_i}{\mu_j} \right) x_i$$

Deux cas de figure :

— Si $\mu_i \leqslant 0$ alors vu que λ_j et μ_j sont positifs, $\lambda_j \frac{\mu_i}{\mu_j} \leqslant 0$ ce qui nous donne $\lambda_i - \lambda_j \frac{\mu_i}{\mu_j} \geqslant 0$

— Si $\mu_i > 0$ alors par choix de j : $\frac{\lambda_j}{\mu_j} \leqslant \frac{\lambda_i}{\mu_i}$ d'où $\lambda_i - \lambda_j \frac{\mu_i}{\mu_j} \geqslant 0$

De plus :

$$\begin{aligned} \sum_{i \neq j} \left(\lambda_i - \lambda_j \frac{\mu_i}{\mu_j} \right) &= (1 - \lambda_j) - \lambda_j \sum_{i \neq j} \frac{\mu_i}{\mu_j} \\ &= (1 - \lambda_j) + \lambda_j \\ &= 1 \end{aligned}$$

On c'est bien ramené à un barycentre à poids positifs à $p - 1$ points et on conclut par hypothèse de récurrence.

$C(A)$ étant l'ensemble des barycentres à poids positifs de A, d'après ce que l'on vient de montrer c'est aussi l'ensemble des barycentres à poids positifs d'au plus $n + 1$ points de A. Ainsi s'achève la démonstration du théorème de Carathéodory.

6. Posons $\Lambda = \{(\lambda_1, \ldots, \lambda_{n+1}) \in \mathbf{R}_+^{n+1}, \ \sum_{i=1}^{n+1} \lambda_i = 1\}$

   Λ est un fermé en effet $\Lambda = f^{-1}(\{1\})$ où $f : (a_1, \ldots, a_{n+1}) \in \mathbf{R}^{n+1} \mapsto \sum_{i=1}^{n+1} \max(0, a_i)$ continue.

   Et étant borné (toute les normes sont équivalentes en dimension finies, prendre $\|.\|_\infty$) Λ est un compact.

   Le produit de compacts étant compact $\Lambda \times A^{n+1}$ est un compact. Posons

$$g : (\lambda_1, \ldots, \lambda_{n+1}, x_1, \ldots, x_{n+1}) \in \Lambda \times A^{n+1} \mapsto \sum_{i=1}^{n+1} \lambda_i x_i$$

   g est continue et $g(\Lambda \times A^{n+1}) = C(A)$ ce qui conclut la preuve.

□

3.102 Projection sur un convexe fermé d'un espace euclidien

Soit $(E, \langle .|. \rangle)$ un espace euclidien et $\|.\|$ la norme associée. Soit C un convexe fermé non vide de E. (*faire des dessins aide*)

1. Montrez

$$\forall x \in E, \ \exists! p(x) \in C, \ d(x, C) = \|x - p(x)\|$$

2. Montrez

$$\forall x \in E, \forall y \in C, \langle x - p(x) | y - p(x) \rangle \leqslant 0$$

   En déduire que p est 1-lipschitzienne.

Solution. 1. *Existence :* Prenons a un élément quelconque de C. Vu que $\|x-a\| \geqslant d(x,C)$, si cette distance est atteinte, elle l'est pour un élément dans

$$C_a = \{y \in C,\ \|x-y\| \leqslant \|x-a\|\}$$

Or C_a est un fermé borné, nous sommes en dimension finie : c'est un compact. L'application $y \in C_a \mapsto \|y-x\|$ est continue sur C_a est bornée et atteint ses bornes, ce qui conclut la preuve.
Unicité : Soit $y, z \in C$ tels que : $\|x-y\| = \|x-z\| = d(x,C)$
L'identité du parallélogramme nous donne :

$$\begin{aligned} 2(\|x-y\|^2 + \|x-z\|^2) &= \|(x-y)+(x-z)\|^2 + \|(x-y)-(x-z\|^2 \\ &= \|2x-y-z\|^2 + \|z-y\|^2 \\ &= 4\|x - \frac{y+z}{2}\|^2 + \|z-y\|^2 \end{aligned}$$

$\frac{y+z}{2}$ étant dans C, nous avons donc
$\|x-\frac{y+z}{2}\|^2 \geqslant \|x-y\|^2 = \|x-z\|^2$ d'où $\|z-y\|^2 \leqslant 0$ ainsi $z=y$.

