[MPSI – Mathématiques 1]

Sommaire

1 – Vocabulaire de la théorie des ensembles

I Notions de logique

1 – Propositions et connecteurs logiques

Proposition = énoncé qui ne contient pas de variable et auquel on peut attribuer une valeur de vérité (vrai ou faux).
Table de vérité = tableau dans lequel on range des colonnes où l'on écrit toutes les propositions possibles.
Connecteurs logiques = symbole opératoire permettant, à partir de n propositions, d'en définir une nouvelle. On peut le définir par une table de vérité.
Exemples : $\neg P$; $P \wedge Q$; $P \vee Q$; $P \Rightarrow Q$; $P \Leftrightarrow Q$
Tautologie (énoncé toujours vrai) ; Antilogie (énoncé toujours faux)

2 – Propriétés des connecteurs logiques

Commutativité, associativité et distributivité avec le "ou" et le "et".
Lois de De Morgan (non a et non b $\Leftrightarrow$ non(a ou b)).
(a $\Rightarrow$ b) $\Leftrightarrow$(non a ou b)
Le connecteur logique * (F, V, V, V) ou (F, F, F, V) permet de remplacer tous les connecteurs logiques.
(pour le construire, on le cherche tel que $A * A = \neg A$, et que l'on puisse faire un ou ou un et facilement)

3 – Prédicat

Prédicat = énoncé qui comporte certaines variables. Lorsque les variables ont des valeurs, il devient une proposition.
Exemple : "x est un entier pair"

II Notion d'ensemble

1 – Ensembles

Un ensemble est constitué d'éléments. Pour tout objet x et tout ensemble E, l'énoncé "x appartient à E" est un prédicat.
(Ex) Les ensembles ne constituent pas un ensemble [démonstration par l'absurde : $X \in X$ a un sens].
Ensemble des nombres : $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

2 – Ensembles de parties

Partie de E = tout ensemble dont les éléments sont dans E. Le signe $\in$ n'est pas symétrique.
L'ensemble des parties de E est noté $\mathscr{P}_{(E)}$. $A \in \mathscr{P}_{(E)} \Leftrightarrow A \subset E$
Pour tout ensemble E, $\varnothing \subset E$; E ; $\mathscr{P}_{(E)} \neq \varnothing$
Propriétés de $\subset$:

- Réflexive ($E \subset E$)
- Antisymétrique (($F \subset E$ et $E \subset F$) $\Leftrightarrow E = F$)
- Transitive (($E \subset F$ et $F \subset G$) $\Rightarrow E \subset G$)

3 – Réunion, Intersection

Commutatif, Associatif, Distributif l'un par rapport à l'autre.

4 – Différence, Complémentaire

Analogies aux lois de De Morgan (avec $\complement$, union et intersection)
$A \setminus B = A \cap \complement B$
$A \Delta B = (A \cup B) \setminus (A \cap B)$
La différence symétrique (Δ) est commutative [demo]

5 – Quantificateurs

Propriété caractéristique = "$x \in E$"
Prédicats associés à des ensembles.

Analogies :

Prédicats	Ensembles
$\vee$	$\cup$
$\wedge$	$\cap$
$\Leftrightarrow$	$=$
$\Rightarrow$	$\subset$
$\neg$	$\complement$
ou exclusif	Δ

Si $A \subset E$, avec P comme propriété caractéristique, alors
$A = E \Leftrightarrow \forall\, x \in E, P(x)$ quantificateur universel
$A \neq 0 \Leftrightarrow \exists\, x \in E, P(x)$ quantificateur existentiel
Négation d'un quantificateur : on change le quantificateur ($\forall \leftrightarrow \exists$) et on nie ce qu'il y a après [demo]
Exemple: Définition d'une limite de suite

III Produit cartésien, Graphe, Application

1 – Produit cartésien

$$\prod_{i=1}^{n} E_i = \{(x_1, x_2, ..., x_n); x_1 \in E_1; x_2 \in E_2; ...; x_i \in E_i\}$$

2 – Graphe

Un graphe G d'un ensemble E vers un ensemble F est une partie du produit cartésien $E \times F$

3 – Application

Une application est la donnée de 3 informations :
un ensemble de départ E
un ensemble d'arrivée F
un graphe G de E vers F tel que $\forall\, x \in E, \exists\, !\, y \in F, (x, y) \in G$
Notation :
$f : E \to F$
$x \to y = f(x)$
Restriction (diminution de l'ensemble de départ, même ensemble d'arrivée)
Prolongement (augmentation de l'ensemble de départ, même ensemble d'arrivée)
Ex : sinus(x)/x en 0

[TD 1]
A toute application f injective on associe une application s surjective telle que $s \circ f = Id_E$.
A toute application f surjective on associe une application r injective telle que $f \circ r = Id_F$.

4 – Application injective, Application surjective

f injective $\Leftrightarrow \forall\, (a,b) \in E^2, a \neq b \Rightarrow f(a) \neq f(b)$
$\Leftrightarrow \forall\, (a,b) \in E^2, f(a) = f(b) \Rightarrow a = b$ c'est–à–dire images toutes différentes
f surjective $\Leftrightarrow \forall\, y \in F, \exists\, x \in E, y = f(x)$ c'est–à–dire tout l'ensemble d'arrivée atteint
f bijective $\Leftrightarrow$ f injective et f surjective
Permutation d'un ensemble E = bijection de E vers E

5 – Composition des applications

Associativité de la composition $\circ$ [demo]
La composée de 2 injections est une injection.
La composée de 2 surjections est une surjection.
La composée de 2 bijections est une bijection.

6 – Application réciproque d'une bijection

f est bijective $\Leftrightarrow \forall\, y \in F, \exists\, !\, x \in E, y = f(x)$
S'il existe g tel que $g \circ f = Id_E$ et $f \circ g = Id_F$ alors f bijective et $g = f^{-1}$ [demo]
Corollaire : g et f bijectives $\to (g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

7 – Extension aux ensembles de parties

$f(A) = \{ y \in F, \exists x \in A, y = f(x) \}$ — $f(A)$ est l'image directe de A par f

$f^{-1}(B) = \{ x \in E, f(x) \in B \}$ — $f^{-1}(B)$ est l'image réciproque, ou pré–image de B par f

A est stable par f $\Leftrightarrow f(A) \subset A$.
On peut alors définir l'application induite g, de A vers A, qui à x associe f(x).
On démontre que, pour $f : E \to F$,

- $f(E) = F \Leftrightarrow$ f surjective
- $f^{-1}(f(E)) = E \Leftrightarrow$ f injective
- $f(f^{-1}(F)) = F \Leftrightarrow$ f surjective

8 – Application caractéristique

$A \subset E$, on appelle application caractéristique de A l'application de E vers $\{0, 1\}$ notée

$\chi_A : E \to \{0, 1\}$
$x \to 1$ si x appartient à A, sinon, 0

On note F^E ou $\mathscr{F}_{(E,F)}$ l'ensemble des applications de E vers F.

Prop : L'application $A \in \mathscr{P}_{(E)} \to \chi_A \; \{ 0,1 \}^E$ est bijective.

$\chi_{\complement A} = 1 - \chi_A$

$\chi_{A \cap B} = \chi_A \cdot \chi_B$

$\chi_{A \cup B} = \chi_A + \chi_A - \chi_A \cdot \chi_B$

$\chi_{A \Delta B} = \chi_A + \chi_A - 2\, \chi_A \cdot \chi_B$

9 – Famille

On appelle famille d'éléments de E indexée par un ensemble I d'indices une application de I dans E.
Notation : $(x_i)_{i \in I}$ au lieu de $f : I \to E$. On a $x_i = f(i)$ pour tout i dans I.
A toute famille de E on peut associer la partie de E $\{ x_i, i \in I \} = f(I)$
A une partie A de E on peut associer une famille $(a \to a)$
Famille de parties d'un ensemble $(A_i)_{i \in I}$ où $A \subset E$

IV Relations binaires

1 – Relation binaire sur un ensemble

Une relation binaire sur un ensemble E est la donnée de 2 informations (E, G) où $G \subset E^2$ est appelé graphe de cette relation. $x \mathfrak{R} y \Leftrightarrow (x,y) \in G$

2 – Relation d'équivalence

C'est une relation binaire réflexive ($x \mathfrak{R} x$), symétrique ($x \mathfrak{R} y \Rightarrow y \mathfrak{R} x$) et transitive ($x \mathfrak{R} y$ et $y \mathfrak{R} z \Rightarrow x \mathfrak{R} z$).
Ex : =, ≡, //
Une partition de E est une famille de parties de E $(A_i)_{i \in I}$ telle que :

- $\forall i \in I, A_i \neq \varnothing$
- $\forall (i, j) \in I^2, A_i \cap A_j = \varnothing$ ou $i = j$
- $\cup A_i = E$

La classe de x est la partie de E constituée par l'ensemble des éléments en relation avec x.

$\bar{x} = \{ y \in E, y \mathfrak{R} x \}$

Propriétés :

- La classe de x n'est jamais l'ensemble vide (car il contient au moins x).
- Pour deux éléments x et y de E, soit ils sont de même classe, soit l'intersection entre leur classe est vide.

On appelle système fondamental de représentants une partie I de E telle que $\forall (x, y) \in I^2, x \neq y \Rightarrow \neg\, x \mathfrak{R} y$ et $\forall y \in E, \exists x \in I, y \mathfrak{R} x$.
La famille de l'ensemble des classes I de E est une partition de E.

[TD 2]

On note $E / \mathfrak{R}$ le sous ensemble de $\mathscr{P}_{(E)}$ constitué des classes d'équivalence de E pour la relation $\mathfrak{R}$. On peut définir des LCI dedans, dites loi quotient, déduites de la LCI de E.

3 – Relation d'ordre

C'est une relation binaire réflexive, antisymétrique ($x \mathfrak{R} y$ et $y \mathfrak{R} x \Rightarrow x = y$) et transitive.
Ex : $\subset, \leq, |$
On parle d'ordre total si sur l'ensemble considéré, deux éléments sont toujours comparables, c'est–à–dire

$$\forall (a, b) \in A^2, a \mathfrak{R} b \text{ ou } b \mathfrak{R} a$$

ou encore $\forall (a, b) \in A^2, (\text{non } a \mathfrak{R} b) \Rightarrow b \mathfrak{R} a$

Dans le cas contraire, on parle d'ordre partiel.
$\mathbb{N}$ est dit totalement ordonné par $\leq$ et partiellement ordonné par $|$.

x majore A $\Leftrightarrow \forall a \in A, a \mathfrak{R} x$
x = Max A $\Leftrightarrow$ x majore A et $x \in A$
x = Sup A $\Leftrightarrow$ x est le plus petit des majorants de A
(Th) : Dans $\mathbb{R}$, toute partie non vide et majorée admet une borne supérieure.

[EXOS 2]
Ordre lexicographique (ordre alphabétique).

V Loi de composition interne (LCI)

1 – Définition

Une LCI de E est une application de E^2 vers E.
Un magma est un ensemble muni d'une LCI. Noté (E, *)
Pour munir un ensemble d'une structure algébrique, il faut définir une ou plusieurs LCI vérifiant un certain nombre de propriétés, qui sont les axiomes de la structure algébrique.

2 – Propriétés éventuelles d'une LCI

(E, *) est associatif si $\forall (x, y, z) \in E^3, x * (y * z) = (x * y) * z$
(E, *) est commutatif si $\forall (x, y) \in E^2, x * y = y * x$
$e \in E$ est neutre pour (E, *) si $\forall x \in E, e * x = x * e = x$ [notion de gauche / droite]
Si (E, *) possède un élément neutre, c'est un magma <u>unifère</u>.
Si (E, *) est associatif et unifère, il est appelé <u>monoïde</u>.
Dans un magma unifère, $x \in E$ est dit symétrisable $\Leftrightarrow \exists x' \in E, x' * x = x * x' = e$. [notion de gauche / droite]
Dans un monoïde, le symétrique de $x * y$ est $y' * x'$, et le symétrique de x est unique [demo]
$x \in E$ est régulier $\Leftrightarrow \forall (y, z) \in E^2, x * y = x * z \Rightarrow y = z$ et $y * x = z * x \Rightarrow y = z$ [notion de gauche / droite]
Dans un monoïde, tout élément symétrisable (= inversible) est régulier [demo].
* est distributif par rapport à T $\Leftrightarrow \forall (x, y, z) \in E^3, x * (y \text{ T } z) = (x * y) \text{ T } (x * z)$ et à droite
* est compatible avec $\mathfrak{R} \Leftrightarrow \forall (x, y, x', y') \in E^4, (x \mathfrak{R} y \text{ et } x' \mathfrak{R} y') \Rightarrow x * x' \mathfrak{R} y * y'$

3 – Notations additives et multiplicatives

On notera + une LCI associative et commutative.
Si (E, +) est unifère, on notera 0 son élément neutre.
Si x a un symétrique, on le notera $-x$ ("l'opposé").
Définition de $\Sigma x_i = x_1 + x_2 + ... + x_n$
Remarque : $(x y)^n \neq x^n y^n$ dans le cas général

On notera $\times$ une loi associative.
Si $(E, \times)$ est unifère, on notera 1 son élément neutre.
Si x a un symétrique, on le notera x^{-1} ("l'inverse")
Définition de $\Pi x_i = x_1 . x_2 . \ ... . x_n$

4 – Morphisme

$f : E \to F$ est un morphisme pour * et T $\Leftrightarrow \forall (x, y) \in E^2, f(x * y) = f(x) \text{ T } f(y)$
Lorsque l'ensemble de départ est le même que l'ensemble d'arrivée, et que la loi est la même, on parle d'endomorphisme. Quand f est bijective, on parle d'isomorphisme.
Si f réunit ces deux propriétés, f est un automorphisme.
Si f et g sont des morphismes, $f \circ g$ en est un [demo].

