Annexe A

Espaces vectoriels, applications linéaires

A.1 Espaces vectoriels

Dans toute la suite de ce chapitre $\mathbb{K}$ est corps commutatif(note [1]. Le programme impose que ce soit un un sous-corps de $\mathbb{C}$. Mais tous ce qui va suivre reste valable si $\mathbb{K}$ est un corps (commutatif) quelconque par exemple $\frac{\mathbb{Z}}{p\mathbb{Z}}$ si p est premier.

Définition A.1 *Un espace vectoriel E sur le corps $\mathbb{K}$ est un ensemble muni d'une loi interne $+$ et d'une loi externe $.$ à opérateurs dans $\mathbb{K}$ telles que :*

- $(E,+)$ *est un groupe commutatif.*
- $\forall(\alpha,\beta)\in\mathbb{K}^2$, $\forall x\in E$: $(\alpha+\beta).x=\alpha.x+\beta.x$, $(\alpha\beta).x=\alpha.(\beta.x)$.
- $\forall\alpha\in\mathbb{K}$, $\forall(x,y)\in E^2$: $\alpha.(x+y)=\alpha.x+\alpha.y$.
- $\forall x\in\mathbb{K}$: $1.x=x$.

En toute rigueur un espace vectoriel devrait être un triplet $(E,+,.)$, voire même un quadruplet $(E,+,.,(\mathbb{K},+,\times))$. On remarquera en particulier que lorsqu'on calcule dans un espace vectoriel on calcule avec une addition interne sur E et une autre sur $\mathbb{K}$. Ce ne sont pas les mêmes opérations, même si elle sont notées par le même symbole $+$. De même il y a deux mutiplications, une multiplication interne sur $\mathbb{K}$ et une multiplication externe sur E à opérateurs dans $\mathbb{K}$. Très souvent ces lois sont sous-entendues par juxtapositions des variables.

Il y a donc un risque de confusion. Pour augmenter l'information contenue dans une formule il est donc traditionnel, et nous nous efforcerons de respecter cette tradition, d'utiliser les lettres grecques pour les scalaires et les lettres latines pour les vecteurs.

On écrit donc par exemple $(\alpha+\beta)x=\alpha x+\beta x$ au lieu de l'écriture plus précise mais trop lourde :

$$(\alpha+_{\mathbb{K}}\beta).x=\alpha.x+_E\beta.x$$

Retenez qu'une expression $\alpha+x$ heurte un lecteur mathématicien, car pour lui α est plutôt un scalaire et x un vecteur. Que dire si α est effectivement un scalaire et x un vecteur !

De même une expression $x\alpha$ n'a pas beaucoup de sens car la multiplication externe est une multiplication à gauche.

A.2 Bases

On peut supposer que les espaces vectoriels considérés dans ce chapitre sont des espaces vectoriels sur un sous-corps $\mathbb{K}$ de $\mathbb{C}$ (convention du programme). Mais il nous suffira de choisir un corps commutatif de caractéristique différente de 2.

A.2.1 Familles à support fini

Une famille $(\lambda_i)_{i\in I}$ d'éléments d'un groupe commutatif est dite à support fini si et seulement si l'ensemble des i pour lesquels $\lambda_i\neq 0$ est fini. On peut parler d'une famille de vecteurs à support fini, d'une famille de scalaires à support fini. Remarquons que la famille $(\lambda_i x_i)$ est à support fini si l'une des deux familles (λ_i) ou (x_i) est à support fini (mais la réciproque n'est pas vraie).

1. Dans le programme, et cela correspond au consensus actuel entre les mathématiciens, un corps est toujours commutatif. Cela n'a pas toujours été le cas. Auparavant on parlait de corps pour désigner un anneau avec élément unité (maintenant les anneaux sont aussi supposé unitaires) dans lequel tout élément non nul est inversible. L'appellation actuelle pour un tel objet est « algèbre à division ».

Par exemple, l'ensemble $\mathbb{K}[X]$ est l'ensemble des suites d'éléments de $\mathbb{K}$, à support fini.

Soit $(x_i)_{i\in I}$ une famille à support fini d'éléments d'un groupe commutatif, notons K l'ensemble des i tels que $\lambda_i \neq 0$. Si J est une partie de I contenant K alors $\sum_{i\in J} x_i = \sum_{i\in K} x_i$. Le membre de gauche est indépendant de J on le note $\sum_{i\in I} x_i$.

On vérifie facilement que dans un groupe commutatif, si $(x_i)_{i\in I}$ et $(y_i)_{i\in I}$ sont deux familles à support fini alors il en est de même de $(x_i + y_i)_{i\in I}$ et

$$\sum_{i\in I}(x_i + y_i) = \sum_{i\in I} x_i + \sum_{i\in I} y_i.$$

Dans un espace vectoriel on pourra de même multiplier par un scalaire.

Soit $(\lambda_i)_{i\in I}$ une famille de scalaires à support fini, $(x_i)_{i\in I}$ une famille quelconque de vecteurs, la famille $(\lambda_i x_i)_{i\in I}$ est à support fini et sa somme $\sum_{i\in I} \lambda_i x_i$ s'appelle une combinaison linéaire des (x_i).

Proposition A.1 *Si S est une partie d'un espace vectoriel, le sous-espace vectoriel engendré par S est l'ensemble des combinaisons linéaires $\sum_{s\in S} \lambda_s s$.*

A.2.2 Familles libres, génératrices ; bases

Définition A.2 *Une famille $(x_i)_{i\in I}$ d'éléments de l'espace vectoriel E est libre si et seulement si la seule famille à support fini de scalaires $(\lambda_i)_{i\in I}$ pour laquelle $\sum_{i\in I} \lambda_i x_i = 0$ est la famille nulle.*

Notons $\mathbb{K}^{(I)}$ l'ensemble des familles à support fini d'éléments de $\mathbb{K}$, alors formellement la famille $(x_i)_{i\in I}$ d'éléments de l'espace vectoriel E est libre si et seulement si :

$$\forall(\lambda_i) \in \mathbb{K}^{(I)} : \quad \sum_{i\in I} \lambda_i x_i = 0 \Rightarrow \forall i \in I \ \lambda_i = 0.$$

Une famille de vecteurs qui n'est pas libre est dite liée.

Exemple : la famille $(e^{cx})_{c\in\mathbb{C}}$ est libre.

Définition A.3 *Un famille $(x_i)_{i\in I}$ de vecteurs de l'espace vectoriel E est génératrice si et seulement si l'ensemble $\{x_i ; i \in I\}$ engendre E.*

Ceci s'écrit formellement :

$$\forall x \in E\ \exists(\lambda_i) \in \mathbb{K}^{(I)} \quad x = \sum_{i\in I} \lambda_i x_i.$$

Définition A.4 *Une famille de vecteurs qui est à la fois libre et génératrice s'appelle une base.*

Ceci s'écrit formellement :

$$\forall x \in E\ \exists!\, (\lambda_i) \in \mathbb{K}^{(I)} \quad x = \sum_{i\in I} \lambda_i x_i.$$

Les λ_i s'appelle les coordonnées (ou composantes) de x dans dans la base.

Exemple (officiel) : la famille $(X^n)_{n\in\mathbb{N}}$ est une base de $\mathbb{K}[X]$.

Exemple (officiel) : on note $\mathbb{K}[x_1, \dots, x_n]$ la sous-algèbre des fonctions numériques engendrée par les fonctions

$$(x_1, \dots, x_n) \mapsto x_k,\ 1 \leq k \leq n.$$

Si $\mathbb{K}$ est infini, une base de cet espace vectoriel est la famille

$$(x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n})_{(i_1,\dots,i_n)\in N^n}.$$

A.2.3 Bases et applications linéaires

Une application linéaire d'un espace vectoriel E vers un espace vectoriel F est un morphisme d'espaces vectoriel. C'est donc une application f vérifiant :

$$\forall(x, y, \lambda) \in E^2 \times \mathbb{K} \quad f(x + y) = f(x) + f(y), \quad f(\lambda x) = \lambda f(x).$$

Proposition A.2 *Donnons nous une base $(e_i)_{i\in I}$ de vecteurs d'un espace vectoriel E (sur $\mathbb{K}$) et une famille $(f_i)_{i\in I}$ d'éléments d'un espace vectoriel F(sur $\mathbb{K}$). Il existe une unique application linéaire f de E vers F telle que pour tout i on ait $f(e_i) = f_i$.*

C'est l'application telle que pour toute famille $(\lambda_i) \in K^{(I)}$:

$$f(\sum_{i\in I} \lambda_i e_i) = \sum_{i\in I} \lambda_i f_i.$$

Cette application est injective si la famille $(f_i)_{i\in I}$ est libre, surjective si elle est génératrice. C'est un isomorphisme si la famille est une base.

A.3 Sommes, sommes directes

A.3.1 Somme d'une famille de sous-espaces

Définition A.5 *Soit $(E_i)_{i\in I}$ une famille (finie) de sous-espaces vectoriels de E. On appelle somme de ces sous-espaces le plus petit sous-espace vectoriel de E qui contient la réunion des E_i. On le note $\sum_{i\in I} E_i$. Il est formé des sommes $\sum_{i\in I} x_i$ (à support fini dans le cas où l'ensemble I n'est pas fini), où pour tout i l'élément x_i appartient à E_i.*

Définition A.6 *Avec les mêmes notations, les conditions suivantes sont équivalentes :*

$$\begin{cases} \forall j \in I \quad E_j \bigcap \sum_{i\in I-\{j\}} E_i = \{0\}, \\ \forall (x_i) \in E^{(I)} \quad (\sum_{i\in I} x_i = 0 \text{ et } \forall i \in I\, x_i \in E_i) \Rightarrow \forall i \in I\ x_i = 0, \\ \forall x \in \sum_{i\in I} E_i\, \exists!(x_i) \in E^{(I)} \quad \forall i \in I\ x_i \in E_i) \text{ et } x = \sum_{i\in I} x_i. \end{cases}$$

Si ces hypothèses sont vérifiées on dit que la somme des E_i est directe et on écrit :

$$\sum_{i\in I} E_i = \bigoplus_{i\in I} E_i.$$

Exemple : deux sous-espaces.

Exemple : trois sous-espaces.

Définition A.7 *Soit F un sous-espace vectoriel de E, tout sous-espace G de E tel que $F \oplus G = E$ s'appelle un supplémentaire de F. On dit aussi que F et G sont supplémentaires.*

Attention ! Ne pas confondre supplémentaire et complémentaire.