2. Soit x dans E, y dans C et λ dans $[0,1]$. Par convexité de C :

$$\lambda p(x) + (1-\lambda)y \in C$$

Par définition de $p(x)$:

$$\|x-p(x)\|^2 \leqslant \|x-(\lambda p(x)+(1-\lambda)y)\|^2 = \|(x-p(x))+(1-\lambda)(p(x)-y)\|^2$$

Et

$$\|(x-p(x))+(1-\lambda)(p(x)-y)\|^2 = \|x-p(x)\|^2 + 2(1-\lambda)\langle x-p(x)|p(x)-y\rangle + (1-\lambda)^2\|p(x)-y\|^2$$

Donc

$$2(1-\lambda)\langle x-p(x)|y-p(x)\rangle \leqslant (1-\lambda)^2\|p(x)-y\|^2$$

Pour $\lambda \neq 1$, on divise par $(1-\lambda)$ et on fait tendre λ vers 1 (par valeurs inférieures) ce qui nous donne bien $\langle x-p(x)|y-p(x)\rangle \leqslant 0$
Soit maintenant x, y dans E. Nous avons avec le résultat précédent et la bilinéarité du produit scalaire :

$$\langle x-p(x)|p(y)-p(x)\rangle \leqslant 0, \quad \langle p(y)-y|p(y)-p(x)\rangle \leqslant 0$$

Sommons :

$$0 \geqslant \langle p(y)-p(x)|x-y+p(y)-p(x)\rangle = \|p(y)-p(x)\|^2 + \langle p(y)-p(x)|x-y\rangle$$

Soit par CAUCHY-SCHWARZ :

$$\|p(y)-p(x)\|^2 \leqslant \langle p(y)-p(x)|y-x\rangle \leqslant \|p(y)-p(x)\|\|y-x\|$$

Lorsque $p(y)=p(x)$ le résultat est clair sinon on divise l'inégalité par $\|p(y)-p(x)\|$.

□

4 Connexité

4.103 Composante connexe d'un R-ev coup par un hyperplan

E un $\mathbf{R}$-espace vectoriel normé de dimension finie et H un hyperplan. Montrer que $E \setminus H$ possède 2 composantes connexes.

Solution. Comme H est un hyperplan, $\exists\, \phi : E \to \mathbf{R}$ une forme linéaire non nulle tel que $H = \ker \phi$.

On note $E^+ = \{x \in E, \phi(x) > 0\}$ et $E^- = \{x \in E, \phi(x) < 0\}$

Soient $x, y \in E \setminus H$:

1er cas : $x, y \in E^+$ alors on note $\gamma : t \in [0,1] \mapsto (1-t)x + ty$. On a bien $\gamma(1) = y$ et $\gamma(0) = x$.

$$\phi((1-t)x + ty) = (1-t)\phi(x) + t\phi(y) > 0$$

donc $\forall t \in [0,1], \gamma(t) \in E^+$. Donc E^+ connexe par arcs. Pareil pour E^-.

2ème cas : $x \in E^+, y \in E^-$ quitte à renommer.

Par l'absurde si il existe γ un chemin dans $E \setminus H$ tel que $x \xrightarrow{\gamma} y$.

Alors comme ϕ est continue car nous sommes en dimension finie. $\phi \circ \gamma$ l'est aussi et est jamais nul car $\gamma(t) \notin H$.

Or $\phi \circ \gamma(0) = \phi(x) > 0$ et $\phi \circ \gamma(1) = \phi(y) < 0$. Donc par le théorème des valeurs intermdiaires $\phi \circ \gamma$ s'annule sur $[0,1]$ ce qui est absurde.

Donc E^+ et E^- sont bien les 2 composantes connexes

□

Quatrième partie
Probabilités

0.104 Lemme de Borel-Cantelli

Si la somme des probabilités d'une suite $(A_n)_{n\geqslant 0}$ d'événements d'un espace probabilisé $(\Omega, \mathcal{A}, \mathbf{P})$ est finie, alors la probabilité qu'une infinité d'entre eux se réalisent simultanément est nulle.