5 – Partie stable, loi induite

Soit $A \subset E$, et (E, *) un magma.
A stable pour * $\Leftrightarrow \forall (x, y) \in A^2, x * y \in A$
La loi induite $*_A$ conserve certaines des propriétés de *
(Associativité, Commutativité ; si e = élément neutre pour * et $e \in A$ alors e = élément neutre pour $*_A$)
Si f est un morphisme de (E, *) vers (F, T), f(E) est stable pour T ; T hérite des propriétés de (E, *) dans f(E) [demos]

2 – Nombres entiers et dénombrement

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

1 – Propriétés caractéristiques liées à l'ordre

ADMIS : Il existe un ensemble $\mathbb{N}$ dit ensemble des entiers naturels ayant les propriétés suivantes :

- Il est ordonné. La relation d'ordre est notée $\leq$
- Il suit les 3 axiomes de Péano
  - Toute partie non vide de $\mathbb{N}$ a un plus petit élément
  - Toute partie non vide et majorée a un plus grand élément
  - $\mathbb{N}$ lui–même n'a pas de plus grand élément

Notation : $0 = \text{Min}(\mathbb{N})$

$\mathbb{N}$ est un ensemble totalement ordonné [demo]

2 – Successeur

$\forall\ n \in \mathbb{N}^*, \exists\ !\ n' \in \mathbb{N}, n < n'$ et $(\forall\ p \in \mathbb{N}, p \leq n$ ou $n' \leq p)$ [demo]

L'application $\sigma : n \in \mathbb{N} \to \sigma(n) = n' \in \mathbb{N}^*$ est une bijection [demo]

Notation : $1 = \sigma(0)$

3 – Raisonnement par récurrence

Théorème : Soit $A \subset \mathbb{N}$, $0 \in A$ et $\forall\ n \in \mathbb{N}, n \in A \Rightarrow \sigma(n) \in A$. Alors $A = \mathbb{N}$ [demo]

Principe du raisonnement par récurrence (HR faible, forte)

II Ensembles finis, cardinal

1 – Ensembles $\mathbb{N}_n$

$\forall\ n \in \mathbb{N}, \mathbb{N}_n = \{\ p \in \mathbb{N}, 1 \leq p \leq n\ \}$

$\mathbb{N}_0 = \varnothing \qquad \mathbb{N}_1 = \{\ 1\ \}$

$\forall\ (n, p) \in \mathbb{N}^2, (\ \exists\ f : \mathbb{N}_n \to \mathbb{N}_p$ injective $) \quad \Rightarrow n \leq p$

[démonstration par récurrence sur n]

Corollaires : $\forall\ (n, p) \in \mathbb{N}^2, (\ \exists\ f : \mathbb{N}_n \to \mathbb{N}_p$ surjective $) \quad \Rightarrow p \leq n$

$\forall\ (n, p) \in \mathbb{N}^2, (\ \exists\ f : \mathbb{N}_n \to \mathbb{N}_p$ bijective $) \quad \Rightarrow n = p$

$f : \mathbb{N}_n \to \mathbb{N}_n$ $(1 \leq n)$ injective alors elle est bijective.

[démonstration zarbe par récurrence sur n]

Corollaire : $f : \mathbb{N}_n \to \mathbb{N}_n$ $(1 \leq n)$ surjective alors elle est bijective.

2 – Cardinal

Deux ensembles sont équipotents s'il existe une bijection du premier dans le second. La relation d'équipotence est réflexive, symétrique, et transitive (on ne parle pas de relation d'équivalence car il n'existe pas l'ensemble des ensembles).

E est fini $\Leftrightarrow E = \varnothing$ ou $\exists\ n \in \mathbb{N}^*$, E équipotent à $\mathbb{N}_n$.

Si un ensemble est fini et non vide, $\exists\ !\ n \in \mathbb{N}^*$, E équipotent à $\mathbb{N}_n$. Ce nombre est appelé le cardinal de E, noté $\#(E)$.

3 – Propriétés :

$\forall\ A \subset \mathbb{N}$, non vide : A finie $\Leftrightarrow$ A majorée

[démonstration par récurrence]

Soit $A \subset E$, E fini, alors : A fini

$\#(A) \leq \#(E)$ [demos]

$\#(A) = \#(E) \Rightarrow A = E$

Corollaires : Si un ensemble E est équipotent à l'un de ses sous–ensembles A, $A \neq E$, alors E est infini.

E est F sont deux ensembles finis non vides, et $f : E \to F$. Si $\#(E) = \#(F)$, alors 1, 2, 3 sont équivalentes :

1) f injective

2) f surjective [demos]
3) f bijective

Etude des ensembles dénombrables, c'est–à–dire en bijection avec $\mathbb{N}$. [TD 4]

4 – Loi de composition interne dans $\mathbb{N}$

$\forall$ (n, p) $\in (\mathbb{N}^*)^2$,
Soit A fini de cardinal n, et B fini de cardinal p, A et B disjoints
[on démontre que $A \cup B$ est fini]
[on démontre que A' équipotent à A et B' équipotent à B, tous disjoints $\Rightarrow$ $A' \cup B'$ est équipotent à $A \cup B$]
On définit alors $n + p = \#(A \cup B)$ – Les propriétés de + découlent de celles de $\cup$

$\forall$ (n, p) $\in (\mathbb{N}^*)^2$,
Soit A fini de cardinal n, et B fini de cardinal p,
[on démontre que $A \times B$ est fini]
[on démontre que si A' équipotent à A et B' équipotent à B, alors $A' \times B'$ est équipotent à $A \times B$]
On définit alors $n \times p = \#(A \times B)$
Element neutre : 1

5 – Somme et produit dans un monoïde commutatif

Notations :
$$\sum_{i=1}^{n} x_i = x_1 + x_2 + \ldots + x_n$$
$$\prod_{i=1}^{n} x_i = x_1 \times x_2 \times \ldots \times x_n$$

$\forall A \subset E$, E fini, $\#(A) = \sum \chi_A(x)$

$\forall (A, B) \in \mathscr{P}(E)^2$, $\#(A \cup B) = \#(A) + \#(B) - \#(A \cap B)$ [demo]

$\forall (A, B, C) \in \mathscr{P}(E)^3$, $\#(A \cup B \cup C) = \#(A) + \#(B) + \#(C) - \#(A \cap B) - \#(A \cap C) - \#(B \cap C) + \#(A \cap B \cap C)$.

Généralisation : [hum]

6 – Division euclidienne

Théorème : $\forall (a,b) \in \mathbb{N} \times \mathbb{N}^*, \exists ! (q, r) \in \mathbb{N}^2, a = b q + r$ et $r < b$

[demo : existence, en prenant b = Min { x, x ≡ a [q] } ; unicité]

III Numération

1 – Base de numération

On définit un système de numération en base B par la donnée de B symboles qui vont représenter tous les entiers compris entre 0 et B – 1.

Théorème : $\forall x \in \mathbb{N}^*, \exists ! n \in \mathbb{N}$ et $\exists ! (x_0, x_1, ..., x_n) \in \{0, 1, ..., B-1\}^{n+1}, x = \sum x_i B^i$ et $x_n \neq 0$

[demo : existence, par divisions euclidiennes en rafales, et unicité par inégalités variées : n = m puis $x_i = y_i$]

2 – Avantages d'un système de numération

- Seulement B symboles
- E(ln x / ln B) + 1 chiffres seulement pour écrire x

Comparaison : on regarde le nombre de chiffres puis on utilise l'ordre lexicographique [demo]

Opérations :

- Somme (on suppose les nombre de chiffres égaux). [demo : divisions euclidiennes des $x_i + y_i$ et retenues : z_i]
- Produit (d'un entier par un chiffre) [demo : pareil, à peu de choses près]

3 – Systèmes de numération courants

Dix, Deux, Huit, Seize

Méthodes de conversions :

- Suite de divisions euclidiennes
- Calcul direct par définition de l'écriture d'un nombre en base B

Cas particuliers :

- Si $\exists\, k \in \mathbb{N}^*$, $B' = B^k$, alors on détermine directement les nombres de la base B'
- Si $\exists\, k \in \mathbb{N}^*$, $B = B'^{\,k}$, alors on détermine directement les nombres de la base B'

4 – Exponentiation rapide

Avec le calcul de x^y, on risque d'y passer le temps de y – 1 multiplications.
Méthode : décomposer y en binaire, et calculer $x^{(2^{**}p)}$ où $p = E(\ln y / \ln 2) + 1$.
[Algorithme]

IV Analyse combinatoire

1 – Cardinal de l'ensemble des parties d'un ensemble fini

Théorème : $\#(E) = n \Rightarrow \#(\mathscr{P}_{(E)}) = 2^n$ [demo par récurrence sur n, en fixant un point a]

Théorème : $(A_i)_{i \in I}$ une partition de E fini, alors :

- $\forall\, i \in I$, A_i est fini
- I est fini
- $\#(E) = \Sigma\, \#(A_i)$

[demo : utilisation d'une fonction injective, qui à i associe A_i]

Principe des bergers : Si $f \in F^E$ est surjective, et que $\forall\, y \in F$, $f^{-1}\{y\}$ est fini, alors :

- E fini
- $\#(E) = \sum \#(f^{-1}\{y\})$

Cas particulier : Si $\exists\, k \in \mathbb{N}^*$, $\forall\, x \in f^{-1}\{y\} = k$, alors $\#(E) = k\,\#(F)$
[demo d'après le précédent]

2 – Dénombrement de l'ensemble des applications d'un ensemble fini dans un autre

Théorème : E et F finis $\Rightarrow F^E$ fini, et $\#(F^E) = \#(F)^{\#(E)}$
[demo par récurrence sur n = #(E), en fixant un point a puis bergers]

3 – Dénombrement de l'ensemble d'injections d'un ensemble fini dans un autre

Théorème : E et F finis $\Rightarrow \#(I(E,F)) = (\#(F))\,!\,/\,(\#(F) - \#(E))\,!$
[demo par récurrence sur n = #(E), en fixant un point a puis bergers]
Arrangement de p objets parmi n : $A_n^p = p\,!\,/\,(n-p)\,!$
[équipotence avec l'ensemble des injections d'un ensemble à p éléments dans un autre à n éléments]

4 – Nombre de combinaisons

Soit $\mathscr{P}_{p(E)} = \{ A \subset E, \#(A) = p \}$

Le nombre de combinaisons de p éléments dans n est équipotent à $\mathscr{P}_{p(E)}$, où #(E) = n.
[demo sans récurrence – bergers dans un cas général]

On a : $C_n^p = \dfrac{n!}{p!\,(n-p)!}$

Propriétés :

- $C_n^0 = C_n^n = 1$ [demo]
- $C_n^p = C_n^{n-p}$ [demo : $A \in \mathscr{P}_{(E)} \to \complement A$ est une bijection]
- $C_n^p = C_{n-1}^p + C_{n-1}^{p-1}$ [demo : on fixe un point a]
- Triangle de Pascal
- Formule du binôme de Newton : $(a + b)^n = \sum C_n^p a^p b^{n-p}$ [demo par récurrence sur n]
- Exercices liés aux racines $n^{\text{ièmes}}$ de l'unité : Calcul de $\displaystyle\sum_{k=0}^{E\left(\frac{n-a}{p}\right)} C_n^{pk+a}$ où $a \in \{0, ..., p-1\}$
- $\sum C_n^k = 2^n$ $\sum (-1)^k C_n^k = 0$
- $\sum k\, C_n^k = n\, 2^{n-1}$. [SPE TD 5/09/00 : $\sum k\, C_n^k = \sum (n-k)\, C_n^k$ ou dérivation de $(X + 1)^n$]
- $\sum (C_n^k)^2 = C_{2n}^n$. [SPE TD 5/09/00 : $(X + 1)^{2n}$, coefficient de X^n]

3 – Structures algébriques

I Structure de groupe

1 – Axiomes de la structure

Un groupe = ensemble muni d'une LCI associative, avec élément neutre, et tel que tout élément est symétrisable.
Si la loi est commutative, le groupe est dit abélien.
Conséquences :

- Unicité du neutre, du symétrique
- Si x' est le symétrique de x, x est le symétrique de x'

Propriétés :

- Tout élément est régulier [demo avec le symétrique]
- L'équation "$x * a = b$" a une solution unique : $x = b * a^{-1}$

Notation :

- Si le groupe est abélien : notation additive
- Sinon : notation multiplicative

Le centre d'un groupe G est $\{ a \in G, \forall b \in G, a * b = b * a \}$ [EXOS 21]

2 – Exemples

Groupes abéliens : $\mathbb{Z}, +$ $\mathscr{P}_{(E)}, \Delta$ $\mathbb{Q}^*, \times$
Groupes non–abéliens : ensemble des permutations de E dans E, $\circ$

3 – Groupes finis

Notion de table du groupe
Dans chaque ligne et dans chaque colonne de la table, chaque élément de G apparaît exactement une fois.
[demo : $y \to x\,y$ bijective]
Si $\#(G) = 1$, $G = \{ e \}$ Ex : $\{ \varnothing \}, \Delta$ $\{ 0 \}, +$
Si $\#(G) = 2$, $G = \{ e, a \}$ – table du groupe imposée par la définition du groupe. Ex : $\{ \varnothing, \{x\} \}, \Delta$
Si $\#(G) = 3$, $G = \{ e, a, b \}$ – table du groupe également imposée. Ex : $(\{ 1, j, j^2 \}, \times)$; $(\mathbb{Z}/n\mathbb{Z}, +)$
$\forall n \in \mathbb{N}^*$, $\mathbf{U}_n = \{ z \in \mathbb{C}, z^n = 1 \}$ – Chaque $\mathbf{U}_n$ est un groupe abélien de cardinal n (LCI : $\times$) [demo]

4 – Morphismes de groupe

$f : G \to G'$ est un morphisme de groupe si $\forall (x, y) \in G^2, f(xy) = f(x)\, f(y)$ et G et G' sont deux groupes multiplicatifs.
Propriétés :

- $f(e) = e'$ [demo avec f(ee).e' et le fait que tout élément est régulier]
- $(f(x))^{-1} = f(x^{-1})$ [demo par calcul de $f(x)\, f(x^{-1})$]
- La composée de deux morphismes de groupe est un morphisme de groupe

Remarque : Si $f : G \to E$ est un morphisme pour (G, .) et pour $(E,*)$, alors f(G) est un groupe pour $*$.