A.3.2 Cas de la dimension finie

Par définition un espace vectoriel est de dimension finie s'il possède un système générateur fini. Il possède alors une base de cardinal fini et toute les bases ont le même cardinal. Ce cardinal s'appelle la dimension de l'espace.

Dans un espace vectoriel E de dimension finie n, on a les résultats suivants :
- Toute famille génératrice possède au moins n vecteurs, et si elle possède n vecteurs c'est une base de E.
- Toute partie libre possède au plus n vecteurs, et si elle possède n vecteurs c'est une base.
- Toute partie libre (même vide) peut être complétée en une base en extrayant des vecteurs d'une famille génératrice. (En particulier de toute famille génératrice on peut extraire une base).
- Tout sous espace vectoriel F de est de dimension finie et inférieure à n.
- Deux sous-espaces vectoriels de E sont égaux si l'un contient l'autre et ils sont de même dimension.
- Si F est un autre espace de dimension finie, il en est de même de $\mathcal{L}(E, F)$ et $E \times F$, qui sont de dimensions $\dim E.\dim F$ et $\dim E + \dim F$.

Si $(E_i)_{1\leq i\leq p}$ est une famille finie de sous-espaces de dimension finie, alors leur somme est de dimension finie, au plus égale à la somme des dimensions des sous-espaces considérés. De plus la somme est directe si et seulement si la dimension de la somme est égale à la somme des dimensions.

Plus précisément on a le théorème des quatre dimensions :

Théorème A.1 (théorème des quatre dimensions) *Si F et G sont deux sous-espaces vectoriel de dimension finie, il en est de même de $F + G$ et $F \cap G$ et :*

$$\dim F + \dim G = \dim(F + G) + \dim(F \cap G).$$

Théorème A.2 *Si $(E_i)_{i\in I}$ est une famille finie de sous-espaces en somme directe d'un espace vectoriel E alors*

$$\dim \bigoplus E_i = \sum \dim E_i$$

De plus $E = \bigoplus E_i$ si et seulement $\dim E = \sum \dim E_i$.

Proposition A.3 *Dans un espace vectoriel de dimension finie, tout sous-espace admet au moins un supplémentaire.*

Remarque : il en admet généralement une infinité.

Un exemple officiellement au programme : Dans $\mathbb{K}[X]$ l'idéal engendré par un polynôme de degré $n+1$ est un sous-espace vectoriel qui admet pour supplémentaire l'ensemble $\mathbb{K}_n[X]$ des polynômes de degré inférieur ou égal à n.

A.3.3 Bases adaptées

Définition A.8 *Une base $(e_1, \dots, e_n)$ d'un espace vectoriel E (de dimension finie) est adaptée au sous espace F de E s'il existe un p tel que $(e_1, \dots, e_p)$ soit une base de F. Elle est adaptée à la décomposition $E = F \oplus G$ si il existe p tel que $(e_1, \dots, e_p)$ soit une base de F et $(e_{p+1}, \dots, e_n)$ une base de G*

Une telle définition s'étend facilement à celle d'une base adaptée à une décomposition en somme directe de r sous-espaces. Si $E = \bigoplus_{1\leq i\leq r} E_i$ on obtient une base adaptée à cette décomposition en concaténant des base $\mathcal{B}_1, \dots, \mathcal{B}_r$ des E_i. En particulier il existe toujours au moins une base adaptée.

A.4 Recollement d'applications linéaires

Si $E = \bigoplus_{i\in I} E_i$ et si $(u_i)_{i\in I}$ est une famille d'applications linéaires de E_i vers F, alors il existe une unique application linéaire de E vers F dont la restriction à chaque E_i soit u_i.

Un exemple : Si $E = \bigoplus_{1\leq i\leq r} E_i$, il existe une unique application linéaire p_i telle $p_i(x) = x$ si x appartient à E_i et $p_i(x) = 0$ si x appartient à E_j, $i \neq j$. p_i est la projection sur E_i parallèlement à $\bigoplus_{j\neq i} E_j$. La famille $(p_1, \dots, p_r)$ vérifie

1. $\forall i\ p_i \circ p_i = p_i$ (p_i est un projecteur) ;
2. pour $i \neq j$ $p_i \circ p_j = 0$;
3. $\mathrm{Id}_E = p_1 + \cdots + p_r$.

Réciproquement si on se donne une famille $(p_1, \dots, p_r)$ d'applications linéaires vérifiant les relations précédentes, alors E est la somme directe de Im p_i et p_i est la projection sur Im p_i parallèlement à Ker $p_i = \bigoplus_{j\neq i} E_j$.

A.5 Image et noyau d'une application linéaire

On rappelle que le noyau Ker $f = \{x; f(x) = 0\}$ et l'image Im $f = f(E) = \{f(x); x \in E\}$ d'une application linéaire f sont des sous-espaces vectoriels de E et F. f est injective si et seulement si Ker $f = \{0\}$, surjective si et seulement si Im $f = F$.

Exercice : D'un manière plus générale, prouver que l'image d'un sous-espace vectoriel et l'image réciproque d'un sous-espace vectoriel sont des sous-espaces vectoriels.

Exemple : Soit $(x_1, \dots, x_p)$ une famille de vecteurs de E, l'application

$$\begin{array}{cccc} f & : & \mathbb{K}^p & \to & E \\ & & (\lambda_1, \dots, \lambda_p) & \mapsto & \sum_{k=1}^p \lambda_k x_k \end{array}$$

est linéaire. Elle est injective si et seulement si $(x_1, \dots, x_p)$ est libre, surjective si et seulement si $(x_1, \dots, x_p)$ est génératrice. C'est un isomorphisme si et seulement si $(x_1, \dots, x_p)$ est une base de E.

Théorème A.3 *Si u est une application linéaire de E vers F, la restriction de u à tout supplémentaire de* Ker *u définit un isomorphisme de ce supplémentaire sur* Im *u.*

Remarque : il n'est pas besoin de supposer les espaces de dimension finie.

Application : Le théorème du rang.

Théorème A.4 (Le théorème du rang) *Si u est une application linéaire d'un space de dimension finie E vers un espace F, qui n'est pas supposé de dimension finie, alors* Im *u est de dimension finie et en notant* $\mathrm{rg}\,(u) = \dim \mathrm{Im}\ u$ *(le rang de u) on a :*

$$\dim E = \dim \mathrm{Ker}\ u + \mathrm{rg}\ u.$$

Rappel : caractérisation des applications linéaires injectives, surjectives et bijectives en dimension finie.

A.5.1 Application : Le polynôme d'interpolation de Lagrange

A.5.1.1 Première version

Soit $(a_0, \ldots, a_n)$ $n+1$ éléments disctincts du corps $\mathbb{K}$. L'application

$$\begin{array}{ccccc} \phi & : & \mathbb{K}[X] & \to & \mathbb{K}^{n+1} \\ & & P & \mapsto & (P(a_0), \ldots, P(a_n)) \end{array}$$

est linéaire. D'après le théorème de Gauss son noyau est l'idéal engendré par $T = (X-a_0)\cdots(X-a_n)$. Un supplémentaire de ce sous-espace est $\mathbb{K}_n[X]$, ϕ réalise donc un isomorphisme de $\mathbb{K}_n[X]$ sur son image. Celle-ci est par conséquent de dimension $n+1$, et donc égale à $\mathbb{K}^{n+1}$.Ceci prouve que ϕ est un isomorphisme. Il en résulte :

$$\forall (y_0, \ldots, y_n) \in \mathbb{K}^{n+1} \quad \exists ! P \in \mathbb{K}_n[X] \quad \forall i \in [0,n] \ P(a_i) = y_i.$$

Si les y_i sont les valeurs d'une fonction en les a_i, on dit que P est le polynôme d'interpolation de Lagrange de f en ces points.

L'inconvénient de cette version est qu'elle n'est pas constructive. Elle ne nous donne pas directement le polynôme. Son avantage est qu'elle peut s'adapter pour obtenir un polynôme d'interpolation à un ordre supérieur.

A.5.1.2 Deuxième version

Elle peut déjà avoir été vue lors d'une extension du lemme des restes chinois aux polynômes.

Il s'agit en fait de résoudre les congruences

$$P \equiv y_i \bmod (X - a_i),\ 0 \le i \le n.$$

Puisque les $(X - a_i)$ sont premiers entre eux deux à deux, d'après le lemme des restes chinois il existe une unique solution modulo T. Ceci ce démontre d'ailleurs directement : deux solutions sont congrues modulo T et si P tout polynôme congru à p modulo T est aussi une solution ; il suffit donc d'obtenir une solution. Pour cela on adapte la méthode de Gauss pour les entiers à $\mathbb{K}[X]$. On cherche une famille de polynômes L_i tels que pour tout i on ait $L_i \equiv 1 \bmod (X - a_i)$ et pour j différent de i $L_i \equiv 0 \bmod (X - a_j)$. Un tel polynôme de degré inférieur ou égal à n est nécessairement de la forme

$$L_i = \lambda \prod_{j \ne i} (X - a_j),$$

la condition $L_i \equiv 1 \bmod (X - a_i)$ conduisant finalement à

$$L_i = \frac{\prod_{j \ne i}(X - a_j)}{\prod_{j \ne i}(a_i - a_j)}.$$

Une solution du système de congruences est

$$\sum_{i=0}^{n} y_i L_i = \sum_{i=0}^{n} y_i \frac{\prod_{j \ne i}(X - a_j)}{\prod_{j \ne i}(a_i - a_j)}.$$

C'est bien un polynôme de degré inférieur ou égal à n.

A.5.1.3 Troisième version

Résolution directe d'un système , en utilisant un déterminant de Vandermonde [2].

Proposition A.4 *Soit E' un sous-espace vectoriel de l'espace vectoriel E. Soient F_1 et F_2 deux supplémentaires de E', alors la projection de E sur F_1 parallèlement à E' induit un isomorphisme de F_2 sur F_1*

Définition A.9 *On dit qu'un sous-espace F de E est de codimension finie si il admet un supplémentaire de dimension finie. Sa codimension est la dimension de ce supplémentaire.*

Remarque : d'après la proposition précédente tous les supplémentaires ont même dimension, la définition est donc cohérente.

Remarque : on peut montrer qu'un sous-espace F est de codimension finie si et seulement si il existe G de dimension finie tel que $F + G = E$.