Démonstration. L'évènement "une infinité de A_n se réalisent" peut s'écrire :

$$B = \bigcap_{n\geqslant 0} \bigcup_{k\geqslant n} A_k.$$

Ainsi, comme B est une intersection décroissante d'évènements, on a :

$$B = \lim_{n\to+\infty} P\left(\bigcup_{k\geqslant n} A_k\right)$$

$$\leqslant \lim_{n\to+\infty} \sum_{k\geqslant n} P(A_k) = 0.$$

L'inégalité découle de la sous-additivité de P, et la limite est nulle car c'est un reste de série convergente. $\square$

0.105 Zéro-Un de Borel Cantelli

Soit (A_n) des évènements **indépendants** tels que $\sum_{n\in\mathbb{N}} \mathbb{P}(A_n) = +\infty$, alors l'évènement $\{\omega \in \Omega, \{n \in \mathbb{N}, \omega \in A_n\}$ est infini$\}$ est certain.

Démonstration. Un peu plus difficile. $\square$

0.106 Un résultat de Kosmanek

Soit $(\Omega, \mathcal{A}, P)$ un espace probabilisé et $A, B \in \mathcal{A}$. Montrer que $|P(A\cap B) - P(A)P(B)| \leqslant \frac{1}{4}$

Solution. On sait que $(A\cap B, A\cap\overline{B}, \overline{A}\cap B, \overline{A}\cap\overline{B})$ est un système complet. On note $a = P(A\cap B),\ b = P(A\cap\overline{B}),\ c = P(\overline{A}\cap B),\ d = P(\overline{A}\cap\overline{B})$.

On a : $a+b+c+d = 1$ et

$$\begin{aligned} P(A\cap B) - P(A)P(B) &= a - (a+b)(a+c) \\ &= a - a^2 - ab - ac - bc \qquad = a(1-a-b-c) - bc = ad - bc \end{aligned}$$

Or $ad - bc \leqslant ad$ et $\sqrt{ad} \leqslant \frac{a+d}{2} \leqslant \frac{1}{2}$

Donc $ad \leqslant \frac{1}{4}$

et de même $-\frac{1}{4} \leqslant -bc \leqslant ad - bc$ d'où la conclusion. $\square$

0.107 Variable aléatoire donnant le premier succès

On note $(X_n)_{n\geqslant 1}$ une suite de variables aléatoires réelles discrètes indépendantes de loi $\mathcal{B}(p)$.
On note $(\Omega, \mathcal{A}, P)$ l'espace probabilisé correspondant.
On note pour $\omega \in \Omega, T(\omega) = \min\{n \in \mathbf{N}^*, X_n(w) = 1\}$ et on convient que $\min \emptyset = +\infty$.
Montrer que T est une variable aléatoire discrète et donner sa loi.

Solution. Tout d'abord, $T(\Omega) = \mathbf{N}^* \cup \{+\infty\}$ est dénombrable.

Puis,

$$\forall n \in \mathbf{N}^*, \quad [T = n] = \underbrace{[X_1 = 0, \ldots, X_{n-1} = 0, X_n = 1]}_{\in \mathcal{A}}$$

et

$$[T = +\infty] = (\bigcup_{n \in \mathbf{N}^*} [T = n])^c \in \mathcal{A}$$

Ainsi T est une variable discrète.
Puis pour $n \in \mathbf{N}^*$,

$$\begin{aligned} P(T = n) &= P(X_1 = 0, \ldots, X_{n-1} = 0, X_n = 1) \\ &= P(X_1 = 0) \ldots P(X_{n-1} = 0) P(X_n = 1) \text{ Par indépendance des VARD} \\ &= q^{n-1} p \text{ avec q = 1-p} \end{aligned}$$

□

0.108 Marche aléatoire sur $\mathbb{Z}$ et $\mathbb{Z}^2$

La marche aléatoire équilibrée sur $\mathbb{Z}$ et $\mathbb{Z}^2$ est récurrente.

0.109 Formule de Wald

Soit (X_n) une suite de variables aléatoires i.i.d (disons de même loi que X) L^1 et $N \in L^1$ une variable aléatoire indépendante de X à valeurs dans $\mathbb{N}$. On note $S = \sum_{k=1}^{N} X_k$, alors :

$$\mathbb{E}(S) = \mathbb{E}(N)\mathbb{E}(X)$$

et plus généralement, on a :

$$\forall t \in [-1, 1], G_S(t) = G_N \circ G_X(t)$$

Démonstration. Simplement conditionner par les évènements $N = n$ ... □

0.110 Processus de Galton-Watson

...