5 – Sous–groupes

H est un sous–groupe de G si :

- H est une partie de G
- H stable par la loi du groupe
- H est un groupe pour la loi induite de celle de G

Si H est un sous–groupe de G, ils ont le même neutre, et les éléments ont les mêmes symétriques
[demo : création d'un morphisme identité de groupe de H vers G]
Théorème : Soit H une partie de G. C'est un sous–groupe si et seulement si :

- $H \neq \varnothing$
- H stable [demo $\Leftrightarrow$]
- $\forall x \in H, x^{-1} \in H$

Corollaire : Soit H une partie de G. C'est un sous–groupe si et seulement si :

- $H \neq \varnothing$
- $\forall (x,y) \in H^2, x\,y^{-1} \in H$ [demo $\Leftrightarrow$]

Ex : $U_n = \{ z \in \mathbb{C}, z^n = 1 \}$ est un sous–groupe de $(\mathbb{C}^*, \times)$
Remarque : dans un groupe, il y a toujours au moins deux sous–groupes : {e}, et G.

Notation : $n\mathbb{Z} = \{ n\,k, k \in \mathbb{Z} \}$

Les sous–groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$, où $n \in \mathbb{N}$. [demo – utilisation de la division euclidienne]

Division euclidienne dans $\mathbb{Z}$. [demo]

Soit G un groupe multiplicatif, et $(H_i)_{i \in I}$ une famille de sous–groupes de G. Alors $\cap H_i$ est un sous–groupe. [demo]

Si Hi est la famille de tous les sous–groupes de G contenant A, $H = \cap H_i$ est le sous–groupe engendré par A. On le note gr(A)

Cas particulier : $gr\{x\} = \{ x^n, n \in \mathbb{Z} \}$ – groupe monogène (si infini), ou cyclique (si fini) [demo]

Si $f : G \to G'$ est un morphisme de groupe.

H est un sous–groupe de G $\Rightarrow$ f(H) est un sous–groupe de G' [demo]

H' est un sous–groupe de H $\Rightarrow$ $f^{-1}(H)$ est un sous–groupe de G

On appelle image du morphisme f le sous–groupe f(G), noté Im(f).

On appelle noyau du morphisme f le sous–groupe $f^{-1}\{e'\}$, noté Ker(f).

f surjective $\Leftrightarrow$ Im(f) = G' [demo]

f injective $\Leftrightarrow$ Ker(f) = {e} [demo]

II Structure d'anneau

1 – Axiomes de la structure

Anneau = ensemble muni de deux LCI (notées $\times$ et +), tel qu'il forme un groupe abélien avec le + et que le $\times$ soit associatif, distributif par rapport au +, et qu'il possède un élément neutre.

Exemples : $\mathbb{Z}, +, \times$ $\mathscr{P}_{(E)}, \Delta, \cap$

2 – Anneau d'applications

Si A est un anneau et E un ensemble non vide, A^E est un anneau [demo]

3 – Calculs dans un anneau

[Notations additives et multiplicatives]

Propriétés :

- $x \sum a_i = \sum x\, a_i$
- $\sum \sum a_i\, b_j = \ldots$
- $a \,.\, 0 = 0 \,.\, a = 0$ [demo : calcul de a(0+b)]
- $a \,.\, (-b) = (-a) \,.\, b = -ab$ [demo : calcul de a(–b+b)]
- $a \,.\, (b - c) = ab - ac$ et $(b - c) \,.\, a = ba - ca$ [demo : calcul de a((b–c)+c)]

Pour un anneau commutatif :

- Formule du binôme
- Somme des termes d'une suite géométrique : $(1-q)\, S_n = u_0\, (1 - q^{n+1})$ [demo]
- Somme des termes d'une suite arithmétique :
  - $S_1 = 1 + 2 + 3 + \ldots + n = \dfrac{n\,(n+1)}{2}$
  - $S_2 = 1^2 + 2^2 + 3^2 + \ldots + n^2 = \dfrac{n\,(n+1)\,(2n+1)}{6}$
  - $S_3 = 1^3 + 2^3 + 3^3 + \ldots + n^3 = \dfrac{n^2\,(n+1)^2}{4}$

Démonstration :

$$(n+1)^{N+1} = n^{N+1} + (N+1)\, n^N + \sum_{k=1}^{N-1} C_{N+1}^k\, n^k + 1$$

$$n^{N+1} = (n-1)^{N+1} + (N+1)\, (n-1)^N + \sum_{k=1}^{N-1} C_{N+1}^k\, (n-1)^k + 1$$

...

$$2^{N+1} = 1^{N+1} + (N+1)\, 1^N + \sum_{k=1}^{N-1} C_{N+1}^k\, 1^k + 1$$

En sommant ces égalités, on obtient :

$$(n+1)^{N+1} = (N+1)S_N + \sum_{k=1}^{n-1} C_{N+1}^k\, S_k + n + 1)$$

D'où :

$$S_N = \frac{1}{N+1}\left((n+1)^{N+1} - \sum_{k=1}^{N-1} C_{N+1}^k\, S_k - n - 1 \right)$$

4 – Eléments inversibles

x est inversible s'il existe y dans A tel que x. y = y. x = 1

Dans un anneau, les éléments inversibles forment un groupe multiplicatif [demo]

5 – Diviseurs de zéro

x est un diviseur de 0 si x non nul et il existe y dans A tel que $x.\,y = 0$
Si un anneau est commutatif et sans diviseurs de zéro, il est dit intègre.

Exemples : $\mathbb{Z}, +, \times$ est intègre ; $\mathscr{P}(E)$, Δ , $\cap$ n'est pas intègre.
Un élément x d'un anneau A est nilpotent si $\exists\ n \in \mathbb{N}, x^n = 0$ [EXOS 5]

6 – Sous–anneaux

B est un sous–anneau de A si
- B stable pour + et $\times$
- Muni des lois induites, c'est un anneau
- $1_A \in B$

B est un sous–anneau de A si
- $B \neq \varnothing$
- $\forall\ (x,y) \in B^2, x - y \in B$
- $\forall\ (x,y) \in B^2, x\,.\,y \in B$
- $1_A \in B$

Seul $(\mathbb{Z}, +, \times)$ est un sous–anneau de $\mathbb{Z}$. [demo]

7 – Morphisme d'anneaux

$f : A \to A'$ est un morphisme d'anneau si
- $\forall\ (x, y) \in A^2, f(x + y) = f(x) + f(y)$
- $\forall\ (x, y) \in A^2, f(x\,y) = f(x)\,.\,f(y)$
- $f(1_A) = 1_{A'}$

Si f est un sous–anneau, l'image de tout sous–anneau de A est un sous–anneau de A'.

III Corps

1 – Axiomes de la structure

K est un corps si c'est un anneau pour 2 lois, tel que $\forall\ x \in \mathbf{K} \setminus \{0\}$, x admet un inverse.
Exemples : $\mathbb{Q}$ $\mathbb{R}$ $\mathbb{C}$

K est un corps $\Leftrightarrow$ $(\mathbf{K},+)$ est un groupe abélien
$(\mathbf{K}^*, \times)$ est un groupe
$\times$ est distributive par rapport à +

Si la loi $\times$ est commutative, le corps est dit commutatif.

2 – Sous–corps

K ' est un sous–corps de **K** si [def]
- **K** ' stable pour + et $\times$
- **K** ' est un corps avec les lois induites

K ' est un sous–corps de **K** si [prop]
- $\mathbf{K}' \neq \varnothing$
- $\forall\ (x,y) \in \mathbf{K}'^2, x - y \in \mathbf{K}'$
- $\forall\ (x,y) \in \mathbf{K}'^{*2}, x\,.\,y^{-1} \in \mathbf{K}'^*$

3 – Morphisme de corps

$f : \mathbf{K} \to \mathbf{K}'$ est un morphisme de corps si c'est un morphisme d'anneau.
$f(\mathbf{K})$ est un sous–corps de **K** '
Un morphisme de corps est toujours une application injective. [demo avec Ker f]

4 – Diviseurs de zéro

Un corps commutatif ne contient pas de diviseurs de zéro. [demo]
Tout anneau commutatif, intègre et fini est un corps. [EXOS 5]

4 – Arithmétique des entiers relatifs, corps des rationnels et des réels

I Arithmétique de $\mathbb{Z}$

$\mathbb{Z}$ est un anneau commutatif intègre. Les sous–groupes additifs de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$, qui est stable par $\times$ mais ce n'est pas un sous–anneau si $n \neq 1$.

[TD 3]
Construction de $\mathbb{Z}$
On définit sur $\mathbb{N}^2$ une relation d'équivalence : $(a, b) \,\mathfrak{R}\, (c, d) \Leftrightarrow a + d = c + b$
et deux lois de composition interne : $(a, b) + (c, d) = (a + c, b + d)$
$(a, b) \times (c, d) = (ac + bd, ad + bc)$
On démontre que ces lois sont compatibles avec $\mathfrak{R}$. On étudie alors $\mathbb{N}^2/\mathfrak{R} = \mathbb{Z}$ pour que $\mathbb{N}$ en soit une partie, et que l'on retrouve les notations habituelles pour $\mathbb{Z}$, ainsi que l'opposé.

1 – Divisibilité

$\forall$ $(a,b) \in \mathbb{Z}^2$, $b \mid a \Leftrightarrow \exists\, q \in \mathbb{Z}, a = b q \Leftrightarrow a\mathbb{Z} \subset b\mathbb{Z}$
La relation | est réfléxive et transitive (non antisymétrique dans $\mathbb{Z}$)
$\forall$ $(a,b) \in \mathbb{Z}^2$, $b \mid a$ et $a \mid b \Leftrightarrow |a| = |b| \Leftrightarrow a\mathbb{Z} = b\mathbb{Z}$: a et b sont alors dits associés
Propriétés :

- $b|a$ et $b \neq 0 \Rightarrow \exists\,!\, q \in \mathbb{Z}$, $a = b q$ [demo]
- $0 \mid a \Rightarrow a = 0$
- $b \mid 0 \Rightarrow$ rien du tout (b n'est pas un Diviseur de Zéro)
- $a, -a, 1, -1$ divisent toujours a
- Si n divise chaque élément d'un uplet, alors n divise toute combinaison linéaire de l'uplet.

2 – PGCD

$\forall$ $(a,b) \in \mathbb{Z}^2, \exists\,!\, d \in \mathbb{N}$,
$d \mid a$ et $d \mid b$
$\forall\, c \in \mathbb{Z}, c \mid a$ et $c \mid b \Leftrightarrow c \mid d$ [demo avec l'ensemble des combinaisons linéaires de (a,b)]
Généralisation de la définition du PGCD
Cas particuliers : $a \wedge 0 = |a|$ et $a \wedge a = |a|$
La loi $\wedge$ est associative et commutative, et $(-a) \wedge b = a \wedge b$ [demos]
Algorithme d'Euclide : divisions euclidiennes en rafales [demo]
Si $d = a \wedge b$, alors $\forall\, k \in \mathbb{Z}^*$, $|k|d = ka \wedge kb$ [demo par double division]
Si $k' \in \mathbb{Z}^*$ est un diviseur de a et de b, $\exists\, (a',b',d') \in \mathbb{Z}^2 \times \mathbb{N}$, $a = a' k'$, $b = b' k'$, et $d = d' k'$, alors $d' = a' \wedge b'$
[demo très vague]
a et b sont premiers entre eux $\Leftrightarrow$ l'ensemble de leurs diviseurs est $\{ -1, 1 \}$
$\Leftrightarrow a \wedge b = 1$ [demo]
Généralisation : premiers entre eux dans leur ensemble $\Leftrightarrow a_1 \wedge a_2 \wedge ... \wedge a_n = 1$
$a \wedge b = d \Leftrightarrow \exists\, (a', b') \in \mathbb{Z}^2$, $a = d a'$ et $b = d b'$ et $a' \wedge b' = 1$.
Théorème de Bezout : $\forall$ $(a, b) \in \mathbb{Z}^2$, $a \wedge b = 1 \Leftrightarrow \exists\, (u,v) \in \mathbb{Z}^2$, $au + bv = 1$ [demo]
Généralisation...
Conséquences :

- $\forall$ $(a, b, c) \in \mathbb{Z}^3$, $a \wedge b = 1$ et $a \wedge c = 1 \Rightarrow a \wedge b c = 1$ [demo]
  Généralisation : $a \wedge b_1 = a \wedge b_2 = ... = a \wedge b_n = 1 \Rightarrow a \wedge \Pi\, b_i = 1$
  Cas particulier : $a \wedge b = 1 \Rightarrow \forall\, (n, p) \in \mathbb{N}^2$, $a^n \wedge b^p = 1$
- Théorème de Gauss : $\forall$ $(a, b, c) \in \mathbb{Z}^3$, $a \mid b c = 1$ et $a \wedge b = 1 \Rightarrow a \mid c$ [demo]
- Extension : $\forall$ (i, j), $a_i \mid c$ et ($a_i \wedge a_j = 1$ ou $i = j$) $\Rightarrow \Pi\, a_i \mid c$ [demo par récurrence]

3 – Entiers irréductibles

a est irréductible $\Leftrightarrow$ a n'est pas inversible et il n'a comme diviseurs que $1, -1, a, -a$.
a est premier $\Leftrightarrow$ a est irréductible et $a > 0$
Il y a une infinité de nombre permiers. Cette partie de $\mathbb{N}$ est dénombrable et infinie. [demo par l'absurde]
(DFP) $\forall\ n > 1, \exists\ k \in \mathbb{N}^*,\ \exists\ (a_1, a_2, ..., a_k) \in \mathbb{N}^{*\,k}, \exists\ (p_1, p_2, ..., p_k) \in \mathbb{N}^{*\,k}$ 2 à 2 distincts et premiers, $n = \Pi\ p_j^{\ aj}$
[démo par récurrence forte ; unicité à l'ordre près des facteurs]
Détermination du PGCD de deux nombres (en utilisant le Min des exposants de chaque facteur premier).
n est premier $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ est un corps [TD 5 : théorème chinois]

4 – PPCM

$\forall\ (a, b) \in \mathbb{Z}^2, \exists\ !\ m \in \mathbb{N}, a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. m est alors $a \vee b$ [demo]
$\vee$ est associatif et commutatif
Extension : $\forall\ (a_1, a_2, ..., a_n) \in \mathbb{Z}^n, \exists\ !\ m \in \mathbb{N}, \cap\ a_i\mathbb{Z} = m\mathbb{Z}$
Propriétés :
$\forall\ (a, b) \in \mathbb{Z}^2, (a \wedge b)\ (a \vee b) = |a\ b|$ [demo par double divisibilité]
Détermination du PPCM de deux nombres (en utilisant le Max des exposants de chaque facteur premier).