2. Vandermonde Alexandre Paris 1735-Paris 1796

Définition A.10 *Un sous-espace de codimension* 1 *s'appelle un hyperplan.*

Proposition A.5 *Si F est un sous-espace d'un espace de dimension finie E alors*

$$\dim F + \operatorname{codim} F = \dim E.$$

Proposition A.6 *Soit u une application linéaire de E vers F, où F est un sous-espace de dimension finie. Son noyau est de codimension finie et l'on a :*

$$\operatorname{rg}\ u = \dim \operatorname{Im}\ u = \operatorname{codim}\ \operatorname{Ker}\ u.$$

Remarque : dans la proposition précédente, l'existence du supplémentaire doit être justifiée, il ne suffit pas de démontrer qu'un tel supplémentaire est de dimension finie.

A.6 L'espace dual

Définition A.11 *Soit E un espace vectoriel sur K. Le dual de E est l'espace vectoriel des formes linéaires sur E, noté E^*.*

Exemple de forme linéaire : $\delta_a : f \mapsto f(a)$

Proposition A.7 *Soit H un sous-espace vectoriel. H est un hyperplan si et seulement si il existe une forme linéaire non nulle φ telle que $H = \operatorname{Ker}\ \varphi$. De plus les formes linéaires ayant cette propriété sont exactement les multiples de φ. On dit que φ est une équation de H.*

Définition A.12 *L'application de $E^* \times E$ vers $\mathbb{K}$, qui à (ϕ, x) associe le scalaire $< \phi, x >= \phi(x)$ est une forme bilinéaire, dite canonique. On parle aussi parfois du crochet de dualité.*

A.7 Dualité en dimension finie

Théorème A.5 *Si E est de dimension finie alors le dual de E est de dimension finie et il est de même dimension que E.*

En effet, la dimension de $L(E, F)$ est finie si E et F sont de dimension finie, et sa valeur est $(\dim E) \times (\dim F)$. Il suffit ici d'appliquer ce résultat avec $F = \mathbb{K}$.

Remarque : E et son dual sont donc isomorphes.

Proposition A.8 *Si $\mathcal{B} = (e_1, \ldots, e_n)$ est une base de E, il existe un unique n-uplet $(e_1^*, \ldots, e_n^*)$ de E^* tel que pour tout couple (i, j) on ait : $e_j^*(e_i) = \delta_{i,j}$. Ce n-uplet est une base de E^* dite base duale de $(e_1, \ldots, e_n)$, notée $\mathcal{B}^*$.*

L'existence du n-uplet résulte de ce que toute application linéaire est définie de manière unique par l'image d'une base, donc chaque e_j^* existe et est unique. Soit y^* un élément de E^*, s'il s'écrit sous la forme $a_1 e_1^* + ... + a_n e_n^*$, alors pour tout i on aura $y^*(e_i) = a_1 e_1^*(e_i) + \cdots + a_n e_n^*(e_i) = a_i$, donc les a_i sont déterminés de manière unique et le n-uplet est libre. D'après le théorème précédent, la dimension de $E*$ est n, donc le n-uplet, système libre de cardinal n est une base. On peut aussi remarquer que le système est générateur, puisque l'élément $y^*(e_1)e_1 * + ... + y^*(e_n)e_n *$ possédant même image que y^* sur une base de E lui est égal.

Remarque : On démontre à nouveau ainsi le théorème précédent. Un isomorphisme étant celui qui transforme une base en sa base duale. Cet isomorphisme n'est pas canonique, il dépend de la base initialement choisie.

Proposition A.9 *Si x est un élément non nul de E, il existe une forme linéaire φ telle que $\phi(x) = 1$.*

Corollaire A.1 *Le seul vecteur annulé par toutes les formes linéaires est le vecteur nul.*

Proposition A.10 *Si $\mathcal{B} = (\phi_1, \ldots, \phi_n)$ est une base de E^*, il existe un unique n-uplet $(e_1, \ldots, e_n)$ de E tel que pour tout couple (i, j) on ait : $\phi_j(e_i) = \delta_{i,j}$. Ce n-uplet est une base de E dite base anté-duale de $(\phi_1, \ldots, \phi_n)$.*

Proposition A.11 *Si F est un sous-espace de E de dimension p l'ensemble des formes linéaires s'annulant sur F est un sous-espace de E^* de dimension $n - p$.*

Proposition A.12 *Soit $(\phi_1, \ldots, \phi_q)$ est une famille libre de formes linéaires sur un espace E de dimension n, l'intersection des noyaux des ϕ_i est un sous-espace vectoriel F de E de dimension $n - q$. Une forme linéaire est nulle sur F si et seulement si elle une combinaison linéaire des ϕ_i.*

A.8 Trace d'un endomorphisme

Définition A.13 *Si $A = (a_{i,j}$ est une matrice carrée appartenant à $M_n(\mathbb{K})$, on appelle trace de A le nombre* $\operatorname{tr}(A) = \sum_{i=1}^{n} a_{i,i}$

Proposition A.13 *L'application*

$$\begin{array}{cccc} \operatorname{tr} & : & M_n(\mathbb{K}) & \to & \mathbb{K} \\ & & A & \mapsto & \operatorname{tr} A \end{array}$$

est une forme linéaire.

Exercice. Montrer que toute forme linéaire sur $M_n(\mathbb{K})$ est de la forme $\varphi_A : M \mapsto \operatorname{tr} AM$.

Proposition A.14 *Si A et B sont deux matrices de $M_n(K)$,* $\operatorname{tr}(AB) = \operatorname{tr}(BA)$.

Exercice : montrer que ce résultat reste vrai si A appartient à $M_{n,p}(\mathbb{K})$ et B à $M_{p,n}(\mathbb{K})$.

Corollaire A.2 *Si P est une matrice inversible de $M_n(\mathbb{K})$ et A une matrice de $M_n(\mathbb{K})$ alors* $\operatorname{tr}(P^{-1}AP) = \operatorname{tr}(A)$.

Application : si u est un endomophisme de E. La trace de la matrice de u dans une base $\mathcal{B}$ ne dépent pas de $\mathcal{B}$. On l'appelle la trace de u, toujours notée tr u.

Proposition A.15 *L'application*

$$\begin{array}{cccc} \operatorname{tr} & : & \mathcal{L}(E) & \to & \mathbb{K} \\ & & u & \mapsto & \operatorname{tr} u \end{array}$$

est une forme linéaire.

Proposition A.16 *Le rang d'un projecteur est égal à sa trace.*

A.9 Calcul matriciel

Rappel : matrices équivalentes, interprétation en termes d'applications linéaires. Caractérisation par le rang. Application à A et ${}^tA$. Caractérisation du rang par les mineurs.

A.9.1 Opérations élémentaires sur les lignes et les colonnes d'une matrice

Définition A.14 *Soit M une matrice de $M_{n,p}(\mathbb{K})$. Nous appellerons opération élémentaire sur la matrice M l'une des opérations suivantes :*

1. *Permutation de deux lignes de M,*
2. *Permutation de deux colonnes de M,*
3. *Ajout à une ligne d'un multiple quelconque d'une autre ligne.*
4. *Ajout à une colonne d'un multiple quelconque d'une autre colonne.*
5. *Multiplication d'une ligne par un scalaire non nul.*
6. *Multiplication d'une colonne par un scalaire non nul.*

A.9.2 Interprétation en termes de produits matriciels

Notation : On notera :

$E_{k,l,n,p}$ la matrice $(\delta_{i,k}\delta_{j,l})_{1\leq i\leq n, 1\leq j\leq p)}$, (la famille des $E_{k,l,n,p}$ est la base canonique de $M_{n,p}(\mathbb{K})$).

$D_{k,n}(\lambda)$ la matrice $I_n + (\lambda - 1)E_{k,k}$, pour $\lambda \neq 0$.

$P_{k,l,n}$ la matrice $(a_{i,j})_{1\leq i\leq n, 1\leq j\leq n)}$, pour $k \neq l$, avec $a_{i,j} = \delta_{i,j}$ sauf si $\{i,j\} = \{k,l\}$ et de plus $a_{k,l} = a_{l,k} = 1$ et $a_{k,k} = a_{l,l} = 0$.

$Tk, l, n(\lambda)$ la matrice $I_n + \lambda E_{k,l,n,n}$ pour $k \neq l$.

On remarquera que chacune de ces matrices est inversible ce qui aura une importance capitale dans la suite.

Proposition A.17 *Avec les notations précédentes, les opérations élémentaires sur une matrice $M_{n,p}(\mathbb{K})$ peuvent s'interprèter comme une multiplication à droite ou à gauche par l'une des matrices précédentes.*

1. *Permutation des lignes k et l de M : Multiplication à gauche par la matrice $P_{k,l,n}$,*
2. *Permutation des colonnes k et l de M : Multiplication à droite par la matrice $P_{k,l,p}$,*
3. *Ajout à la ligne k de λ fois la ligne l : Multiplication à gauche par la matrice $T_{k,l,n}(\lambda)$,*
4. *Ajout à la colonne l de λ fois la colonne k : Multiplication à droite par la matrice $T_{l,k,p}(\lambda)$,*
5. *Multiplication de la ligne k par le scalaire λ non nul : Multiplication à gauche par la matrice $D_{k,n}(l)$,*
6. *Multiplication de la colonne k par le scalaire λ non nul : Multiplication à droite par la matrice $D_{k,n}(l)$.*

A.9.3 Application à la recherche du rang d'une matrice

Théorème A.6 *Le rang d'une matrice ne change pas si l'on effectue sur cette matrice l'une des opérations élémentaires.*

Théorème A.7 *Il est possible par une suite d'opérations élémentaires sur les colonnes d'une matrice $M = (a_{i,j})$ de la transformer en une matrice $M' = (b_{i,j})$ telle que la fonction définie par $f(j) = \min\{i \in \{1, ..., n\}, b_{i,j} \neq 0\}$ si cet ensemble est non vide et $+\infty$ si cet ensemble vide, soit croissante sur $\{1, ..., n\}$ et strictement croissante sur $f^{-1}(\mathbb{N})$. Une telle matrice est dite échelonnée en colonnes.Le rang de la matrice M est alors le nombre de colonnes non nulles de la matrice M'.*

Remarque : Il existe un théorème similaire utilisant les transformations élémentaires sur les lignes.