Cinquième partie
Calcul différentiel

FIGURE 1 – Rare image illustrant la popularité du calcul différentiel

0.111 Equation de transport

L'objectif de cette partie est de traiter l'équation de transport :

$$\begin{cases} \partial_t u + c \cdot \nabla_x u = 0 \quad t \geqslant 0, x \in \mathbb{R}^n \\ u(x,0) = u_0(x) \end{cases}$$

où u_0 est une fonction $\mathcal{C}^1(\mathbb{R}^n, \mathbb{R})$ et $c \in \mathbb{R}^n$.
Il existe une unique solution $u \in \mathcal{C}^1(\mathbb{R}_+ \times \mathbb{R}^n, \mathbb{R})$ à cette équation.

Remarque

Cette équation apparaît un peu partout en physique et englobe beaucoup d'équations que vous connaissez déjà.

Démonstration. Supposons qu'une telle solution u existe. On cherche une fonction $X : t \in \mathbb{R}_+ \longmapsto X(t) \in \mathbb{R}^n$ de classe $\mathcal{C}^1$ telle que $\varphi : t \mapsto u(t, X(t))$ est constante. On calcule :

$$\begin{aligned} \varphi'(t) &= \partial_t u(t, X(t)) + X'(t) \cdot \nabla_x u(t, X(t)) \\ &= (X'(t) - c) \cdot \nabla_x u(t, X(t)) \end{aligned}$$

En physique, $\varphi'(t)$ serait en fait noté $\frac{\mathrm{d}u}{\mathrm{d}t}$ (la fameuse dérivée totale), par opposition avec $\frac{\partial u}{\partial t}$.
Il suffit alors de prendre $X'(t) = c$ pour tout réel t.

Fixons $x \in \mathbb{R}^n$ de sorte que $X(0) = x$, alors $X(t) = tc + x$ [2]. Puisque $\varphi(t)$ est constante, on en déduit :

$$\forall t \in \mathbb{R}_+, \varphi(t) = \varphi(0)$$

Ce qui se réécrit :

$$\forall t \in \mathbb{R}_+, u(t, x + tc) = u(0, x) = u_0(x)$$

On en déduit finalement la forme de la solution :

$$\forall x \in \mathbb{R}^n, \forall t \in \mathbb{R}_+, u(t, x) = u_0(x - tc)$$

On vérifie facilement qu'il s'agit effectivement d'une solution. □

Remarque

X est une courbe paramétrée de $\mathbb{R}^n$ au long de laquelle u est constante ... En suivant cette courbe que l'on appelle courbe caractéristique, on peut "remonter" le temps.
Vous pouvez aussi vous exercer sur l'équation avec second membre :

$$\begin{cases} \partial_t u + c \cdot \nabla_x u = f & t \geqslant 0, x \in \mathbb{R}^n \\ u(x, 0) = u_0(x) \end{cases}$$

où f est $\mathcal{C}^1(\mathbb{R}_+ \times \mathbb{R}^n$. La solution de cette équation est donnée par :

$$u(t, x) = u_0(x - tc) + \int_0^t f\big(t', x + (t - t')c\big) \mathrm{d}t'$$

Plutôt que de demander que φ est constante, on peut aussi demander que φ vérifie une EDO simple (que l'on est capable de résoudre). La courbe X associée est aussi appelée courbe caractéristique... Cela se produit

0.112 Equation des ondes

Ceci est une application du résultat précédent. On considère l'équation des ondes générales.

$$\begin{cases} \frac{\partial^2 u}{\partial t^2} u - c^2 \frac{\partial^2 u}{\partial x^2} = 0 & (t, x) \in [0, +\infty[\times \mathbb{R} \\ u(t = 0, x) = f(x) & \forall x \in \mathbb{R} \\ \frac{\partial u}{\partial t}(t = 0, x) = g(x) & \forall x \in \mathbb{R} \end{cases}$$

où f et g sont respectivement $\mathcal{C}^2$ et $\mathcal{C}^1$ et $c \in \mathbb{R}$.
Cette équation admet une unique solution $u \in \mathcal{C}^2(\mathbb{R}_+ \times \mathbb{R})$.