II Le corps des rationnels

1 – Construction de $\mathbb{Q}$

Dans $\mathbb{Z} \times \mathbb{Z}^*$, on définit une relation, et deux LCI

$$(a, b)\ \mathfrak{R}\ (a', b') \Leftrightarrow ab' = a'b$$
$$(a, b) + (a', b') = (ab' + a'b, bb')$$
$$(a, b) \times (a', b') = (aa', bb')$$

On vérifie que $\mathfrak{R}$ est une relation d'équivalence, et que les deux LCI sont associatives, commutatives, qu'elles possèdent un neutre, que $\times$ est distributif par rapport à +, et que $\mathfrak{R}$ est compatible avec + et $\times$.
Dans $\mathbb{Z} \times \mathbb{Z}^* / \mathfrak{R}$, on définit les lois quotient sur les classes qu'équivalence. L'application, qui à un couple (a,b) associe sa classe est donc un morphisme surjectif pour + et $\times$. C'est donc un anneau commutatif. Or, on peut trouver un inverse à tout couple non nul, donc c'est bien un corps commutatif. Cette construction est valide pour n'importe quel anneau intègre ; on créé alors son corps des fractions. Alors on pose $\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^* / \mathfrak{R}$, et on identifie la classe de (a,1) avec a.
$\forall\ (a,b) \in \mathbb{Z}^* \times \mathbb{Z}^*, \exists\ !\ (a', b') \in \mathbb{Z}^* \times \mathbb{N}^*, (a, b)\ \mathfrak{R}\ (a', b')$ et $a' \wedge b' = 1$ [demo existence + unicité]
Le couple (a', b') est dit irréductible.
Le seul automorphisme de $\mathbb{Q}$ est l'identité. [EXOS 5]

2 – Relation d'ordre

Dans $\mathbb{N}$, $\leq$
Dans $\mathbb{Z}$, $x \leq y \Leftrightarrow y - x \in \mathbb{N}$
Compatibilité avec les opérateurs [demo]
Règle des signes : $xy \leq 0 \Leftrightarrow$ x et y sont de signe contraire [demo]
Valeur absolue :
$|x| = 0 \Leftrightarrow x = 0$
$|x + y| \leq |x| + |y|$ [demo en faisant plein de cas]
$||x| - |y|| \leq |x - y|$ [demo d'après le précédent]
Dans $\mathbb{Q}$, $a/b \leq c/d \Leftrightarrow 0 \leq c\ b - a\ d$. Cette relation a la même valeur de vérité quels que soient les représentants des rationnels choisis. On démontre que c'est une relation d'ordre total.
Un corps C est archimédien $\Leftrightarrow \forall\ (x, y) \in C_+^* \times C, \exists\ n \in \mathbb{N}, nx > y$ [def]
$\Leftrightarrow \forall\ z \in C, \exists\ n \in \mathbb{N}, n.1_C > z$. [demo $\Leftrightarrow$]
$\mathbb{Q}$ est un corps commutatif totalement ordonné, dense et archimédien. [demo]

III Le corps des réels

1 – Nécessité d'une extension de $\mathbb{Q}$

Le carré de la longueur de la diagonale d'un carré de côté 1 est 2.

Or $x^2 = 2$ n'a pas de solution dans $\mathbb{Q}$. [demo absurde]
$A = \{ x \in \mathbb{Q}_+, x^2 < 2 \}$ n'a pas de borne supérieure [demo absurde]

2 – Existence

[ADMIS] Il existe un ensemble $\mathbb{R}$ qui est un corps commutatif, totalement ordonné, ayant la propriété de la borne supérieure (c'est–à–dire toute partie majorée admet une borne supérieure).
Remarque : Toute partie minorée admet une borne inférieure [demo]

[TD 6]
Construction de $\mathbb{R}$ grace aux sections commençantes ouvertes.
s est une section commençante ouverte $\Leftrightarrow$

- $s \subset \mathbb{Q}$; $s \neq \varnothing$; $s \neq \mathbb{Q}$
- $\forall (x, y) \in s \times \mathbb{Q}, y \leq x \Rightarrow y \in s$
- s n'a pas de plus grand élément

$\mathbb{R}$ est ensuite défini par l'ensemble des sections commançantes ouvertes,
et on identifie chaque élément a de $\mathbb{Q}$ à $s(a) = \{ x \in \mathbb{Q}, x < a \}$. D'où $\mathbb{Q} \subset \mathbb{R}$

3 – Propriétés de ℝ vis à vis de l'ordre

Valeur absolue
Intervalles : $I \subset \mathbb{R}$, I non nul, est un intervalle de $\mathbb{R} \Leftrightarrow \forall (a,b) \in I^2, a \leq b, \forall x \in \mathbb{R}, a \leq x \leq b \Rightarrow x \in I$
[demo que ça correspond à intervalle du type [a, b] ou]b, a[ou]a, →], etc.]

4 – La droite numérique achevée

$0 < 1$ car $1 = 1^2$ et $0 \leq a^2$ et $1 \neq 0$ car sinon $\mathbb{R} = \{ 0 \}$
$\Rightarrow \mathbb{R}$ ni majorée ni minorée [demo : 1 + Sup $\mathbb{R}$]

On pose $\overline{\mathbb{R}} = \mathbb{R} \cup \{ -\infty, +\infty \}$

Redéfinition de l'ordre $\leq$ dans $\overline{\mathbb{R}}$.

Dans $\overline{\mathbb{R}}$, toute partie non vide admet une borne supérieure et une borne inférieure.

La définition d'un intervalle de $\overline{\mathbb{R}}$ est la même qu'un intervalle de $\mathbb{R}$.

Soit I un intervalle de $\overline{\mathbb{R}}$. $c = \text{Inf}(I)$ et $d = \text{Sup}(I) \Rightarrow]c, d[\subset I \subset [c, d]$ [demo]
$\mathbb{R} = \ ]-\infty, +\infty[$

Problème des LCI dans $\overline{\mathbb{R}}$: indéterminations.

5 – Densité de ℚ dans ℝ

$f : \mathbb{N} \to \mathbb{R}$
$n \to n \, . \, 1_{\mathbb{R}}$ est un morphisme injectif (démo par récurrence). On identifie $f(\mathbb{N})$ avec $\mathbb{N}$, et n avec $n.1_{\mathbb{R}}$.
$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ (car $\mathbb{R}$ est un corps commutatif)
$\mathbb{R}$ archimédien [demo par l'absurde : $\mathbb{N}$ majorée dans $\mathbb{R}$?]
Partie entière : $\forall x \in \mathbb{R}, \exists ! n \in \mathbb{Z}, n \leq x < n+1$ [demo : existence suivant le signe de x ; unicité]
$\mathbb{Q}$ est dense dans $\mathbb{R}$, c'est–à–dire $\forall (x, y) \in \mathbb{R}^2, x < y \Rightarrow \exists r \in \mathbb{Q}, x < r < y$ [demo]

6 – Sous–groupes additifs de ℝ

DEMO :
$\forall a \in \mathbb{R}$, $a\mathbb{Z} = \{ ka, k \in \mathbb{Z} \} = gr(a)$
Soit H un sous–groupe de $(\mathbb{R},+)$ différent de $\{ 0 \}$
Soit $a = \text{Inf}(H \cap \mathbb{R}_+^*)$
si $a > 0$ alors H est de la forme $a\mathbb{Z}$ [demo]
si $a = 0$ alors H est dense dans $\mathbb{R}$. [demo]
Les sous–groupes additifs de $\mathbb{R}$ sont de deux formes :

- discrets : de la forme $a\mathbb{Z}$
- denses dans $\mathbb{R}$

[EXOS 6]
Les sous–groupes multiplicatifs de $\mathbb{R}_+^*$ sont de deux formes :
- discrets : de la forme $a^{\mathbb{Z}}$
- denses dans $\mathbb{R}_+^*$ (utilisation du morphisme exponentiel)

7 – Irrationnels

$\forall\ (x, n) \in \mathbb{R}_+ \times \mathbb{N}^*, \exists\ !\ y \in \mathbb{R}_+ ,\ y^n = x$ [demo en prenant Sup { $t \in \mathbb{R}_+^*, t^n \leq x$ } ; unicité]
$\forall\ n \in \mathbb{N}, \sqrt{n} \in \mathbb{Q} \Rightarrow$ n est le carré d'un nombre entier.
$\mathbb{R} \setminus \mathbb{Q}$ est dense dans $\mathbb{R}$: $\forall\ (x, y) \in \mathbb{R}^2, x < y \Rightarrow \exists\ i \in \mathbb{R} \setminus \mathbb{Q}, x < i < y$ [demo]

8 – Ensembles adjacents

(Déf) A et B sont dits adjacents $\Leftrightarrow \left\{ \begin{array}{l} A \subset \mathbb{R} \text{ et } B \subset \mathbb{R} \\ A \neq \varnothing \text{ et } B \neq \varnothing \\ \forall\ (a,b) \in A \times B,\ a \leq b \\ \forall\ \varepsilon > 0, \exists\ (a,b) \in A \times B,\ 0 < b - a < \varepsilon \end{array} \right.$

(Th) Si A et B sont adjacents, Sup A = Inf B [demo]

5 – Espaces vectoriels

I Définition et premières propriétés

1 – Loi de composition externe

Exemple : produit d'une suite par un scalaire.
Une loi de composition externe sur un ensemble E de domaine d'opérateurs Ω est une application de $\Omega \times E$ vers E.

2 – Structure d'espace vectoriel

Soit **K** un corps commutatif, et E un ensemble.
E est un **K** – espace vectoriel s'il est muni d'une LCI + telle que (E, +) soit un groupe abélien, et d'une LCE . de domaine d'opérateurs **K**, telle que
$\forall (\lambda, \mu, x, y) \in \mathbf{K}^2 \times E^2$,

1. $\lambda . (x + y) = \lambda . x + \lambda . y$
2. $(\lambda + \mu) . x = \lambda . x + \mu . x$
3. $\lambda .(\mu . x) = (\lambda .\mu) . x$
4. $1_{\mathbf{K}} . x = x$

Exemples : suites réelles, $\mathbb{R}$, $\mathbb{R}^2$, etc...
Tout corps est un espace vectoriel sur chacun de ses sous–corps.
$\mathbf{K}^n$ est un **K** – espace vectoriel.
E^X est un **K** – espace vectoriel, où X est un ensemble et E un espace vectoriel.
$\mathbf{K}^X$ est un **K** – espace vectoriel. Exemple : $\mathbb{R}^{[a, b]}$
Les éléments d'un espace vectoriel sont appelés vecteurs, et les éléments d'un domaine d'opérateurs sont appelés scalaires.
Une algèbre (ou **K** – algèbre) est un **K** – espace vectoriel pour + et . et un anneau pour + et $\times$, tel que

$\forall (\lambda, x, y) \in \mathbf{K} \times E^2, \lambda . (x \times y) = (\lambda . x) \times y = x \times (\lambda . y)$

[notion d'algèbre commutative]
Exemples : $\mathbb{R}^{\mathbb{N}}$ est une $\mathbb{R}$ – algèbre commutative
pour tout sous–corps **K** ' de **K**, **K** est une **K** ' – algèbre commutative

3 – Conséquences des axiomes

(E, +) est un groupe $\Rightarrow$ il est non vide ; il contient le vecteur nul, et chaque élément a son symétrique.
$\forall (\lambda, \mu, x, y) \in \mathbf{K}^2 \times E^2$,

1. $\lambda . (x - y) = \lambda . x - \lambda . y$
2. $(\lambda - \mu) . x = \lambda . x - \mu . x$ [demos]
3. $0_{\mathbf{K}} . x = 0_E$
4. $\lambda . x = 0_E \Leftrightarrow \lambda = 0_{\mathbf{K}}$ ou $x = 0_E$.

II Sous–espaces vectoriels

1 – Définition

$A \subset E$; A est stable pour la LCE si $\forall (\lambda, x) \in \mathbf{K} \times E, \lambda . x \in A$.
$F \subset E$ est un sous–espace vectoriel de E si

- F stable pour + et .
- F, muni de la loi interne induite par + et de la loi externe induite par ., est un **K** – espace vectoriel.

2 – Caractérisation

$F \subset E$ est un sous–espace vectoriel de E si [def]

- $F \neq \varnothing$
- F stable pour +
- F stable pour .