A.9.4 Application à la résolution des systèmes linéaires

Définition A.15 *Si $AX = B$ est un système linéaire de n équations à p inconnues écrit sous forme matricielle, avec $A \in M_{n,p}(\mathbb{K})$, $B \in M_{n,1}(\mathbb{K})$ et $X \in M_{p,1}(\mathbb{K})$, on appellera matrice associée au système la matrice de $M_{n,p+1}(K)$ égale à $(A\,|\,B)$.*

Méthode : Pour résoudre le système $AX = B$ on transforme à l'aide de transformations élémentaires sur les lignes la matrice associée à ce système pour obtenir une matrice $M' = (c_{i,j})$ telle que la fonction f définie sur $\{1, ..., n\}$ par $f(i) = \min\{j \in \{1, ..., p+1\}, c_{i,j} \neq 0$ si cet ensemble n'est pas vide et $f(i) = +\infty$ sinon, soit croissante sur $\{1, ..., n\}$ et strictement croissante sur $f^{-1}(\mathbb{N})$. Une telle matrice est dite échelonnée en lignes. Deux cas sont alors possibles :

1. Il existe un i tel que $f(i) = p + 1$. Le système n'admet aucune solution.
2. Il n'existe pas de i tel que $f(i) = p + 1$. Le système admet alors une solution au moins. On peut obtenir toutes les solutions en exprimant les inconnues $x_{f(i)}$ pour $f(i) \neq +\infty$ à l'aide des autres inconnues par la formule :

$$c_{i,f(i)}x_{f(i)} = c_{i,p+1} - \sum_{k=f(i)+1}^{p} c_{i,k}x_k,$$

i décroissant de $r = \max\{i; f(i) \neq +\infty\}$ à 1. (Si ce max n'existe pas tout X est solution).

Remarque : r est le rang de la matrice A.

S'il est non vide, l'espace des solutions est une variété affine de dimension $p-r$. L'espace des solutions de l'équation homogène est la direction de la variété des solutions de l'équation avec second membre.

Soit $\mathcal{E} = \{1, \ldots, p\} - \mathrm{Im}\, f$, soit j dans $\mathcal{E}$, on peut construire une unique solution du système $v_j = (x_{i,j})_{1\leq i\leq p}$ en posant $x_{j,j} = 1$, $x_{i,j} = 0$ si $i \in \mathcal{E}$ et $i \neq j$, puis en calculant les $(x_{i,j}$ restants par (2). On peut prouver que (v_j) est une base de l'espace vectoriel des solutions du système homogène.

A.9.5 Application à la recherche de l'inverse d'une matrice

Théorème A.8 *Il est possible par une suite d'opérations élémentaires sur les colonnes d'une matrice inversible de la transformer en la matrice unité. Les mêmes transformations appliquées à la matrice unité la transforme en l'inverse de la matrice initiale.*

Remarque : Il est possible d'utiliser la même méthode mais en opérant sur les lignes. Mais il est interdit d'opérer simultanément sur les lignes et les colonnes.

Remarque : si la matrice n'est pas inversible on s'en aperçoit en cours de route.

Remarque : il est possible de calculer l'inverse d'une matrice en $\mathcal{O}(n^3)$ opérations.

Remarque : condition pour qu'il ne soit pas nécessaire d'utiliser de permutations ; décomposition LU.

A.9.6 Application au calcul des déterminants

Théorème A.9 *Il est possible, par une suite d'opérations élémentaires sur les colonnes d'une matrice autres que la multiplication d'une d'une colonne par un scalaire, de la transformer en une matrice diagonale inférieure. Son déterminant est alors égal au signe près au produit des termes diagonaux de cette matrice, et le signe doit être changé pour chaque permutation de colonne opérée.*

Remarque : il est possible, en n'utilisant que des transvections sur les colonnes de transformer A en $\begin{pmatrix} I_r & 0 \\ 0 & O \end{pmatrix}$ si $r < n$ est le rang de A, ou $\begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix}$.

Application : $SL(n, \mathbb{K})$ est engendré par les transvections.

Application : déterminer les applications de $M_n(\mathbb{K})$ vers $\mathbb{K}$ telles que $f(AB) = f(A)f(B)$.

A.10 Exercices

A.10.1 Applications linéaires

Exercice 1: Soit E et F deux espaces vectoriels et u une application linéaire de E vers F.

1) On suppose qu'il existe une application linéaire v de F vers E telle que $u \circ v = \mathrm{id}_F$. Montrer que u est surjective et que $E = \mathrm{Ker}\ u \oplus \mathrm{Im}\ v$.

Réciproquement : si u est surjective et si $E = \mathrm{Ker}\ u \oplus E'$, alors il existe une application linéaire v, de F vers E, et une seule telle que $u \circ v = \mathrm{id}_F$ et $\mathrm{Im}\ v = E'$.

2) On suppose qu'il existe une application linéaire v de F vers E telle que $v \circ u = \mathrm{id}_E$. Montrer que u est injective et que $E = \mathrm{Ker}\ v \oplus \mathrm{Im}\ u$.

Réciproquement : si u est injective et si $F = \mathrm{Im}\ u \oplus F'$, alors il existe une application linéaire v, de F vers E, et une seule telle que $v \circ u = \mathrm{id}_E$ et $\mathrm{Ker}\ v = F'$.

Annexe B

Rappels de notions générales

B.1 Théorie des ensembles

B.1.1 Vocabulaire de la théorie des ensembles

On considère comme connu le sens les symboles courants. $\cup$, $\cap$, Δ, $\exists$, $\forall$, $\mathcal{P}(E)$.
Reamrquer que $\exists$ se prononce dans la plupart des cas « appartenant à »et non pas « appartient ».

Définition B.1 *Si A est une partie de l'ensemble E, sa fonction caractéristique, notée χ_A est la fonction de E vers $\mathbb{R}$ telle que $\chi_A(x) = 1$ si x appartient à A, 0 sinon.*

Ex 2:

1) Déterminer les fonctions caractéristique de la réunion, de l'intersection, du complémentaire de la différence symétrique de deux parties A et B de E à l'aide des fonctions caractéristiques de A et B.
2) Montrer que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif.

Ex 3:

1) En remarquant que si E est un ensemble fini et A une partie de E on a

$$\operatorname{Card} A = \sum_{x \in E} \chi_A(x)$$

déterminer $\operatorname{Card} A \cup B$, $\operatorname{Card} E - A$ et $\operatorname{Card} A \Delta B$ à l'aide de $\operatorname{Card} A$, $\operatorname{Card} B$ et $\operatorname{Card} A \cap B$.
2) Soit $(A_1, \ldots, A_p)$ une famille de parties finies de l'ensemble E. Exprimer le cardinal de leur réunion à l'aide des cardinaux de ces ensembles et des cardinaux de leurs intersections mutuelles. On pourra commencer par expliciter la formule pour $p = 3$ et $p = 4$ avant d'essayer d'en donner une expression formelle plus générale.
3) En déduire une expression donnant le nombre de dérangements, c'est-à-dire de permutations sans point fixe d'un ensemble à n éléments.
4) En déduire une expression donnant le nombre de surjections d'un ensemble à n éléments vers un ensemble à p éléments.
5) Si $n = p_1^{m_1} \cdots p_r^{m_r}$ où $(p_1, \ldots, p_r)$ sont des nombres premiers distincts, donner une expression simple de $\phi(n)$, le nombre d'entiers compris entre 1 et n et premiers avec n.

B.1.2 Applications

Définition B.2 *Une application d'un ensemble E vers un ensemble F est un triplet $f = (E, F, G)$ où F est une partie de $E \times F$ telle que*

$$\forall x \in E \quad \exists! y \in F \ (x, y) \in G$$

Si $f = (E, F, G)$ est une application et si x appartient à E il existe un unique y dans F tel que (x, y) appartienne à G. On le note traditionnellement $f(x)$. On dit que f associe $f(x)$ à x, $f(x)$ s'appelle l'image de x par f. E s'appelle l'ensemble de départ, F l'ensemble d'arrivée et G le graphe de f. G est l'ensemble $\{(x, f(x)); x \in E\}$. La représentation simplifiée d'une application est $f : E \to F$ ou

$$\begin{array}{cccc} f & : & E & \to & F \\ & & x & \mapsto & f(x) \end{array}$$

Exemple Id_E est l'application

$$\begin{array}{cccc} \mathrm{Id}_E & : & E & \to & E \\ & & x & \mapsto & x \end{array}$$

Ex 4:

Soient u dans $\mathcal{L}(F, H)$ et v dans $\mathcal{L}(G, H)$, où H est un espace vectoriel, F et G deux sous-espaces de l'espace vectoriel de dimension finie E tels que $E = F + G$. Montrer

$$\big(\exists w \in \mathcal{L}(E, H)\ w_{|F} = u \text{ et } w_{|G} = v\big) \Longleftrightarrow u_{|F\cap G} = u_{|F\cap G}$$

Définition B.3 *Une fonction d'un ensemble E vers un ensemble F est un triplet $f = (E, F, G)$ où F est une partie de $E \times F$ telle que*

$$\forall x \in E \quad ((x, y) \in G \text{ et} (x, y') \in G) \Rightarrow y = y'$$

L'ensemble $\{x \in E; \exists y \in f\ (x, y) \in G\}$ s'appelle alors le domaine de définition de la fonction f.

On se reportera au cours de première année pour la définition formelle de la composée de deux applications.

Définition B.4 *Une application $f : E \to F$ est injective si et seulement si*

$$\forall (x, y) \in E^2 \quad f(x) = f(y) \Rightarrow x = y.$$

Définition B.5 *Une application $f : E \to F$ est surjective si et seulement si*

$$\forall y \in F\ \exists x \in E\ y = f(x).$$

Définition B.6 *Une application $f : E \to F$ est bijective si et seulement si elle vérifie une des deux conditions équivalentes suivantes :*

1. $\forall y \in F\ \exists! x \in E\ y = f(x)$,
2. *f est injective et surjective.*

On peut alors définir une application $g : F \to E$ qui à x de F associe l'unique élément y de E tel que $f(y) = x$. On l'appelle la réciproque de f et on la note f^{-1}.

Définition B.7 *Si $f : E \to F$ est une application, si A est une partie de E, l'image de A par f, notée $f(A)$, est l'ensemble : $\{f(x); x \in A\}$ ou $\{y \in F; \exists x \in A\ y = f(x)\}$.*

Définition B.8 *Si $f : E \to F$ est une application, si A est une partie de E, l'image réciproque de B par f, notée $f^{-1}(B)$ est l'ensemble :$\{x \in E; f(x) \in B)\}$.*

L'image réciproque par une application f d'une partie de F existe toujours, même si f n'est pas bijective. Si f est bijective, la notation $f^{-1}(B)$ désigne deux objets a priori différents : l'image réciproque de B par f et l'image directe de B par f^{-1}. Fort heureusement ces deux parties sont égales.