Démonstration. On va se ramener au résultat précédent en "vectorisant" l'équation comme vous savez bien le faire pour les équations différentielles d'ordre supérieure.
On considère $U = \begin{pmatrix} \partial_t u \\ \partial_x u \end{pmatrix}$, $C = \begin{pmatrix} 0 & c^2 \\ 1 & 0 \end{pmatrix}$ et $U_0 = \begin{pmatrix} g(x) \\ f(x) \end{pmatrix}$. L'équation se réécrit alors en :

$$\begin{cases} \frac{\partial U}{\partial t} - C \frac{\partial U}{\partial x} = 0 \\ U(t = 0, x) = U_0(x) \end{cases}$$

2. Oui oui tc ... scalaire multiplié par vecteur ... Mais en dimension 1, on prééfèrera ct évidemment ...

On diagonalise C :

$$C = PDP^{-1} \qquad \text{avec} \qquad D = \begin{pmatrix} -c & 0 \\ 0 & c \end{pmatrix}$$

L'équation se réécrit alors :

$$\frac{\partial PU}{\partial t} - PC\frac{\partial U}{\partial x} = 0 \Longleftrightarrow \frac{\partial PU}{\partial t} - D\frac{\partial PU}{\partial x} = 0$$

On note $Q = PU = \begin{pmatrix} q_1 \\ q_2 \end{pmatrix}$, de sorte qu'on se retrouve avec deux équations de transports scalaires :

$$\begin{cases} \partial_t q_1 + c\partial_x q_1 = 0 \\ \partial_t q_2 - c\partial_x q_2 = 0 \end{cases}$$

On en déduit alors par la partie précédente :

$$\begin{cases} q_1(t,x) &= & q_1\big(t=0, x-ct\big) \\ q_2(t,x) &= & q_2\big(t=0, x+ct\big) \end{cases}$$

Finalement :

$$U(t,x) = \begin{pmatrix} c(q_2 - q_1) \\ q_1 + q_2 \end{pmatrix}$$

On retrouve bien la somme d'une onde se déplaçant dans le sens des x croissants et une onde se déplaçant dans le sens des x décroissants. $\square$

Remarque

Nous avons étudié dans la partie précédente la résolution des équations de transport pour une condition initiale $\mathcal{C}^1$ ... Cependant, il arrive qu'on n'ait pas autant de souplesse initialement, il faut affaiblir la notion de solutions.
On note $\mathcal{C}_c^\infty(E)$ l'ensemble des fonctions $\mathcal{C}^\infty$ à support compact, on appelle aussi ces fonctions des fonctions tests.
On reprend l'équation :

$$\begin{cases} \partial_t u + c \cdot \nabla_x u = 0 \quad t \geqslant 0, x \in \mathbb{R}^n \\ u(x,0) = u_0(x) \end{cases}$$

où cette fois u_0 est continue par morceaux [a] et bornée.
On dit que u est solution faible lorsque :

$$\forall \varphi \in \mathcal{C}_c^\infty(\mathbb{R}_+ \times \mathbb{R}^n), \int_{\mathbb{R}_+ \times \mathbb{R}^n} u\big(\partial_t \varphi + c \cdot \nabla \varphi\big) \mathrm{d}t\mathrm{d}x + \int_{\mathbb{R}^n} u_0(x)\varphi(0,x)\mathrm{d}x = 0$$

Cette définition est justifiée par le fait que si u est $\mathcal{C}^1$ et est solution faible, alors elle est solution (au sens classique) de l'équation initiale ... Vous pouvez le vérifier formellement en intervertissant les intégrales sans justification et en intégrant par parties.

De plus, le même génre de théorème d'existence tient : pour une condtion initiale L^∞, il existe une unique solution faible L^1... Je ne détaille pas car les problèmes d'intégration ne sont pas vraiment au centre du programme.

a. La notion de continuité par morceaux n'existe pas réellement en maths ... Dans la vraie vie, on parle plutôt de "mesurable", mais vous verrez ça l'année prochaine

0.113 Théorèmes de point fixe

1. Soit (E, d) un espace complet et $f : E \to E$ une fonction contractante (ie k-lipschitzienne avec $k < 1$), alors f a un unique point fixe x_∞.
2. Soit (E, d) un espace complet et T un espace métrique (même topologique) et $f : T \times X \to X$ continue et contractante par rapport à la deuxième variable.
   La fonction $f_t : x \mapsto f(t, x)$ a un unique point fixe $g(t)$ et g est continue sur T.