Corollaire : $F \subset E$ est un sous–espace vectoriel de E si [prop]

- F non vide
- $\forall (\lambda, \mu, x, y) \in \mathbf{K}^2 \times F^2, \lambda . x + \mu . y \in F$

Corollaire : $F \subset E$ est un sous–espace vectoriel de E si [prop]

- $F \neq \varnothing$
- $\forall (\lambda, x, y) \in \mathbf{K} \times F^2, \lambda . x + y \in F$

Exemple : $F = \{ (x_1, ..., x_n) ; a_1 . x_1 + ... + a_n . x_n = 0 \}$ où $a_i \in \mathbf{K}$, est un sous–espace vectoriel de $\mathbf{K}^n$.
F est une sous–algèbre de E, qui est une $\mathbf{K}$ – algèbre, si : [def]

- F stable pour $+, \times, .$
- F est un $\mathbf{K}$ – algèbre pour les lois induites
- $1_E \in F$

F est une sous–algèbre si [prop]

- $F \neq \varnothing$
- $\forall (\lambda, x, y) \in \mathbf{K} \times F^2, \lambda . x + y \in F$ et $x y \in F$
- $1_E \in F$

Exemple : L'ensemble des suites bornées

3 – Sous–espaces vectoriels engendrés

Soit $(F_i)_{i\in I}$ une famille de sous–espaces vectoriels de E. Alors $\cap F_i$ est un sous–espace vectoriel de E. [~ demo]
$\text{Vect}(A) = \cap F_i$ où $(F_i)_{i\in I}$ est la famille des sous–espaces vectoriels de E contenant A.
Exemple : combinaison linéaire dans $\mathbb{R}^3$. [demo]
Si $A = \{ x_1, ..., x_p \}$ $\text{Vect}(A) = \{ x \in E, \exists (a_1, ..., a_p) \in \mathbf{K}^p, x = \Sigma a_i x_i \}$: l'ensemble des combinaisons linéaires
Si $(x_i)_{i\in I}$ est une famille finie de vecteurs de E, $\text{Vect}(x_i, i = 1..p) = \{ x \in E, \exists (a_1, ..., a_p) \in \mathbf{K}^p, x = \Sigma a_i x_i \}$
Si $(x_i)_{i\in I}$ est une famille infinie de vecteurs de E, une combinaison linéaire des vecteurs de E est un vecteur de la forme $\Sigma \lambda_i x_i$ où $(\lambda_i)_{i\in I}$ est une famille de scalaires presque tous nuls, c'est–à–dire seuls un nombre fini d'entre eux sont non nuls.
(x_i) est un système de générateurs de $\text{Vect}(x_i; i = 1..p)$

4 – Somme de sous–espaces vectoriels

$\text{Vect}(F \cup G) = F + G$ [demo]
Généralisation : $F_1 + ... + F_p = \{ y \in E, \exists (x_1, ..., x_p) \in F_1 \times ... \times F_p, y = \Sigma x_i \} = \text{Vect}(\cup Fi)$

5 – Sous–espaces vectoriels supplémentaires

Deux sous–espaces vectoriels F et G de E sont supplémentaires si

- $E = F + G$
- $F \cap G = \{ 0 \}$

On note alors $E = F \oplus G$
En fait, ces 3 propositions sont équivalentes, si F et G sont deux sous–espaces vectoriels de E

1. $E = F \oplus G$
2. $\forall x \in E, \exists ! (y, z) \in F \times G, x = y + z$ [demo]
3. $\forall x \in E, \exists (y, z) \in F \times G, x = y + z$ et $\forall (y, z) \in F \times G, y + z = 0 \Rightarrow y = z = 0$

D'où une bijection entre E et $F \times G$
Tout sous–espace vectoriel admet au moins un supplémentaire [ADMIS]

III Applications linéaires

1 – Définition

$f : E \to E'$ est linéaire si

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

Si f et g sont linéaires, $g \circ f$ est linéaire.
Si f est un isomorphisme, f^{-1} est un isomorphisme.
Exemple : homothétie vectorielle = application linéaire f de E dans E, telle que $\exists \lambda \in \mathbf{K}, \forall x \in E, f(x) = \lambda x$
Conséquences :

$f(0) = 0$
$f(-x) = -f(x)$
$\forall (\lambda, \mu, x, y) \in \mathbf{K}^2 \times F^2, f(\lambda . x + \mu . y) = \lambda . f(x) + \mu . f(y)$ [+ généralisation...]

f est un morphisme d'algèbre si c'est une application linéaire et un morphisme d'anneaux.

2 – Applications linéaires et sous–espaces vectoriels

Si $f : E \to E'$ est linéaire, $f(F)$ est un sous–espace vectoriel de E'. [demo]
$f^{-1}(F')$ est un sous–espace vectoriel de E.

f surjective $\Leftrightarrow \mathrm{Im}(f) = G'$

f injective $\Leftrightarrow \mathrm{Ker}(f) = \{e\}$

Exemple : si $E = F \oplus G$, on peut connaître le comportement de F si on connaît son comportement sur les images des éléments de F et sur ceux de G. [demo]

Si $f : E \to E'$ est linéaire, il existe F tel que $E = F \oplus \mathrm{Ker}(f)$; alors, l'application de F vers Im(f) qui à y associe f(y) est un isomorphisme. [demo]

3 – Espace vectoriel ou algèbre d'applications linéaires

On note $\mathcal{L}(E,E')$ l'ensemble des applications linéaires de E dans E'.

$\mathcal{L}(E,E')$ est un $\mathbf{K}$ – espace vectoriel. [demo]

$\mathcal{L}(E,E) = \mathcal{L}(E)$ est une $\mathbf{K}$ – algèbre <u>non commutative</u>, le produit était la composition $\circ$, distributive par rapport à +.

Si f et g sont linéaires de E vers E ' et de E ' vers E '', $g \circ f$ est linéaire de E vers E '', et

$\mathrm{Im}(g \circ f) \subset \mathrm{Im}(g)$

$\mathrm{Ker}(f) \subset \mathrm{Ker}(g \circ f)$

$g \circ f = 0 \Leftrightarrow \mathrm{Im}(f) \subset \mathrm{Ker}(g)$ [demo]

GL(E) désigne l'ensemble des automorphisme de E (*Groupe Linéaire*).

4 – Projecteurs

Soit $E = F \oplus G$.

$p : E \to E$ est une projection de E sur F parallèlement à G est définie ainsi :

$\forall x \in E, \exists ! (y, z) \in F \times G, x = y + z ; p(x) = y$

alors p est linéaire ; $\mathrm{Im}(p) = F$; $\mathrm{Ker}(p) = G$; $p \circ p = \mathrm{Id}_E$ [demos]

$p \in \mathcal{L}(E)$ est un projecteur si $p \circ p = p$. Alors $E = \mathrm{Ker}(f) \oplus \mathrm{Im}(f)$ [demo]

6 – Familles libres, familles liées, bases, dimensions

I Familles libres, liées, génératrices

1 – Familles libres, familles liées

Une famille finie $(x_i)_{i \in \mathbb{N}p}$ est dite libre si

$\forall (a_1, ..., a_p) \in \mathbf{K}^p, \Sigma a_i x_i = 0 \Rightarrow \forall i \in \mathbb{N}_p, a_i = 0$

On parle aussi de système de vecteurs linéairement indépendants.

Une famille finie $(x_i)_{i \in \mathbb{N}p}$ est dite liée si elle n'est pas libre, c'est–à–dire si

$\exists (a_1, ..., a_p) \in \mathbf{K}^p, \Sigma a_i x_i = 0$ et $\exists i \in \mathbb{N}_p, a_i \neq 0$

On parle aussi de système de vecteurs linéairement dépendants.

Notions sur les familles :

- Une sous–famille de $(x_i)_{i\in I}$ est de la forme $(x_i)_{i\in J}$ où $J \subset I$.
- Une sur–famille de $(x_i)_{i\in I}$ est de la forme $(x_i)_{i\in K}$ où $I \subset K$.
- Deux familles $(x_i)_{i\in I}$ et $(y_i)_{i\in J}$ sont disjointes si $I \cap J = \emptyset$ et que $\forall (i, j) \in I \times J, x_i \neq y_j$
- Réunion de deux familles disjointes (création d'une famille sur l'ensemble d'index $K = I \cup J$)
- Adjonction d'un élément à une famille (on ajoute un index qui n'y était pas au départ)
- Suppression d'un élément à une famille (la famille créée a pour ensemble d'index $I \setminus \{ i_0 \}$)

Généralisation

Soit $(x_i)_{i\in I}$ une famille infinie de vecteurs de E. Elle est libre si

$\forall (\lambda_i)_{i\in I}$ une famille de scalaires presque tous nuls, $\Sigma \lambda_i x_i = 0 \Rightarrow \forall i \in I, \lambda_i = 0$

Une famille infinie est libre $\Leftrightarrow$ toute sous–famille finie est libre.

Soit $(x_i)_{i\in I}$ une famille infinie de vecteurs de E. Elle est liée si

$\forall (\lambda_i)_{i\in I}$ une famille de scalaires presque tous nuls mais non tous nuls, $\Sigma \lambda_i x_i = 0$

Une famille infinie est liée $\Leftrightarrow$ une sous–famille est liée

Exemple : applications puissances dans l'ensemble des applications polynômes

$A \subset E$, $A \neq \emptyset$, A est une partie libre (ou liée) si la famille $(a)_{a\in A}$ est libre (ou liée)

Exemple : dans $\mathbf{K}^n$, l'ensemble des vecteurs $a_i = (\delta_{1,i}, \delta_{2,i}, ... \delta_{n,i})$ est libre.

Propriétés

Toute sous–famille d'une famille libre est libre. Toute surfamille d'une famille liée est liée. [demo]

Le vecteur nul n'appartient jamais à une famille libre. S'il appartient à une famille, elle est liée.

Dans une famille qui a plus d'un vecteur, les vecteurs sont tous distincts deux à deux. [~ demo]

Une famille est liée $\Leftrightarrow \exists i_0 \in I, x_{i0} \in \mathrm{Vect}\{x_i, i \in I \setminus \{ i_0 \}\}$ [demo]

$(x_i)_{i\in I}$ est libre, et $\exists x \in E, (x_i)_{i\in I} \cup \{ x \}$ est liée $\Rightarrow x \in \mathrm{Vect}\{x_i, i \in I\}$ [demo]

2 – Familles génératrices, bases

$(x_i)_{i\in I}$ est une famille génératrice de E si $E = \mathrm{Vect}\{x_i, i \in I\}$, c'est–à–dire si

$\forall x \in E, \exists (\lambda_i)_{i\in I}$ presque tous nuls, $x = \Sigma \lambda_\iota x_i$

Exemple : les fonctions puissances génèrent les polynômes.

Une base d'un espace vectoriel est une famille libre et génératrice.

Une famille est une base de E $\Leftrightarrow \forall x \in E, \exists ! (\lambda_i)_{i\in I}$ presque tous nuls, $x = \Sigma \lambda_i x_i$ [demo]

On appelle coordonnées d'un vecteur x dans la base $(x_i)_{i\in I}$ la famille $(\lambda_i)_{i\in I}$.

Remarque : l'ordre des vecteurs figurant dans la base est important quand on considère les coordonnées de vecteurs.

Les 3 énoncés suivants sont équivalents :

- B est une base
- B est libre maximale (c'est–à–dire si on y ajoute un élément, elle n'est plus libre) [demos]
- B est génératrice minimale (c'est–à–dire si elle perd un élément, elle n'est plus génératrice)

3 – Existence des bases

Si $\mathscr{L}$ est une famille libre de E et $\mathscr{G}$ une famille génératice de E telles que $\mathscr{L} \subset \mathscr{G}$, alors il existe une base B, telle que

$\mathscr{L} \subset B \subset \mathscr{G}$ [ADMIS]

Corollaires :

- Si $E \neq \{ 0 \}$, E comporte des bases [demo]

- Théorème de la base incomplète : Si $\mathscr{L}$ est une famille libre de E et $\mathscr{G}$ une famille génératice de E, $\mathscr{L}$ est une base ou bien il existe $\mathscr{L}'$ une sous–famille de $\mathscr{G}$, telle que $\mathscr{L} \cup \mathscr{L}'$ soit une base. [demo]

4 – Existence de supplémentaires

Si on réalise une partition d'une base, on peut engendrer deux sous–espaces vectoriels supplémentaires. [demo]
Réciproque : en réunissant deux familles libres et disjointes d'une base, on peut créer une base, si les sous–espaces vectoriels engendrés par les deux familles sont supplémentaires.
Si F_1 et F_2 sont deux supplémentaires de F, alors ils sont isomorphes. [demo en utilisant une projection]

5 – Caractérisation d'une application linéaire par l'image d'une base

Théorème : Si E et E ' sont deux **K** – espaces vectoriels, B une base de E et B ' une famille quelconque de vecteurs E ' de même ensemble d'index I, alors

$\exists\,!\, f \in \mathscr{L}(E,E'),\ \forall\, i \in I,\ f(b_i) = b'_i.$ [demo]

f est injective $\Leftrightarrow$ B ' est libre
f est surjective $\Leftrightarrow$ B ' est génératrice [demos]
f est bijective $\Leftrightarrow$ B ' est une base de E '

II Dimension

1 – Espace vectoriel de dimension finie

Un espace vectoriel de dimension finie est un espace vectoriel qui peut être engendré par une famille finie.
Exemple : $\mathbf{K}^n$.

2 – Existence de bases dans un espace vectoriel de dimension finie

E est un espace vectoriel de dimension finie, non réduit au singleton vecteur nul.
Si $\mathscr{L}$ est une famille libre de E et $\mathscr{G}$ une famille génératice de E telles que $\mathscr{L} \subset \mathscr{G}$, alors il existe une base B, telle que

$\mathscr{L} \subset B \subset \mathscr{G}$

[Démonstration : on étudie l'ensemble des familles libres contenues dans $\mathscr{G}$ et contenant $\mathscr{L}$]
Corollaires :

- Si $\mathscr{G}$ est une famille génératice finie de E, il existe une sous–famille de $\mathscr{G}$ qui soit une base de E. [demo]
- Tout espace vectoriel de dimension finie non réduit au singleton vecteur nul admet une base finie.
- Théorème de la base incomplète : Si $\mathscr{L}$ est une famille libre de E et $\mathscr{G}$ une famille génératice de E, $\mathscr{L}$ est une base ou bien il existe $\mathscr{L}'$ une sous–famille de $\mathscr{G}$, telle que $\mathscr{L} \cup \mathscr{L}'$ soit une base.