Ex 5:

Comparer $f(A\cap B)$ et $f(A)\cap f(B)$, $f(A\cup B)$ et $f(A)\cup f(B)$, $f^{-1}(A\cap B)$ et $f^{-1}(A)\cap f^{-1}(B)$, $f^{-1}(A\cup B)$ et $f^{-1}(A)\cup f^{-1}(B)$, $f(f^{-1}(A))$ et A, $f^{-1}(f(A))$ et A. Dans quels cas (condition sur f) a-t-on égalité pour tout couple (A, B) de parties ?

B.2 Relations

B.2.1 Relations sur un ensemble

Définition B.9 *Une relation sur un ensemble E est une partie de $E \times E$. Si $\mathcal{R}$ est une relation sur E, on écrira $x\mathcal{R}y$ plutôt que $(x, y) \in \mathcal{R}$.*

B.2.2 Relations d'équivalence

Définition B.10 *Une relation est une relation d'équivalence si et seulement si elle est réflexive, symétrique et transitive.*

Une relation $\mathcal{R}$ sur E est donc une relation d'équivalence si et seulement si :

réflexivité

$$\forall x \in E \quad x\mathcal{R}x$$

symétrie

$$\forall (x,y) \in E^2 \quad x\mathcal{R}y \Rightarrow x\mathcal{R}y$$

transitivité

$$\forall (x,y,z) \in E^3 \quad x\mathcal{R}y \text{ et } y\mathcal{R}z \Rightarrow x\mathcal{R}z$$

B.2.3 Relation d'ordre

Définition B.11 *Une relation est une relation d'ordre si et seulement si elle est réflexive, antisymétrique et transitive.*

Une relation $\mathcal{R}$ sur E est donc une relation d'ordre si et seulement si :

réflexivité

$$\forall x \in E \quad x\mathcal{R}x$$

antisymétrie

$$\forall (x,y) \in E^2 \quad x\mathcal{R}y \text{ et } y\mathcal{R}x \Rightarrow x = y$$

transitivité

$$\forall (x,y,z) \in E^3 \quad x\mathcal{R}y \text{ et } y\mathcal{R}z \Rightarrow x\mathcal{R}z$$

Un couple $(E, \leq)$ où $\leq$ est une relation d'ordre sur E s'appelle un ensemble ordonné. On dit aussi qu'on a défini un ordre sur E.

Définition B.12 *Une relation $\leq$ sur E est une relation d'ordre total si et seulement si*

$$\forall (x,y) \in E^2 \quad x \leq y \text{ ou } y \leq x.$$

Une relation qui n'est pas d'ordre total est dite d'ordre partiel. On parle aussi d'ensemble totalement ordonné ou d'ensemble partiellement ordonné.

Dans la suite de cette section E désigne un ensemble ordonné par la relation $\leq$.

Définition B.13 *Un élément a de E est un majorant (resp. minorant) de l'ensemble A si et seulement si*

$$\forall x \in A \quad x \leq a \text{ (resp. } \forall x \in A \quad a \leq x).$$

Si a appartient à A il est alors unique. On dit qu'il s'agit du maximum (resp. minimum) de A, ou du plus grand élément (resp. du plus petit élément) de A. On le note $\max A$ (resp. $\min A$).

Définition B.14 *Soit A une partie de E. Si l'ensemble des majorants (resp. minorants) de A possède un plus petit (resp. un plus grand) élément on dit que A possède une borne supérieure. On la note $\sup A$ (resp. $\inf A$).*

Proposition B.1 *Caractérisation de la borne supérieure. Soit A une partie d'un ensemble ordonné E. Un élément M de E est la borne supérieure de A si et seulement si :*
- $\forall x \in A \quad x \leq M$
- $\forall y \in E \ (\forall x \in A \ x \leq y) \Rightarrow M \leq y$.

Dans le cas ou l'ensemble est totalement ordonné (par exemple dans le cas usuel de $\mathbb{R}$) la caractérisation prend une forme plus facile à utiliser.
- $\forall x \in A \quad x \leq M$
- $\forall y \in E \ y < M \Rightarrow \exists x \in A \ y < x$.

Exemples : pgcd et ppcm de deux entiers non nuls, somme et intersection de deux sous-espaces.

Ex 6:

Soit E un ensemble totalement ordonné, A et B deux parties de E admettant des bornes supérieures. Prouver :

$$\sup A \leq \sup B \Leftrightarrow \big(\forall x \in E \ x < \sup A \Rightarrow x \leq \sup B\big)$$

Définition B.15 *Si E est un ensemble ordonné, un élément m de A est un élément minimal de A si et seulement si*

$$x \leq m \text{ et } x \in A \Rightarrow x = m.$$

On définit symétriquement la notion d'élément maximal.

Dans un ensemble totalement ordonné les notions d'élément maximal ou d'élément maximum sont équivalentes. Mais dans un ensemble partiellement ordonné tout élément maximum est maximal, mais la réciproque est fausse.
Exemples : nombres premiers, droites et hyperplans.

B.3 $\mathbb{N}$ et le dénombrement

Il existe une définition axiomatique de l'ensemble $\mathbb{N}$ des entiers naturels, voir pour cela les axiones de Zermelo-Fraenkel (note [1]). Une définition compréhensible avec les connaissances d'un élève de classe préparatoire peut être celle-ci :
Deux ensembles sont dits équipotents s'il existe une bijection de l'un sur l'autre. Un ensemble est infini s'il est équipotent à une partie stricte de lui même. Un ensemble est fini si et seulement si il n'est pas infini. La relation d'équipotence sur les ensembles est une relation d'équivalence. Une classe d'équivalence pour cette relation s'appelle un cardinal. On admet que la collection des cardinaux finis est un ensemble qui s'appelle l'ensemble des entiers naturels, noté $\mathbb{N}$. On peut définir sur $\mathbb{N}$ une addition, une multiplication et une relation d'ordre total compatible avec l'addition et la multiplication. De plus pour cette relation d'ordre toute partie non vide possède un plus petit élément (on dit que $\mathbb{N}$ est bien ordonné). $\mathbb{N}$ est infini.

B.3.1 Coefficients du binôme

Parties d'un ensemble fini L'ensemble des parties à p éléments d'un ensemble à n éléments est un ensemble fini. Son cardinal se note $\binom{n}{p}$ ou anciennement C_n^p (note [2].

On a $\binom{n}{p} = \dfrac{n!}{p!(n-p)!} = \dfrac{n(n-1)\cdots(n-p+1)}{p!}$. En particulier $n \mapsto \binom{n}{p}$ est une fonction polynomiale de n de degré p. On verra que cela permet d'étendre sa définition à des valeurs de n non entières.

Coefficients du binôme

Proposition B.2 *(Relations entre les coefficients binomiaux.) On a les relations importantes :*

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

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

et

$$\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1}$$

pour $n \geq 1$ et $p \geq 1$.

Ex 7:

Ecrire deux programmes, dans le langage de votre choix, permettant de calculer $\binom{n}{p}$ en utilisant les relations précédentes. Comparer les vitesses d'exécution de ces programmes. Expliquer cette différence.

Proposition B.3 *(Formule du binôme dans un anneau non nécessairement commutatif.) Si x et y sont deux éléments d'un anneau qui commutent et n un entier*

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

1. Enst Zermelo, Berlin 1871, Fribourg-en-Brisgau 1953, allemand — Adolf Abraham Fraenkel,Munich 1891, Jérusalem 1965, mathématicien israélien d'origine allemande

2. En toute rigueur $\binom{n}{p}$, le symbole anglo-saxon devenu international, désigne les coefficients du binôme, et C_n^p le nombre de combinaisons à p éléments dans un ensemble à n éléments. Or ces deux nombres sont égaux ce qui explique la disparition d'un des symboles

Ex 8:
On définit sur $\mathbb{R}[X]$ l'endomorphisme

$$\begin{array}{rcl} \Delta \ : \ \mathbb{R}[X] & \to & \mathbb{R}[X] \\ P & \mapsto & P(X+1)-P(X) \end{array}$$

On désigne par Δ^n son itéré à l'ordre n pour la composition. Montrer que pour tout entier n il existe une suite $(a_{k,n})$ tel que pour tout P

$$\Delta^n(P)=\sum_{k=0}^{n} a_{k,n}P(X+k).$$

Si P est degré n tel que $P(k)=r^k$ pour $0\leq k\leq n$, que vaut $P(n+1)$?

B.3.2 Ensembles dénombrables

Définition B.16 *Un ensemble E est dénombrable si il existe une injection de E vers $\mathbb{N}$ ou une surjection de $\mathbb{N}$ vers E. Si E est dénombrable et infini il existe alors une bijection de $\mathbb{N}$ sur E.*

Certains imposent à un ensemble dénombrable d'être infini, ils disent alors fini ou dénombrable dans le cas précédent.
Exemples : $\mathbb{N}$, $\mathbb{N}\times\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$. Toute réunion dénombrable d'ensembles dénombrables est dénombrable.

Ex 9:
Le parcours en spirale de la tortue dans $\mathbb{Z}^2$.

B.4 Le corps des nombres réels

Définition Le corps $\mathbb{R}$ des nombres réel est un corps totalement ordonné archimédien dans lequel toute partie non vide majorée possède une borne supérieure. Plus précisément on peut montrer qu'il existe un tel corps (il existe plusieurs constructions) et que tout corps vérifiant ces propriétés est isomorphe à $\mathbb{R}$, cet isomorphisme conservant les relations d'ordre.

Explications :
- $\mathbb{R}$ est un corps totalement ordonné car il est muni d'une relation d'ordre total telle que $0\leq x$ et $0\leq y$ implique $0\leq x+y$ et $0\leq xy$.
- $\mathbb{R}$ est archimédien veut dire que

$$\forall(x,y)\in\mathbb{R}^{*+}\exists n\in\mathbb{N}\ x<n.y$$

  En choisissant $y=1$ on peut ainsi définir la partie entière d'un réel positif x (le plus grand entier inférieur ou égal à x), puis la partie entière d'un réel négatif.

Ex 10:
Comparer $E(-x)$ et $E(x)$, $E(x+y)$ et $E(x)+E(y)$, $E(x)$ et $E(\frac{x}{2})+E(\frac{x+1}{2})$.

Automorphismes de $\mathbb{R}$ (Exercice classique corrigé)

Proposition B.4 *La seule application non nulle f de $\mathbb{R}$ vers $\mathbb{R}$ telle que*

$$\forall(x,y)\in\mathbb{R}^2\quad f(x+y)=f(x)+f(y)\ \text{et}\ f(xy)=f(x)f(y)$$

est l'application identique.

