Cours d'algèbre et d'analyse du premier semestre de L1

(écrit par Jean-Yves Ducloux [(*)], version de 2023 avec table des matières)

Table des matières

Sources :

• Liret et Martinais, *Mathématiques pour le DEUG. Algèbre 1ère année.* Éd. Dunod. [512 LIR]

• Liret et Martinais, *Mathématiques pour le DEUG. Analyse 1ère année.* Éd. Dunod. [517 LIR]

• E. Ramis, C. Deschamps, J. Odoux, Cours de mathématiques [51 L RAM] :
[512 RAM], [514 RAM], [515 RAM], [517 RAM], [517 RAM], niveau L1 seul dans [51 L1 RAM]

• Marc Hindry, *Cours de Mathématiques, Première Année.* Université Paris 7.
(`http://www.imj-prg.fr/~marc.hindry/Cours-L1.pdf`)

Précisions :

Le fichier source contient :

– *des démonstrations* qu'on fait apparaître en vert en remplaçant

`\long\def\invisible#1{}` par `%\long\def\invisible#1{}`

– des compléments, pour s'adapter à d'éventuels nouveaux programmes plus complets, qu'on fait apparaître en rouge en remplaçant

`\long\def\horsprogramme#1{}` par `%\long\def\horsprogramme#1{}`

Ce fichier source est utilisable librement par tous les enseignants de l'UFR de mathématiques de l'université Paris Cité. Vous pouvez réutiliser le fichier source et le modifier significativement sans me citer pour votre enseignement. Merci de me citer si vous reproduisez des chapitres quasiment à l'identique.

(*) Pour me contacter : Jean-Yves Ducloux <`ducloux@math.univ-paris-diderot.fr`>

Ch. 1. Études de fonctions (rappels)

Plan
I. Fonctions réelles d'une variable réelle
II. Bijection, réciproque
III. Limites, asymptotes
IV. Continuité et dérivabilité

I. Fonctions réelles d'une variable réelle

1. Généralités

Définition

Soient E et F des ensembles, et $\overbrace{A \text{ une partie de } E}^{\text{ce qui se note « } A \subseteq E \text{ »}}$.

(a) On appelle *fonction* de E dans F une loi f qui à tout élément x de E fait correspondre au plus un élément y de F, appelé quand il existe « image de x par f » et noté $f(x)$.
Dans ce cas, on dit que : E est *l'ensemble de départ de* f, F est *l'ensemble d'arrivée de* f, et l'ensemble D_f des éléments de E qui ont une image par f est *l'ensemble de définition de* f.

(b) On appelle *application* de E dans F une loi f qui à tout élément x de E associe un unique élément y de F, noté $f(x)$. Il s'agit donc d'une fonction f de E dans F telle que $D_f = E$.

On écrira en abrégé « $f : E \to F$ » pour exprimer que f est une application de E dans F, et « $f : \begin{array}{l} E \to F \\ x \mapsto y_x \end{array}$ » pour exprimer que f est l'application de E dans F qui envoie x sur y_x.

(c) Soit $f : E \to F$. La *restriction* de f à A est l'application $f|_A : \begin{array}{l} A \to F \\ x \mapsto f(x) \end{array}$.

Exemple

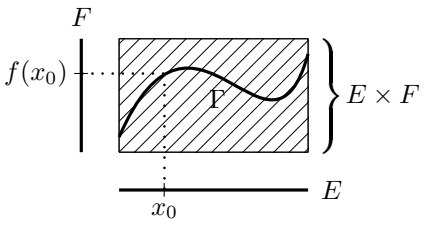
Soit E un ensemble. L'application $\mathrm{id}_E : \begin{array}{l} E \to E \\ x \mapsto x \end{array}$ s'appelle *l'application identité de* E.