3 – Dimension d'un espace vectoriel de dimension finie

[LEMME] : $\forall\, (x_1, x_2, \ldots, x_p) \in E^p,\ \forall\, (y_1, y_2, \ldots, y_{p+1}) \in E^{p+1},\ \forall\, j \in \mathbb{N}_{p+1},\ y_j \in \mathrm{Vect}\ \{ x_i, i \in \mathbb{N}_p \}$
alors $(y_i)_{i \in \mathbb{N}p+1}$ est liée.
[**DEMO** par récurrence sur p]
Théorème : Toutes les bases d'un espace vectoriel de dimension finie, non réduit au singleton vecteur nul, sont finies et ont le même cardinal. [demo]
Si E est un espace vectoriel de dimension finie, si E = { 0 }, dim E = 0, sinon, dim E = # (B) où B est une base de E.
Exemple : dim $\mathbf{K}^n = n$; polynômes engendrés par les fonctions puissances sont de dimension infinie.
Attention : la notion de dimension est dépendente du corps de base :
L étant un sous–corps de **K**, et E un **K** – espace vectoriel, on a $\dim_L E = \dim_L \mathbf{K} \,.\, \dim_{\mathbf{K}} E$ [EXOS 7]
Théorème : Si est un espace vectoriel de dimension finie, non réduit au singleton vecteur nul,

dim E = n $\Leftrightarrow$ E est isomorphe à $\mathbf{K}^n$. [demo]

Soit E de dimension $n \geq 1$, et $(x_i)_{i \in \mathbb{N}p}$ une famille de p vecteurs de E.

- Si elle est génératrice, $p \geq n$, et si p = n, c'est une base.
- Si elle est libre, $n \leq p$, et si p = n, c'est une base.

4 – Dimension d'un sous–espace vectoriel

Si F est un sous–espace vectoriel de E de dimension finie, alors dim F ≤ dim E, et F = E $\Leftrightarrow$ dim F = dim E [demo]

Si $E = F \oplus G$, et E de dimension finie, alors dim E = dim F + dim G [demo et contrexemple de la réciproque]

III Applications linéaires et dimension

1 – Rang d'un système de vecteurs

Le rang d'un système de vecteurs est (si elle existe) la dimension de l'espace vectoriel qu'ils engendrent.
Soit $(x_i)_{i \in I}$ une famille quelconque de vecteurs de E, et F l'espace–vectoriel qu'ils engendrent.

- Si E est de dimension finie, alors le rang existe, et $rg(x_i)_{i \in I} \leq \dim E$
- Si I est finie, alors le rang existe, et $rg(x_i)_{i \in I} \leq \#(I)$
- Si E est de dimension finie et I finie, alors le rang existe, et $rg(x_i)_{i \in I} \leq Min(\dim E, \#(I))$

Cas particulier : soit E de dimension finie différent du singleton vecteur nul. On considère une base $(b_i)_{i \in \mathbb{N}_n}$ et une famille finie $(x_j)_{j \in \mathbb{N}_p}$. On a : $\forall j \in \mathbb{N}_p, \exists (\lambda_i)_{i \in \mathbb{N}_p}, x_j = \sum_{i=1}^{n} \lambda_{i,j}.b_i$

On classe les coefficients $(\lambda_{i,j})$ dans un tableau.

$rg(x_j)_{j \in \mathbb{N}_p} = p \Leftrightarrow (x_j)_{j \in \mathbb{N}_p}$ est libre.

On se ramène à un cas particulier : un système étagé

$\forall j \in \mathbb{N}_p, \lambda_{i,j} \neq 0$

$\forall (i, j) \in \mathbb{N}_n \times \mathbb{N}_p, i < j \Rightarrow \lambda_{i,j} = 0$

ou

$\forall (i, j) \in \mathbb{N}_n \times \mathbb{N}_p, i > j \Rightarrow \lambda_{i,j} = 0$

Un système étagé est toujours libre. [demo par récurrence]

Soit $\mathscr{S} = (x_i)_{i \in I}$ un système quelconque de vecteurs de E, et $\mathscr{S}' = (x'_i)_{i \in I'}$ un système de vecteurs quelconques de vecteurs de E déduits de $\mathscr{S}$, car $\exists j \in I, \forall j \in I, i \neq j \Rightarrow x_i = x'_i$ et $\exists (\lambda_i)_{i \in I}, x'_j = \Sigma \lambda_i x_i$ et $\lambda j \neq 0$;

Alors, $Vect(\mathscr{S}) = Vect(\mathscr{S}')$ [demo]

Exemples dans $\mathbb{R}^4$.

Si f est un isomorphisme de E vers E', et que $\mathscr{S} = (x_i)_{i \in I}$ est une famille de vecteurs de E de rang p, alors $\mathscr{S}' = (f(x_i))_{i \in I}$ est de rang p. [demo en créant un autre isomorphisme restreint]

2 – Rang d'une application linéaire

Si Im(f) est de dimension finie, sa dimension est le rang de f.

- Si E ' est de dimension finie, Im(f) est de dimension finie, et $rg(f) \leq \dim(E')$
- Si E est de dimension finie, Im(f) est de dimension finie, et $rg(f) \leq \dim(E)$ [demo]

Théorème du rang : si f est une application linéaire de E vers E', de dimension finis, alors

dim Ker(f) + dim Im(f) = dim E [demo]

Corollaire : f injective $\Leftrightarrow rg(f) = \dim E$

f surjective $\Leftrightarrow rg(f) = \dim E'$

Si f est une application de E vers E ' et que dim E = dim E ', alors ces propositions sont équivalentes :

1. f injective
2. f surjective [~ demo]
3. f bijective

Cas particulier : f est un endomorphisme de E, ev de dimension finie.
Si E est de dimension infinie, f injective et f surjective sont indépendants [contrexemple : dérivée de polynômes]
Exemples sur les projections et les symétries

3 – Espace vectoriel $\mathcal{L}(E,E')$

[Exemple]
Si dim E ≥ 1 et dim E ' ≥ 1, alors dim $\mathcal{L}(E,E')$ = dim E . dim E'[~ demo]

4 – Dual d'un espace vectoriel

Le dual de E, en tant que **K** – espace vectoriel, est $\mathcal{L}(E, \mathbf{K})$, noté E *. Ses éléments sont nommées "formes linéaires".

Si $\varphi \in E^*$, Im φ est un sous–espace vectoriel de **K**. C'est soit { 0 } soit **K** car dim **K** = 1. Donc soit $\varphi = 0$, soit elle est surjective. Ker φ est soit E si $\varphi = 0$, soit il a comme supplémentaire un espace–vectoriel de dimension 1 c'est–à–dire une droite vectorielle.

On appelle hyperplan d'un espace vectoriel E un sous–espace vectoriel de E supplémentaire d'une droite vectorielle.
H hyperplan de E $\Leftrightarrow \exists\ \varphi \in E^*$, H = Ker φ, et $\varphi \neq 0$. [demo]
Si H est un hyperplan de E tel que H = Ker φ_1 = Ker φ_2 alors φ_1 et φ_2 sont proportionnelles. [demo]

Pour E de dimension finie $n \geq 1$:
H hyperplan de E $\Leftrightarrow$ dim H = n – 1
dim E^* = dim E [demo]
Notion de base duale B^* de E^* à une base B de E : $\forall\ (i, j) \in \mathbb{N}_n \times \mathbb{N}_n$, $b^*_j(b_i) = \delta_{ij}$
Exemple dans $\mathbb{R}^3$: les fonctions b^*_{ij} s'appellent les formes coordonnées.
Soit $(s_1, ..., s_n)$ une base de E^*. Il existe toujours une base de E telle que $(s_1, ..., s_n)$ soit sa duale. [exemple]
L'anneau des formes linéaires (avec pour multiplication $\times$) est intègre. [EXOS 9]
dim F + G = dim F + dim G – dim $F \cap G$ [demo]
Application : Si E = F + G et dim F + dim G = dim E alors $E = F \oplus G$
Si $F \cap G = \{ 0 \}$ et que dim F + dim G = dim E alors $E = F \oplus G$
L'intersection de deux hyperplans de E distincts a pour dimension dim E – 2. [demo]

IV L'algèbre des nombres complexes

1 – Définition de l'ensemble des nombres complexes

• On définit $\mathbb{C}$ comme $\mathbb{R}^2$, muni de sa structure de $\mathbb{R}$ – espace vectoriel.
On définit la multiplication comme : $(a, b) \times (a', b') = (aa' - bb', ab' + a'b)$
On démontre que $(\mathbb{C}, +, \times)$ est un corps commutatif. On identifie $\mathbb{R}$ comme un sous–corps de $\mathbb{C}$.
$\mathbb{C}$ est donc une $\mathbb{R}$ – algèbre commutative de dimension 2, mais il ne peut exister d'ordre compatible avec ses opérations. [~ demo]
• Constructions possibles de $\mathbb{C}$

$$\mathbb{C} = \mathbb{R}^2$$
$$\mathbb{C} = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \Big/ (a, b) \in \mathbb{R}^2 \right\}.$$
$$\mathbb{C} = \mathbb{R}[X] \big/ {}_{(X^2+1)\mathbb{R}[X]}.$$

• L'application : $z \to \bar{z}$ est involutive [demo]
Il n'y a que 2 automorphismes de corps de $\mathbb{C}$: l'identité, et l'application $z \to \bar{z}$.[demo]

2 – Interprétation géométrique

Interprétation géométrique de la somme : translation
Le groupe $(\mathbb{C}, +)$ est isomorphe au groupe des translations du plan pour la loi $\circ$. [demo]

3 – Interprétation trigonométrique

Module d'un nombre complexe. $|z| = \sqrt{(z\bar{z})} = \sqrt{(a^2 + b^2)}$

- $|z| = 0 \Leftrightarrow z = 0$
- $|z_1 z_2| = |z_1||z_2|$ [demo]
- $|z_1 + z_2| \leq |z_1| + |z_2|$ [demo en réécrivant la conclusion au carré]

Conséquences

- $|\Pi\ z_k| = \Pi\ |z_k|$
- $|z^n| = |z|^n$
- $|\Sigma\ z_k| \leq \Sigma\ |z_k|$
- $||z_1| - |z_2|| \leq |z_1 - z_2|$

$1 / z = \bar{z} / |z|$
$\mathbf{U} = \{ z \in \mathbb{C}, |z| = 1 \}$ est un groupe abélien pour $\times$. [demo]
L'application $\mathbb{R} \times \mathbf{U} \to \mathbb{C}$
$(x, u) \to x\,u$ est un isomorphisme de groupe multiplicatif.
où la loi $\times$ est définie sur $\mathbb{R} \times \mathbf{U}$ comme : $(x, u) \times (x', u') = (x\,x', u\,u')$
Morphisme exponentiel :
$\forall\ u \in U, \exists\,!\ (a,b) \in \mathbb{R}^2, u = a + i\,b$ et $\exists\ \theta \in \mathbb{R}, a = \cos(\theta)$ et $b = \sin(\theta)$
L'application $\mathbb{R} \to \mathbf{U}$
$\theta \to e^{i\theta}$ est un morphisme surjectif de $(\mathbb{R}, +)$ sur $(\mathbf{U}, \times)$ [demo]

Notation : $e^{i\theta} = \cos(\theta) + i \sin(\theta)$
Formule de Moivre : $\forall (n, \theta) \in \mathbb{N} \times \mathbb{R}, (e^{i\theta})^n = e^{i\theta n}$
Formules d'Euler : $\cos(\theta) = (e^{i\theta} - e^{-i\theta}) / 2$; $\sin(\theta) = (e^{i\theta} + e^{-i\theta}) / 2i$

Formulaire trigonométrique : (sicocosi cocosisi)

$\cos(a+b) = \cos a \cos b - \sin a \sin b$ $\cos(a-b) = \cos a \cos b + \sin a \sin b$ $\sin(a+b) = \sin a \cos b + \cos a \sin b$ $\sin(a-b) = \sin a \cos b - \cos a \sin b$	$\sin p + \sin q = 2 \sin((p+q)/2) \cos((p-q)/2)$ $\sin p - \sin q = 2 \cos((p+q)/2) \sin((p-q)/2)$ $\cos p + \cos q = 2 \cos((p+q)/2) \cos((p-q)/2)$ $\cos p - \cos q = -2 \sin((p+q)/2) \sin((p-q)/2)$
$\cos(2a) = \cos^2 a - \sin^2 a = 1-2\sin^2 a = 2\cos^2 a - 1$	$\sin(2a) = 2 \sin a \cos a$
$\cos^2 a = \dfrac{1 + \cos 2a}{2}$	$\sin^2 a = \dfrac{1 - \cos 2a}{2}$

Conséquences : expression de $\cos(n\theta)$ en fonction de $\cos^k(\theta)$ [exemple : utilisation de Moivre]
expression de $\cos^k(\theta)$ en fonction de $\cos(n\theta)$ [exemple : utilisation d'Euler]

⌦ il faut connaître les formules de trigonométrie (Centrale2000)

$\forall z \in \mathbb{Z}, \exists \theta \in \mathbb{R}, e^{i\theta} = z / |z|$; θ est une mesure de l'argument de z.
$\forall z \in \mathbb{Z}, \exists (\rho, \theta) \in \mathbb{R}_+^* \times \mathbb{R}, z = \rho e^{i\theta}$ (forme trigonométrique)
Egalité de deux complexes ⇔ Egalité de leurs modules et égalité à 2π près d'une mesure de leur argument.
L'application $f : \mathbb{R}_+^* \times \mathbb{R} \to \mathbb{C}$, telle que $f(\rho, \theta) = \rho e^{i\theta}$ est un morphisme surjectif de groupe.