Sous-groupes de $(\mathbb{R},+)$ (Exercice corrigé)

Proposition B.5 *Tout sous-groupe de $(\mathbb{R},+)$ est de la forme $a\mathbb{Z}=\{n.a;n\in\mathbb{Z}\}$ ou dense.*

On rappelle qu'une partie A de $\mathbb{R}$ est dense si et seulement si $\forall\epsilon\in\mathbb{R}^{*+}\ \forall x\in\mathbb{R}\ \exists y\in A\ |x-y|<\epsilon$.
Démonstration : soit G un sous-groupe.
Si $G=\{0\}$: Dans ce cas $G=0\mathbb{Z}$ et le résultat est prouvé
Sinon $G\neq\{0\}$: Il existe donc dans G un élément non nul x. Puisque $-x$ appartient aussi à G, l'ensemble $\mathbb{R}^{*+}\cap G$ est donc non vide et minoré par 0, il possède par conséquent une borne inférieure a.

Si $a > 0$: Par définition de la borne supérieure il existe un élement b de G dans $[a, 2a[$. S'il en existait deux, par soustraction on obtiendrait un élément de G dans $]0, a[$, ce qui est contraire à la définition de a. Donc $[a, 2a[\cap G$ est réduit à un unique élement qui ne peut-être que a, car la borne inférieure d'un ensemble fini est nécessairement le minimum de cet ensemble.
Puisque G est stable pour l'addition et le passage à l'opposé, on aura $a\mathbb{Z} \subset G$. Réciproquement si x est dans G, $x - E(\frac{x}{a}).a$ est aussi dans G et dans $[0, a[$ et est donc nul. Par conséquent $x = n.a$ est dans $a\mathbb{Z}$, ce qui nous donne l'inclusion opposée et le résultat.

Si $a = 0$: Montrons que G est dense. Soit x dans $\mathbb{R}$ et $\epsilon > 0$. Par définition de la borne inférieure, il existe b dans $G\cap]0, \epsilon[$. Soit $y = E(\frac{x}{b}).b$, y est dans G et $x-y$ appartient à $[0, a[(\subset [0, \epsilon[)$ donc $|x-y| < \epsilon$. C'est le résultat désiré.

B.5 Le corps des nombres complexes

B.5.1 Constructions

Le corps $\mathbb{C}$ des nombres complexes peut être construit

— soit en munissant $\mathbb{R}^2$ des lois

$$(x, y) + (x', y') = (x + x', y + y') \quad (x, y)(x', y') = (xx' - yy', xy' + x'y)$$

qui en font un corps commutatif, contenant le sous-corps $\{(x, 0; x \in \mathbb{R}\}$ isomorphe à $\mathbb{R}$, et donc identifié à $\mathbb{R}$. En notant $i = (0, 1)$ on a alors $i^1 = -1$.

— Soit comme le sous-anneau de $M_2(\mathbb{R})$

$$\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix}; (a, b) \in \mathbb{R}^2\}$$

qui est effectivement un corps qui contient le sous-corps $\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}; a \in \mathbb{R}\}$ isomorphe à $\mathbb{R}$. En identifiant une nouvelle fois ce corps à $\mathbb{R}$ et en posant $i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, on a à nouveau $i^2 = -1$.

Il existe d'autres constructions possibles, elles conduisent à des corps isomorphes. Chacun de ces corps contient un élément i tel que $i^2 = -1$ et est un espace vectoriel sur $\mathbb{R}$ de dimension 2 dont $(1, i)$ est une base. Tout élément s'écrit donc de manière unique $a.1 + b.i$ où a et b sont des nombres réels. On le note plus simplement $a + ib$.

B.5.2 Notation exponentielle, module, argument.

B.5.3 Les nombres complexes et la calculatrice.

B.5.4 Calcul de sommes trigonométriques

Formule de de Moivre (note [3]).

Ex 11: *TPE 00*
Résoudre dans $\mathbb{R}$, si $n \geq 2$.

$$\sum_{k=0}^{n-1} \frac{\cos kx}{(\cos x)^k} = 0.$$

Ex 12: *Mines 97*
Montrer que si n et p sont des entiers non nuls, p premier :

$$\sum_{l=0}^{p-1} \left(2\cos\frac{l\pi}{p}\right)^n \cos\frac{nl\pi}{p}$$

est un entier multiple de p.

3. Abraham de Moivre, Vitry-le-François 1667, Londres 1754, mathématicien anglais d'origine française

B.5.5 Racines n-ième d'un nombre complexe

Racines de l'unité. Racines d'un nombre complexe. Application à la résolution d'équations d'un certain type.

Ex 13: *CENTRALE 98*
Factoriser $(X-1)^n - (X+1)^n$.

B.5.6 Interprétation géométrique

A un point M d'un plan euclidien, rapporté à un repère orthonormal $(O, \overrightarrow{i}, \overrightarrow{j})$, dont l'abscisse et l'ordonnée dans ce repère sont x et y on peut associé le nombre complexe $z = x + iy$ qui s'appelle l'affixe de M. Si M et N sont deux points d'affixes respectives a et b alors le vecteur $\overrightarrow{MN}$ a pour coordonnées $(\Re(b-a), \mathcal{I}\text{m}(b-a))$ dans la base $(\overrightarrow{i}, \overrightarrow{j})$, $|b-a|$ pour norme.
Si M, N et P sont trois points distincts d'affixes respectives a, b, c alors l'angle $(\widehat{\overrightarrow{MN}, \overrightarrow{MP}})$ est l'argument de $\frac{c-a}{b-a}$.
A titre d'exemple, on en déduit que quatre points distints d'affixes respectives a, b, c et d sont cocycliques si et seulement si leur birapport $\left(\frac{c-a}{d-a}\right) \Big/ \left(\frac{c-a}{d-a}\right)$ est réel.

Ex 14:
Soient (A, B, C, D) quatre nombres complexes tels que $AD - BC \neq 0$.
1) Quel est le domaine de définition de la fonction

$$f : \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & \frac{Az+B}{Cz+D} \end{array}$$

2) Montrer que f transforme quatre points alignés ou cocycliques en quatre points alignés ou cocycliques.

Annexe C

Suites de nombres réels ou complexes

Dans ce chapitre $\mathbb{K}$ désignera soit le corps des nombres réels, soit celui des nombres complexes. Dans ce chapitre toutes les suites sont définies sur $\mathbb{N}$, mais les notions s'étendent sans changement notable aux suites définies à partir d'un certain rang.

C.1 Convergence

Définition C.1 *Une suite $(u_n)_{n\in\mathbb{N}}$ de nombres réels ou complexes converge vers a si et seulement si :*

$$\forall\epsilon \in \mathbb{R}^{*+}\ \exists n_0 \in \mathbb{N} \quad \forall n \in \mathbb{N}\ n \geq n_0 \Rightarrow |u_n - a| < \epsilon.$$

On vérifie que l'ensemble des suites convergentes est une sous-algèbre de $\mathbb{K}^{\mathbb{N}}$ et que le passage à la limite est un morphisme d'algèbre. Plus précisément si une suite $(u_n)_{n\in\mathbb{N}}$ converge vers une limite non nulle a, alors il existe n_0 tel que $(\frac{1}{u_n})_{n\geq n_0}$ est définie et tend vers $\frac{1}{a}$. De plus une suite complexe converge si et seulement si sa partie réelle et sa partie imaginaire convergent.

Remarque : la suite $(u_n)_{n\in\mathbb{N}}$ tend vers ℓ si et seulement si $(u_n - \ell)_{n\in\mathbb{N}}$ tend vers 0, c'est-à-dire si et seulement si $(|u_n - \ell|)_{n\in\mathbb{N}}$ tend vers 0.

Proposition C.1 *Toute suite convergente est bornée.*

Définition C.2 (Extension au limites infinies) *Une suite $(u_n)_{n\in\mathbb{N}}$ de nombres réels tend vers $+\infty$ si et seulement si*

$$\forall A \in \mathbb{R}^{*+}\ \exists n_0 \in \mathbb{N}\ \forall n \in \mathbb{N}\ n \geq n_0 \Rightarrow u_n > A$$

La définition se transporte sans difficulté pour caractériser une suite tendant vers $-\infty$.

On peut aussi définir une suite de nombres complexes tendant vers l'infini (∞, sans signe).

Définition C.3 (Suite extraite) *Soit $u : \mathbb{N} \to X$ une suite quelconque, on appelle suite extraite de u une suite $u \circ \phi$ où $\phi : \mathbb{N} \to \mathbb{N}$ est strictement croissante. Si u est notée $(u_n)_{n\in\mathbb{N}}$ une suite extraite sera notée $(u_{\phi(n)})_{n\in\mathbb{N}}$.*

On dit parfois que la fonction ϕ est une extractrice. On remarquera que si ϕ est une extractrice, alors pour tout n $\phi(n) \geq n$. Ce petit lemme technique sert assez régulièrement dans les démonstrations.

Il est clair que tout suite est extraite d'elle-même (réflexivité de la relation)et que si w est extraite de v et v extraite de u alors w est extraite de u (transitivité de la relation).

Un exemple : soit $(u_n)_{n\in\mathbb{N}}$ une suite de nombres réels strictement positifs tendant vers 0, alors il existe une suite extraite de cette suite tendant vers 0 en décroissant. L'exemple de la suite $u_n = \frac{1}{n+1}$ si n est pair $u_n = \frac{1}{2n}$ si n est impair, montre qu'un suite de réels strictement positifs qui tend vers 0 n'est pas nécessairement décroissante à partir d'un certain rang.

Proposition C.2 *Une suite extraite d'une suite convergente reste convergente*

Définition C.4 (Valeur d'adhérence) *On dit que l est une valeur d'adhérence de la suite $(u_n)_{n\in\mathbb{N}}$ si on peut extraire de cette suite une suite convergeant vers l.*

Théorème C.1 (Théorème de la limite monotone) *Toute suite croissante majorée (resp. toute suite décroissante minorée) de réels converge. Sa limite est la borne supérieure (resp. la borne inférieure) de l'ensemble de ses valeurs.*

Définition C.5 (Suites adjacentes) *Deux suites (a_n) et (b_n) de nombres réels sont adjacentes si l'une est croissante, l'autre décroissante et leur différence tend vers 0.*

Théorème C.2 *Deux suites adjacentes de nombres réels convergent et ont même limite.*

Théorème C.3 (Théorème des segments enboîtés) *Soit (I_n) une suite de segments de $\mathbb{R}$ telle que*
- $\forall n \in \mathbb{N} \quad I_{n+1} \subset I_n$
- *la suite des longueur des I_n tend vers zéro.*

Alors l'intersection des I_n est non vide et réduite à un point.