Démonstration.

1. Il suffit d'itérer la suite définie par $x_0 \in E$ et $x_{n+1} = f(x_n)$ de sorte qu'on ait :
$$\|x_p - x_q\| \leqslant \|k^{q-1} + ... + k^p\| \|x - f(x)\| \leqslant \frac{k^p}{1-k} \|x - f(x)\|$$
La suite (x_n) est donc de Cauchy et X est complet, donc (x_n) converge. Par continuité de f, x est un point fixe de f.
2. Soit $t_0 \in T$ et $x_0 = g(t_0)$. f est continue en (t_0, x_0) et $f(t_0, x_0) = x_0$. Fixons ε, il existe un voisinage V de t_0 et il existe α tel que :
$$t \in V, x \in B(x_0, \alpha) \Longrightarrow f(t, x) \in B(x_0, \varepsilon)$$
En particulier, $\|f(t, x) - x_0\| \leqslant \varepsilon$. Pour $x = x_0$, on a :
$$\forall t \in V, \|f_t(x_0) - x_0\| \leqslant \varepsilon$$
Donc, on a :
$$\|f_t^n(x_0) - x_0\| \leqslant \frac{\varepsilon}{1-k}$$
En faisant tendre n vers l'infini, on trouve :
$$\forall t \in V, \|g(t) - x_0\| = \|g(t) - g(t_0)\| \leqslant \frac{\varepsilon}{1-k}$$
Donc, g est continue en t_0.

□

0.114 Homéomorphisme et difféomorphisme

Ce résultat montre que ce que la notion rigide est l'homéomorphisme et non la difféomorphisme.
Si $f : U \to V$ est un homéomorphisme qui est $\mathcal{C}^k$, alors f est un $\mathcal{C}^k$-difféomorphisme si, et seulement si, $\forall x \in U, Df(x)$ est inversible.

Démonstration. Si f est un $\mathcal{C}^k$-difféomorphisme, il suffit de différencier $f \circ f^{-1} = \text{Id}$ et $f^{-1} \circ f = \text{Id}$.

Réciproquement, f^{-1} est différentiable en $y = f(x)$ et :
$$D(f^{-1})(y) = \Big(Df(x)\Big)^{-1} = \Big(Df(f^{-1}(y))\Big)^{-1}$$
On a donc :
$$D(f^{-1}) = \text{Inv} \circ Df \circ f^{-1}$$

où Inv : $u \in GL(E,F) \longmapsto u^{-1} \in \mathcal{L}_c(F,E)$[3]. Inv est $\mathcal{C}^1$ et :

$$D(\text{Inv})(u) \cdot h = -u^{-1} \circ h \circ u^{-1}$$

$D(\text{Inv})$ est la composée de $u \in GL(E,F) \longmapsto (u^{-1}, u^{-1})$ (qui est autant de fois différentiable que Inv) et de :

$$B : (v,w) \in \mathcal{L}_c(F,E) \times \mathcal{L}_c(F,E) \longmapsto \Big(h \mapsto -v \circ h \circ w\Big) \in \mathcal{L}_c(\mathcal{L}_c(E,F), \mathcal{L}_c(F,E))$$

B est bilinéaire et continue de norme $\leqslant \|v\|\|w\|$. Ainsi, B est $\mathcal{C}^\infty$, donc Inv est $\mathcal{C}^\infty$.
Ainsi, f^{-1} est autant de fois différentiable que f. □

0.115 Théorème d'inversion locale

Soit $U \subset E$ un ouvert et F un espace de Banach et $f : U \to F$ une fonction $\mathcal{C}^1$. Soit $a \in U$ tel que $Df(a)$ soit inversible, alors il existe $V \subset U$ un ouvert contenant a et W un ouvert contenant $f(a)$ tel que $f_{|V}$ est un $\mathcal{C}^1$-difféomorphisme de V sur W.

Démonstration. Quitte à composer par $Df(a)^{-1}$, on suppose que $E = F$ et $Df(a) = \text{Id}_E$. On note $b = f(a)$.
On fixe y "près" de b, on cherche x "près" de a tel que $y = f(x)$, ce qui se réécrit :

$$f(x) = y \iff x = x + y - f(x) \iff g_y(x) = x$$

où $g_y(x) = x + y - f(x)$.