4 – Racines d'un nombre complexe

Racines carrées d'un réel négatif a dans $\mathbb{C}$: $i\sqrt{-a}$ et $-i\sqrt{-a}$ [demo]
Racines carrées d'un nombre complexe : expression algébriques des racines carrées [calculs]
Racines $n^{\text{ièmes}}$ d'un nombre complexe non nul : formes trigonométriques.
On cherche z tel que $z^n = Z = \rho e^{i\theta}$.
Il existe $j \in \mathbb{Z}$, $z = \sqrt[n]{p} \,.\, e^{i(\theta + 2j\pi)/n}$. [demo]
$U_n = \{ z \in \mathbb{C}, z^n = 1 \}$
$\forall Z \in \mathbb{Z}$, les racines $n^{\text{ièmes}}$ de Z sont $z_0 \,.\, w$, où w décrit U_n. [demo]
U_n est un groupe cyclique de cardinal n. [demo]
$e^{i(2k\pi)/n}$ est générateur de $U_n \Leftrightarrow k \wedge n = 1$ [demo]
Equation du $2^{\text{ème}}$ degré dans $\mathbb{C}$: mise sous la forme canonique. [calculs]
Une équation de degré n admet dans $\mathbb{C}$ n racines (certaines pouvant être doubles, triples...)

[EXOS 8]
Un nombre complexe est dit algébrique s'il annule un pôlynome à coefficients rationnels. C'est un corps dénombrable qui contient $\mathbb{Q}$. Un nombre non–algébrique est dit transcendant.

⌦ "Ne faut–il pas signaler ici que l'expression $\sqrt{z}$ a maintenant droit de cité depuis des décennies dans les calculatrices et logiciels de calcul (Maple, Mathematica, etc…) ? Il suffit de la prononcer "racine carrée principale" : c'est celle dont l'argument est dans $[-\pi/2; \pi/2]$." (Centrale1999 ; Se méfier)

V Equations différentielles linéaires

1 – Equations différentielles

Une équation différentielle est une équation qui lie une fonction, sa variable et quelques unes de ses dérivées.
Equation différentielle d'ordre 1 : $F(x, y, y') = 0$. où y est une fonction dérivable dans un intervalle I
Exemple : $x + y.y' = 0$
Définition d'une solution de l'équation différentielle.
Equation différentielle d'ordre 2 : $F(x, y, y', y'') = 0$. où y est une fonction dérivable deux fois dans un intervalle I

[TD 7]
L'ensemble des suites vérifiant une relation de récurrence linéaire d'ordre n forme un $\mathbb{R}$ – espace vectoriel de dimension n. On peut chercher une base sous la forme d'une suite géométrique, ce qui aboutit à une équation caractéristique de degré n. Grâce à cette étude on peut déterminer l'expression générale de telles suites.
⌦ Il faut savoir le faire. (X2000)

2 – Equation différentielle linéaire d'ordre 1

Elle est de la forme $a(x)\, y' + b(x)\, y = c(x)$ où a, b, c sont continues dans un intervalle I,
et $\forall x \in I, a(x) \neq 0$.

Les solutions de l'équation sans second membre forment un $\mathbb{R}$ – espace vectoriel de dimension 1. [demo]

Soit $x_0 \in I$.

L'application $\varphi_0 : I \to \mathbb{R}$, $\varphi_0(x) = \exp\left(-\int_{x_0}^{x} \frac{b(t)}{a(t)}\, dt\right)$ est une base de cet espace vectoriel. [solution + génératrice]

⌦ Ce n'est vrai qu'en dimension 1 (X2000).

Equation avec 2ème membre : les solutions sont $y_0 + \varphi$, où φ est une solution de l'équation sans second membre, et y_0 une solution de l'équation avec second membre. [demo]

Exemple : $y' + y = x$.

Les solutions d'une équation différentielle à coefficients constants sont les fonctions définies sur $\mathbb{R}$, de la forme

$x \to \lambda\, e^{-(b/a)x}$, où λ est une constante réelle quelconque

<u>Recherche d'une solution particulière avec 2ème membre</u> :

- Si c est un polynôme de degré n, on prend pour y_0 un polynôme de degré n si $b \neq 0$, et de degré $n + 1$ si $b = 0$
- Si c est de la forme $e^{\alpha x} . P(x)$ où $P(x)$ est un polynôme de degré n : on pose $w(x) = y(x)/e^{\alpha x}$ et on prend pour w un polynôme de degré n si $e^{\alpha x}$ n'est pas solution de l'équation sans second membre, et n+1 si $e^{\alpha x}$ est solution.

Si c est $\sin(\alpha x)$, on cherche y_0 de la forme $\lambda \sin(\alpha x) + \mu \cos(\alpha x)$

Dérivée d'une fonction à valeur complexe : $\forall f \in \mathbb{C}^{\mathbb{R}}, f' = (\mathrm{Re}(f))' + i\, (\mathrm{Im}(f))'$

$\forall a \in \mathbb{C}, (e^{a\,\mathrm{Id}})' = a . e^{a\,\mathrm{Id}}$ [demo]

Si c est de la forme $e^{\alpha x} \sin(\beta x)\, P(x)$ ou $e^{\alpha x} \cos(\beta x)\, P(x)$ (où P est une application polynôme), on leur associe l'équation différentielle dans $\mathbb{C}$:

$a\, y' + by = e^{(\alpha+i\beta)x} P(x)$, dont on trouve une solution particulière comme pour $c = e^{\alpha x} . P(x)$ et on en prend la partie réelle ou imaginaire.

Remarque : Si c est une somme d'applications, la somme d'équations particulières avec chaque second membre est une solution particulière de l'équation générale.

<u>Méthode de variation de la constante</u> :

$a(x)\, y' + b(x)\, y = c(x)$ où a ne s'annule pas. On sait trouver les solutions de l'équation sans second membre.

Solution particulière : on cherche comme solution :

$$y_0(x) = \lambda(x) \exp\left(-\int_{x_0}^{x} \frac{b(t)}{a(t)}\, dt\right) = \lambda(x)\, \varphi_0(x)$$

Alors $\lambda'(x) = \dfrac{c(x)}{a(x)\, \varphi_0(x)}$. il suffit de trouver une primitive [demo]

⌦ Il faut maîtriser cette méthode (Centrale2000).

Exemple : $y' \sin x + y \cos x = 1/\cos x$ sur $]\, 0 \,;\, \pi/2\, [$

3 – Equations différentielles linéaires d'ordre 2 à coefficients constants

$a\, y'' + b\, y' + c\, y = d(x)$ où $a \neq 0$, et d une fonction continue sur I

Les solutions de $a\, y'' + b\, y' + c\, y = 0$ forment un $\mathbb{R}$ – espace vectoriel. On cherche des solutions sous la forme $x \to e^{r x}$ donc $a\, r^2 + b\, r + c = 0$ (équation caractéristique)

Si $\Delta = b^2 - 4\, ac > 0$: r_1 et r_2, deux racines réelles distinctes. $y_1 = e^{r_1 x}$ et $y_2 = e^{r_2 x}$ sont libres [demo]

Si $\Delta = b^2 - 4\, ac = 0$: r, une racine double. $y_1 = e^{r_1 x}$ et $y_2 = x\, e^{r_1 x}$ sont libres, et y_2 est solution [demo]

Si $\Delta = b^2 - 4\, ac < 0$: $r_1 = \alpha + i\, \beta$ et $\bar{r}_1 = \alpha - i\, \beta$, deux racines complexes conjuguées.

$y_1 = e^{\alpha x} \cos \beta x$ et $y_2 = e^{\alpha x} \sin \beta x$ sont libres, et solutions [~demo]

Alors, les y_1 et y_2 sont génératrices [**DEMO**]

Donc la dimension de l'espace vectoriel des solutions de l'équation différentielle est de 2.

<u>Solutions de l'équation avec 2ème membre :</u>

Toutes les solutions sont obtenues en ajoutant à une solution particulière y_0 toutes les solutions de l'équation sans 2e membre.

Recherche d'une solution particulière y_0 :

- Si d est un polynôme de degré n, on prend pour y_0 un polynôme de degré n si $c \neq 0$, de degré n+1 si $c = 0$ et $b \neq 0$ et de degré n+2 si $c = b = 0$.
- Si $d(x) = e^{kx} P(x)$ où P polynome de degré n, on cherche $y_0 = e^{kx} z_0(x)$ où $z_0(x)$ est un polynôme de degré n si k n'est pas solution de l'équation caractéristique, de degré n+1 si k est racine simple et n+2 si k est racine double.
- Si $d(x) = e^{(\alpha + i\beta)x} P(x)$, on procède de même.

7 – Suites réelles

I Généralités

1 – Définition d'une suite

Une suite est une application de $\mathbb{N}$ dans E.

2 – Exemples

(u_n) constante $\Leftrightarrow \forall n \in \mathbb{N}, u_n = u_0$

(u_n) stationnaire $\Leftrightarrow \exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow u_n = u_{n0}$

(u_n) arithmétique $\Leftrightarrow \exists r \in \mathbb{R}, \forall n \in \mathbb{N}, u_{n+1} = u_n + r$

Alors $u_n = u_0 . r^n$

Et $S_n = (n+1)\, u_0 + r . n . (n+1) / 2$

(u_n) géométrique $\Leftrightarrow \exists q \in \mathbb{R}, \forall n \in \mathbb{N}, u_{n+1} = q . u_n$

Alors $u_n = q^n u_0$

Et $S_n =$ $u_0 . (1 - q^{n+1})/(1 - q)$ si $q \neq 1$

$u_0 . (n + 1)$ si $q = 1$

3 – Structure de $\mathbb{R}^{\mathbb{N}}$

$\mathbb{R}^{\mathbb{N}}$ est une $\mathbb{R}$ – algèbre commutative de dimension infinie [demo].

4 – Suites extraites

Soit $(u_n) \in \mathbb{R}^{\mathbb{N}}$; on appelle suite extraite de (u_n) une suite (v_n), telle que

$\exists \varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante, $\forall n \in \mathbb{N}, v_n = u_{\varphi(n)}$

φ est strictement croissante $\Leftrightarrow \forall n \in \mathbb{N}, \varphi(n+1) > \varphi(n)$

$\Leftrightarrow \forall (p, q) \in \mathbb{N}^2, p > q \Rightarrow \varphi(p) > \varphi(q)$

$\Rightarrow \forall n \in \mathbb{N}, \varphi(n) \geq n$

Exemples : suites extraites des termes de rang pair ou impair, suite tronquée...

5 – Suite et relation d'ordre

(u_n) majorée $\Leftrightarrow \exists M \in \mathbb{R}, \forall n \in \mathbb{N}, u_n \leq M$

(u_n) minorée $\Leftrightarrow \exists m \in \mathbb{R}, \forall n \in \mathbb{N}, u_n \geq m$

(u_n) bornée $\Leftrightarrow$ (u_n) majorée et minorée

(u_n) majorée $\Leftrightarrow$ (u_n) majorée à partir d'un certain rang [demo]

(u_n) minorée $\Leftrightarrow$ (u_n) minorée à partir d'un certain rang

(u_n) bornée $\Leftrightarrow$ (u_n) bornée à partir d'un certain rang

(u_n) bornée $\Leftrightarrow \exists a \in \mathbb{R}_+, \forall n \in \mathbb{N}, |u_n| \leq a$ [demo]

(u_n) croissante $\Leftrightarrow \forall n \in \mathbb{N}, u_n \leq u_{n+1}$

(u_n) strictement croissante $\Leftrightarrow \forall n \in \mathbb{N}, u_n < u_{n+1}$

(u_n) croissante $\Leftrightarrow \forall (p, q) \in \mathbb{N}^2, p < q \Rightarrow u_p \leq u_q$

(de même pour les suites décroissantes)

II Suites convergentes

1 – Définition

(u_n) converge vers $\ell \Leftrightarrow \forall \varepsilon \in \mathbb{R}_+, \exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow |u_n - \ell| \leq \varepsilon$

c'est–à–dire $\ell - \varepsilon \leq u_n \leq \ell + \varepsilon$

c'est–à–dire $u_n \in [\ell - \varepsilon, \ell + \varepsilon]$

(u_n) converge vers $\ell \Leftrightarrow \forall \varepsilon \in \mathbb{R}_+, \exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow |u_n - \ell| < \varepsilon$

Notation : $(u_n) \to \ell$

Si $(u_n) \to \ell$ alors ℓ est unique. On l'appelle limite de (u_n), noté $\lim(u_n)$ [demo]

$(u_n) \to \ell \Leftrightarrow (u_n - \ell) \to 0$

2 – Limite et relation d'ordre

Une suite convergente est une suite bornée.[demo et contrexemple de la réciproque]
$(u_n) \to \ell \Rightarrow (|u_n|) \to |\ell|$ [demo]

3 – Exemples

Suite constante, stationnaire, $(1/n)_{n>0}$, suites géométriques de raison $q \in]-1, 1[$ sont convergentes. [demo]
$(u_n) \to \ell \Rightarrow$ Toute suite extraite de (u_n) converge vers ℓ. [demo]
Si on extrait à (u_n) deux suites qui convengent vers 2 limites distinctes, alors (u_n) diverge.
Si on extrait à (u_n) une suite divergeante, alors (u_n) diverge.
Ex: $(\sin(n\pi/2))$ est divergeante.