Théorème C.4 *De toute suite bornée d'éléments de $\mathbb{R}$ ou $\mathbb{C}$ on peut extraire une suite convergente.*

Ce théorème est un cas particulier du théorème de *Bolzano*[1] − *Weierstrass*[2].

Lemme C.1 *De toute suite bornée de nombres réels on peut extraire une sous-suite convergente.*

Première démonstration :

Soit $(x_n)_{n\in\mathbb{N}}$ une suite bornée de nombres réels. Il existe un segment $I_0 = [a, b]$ de $\mathbb{R}$ tel que pour tout n x_n appartiennent à $[a, b]$. Découpons cet intervalle en deux intervalles $I'_0 = [a, (a + b)/2]$ et $I''_0 = [(a + b)/2, b]$ de longeur deux fois plus petite. On peut partitionner $\mathbb{N}$ en deux sous-ensembles $\mathbb{N}' = \{n, x_n \in I'_0\}$ et $\mathbb{N}'' = \mathbb{N} - \mathbb{N}'$. On remarquera qu'un de ces deux sous-ensembles est infini, et que si n appartient à $\mathbb{N}''$ alors x_n appartient à I''_0. Si $\mathbb{N}'$ est infini on choisit $I_1 = I'_0$ sinon $I_1 = I''_0$. On peut ainsi construire par récurrence une suite de segments emboîtés $(I_n)_{n\mathbb{N}}$ dont la suite des longueurs $(\frac{b-a}{2^n})_{n\in\mathbb{N}}$ tend vers 0 et tels que pour tout n l'ensemble $N_n, \{p \in \mathbb{N}_{n-1}, x_p \in I_n\}$ est infini. D'après le théorème des segments emboîtés, l'intersection des I_n se réduit à un point l.

On choisit n_0 dans N_0, puis $n_1 > n_0$ dans N_1. Cela est possible car N_1 est infini. On peut poursuivre cette construction par récurrence et obtenir une suite strictement croissante $(n_p)_{p\in\mathbb{N}}$ telle que n_p appartienne à N_p pour tout p. Définissons ϕ par $\phi(p) = n_p$. La suite $(x_{\phi(n)})_{n\in\mathbb{N}}$ converge vers l car pour tout n, $x_{\phi(n)}$ et l sont éléments de I_n donc $|l - x_{\phi(n)}| \leq \frac{b-a}{2^n}$.

Deuxième démonstration :

Soit $(a_n)_{n\in\mathbb{N}}$ une suite bornée de nombre réels. Définissons la suite $(b_n)_{n\in\mathbb{N}}$ par

$$\forall n \in \mathbb{N} \; b_n = \sup_{p\geq n} a_p$$

Cette suite est bien définie car $(a_n)_{n\in\mathbb{N}}$ est bornée donc majorée. Elle est minorée car la suite $(a_n)_{n\in\mathbb{N}}$ est minorée. De plus elle est décroissante. Elle est donc convergente. Soit l sa limite. On va montrer qu'il existe une suite extraite de $(a_n)_{n\in\mathbb{N}}$ qui converge vers l, en construisant une extractrice ϕ. on pose $\phi(0) = 0$, et son suppose ϕ construite jusqu'à l'ordre p de telle sorte que $|a_{\phi(k)} - l| < \frac{1+|l-a_0|}{2^k}$ pour $0 \leq k \leq p$. On pose $\epsilon = \frac{1+|l-a_0|}{2^{n+1}}$. Puisque $(b_n)_{n\in\mathbb{N}}$ converge vers l il existe n_0 tel que $l - \epsilon < b_n < l + \epsilon$ pour n plus grand que n_0. On choisit alors un tel n strictement supérieur à $\phi(p)$. Par caractérisation de la borne supérieure, puis que $l - \epsilon < b_n = \sup_{q\geq n} a_q$ il existe $\phi(p+1) \geq n(> \phi(p))$ tel que $a_{\phi(p+1)} > l - \epsilon$, comme on a toujours $a_{\phi(p+1)} \leq b_n < l + \epsilon$, on a bien $|l - a_{\phi(p+1)}| < \epsilon$ et on a prolongé par récurrence la définition de ϕ.

Cette limite l est la plus grande des valeurs d'adhérence de la suite $(a_n)_{n\in\mathbb{N}}$, on l'appelle la limite supérieure de la suite $(a_n)_{n\in\mathbb{N}}$. On définit de même la limite inférieure de la suite $(a_n)_{n\in\mathbb{N}}$ comme la limite de la suite (croissante) $(\inf_{p\geq n} a_p)_{n\in\mathbb{N}}$.

Troisième démonstration :

Lemme C.2 *De toute suite de nombres réels on peut extraire une sous-suite monotone.*

En effet soit $(u_n)_{n\in\mathbb{N}}$ une suite de nombre réels. Si l'ensemble

$$\mathcal{E} = \{n \in \mathbb{N}; \forall m \in \mathbb{N} \; m > n \; u_m < u_n\}$$

est fini, alors en notant N son maximum ($N = -1$ si cet ensemble est vide), on aura

$$\forall n \in \mathbb{N} \; n > N \quad \exists m > n \; u_m \geq u_n$$

et on pourra extraire de $(u_n)_{n\in\mathbb{N}}$ une suite croissante au sens large.

Si $\mathcal{E}$ est infini alors la sous-suite $(u_k)_{k\in\mathcal{E}}$ est décroissante. Pour démontrer théorème il suffit de remarquer que si $(u_n)_{n\in\mathbb{N}}$ est bornée alors toute suite monotone qui en est extraite est majorée et/ou minorée, donc convergente.

1. BOLZANO Bernhard, Prague 1781 - Prague 1848
2. WEIERSTRASS Karl Theodor Wilhelm, Osterfelde (Westphalie) 1815 - Berlin 1897

Exercice 15: Si une suite $(a_n)_{n\in\mathbb{N}}$ est bornée et si $(a_{n+1}-a_n)_{n\in\mathbb{N}}$ tend vers 0 alors l'ensemble de ses valeurs d'adhérence est un intervalle.

Lemme C.3 *De toute suite bornée de nombres complexes on peut extraire une suite convergente.*

Soit $(z_n)_{n\in\mathbb{N}}$ une suite bornée de nombres complexes. Décomposons $z_n = x_n + iy_n$ où x_n et y_n sont réels. Puisque pour tout n $|x_n| \leq |z_n|$ et $|y_n| \leq |z_n|$ les suites $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ sont bornées. D'après le lemme précédent on peut extraire de la suite $(x_n)_n$ une suite $(x_{\phi(n)})_{n\in\mathbb{N}}$ convergente. La suite $(y_{\phi(n)})_{n\in\mathbb{N}}$, extraite d'une suite bornée, est bornée. On peut en extraire une suite convergente $(y_{\phi(\psi(n))})_{n\in\mathbb{N}}$. La suite $(x_{\phi(\psi(n))})_{n\in\mathbb{N}}$, extraite d'une suite convergente reste convergente. La suite $(z_{\phi(\psi(n))})_{n\in\mathbb{N}}$ est convergente, car ses parties réelles et imaginaires le sont.

Exercice 16: *Assez classique, Centrale2006 Ecrit* Une suite bornée de nombres réels ou complexes, qui n'admet qu'une valeur d'adhérence est convergente.

Théorème C.5 *(Le lemme de Cesàro[3]) Soit $u = (u_n)_{n\in\mathbb{N}}$ une suite de nombres réels ou complexes. Définissons la suite $(v_n)_{n\in\mathbb{N}}$ par :*

$$\forall n \in \mathbb{N} \quad v_n = \frac{1}{n+1}(u_0 + u_1 + \cdots + u_n).$$

Si la suite $(u_n)_{n\in\mathbb{N}}$ est convergente, il en est de même de la suite $(v_n)_{n\in\mathbb{N}}$ et les deux suites ont même limite

Si la suite $(v_n)_{n\in\mathbb{N}}$ converge on dit que la suite $(u_n)_{n\in\mathbb{N}}$ converge en moyenne. La convergence implique la convergence en moyenne, mais la réciproque est fausse : la suite $((-1)^n)_{n\in\mathbb{N}}$ converge en moyenne vers 0, mais elle ne converge pas.

Ce théorème n'est pas officiellement au programme mais son usage est toléré à l'oral, on verra plus tard comment on peut le ramener rapidement à un théorème sur la sommation des équivalents qui lui est au programme.

La démonstration de ce théorème doit en tout cas être parfaitement maîtrisée. C'est l'archétype du « découpage de epsilon ». Il faut pouvoir l'adapter à d'autres situations qui se présente régulièrement.

Démonstration :

Supposons d'abord que la suite (u_n) converge vers 0. Soit ϵ un réel strictement positif quelconque.

Il existe n_0 tels que

$$n \geq n_0 \Rightarrow |u_n| < \frac{\epsilon}{2}.$$

On en fixe un. Pour n plus grand que n_0 on a

$$\begin{aligned}
|v_n| &\leq \left|\frac{1}{n+1}\sum_{k=0}^{n_0-1} u_k + \frac{1}{n+1}\sum_{k=n_0}^{n} u_k\right| \\
&\leq \frac{1}{n+1}\sum_{k=0}^{n_0-1} |u_k| + \frac{1}{n+1}\sum_{k=n_0}^{n} |u_k| \\
&\leq \frac{C_{n_0}}{n+1} + \frac{1}{n+1}\sum_{k=n_0}^{n} \frac{\epsilon}{2} \\
&\leq \frac{C_{n_0}}{n+1} + \frac{1}{n+1}\sum_{k=n_0}^{n} \frac{\epsilon}{2} \\
&\leq \frac{C_{n_0}}{n+1} + \frac{n-n_0+1}{n+1}\frac{\epsilon}{2} \\
&\leq \frac{C_{n_0}}{n+1} + \frac{\epsilon}{2}
\end{aligned}$$

où C_{n_0} est une constante (dépendant de ϵ via n_0). Or

$$\lim_{n\to+\infty} \frac{C_{n_0}}{n+1} = 0$$

3. Cesàro Ernesto, Naples 1859-Torre Annunziata 1906

il existe donc n_1 tel que

$$n \geq n_1 \Rightarrow \frac{C_{n_0}}{n+1} < \frac{\epsilon}{2}$$

puis en choisissant par exemple $n_2 = \max(n_0, n_1)$:

$$\forall \epsilon > 0 \exists n_2 \quad n \geq n_2 \Rightarrow |v_n| < \epsilon$$

Ceci veut exactement dire

$$\lim_{n \to +\infty} v_n = 0.$$

Dans le cas général, on écrit $u_n = l + u_n - l = l + w_n$ où $(w_n)_{n \in \mathbb{N}}$ tend vers 0. On alors

$$v_n = \frac{(n+1)l}{n+1} + \frac{1}{n+1}(w_0 + u_1 + \cdots + w_n)$$

et en appliquant le résultat obtenu dans le cas particulier on a bien

$$\lim_{n \to +\infty} v_n = l.$$

Exercice 17: *Mines 2006 Ecrit* Soit f une fonction à valeurs réelles, continue sur $\mathbb{R}^+$. On suppose $\lim_{x \to +\infty} f(x) = C$. Montrer

$$\int_0^x f(t)\, dt \sim_{x \to +\infty} Cx.$$

Définition C.6 *Une suite $(u_n)_{n \in \mathbb{N}}$ de nombres réels (ou complexes) est de Cauchy*[4] *(ou vérifie le critère de Cauchy) si et seulement si :*

$$\forall \epsilon > 0 \exists n_0 \quad p \geq n_0, q \geq n_0 \Rightarrow |u_p - u_q| < \epsilon$$

Théorème C.6 *Toute suite convergente est de Cauchy.*

Il y a une réciproque dans les cas de $\mathbb{R}$ et $\mathbb{C}$.