On cherche à appliquer le théorème du point fixe à g_y. On doit pour cela vérifier qu'elle est contractante. On différencie Dg_y.

$$Dg_y = Df(x) - \text{Id}$$

Par continuité de $x \mapsto Df(x)$, il existe une boule fermée $BF(a,r)$ telle que :

$$\|Df(x) - \text{Id}\| \leqslant \frac{1}{2}$$

Par le théorème des accroissements finis, la fonction g_y est $\frac{1}{2}$-contractante sur $BF(a,r)$ pour tout y. Reste à vérifier que g_y stabilise bien $BF(a,r)$.
Prenons $y \in B\left(b, \frac{r}{2}\right)$, on a :

$$g_y(x) - a = x - f(x) - \big(a - f(a)\big) + y - b$$

Ce qui donne :

$$\forall x \in BF(a,r), \|g_y(x) - a\| \leqslant \frac{1}{2}\|x - a\| + \|y - b\| < r$$

Par le théorème du point fixe à paramètres, il existe une fonction h continue de $B\left(b, \frac{r}{2}\right)$ dans $BF(a,r)$ tel que $h(y)$ est point fixe de g_y.

3. L'indice c signifie "continu" ... En dimension finie, c'est toujours le cas !

On pose $W = B\left(b, \frac{r}{2}\right)$ et $V = h(W)$. Sur $BF(a,r)$, $\mathrm{Id} - f$ est $\frac{1}{2}$-contractante, donc f y est injective, donc $h(y)$ est le seul point fixe de g_y sur $BF(a,r)$. On a :

$$h(W) = f^{-1}\left(B\left(b, \frac{r}{2}\right)\right) \cap B(a,r)$$

Donc, V est un ouvert contenant a et h est l'inverse $f_{|V}$. Ainsi, f est un homéomorphisme de V sur W, puisque de plus $D(f)$ est inversible, car $\|\mathrm{Id} - Df(x)\| \leqslant \frac{1}{2}$ (d'inverse $\sum\limits_{n\in\mathbb{N}} Df(x)^n$).
Donc, f est un difféomorphisme de V sur W aussi régulier que f. $\square$

0.116 Théorème des fonctions implicites

Soit E, F, G trois espaces de Banach, $f : U \subset E \times F \longrightarrow G$ de classe $\mathcal{C}^k$. Soit $(a,b) \in U$ tel que $f(a,b) = 0$ et $D_2 f(a,b)$ est inversible de F dans G.
Alors il existe un ouvert V contenant (a,b) et W un ouvert de E contenant a ainsi que $g : W \to F$ de classe $\mathcal{C}^k$ tel que :

$$f(x,y) = 0 \Longleftrightarrow x \in W \text{ et } y = g(x)$$

Démonstration. Soit $H : (x,y) \in U \longmapsto (x, f(x,y)) \in E \times G$ qui est $\mathcal{C}^k$:

$$DH(x,y)\cdot(k,h) = \Big(h, D_1 f(x,y)\cdot h + D_2 f(x,y)\cdot k\Big)$$

L'application $DH(a,b)$ est alors inversible, d'inverse :

$$(h', k') \longmapsto \Big(h', \left[D_2 f(a,b)\right]^{-1}(k' - D_1 f(a,b)\cdot h')\Big)$$

On applique le théorème d'inversion locale à H qui nous donne V un ouvert de V contenant (a,b) tel que $H_{|V}$ soit un $\mathcal{C}^k$-difféomorphisme de V sur un ouvert contenant $H(a,b) = (a,0)$.
Quitte à restreindre, on suppose que cet ouvert est $W \times B(0,r)$ où $a \in W$. On a :

$$\begin{aligned} (x,y) \in V, f(x,y) = 0 &\Longleftrightarrow (x, f(x,y)) = H(x,y) \in W \times B(0,r) \text{ et } H_{|V}(x,y) = (x,0) \\ &\Longleftrightarrow x \in W \text{ et } (x,y) = H_{|V}^{-1}(x,0) \\ &\Longleftrightarrow x \in W \text{ et } y = g(x) \end{aligned}$$

où $g(x)$ est la deuxième coordonnée de $H_{|V}^{-1}(x,0)$ qui est $\mathcal{C}^k$. $\square$