[TD 8]
Suites homographiques : $u_{n+1} = (a\ u_n + b) / (c\ u_n + d)$; On étudie l'équation $cx^2 + (d-a)x - b = 0$.
Si elle a 2 racines, x et y, on démontre que $(u_n - x) / (u_n - y)$ est géométrique.
Suivant le rapport, $(u_n) \to x$, $(u_n) \to y$ ou (u_n) est périodique de période 2.
Si elle a une seule racine, x, on démontre que $1 / (u_n - x)$ est arithmétique, donc $(u_n) \to x$.

4 – Extension à $\overline{\mathbb{R}}$

(u_n) diverge vers $+\infty \Leftrightarrow \forall A \in \mathbb{R}, \exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow u_n \geq A$
(u_n) diverge vers $-\infty \Leftrightarrow \forall A \in \mathbb{R}, \exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow u_n \leq A$
Notation : $(u_n) \to +\infty$
$(u_n) \to +\infty \Rightarrow$ Toute suite extraite de (u_n) diverge vers $+\infty$

III Convergence et structure de $\mathbb{R}$

1 – Opérations sur les limites

Les suites réelles convergentes forment une sous–algèbre de $\mathbb{R}^{\mathbb{N}}$, et l'application qui à (u_n) associe $\lim(u_n)$ est un morphisme d'algèbre :

$\lim(u_n + v_n) = \lim(u_n) + \lim(v_n)$ [demo]
$\lim(u_n \,.\, v_n) = \lim(u_n) \,.\, \lim(v_n)$ [demo]
$\lim(\lambda\ u_n) = \lambda \lim(u_n)$ [demo]
$\lim(v_n / u_n) = \lim(v_n) / \lim(u_n)$ [demo]

Extension à $\overline{\mathbb{R}}$

$(u_n) \to +\infty$ et $(v_n) \to \ell \Rightarrow (u_n + v_n) \to +\infty$ [demo]
(somme, produits, et inverses de limites avec ∞)

[EXOS 10]
Convergence en moyenne de Césaro : si une suite tend vers un réel, il en est de même pour la suite définie comme la moyenne arithmétique (ou pondérée) des n premiers éléments de la suite.
Lemme de l'escalier : si $(u_{n+1} - u_n)$ tend vers un réel a, (u_n/n) tend vers a.

[EXOS 11]
Le seul automorphisme de $\mathbb{R}$ est l'identité.

2 – Comparaison des limites

$\lim(u_n) < \lim(v_n) \Rightarrow \exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow u_n < v_n$
Contraposée : $\exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow u_n \leq v_n$
alors $\lim(u_n) \leq \lim(v_n)$
Théorème des 3 suites (ou des gendarmes) : $\exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow u_n \leq v_n \leq w_n$ et $\lim(u_n) = \lim(w_n)$
alors $\lim(v_n) = \lim(u_n) = \lim(w_n)$

Extension à $\overline{\mathbb{R}}$

$\exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow u_n \leq v_n$
$u_n \to +\infty \Rightarrow v_n \to +\infty$

$v_n \to -\infty \Rightarrow u_n \to -\infty$

3 – Suites monotones

(u_n) croissante et majorée $\Rightarrow$ elle converge [demo]
(u_n) croissante et non majorée $\Rightarrow$ elle diverge vers $+\infty$ [demo]
(de même pour (u_n) décroissante)
(I_n) est une suite de segments emboités si $I_n = [a_n, b_n]$, où (a_n) est croissante, (b_n) décroissante, et $\forall n \in \mathbb{N}, a_n < b_n$
Alors $[\lim(a_n), \lim(b_n)] = \cap [a_n, b_n]$ [demo]
Si (a_n) est croissante, (b_n) décroissante, et $\lim(b_n - a_n) = 0$, (a_n) et (b_n) sont dites adjacentes.
Deux suites adjacentes convergent vers la même limite [demo]
Théorème de Bolzano–Weierstrass (XIXème) : de toute suite bornée de $\mathbb{R}$ on peut extraire une suite convergente
[**DEMO**]

IV Approximation d'un réel

1 – Approximation par des rationnels

Tout réel est limite d'une suite de rationnels. [demo]

2 – Approximation décimale

$\forall x \in \mathbb{R}, \forall n \in \mathbb{N}, \exists ! p_n \in \mathbb{Z}, p_n / 10^n \le x < (p_n + 1) / 10^n$ [~demo]
On pose $(x_n) = (p_n / 10^n)$ et $(y_n) = ((p_n + 1) / 10^n)$
(x_n) et (y_n) sont adjacentes. [demo]
On pose $a_n = p_{n+1} - 10 p_n \in \{0, 1, ..., 9\}$
A tout réel x on associe une suite d'entiers (a_n) tels que $a_0 \in \mathbb{Z}$ et $\forall n \in \mathbb{N}^*, a_k \in \{0, 1, ..., 9\}$ avec

$x = \sum_{k=0}^{+\infty} \frac{a_k}{10^k}$ (Développement décimal illimité de x). [demo]

On a $\forall n \in \mathbb{N}, \exists p \in \mathbb{N}, p > n$ et $a_p \neq 9$ [demo par l'absurde]
Réciproque : A toute suite (a_n) telle que
$a_0 \in \mathbb{Z}$,
$\forall k \in \mathbb{N}^*, a_k \in \{0, 1, ..., 9\}$,
$\forall n \in \mathbb{N}, \exists p \in \mathbb{N}, p > n$ et $a_p \neq 9$
on associe un réel x tel que $x = \Sigma a_k/10^k$. [demo]
$\mathbb{R}$ est non dénombrable [demo par l'absurde]
$\mathbb{R}$ est équipotent à $2^{\mathbb{N}}$. $\mathbb{R}^n$ est équipotent à $\mathbb{R}$. [ADS Spé]
Développement décimal d'un rationnel : un nombre est rationnel si et seulement s'il existe une période dans le développement décimal de celui–ci [demo TD 9]

V Comparaison des suites

1 – Relation de domination

(u_n) est dominée par $(v_n) \Leftrightarrow \exists \alpha > 0, \exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \ge n_0 \Rightarrow |u_n| \le \alpha|v_n|$
Notation : $(u_n) = O(v_n)$
La relation de domination est réflexive et transitive. [~demo]
$(u_n) = O(v_n) \Leftrightarrow \exists n_0 \in \mathbb{N}, \exists (w_n)_{n \ge n0} \in \mathbb{R}^{\mathbb{N}}, (u_n)_{n \ge n0} = (v_n)_{n \ge n0} \times (w_n)_{n \ge n0}$ et $(w_n)_{n \ge n0}$ bornée[demo]
Cas particulier : Si $(V_n) \in (\mathbb{R}^*)^{\mathbb{N}}$, $(u_n) = O(v_n) \Leftrightarrow (u_n / v_n)$ bornée

- $(u_n) = O(w_n)$ et $(v_n) = O(w_n)$ $\Rightarrow (u_n + v_n) = O(w_n)$
- $(u_n) = O(w_n)$ et $(v_n) = O(x_n)$ $\Rightarrow (u_n \times v_n) = O(w_n \times x_n)$ [demo]
- $(u_n) = O(v_n)$ $\Rightarrow (\lambda u_n) = O(v_n)$

Si $(u_n) = O(v_n)$ et $(v_n) \to 0$ alors $(u_n) \to 0$ [demo]
Si $\exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \ge n_0 \Rightarrow \frac{u_{n+1}}{u_n} \le \frac{v_{n+1}}{v_n}$ alors $(u_n) = O(v_n)$ [demo]

Corollaire : Si $\exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \ge n_0 \Rightarrow \frac{u_{n+1}}{u_n} \le \frac{v_{n+1}}{v_n}$ et $(v_n) \to 0$ alors $(u_n) \to 0$

Si $\exists\, k \in \overline{\mathbb{R}}$, $(u_{n+1} / u_n) \to k$ alors

- $|k| < 1 \Rightarrow (u_n) \to 0$
- $|k| > 1 \Rightarrow (|u_n|) \to +\infty$ [demo]

2 – Relation de prépondérance

(u_n) est négligeable devant (v_n) $\Leftrightarrow$ (v_n) est prépondérante devant (u_n)
$\Leftrightarrow\ \forall\, \alpha > 0, \exists\, n_0 \in \mathbb{N}, \forall\, n \in \mathbb{N}, n \geq n_0 \Rightarrow |u_n| \leq \alpha |v_n|$

Notation : $(u_n) = o(v_n)$
La relation de prépondérance est transitive. [demo]

- $(u_n) = o(v_n) \Rightarrow (u_n) = O(w_n)$
- $(u_n) = o(v_n)$ et $(v_n) = O(w_n) \Rightarrow (u_n) = o(w_n)$
- $(u_n) = O(v_n)$ et $(v_n) = o(w_n) \Rightarrow (u_n) = o(w_n)$
- $(u_n) = o(v_n)$ et $(w_n) = o(x_n) \Rightarrow (u_n + w_n) = o(v_n + x_n)$
- $(u_n) = o(v_n)$ et $(w_n) = o(x_n) \Rightarrow (u_n \times w_n) = o(v_n \times x_n)$ [demo]
- $(u_n) = o(v_n) \Rightarrow (\lambda\, u_n) = o(v_n)$

$(u_n) = o(v_n) \Leftrightarrow \exists\, n_0 \in \mathbb{N}, \exists\, (W_n)_{n \geq n0} \in \mathbb{R}^{\mathbb{N}}, (u_n)_{n \geq n0} = (v_n)_{n \geq n0} \times (w_n)_{n \geq n0}$ et $(w_n)_{n \geq n0} \to 0$ [demo]

Cas particulier : Si $(v_n) \in (\mathbb{R}^*)^{\mathbb{N}}$, $(u_n) = o(v_n) \Leftrightarrow (u_n / v_n) \to 0$
Exemples : $((\ln n)^a) = o(n^b)$ $(n^b) = o(c^n)$ $(c^n) = o(n!)$

3 – Relation d'équivalence

$(u_n) \sim (v_n) \Leftrightarrow (u_n - v_n) = o(v_n)$. C'est une relation d'équivalence. [DEMO]
$(u_n) \sim (v_n) \Leftrightarrow \exists\, n_0 \in \mathbb{N}, \exists\, (w_n)_{n \geq n0} \in \mathbb{R}^{\mathbb{N}}, (u_n)_{n \geq n0} = (v_n)_{n \geq n0} \times (w_n)_{n \geq n0}$ et $(w_n)_{n \geq n0} \to 1$ [demo]

Cas particulier : Si $(v_n) \in (\mathbb{R}^*)^{\mathbb{N}}$, $(u_n) \sim (v_n) \Leftrightarrow (u_n / v_n) \to 1$
Exemples : $(\sin u_n) \sim (u_n)$ $(e^{un} - 1) \sim (u_n)$ $(\ln(u_n+1)) \sim (u_n)$

Si $(u_n) \sim (v_n)$ et $(v_n) \to a \in \overline{\mathbb{R}}$, alors $(u_n) \to a$. [demo]
Si $(u_n) \sim (v_n)$ et $(w_n) \sim (x_n)$, alors :

- $(u_n\, w_n) \sim (v_n\, x_n)$
- $(u_n / w_n) \sim (v_n / x_n)$ si la division est possible
- Si $(v_n) = o(x_n)$ alors $(u_n + w_n) \sim (x_n)$
- Si $\exists\, n_0 \in \mathbb{N}, \forall\, n \in \mathbb{N}, n \geq n_0 \Rightarrow v_n > 0$ et $x_n > 0$ alors $(u_n + w_n) \sim (v_n + x_n)$
- Si $\exists\, \alpha \in \mathbb{R}$, $(x_n) \sim (\alpha\, v_n)$, alors :
    - Si $\alpha \neq -1$, alors $(u_n + w_n) \sim ((1+\alpha)\, v_n)$
    - Si $\alpha = -1$, alors $(u_n + w_n) = o(v_n)$ [DEMOS]

Exemples sur les suites fractions de polynômes.

<u>VI Suites complexes</u>

1 – $\mathbb{C}$ – algèbre des suites complexes

$\mathbb{C}^{\mathbb{N}}$ est une $\mathbb{C}$ – algèbre [~demo].
$\forall\, (u_n) \in \mathbb{C}^{\mathbb{N}}, \exists\, ((a_n), (b_n)) \in (\mathbb{R}^{\mathbb{N}})^2, (u_n) = (a_n) + i\,(b_n)$
(u_n) est bornée $\Leftrightarrow \exists\, M \in \mathbb{R}_+, \forall\, n \in \mathbb{N}, |u_n| \leq M$.
L'ensemble des suites bornées forment une sous–algèbre de $\mathbb{C}^{\mathbb{N}}$.
$(u_n) = (a_n) + i\,(b_n)$ est bornée $\Leftrightarrow (a_n)$ et (b_n) sont bornées [~demo]

2 – Suites convergentes

(u_n) converge vers $\ell \Leftrightarrow \forall\, \varepsilon \in \mathbb{R}_+, \exists\, n_0 \in \mathbb{N}, \forall\, n \in \mathbb{N}, n \geq n_0 \Rightarrow |u_n - \ell| \leq \varepsilon$
(u_n) converge $\Rightarrow (u_n)$ bornée [demo]
$(u_n) \to \alpha + i\,\beta \Leftrightarrow (a_n) \to \alpha$ et $(b_n) \to \beta$ [demo]

3 – Opérations sur les limites

$\forall\, ((u_n), (v_n)) \in (\mathbb{C}^{\mathbb{N}})^2$, telles que (u_n) et (v_n) convergent,
$\forall\, (\lambda, \mu) \in \mathbb{C}^2$, $\lim(\lambda\,(u_n) + \mu\,(v_n)) = \lambda \lim(u_n) + \mu \lim(v_n)$
$\lim(u_n\, v_n) = \lim(u_n) \lim(v_n)$

4 – Relations de comparaison

On utilise les mêmes relations binaires qu'avec les suites réelles, mais certaines propriétés ne se retrouvent plus dans $\mathbb{C}^{\mathbb{N}}$ si l'ordre intervient.