Théorème C.7 (Complétude de $\mathbb{R}$ et $\mathbb{C}$) *Toute suite de Cauchy de nombres réels ou complexes converge. On dit que $\mathbb{R}$ et $\mathbb{C}$ sont complets.*

Lemme C.4 *Toute suite de Cauchy est bornée.*

Lemme C.5 *Toute suite de Cauchy qui possède une valeur d'adhérence est convergente.*

Il ne reste plus maintenant qu'à remarquer que toute suite bornée de réels ou de complexes possède une valeur d'adhérence.

C.2 Relations de comparaison

C.2.1 Relation de domination

Définition C.7 *Soit $(u_n)_{n \in \mathbb{N}}$ une suite de nombres réels ou complexes et $(\alpha_n)_{n \in \mathbb{N}}$ une suite de réels positifs. On dit que la suite $(\alpha_n)_{n \in \mathbb{N}}$ domine la suite $(u_n)_{n \in \mathbb{N}}$ et on écrit $u_n = \mathcal{O}(\alpha_n)$ si et seulement si :*

$$\exists M \in \mathbb{R} \quad \exists n_0 \in \mathbb{N} \qquad n \geq n_0 \Rightarrow |u_n| \leq M\alpha_n$$

Cette relation peut être étendue à deux suites à valeurs réelles ou complexes en remplaçant la caractérisation par

$$u_n = \mathcal{O}(v_n) \Leftrightarrow (\exists M \in \mathbb{R} \quad \exists n_0 \in \mathbb{N} \qquad n \geq n_0 \Rightarrow |u_n| \leq M|v_n|)$$

4. Cauchy Augustin-Louis, Paris 1789-Sceaux 1857

C.2.2 Relation de prépondérance

Définition C.8 *Soit $(u_n)_{n\in\mathbb{N}}$ une suite de nombres réels ou complexes et $(\alpha_n)_{n\in\mathbb{N}}$ une suite de réels positifs. On dit que la suite $(\alpha_n)_{n\in\mathbb{N}}$ est prépondérente sur la suite $(u_n)_{n\in\mathbb{N}}$ et on écrit $u_n = \circ(\alpha_n)$ si et seulement si :*

$$\forall\epsilon \in \mathbb{R}^{*+} \quad \exists n_\epsilon \in \mathbb{N} \qquad n \geq n_\epsilon \Rightarrow |u_n| \leq \epsilon\alpha_n$$

On dit aussi que (u_n) est négligeable devant (α_n).

Comme dans le cas précédent on peut étendre cette définition à deux suites de nombres complexes en remplaçant la caractérisation par

$$u_n = \circ(v_n) \Leftrightarrow (\forall\epsilon \in \mathbb{R}^{*+} \quad \exists n_0 \in \mathbb{N} \qquad n \geq n_0 \Rightarrow |u_n| \leq \epsilon|v_n|)$$

C.2.3 Relation d'équivalence

Définition C.9 *Deux suites (u_n) et (v_n) de nombres réels ou complexes sont équivalentes si et seulement si $(u_n - v_n)$ est négligeable devant (u_n).*

C.3 Etude de suites définies par $u_{n+1} = f(u_n)$

Remarquons que si A est une partie stable par f, alors la suite est définie pour toute valeur de u_0 dans A.

C.3.1 Cas ou f est réelle

On commencera par chercher un intervalle stable sur lequel f soit croissante ou contractante. Puis on prouvera qu'en étudiant la suite à partir d'un certain rang on ne perd pas en généralité.
Exemple $x_0 > 0$ et $x_{n+1} = \frac{1}{2}\left(x_n + \frac{1}{x_n}\right)$.

C.3.1.1 Cas où f est croissante

Proposition C.3 *Si f est croissante sur un intervalle I stable par f alors la suite (u_n) est définie et monotone pour toute valeur u_0 de I.*
Si f est de plus continue alors la suite (u_n) converge vers un point fixe de f ou vers une extrémité de I.

Exemple : $u_{n+1} = \frac{1+u_n^2}{2}$
Exemple : $u_{n+1} = \frac{1}{2-\sqrt{u_n}}$

Cas particulier Un cas encore plus simple est celui où $f(0) = 0$ et $0 < f(x) \leq x$ sur $\mathbb{R}^{*+}$. Il apparaît régulièrement dans l'étude des séries à termes positifs.
Exemple : $u_{n+1} = \arctan u_n$

C.3.1.2 Cas où f est contractante

Définition C.10 *Une application f définie sur un intervalle I de $\mathbb{R}$, à valeurs dans I, est dite contractante s'il existe k dans $[0, 1[$ tel que*

$$\forall(x, y) \in I^2 \quad |f(x) - f(y)| \leq k|x - y|$$

Une telle application est nécessairement continue

Exemple si $f : I \to I$ est de classe $\mathcal{C}^1$ alors elle est contractante si et seulement si il existe k dans $[0, 1[$ tel que $|f'(x)| \leq k$ pour tout x de I.

Proposition C.4 *Si $f : [a, b] \to [a, b]$ est contractante, alors elle possède un unique point fixe ℓ, et pour tout u_0 dans $[a, b]$ la suite (u_n) est définie et converge vers l.*

Ce résultat peut être étendu au cas d'une application contractante $f : A \to A$ où A est une partie quelconque de $\mathbb{C}$ (resp. de $\mathbb{R}$) si on sait que f possède un point fixe dans A. On verra ultérieurement que c'est toujours le cas si A est une partie fermée de $\mathbb{C}$ (resp. de $\mathbb{R}$).
Exemple : $u_{n+1} = \cos u_n$.

C.3.1.3 Vitesse de convergence. Accélération

Donner des exemples.
Exemple : Sommes de Riemann (Accélération $\to$ trapèzes $\to$ Simpson)
Exemple : $u_{n+1} = f(u_n)$ avec $f'(\ell) \neq 0$
Exemple : Méthode de Newton

C.3.1.4 Recherche d'un équivalent

La méthode des petits pas : si (u_n) tend vers ℓ, disons par valeurs strictement supérieures, on pose $u_n - \ell = v_n$ et on cherche un α tel que la suite $v_{n+1}^\alpha - v_n^\alpha$ converge vers une limite finie K non nulle. En appliquant le lemme de Cesàro on en déduit $(u_n - \ell) \sim (nK)^{\frac{1}{\alpha}}$.
Exemple : $u_{n+1} = \sin u_n$.

C.3.2 Exemples où f est complexe

La récurrence linéaire du second ordre

Définition C.11 *On dit qu'une suite $(u_n)_{n\in\mathbb{N}}$ de nombres complexes est solution d'une récurrence linéaire d'ordre deux s'il existe trois nombres complexes (a, b, c), a non nul, tels que*

$$\forall n \in \mathbb{N} \quad au_{n+2} - bu_{n+1} + cu_n = 0$$

Proposition C.5 *Soit trois nombres complexes (a, b, c), a non nul. L'ensemble $\mathcal{S}$ des suites (u_n) solution de la récurrence linéaire*

$$\forall n \in \mathbb{N} \quad au_{n+2} - bu_{n+1} + cu_n = 0$$

est un sous-espace vectoriel de dimension 2 de l'espace des suites.
Associons à cette récurrence l'équation (dite caractéristique)

$$ax^2 + bx + c = 0$$

Si celle équation possède deux solutions distinctes r_1 et r_2 alors une base de $\mathcal{S}$ est $((r_1^n)_{n\in\mathbb{N}}, (r_2^n)_{n\in\mathbb{N}})$, si cette équation possède une racine double r alors une base de $\mathcal{S}$ est $((r^n)_{n\in\mathbb{N}}, (nr^{n-1})_{n\in\mathbb{N}})$

PS : on a adopté la convention $y^0 = 1$ si $y = 0$ et $n = 0$ ainsi que $ny^{n-1} = 0$ si $y = 0$ et $n = 0, 1$ si $y = 0$ et $n = 1$.

La suite homographique On appelle suite homographique une suite (z_n) de nombres complexes vérifiant $z_{n+1} = f(z_n)$ avec $f(z) = \frac{az+b}{cz+d}$, $c \neq 0$.
On doit éviter certaines valeurs de z_0 si on désire que la suite soit définie. Mais on peut aussi étendre la définition de f à $\mathbb{C} \cup \{\infty\}$ en posant $f(\infty) = \frac{a}{c}$, $f(-\frac{d}{c}) = \infty$.
Pour étudier une telle suite on détermine les points fixes de f, c'est-à-dire les z vérifiant $z = f(z)$, soit $az + b = z(cz + d)$.
Si cette équation possède deux racines distinctes r_1 et r_2 alors on peut vérifier que la suite $(v_n)_{n\in\mathbb{N}}$ définie par $v_n = \frac{z_n - r_1}{z_n - r_2}$ est une suite géométrique dont il est facile d'étudier la convergence et d'en déduire celle de $(z_n)_{n\in\mathbb{N}}$.
Si cette équation possède une racine double r. On vérifie que $(w_n)_{n\in\mathbb{N}}$ est une suite arithmétique si $w_n = \frac{1}{z_n - r}$.
Exemples :

$$z_{n+1} = \frac{1}{2 - z_n}, \; z_{n+1} = \frac{2z_n - 3}{z_n - 2}, \; z_{n+1} = \frac{z_n - 1}{z_n + 1}, \; z_{n+1} = 5\frac{z_n - 1}{z_n + 1}$$