Définition

Soit $f : E \to F$. On note $E \times F$ l'ensemble formé des couples (x, y) avec $x \in E$ et $y \in F$.

a) Le *graphe de* f est la partie Γ suivante de $E \times F$:

$$\Gamma := \{(x, f(x)) \,;\, x \in E\}$$
$$\text{donc} \qquad \Gamma = \{(x, y) \in E \times F \mid y = f(x)\}.$$



b) Lorsque $E \subseteq \mathbb{R}$ et $F = \mathbb{R}$, le graphe de f s'appelle aussi *la courbe représentative de* f.

Remarque

Pour les mathématiciens, une fonction (resp. une application) d'un ensemble E dans un ensemble F est un triplet (E, F, Γ) où Γ est une partie de $E \times F$ dont l'intersection avec chaque ensemble $\{x_0\} \times F$, $x_0 \in E$, contient au plus un élément (resp. exactement un élément).

Définition

(a) On appelle *fonction réelle de la variable réelle* (resp. *fonction complexe de la variable réelle*) une fonction de $\mathbb{R}$ dans $\mathbb{R}$ (resp. dans $\mathbb{C}$).

(b) Un *intervalle de* $\mathbb{R}$ est un ensemble de l'une des formes : $\emptyset$; $]a,b[$, $]a,b]$, $[a,b[$ avec $a,b \in \mathbb{R}$ et $a < b$; $[a,b]$ avec $a,b \in \mathbb{R}$ et $a \leq b$; $]a,+\infty[$, $[a,+\infty[$ avec $a \in \mathbb{R}$; $]-\infty,b[$, $]-\infty,b]$ avec $b \in \mathbb{R}$; $]-\infty,+\infty[$.

Parmi eux, les *intervalles ouverts* sont $\emptyset$, $]a,b[$ ($a,b \in \mathbb{R}$ et $a < b$), $]a,+\infty[$ ($a \in \mathbb{R}$), $]-\infty,b[$ ($b \in \mathbb{R}$), $]-\infty,+\infty[$; les *segments* sont $[a,b]$ ($a,b \in \mathbb{R}$ et $a \leq b$).

(c) Les bornes inférieure (« $\inf I$ ») et supérieure (« $\sup I$ ») d'un intervalle non vide I sont les coefficients $\alpha, \beta \in \mathbb{R} \cup \{-\infty, +\infty\}$ tels que I est d'une des formes $]\alpha,\beta[$, $]\alpha,\beta]$, $[\alpha,\beta[$, $[\alpha,\beta]$.

Exemple

Soit A une partie de $\mathbb{R}$.

L'application $\mathbb{1}_A : \mathbb{R} \to \mathbb{R}$ s'appelle *la fonction caractéristique de* A.
$x \mapsto \begin{cases} \text{ou } 1 \text{ si } x \in A \\ 0 \text{ si } x \notin A \end{cases}$

Son ensemble de définition est $\mathbb{R}$.

Remarque

On montrera plus tard qu'une partie I de $\mathbb{R}$ est un intervalle si et seulement si :

$$\forall x, y \in I \quad \forall t \in \mathbb{R} \quad (x \leq t \leq y \implies t \in I).$$

2. Certaines propriétés des fonctions

Définition

Soit $f : \underset{\text{partie de } \mathbb{R}}{D} \longrightarrow \mathbb{R}$.

(a) On dit que f est *croissante* (resp. *décroissante*) si :
$f(x) \leq f(y)$ (resp. $f(x) \geq f(y)$) pour tous $x, y \in D$ tels que $x \leq y$

(b) On dit que f est *strictement croissante* (resp. *strictement décroissante*) si :
$f(x) < f(y)$ (resp. $f(x) > f(y)$) pour tous $x, y \in D$ tels que $x < y$

(c) On dit que f est *monotone* (resp. *strictement monotone*) si elle est croissante ou décroissante (resp. strictement croissante ou strictement décroissante).

Définition

Soient $f : \underset{\text{partie de } \mathbb{R}}{D} \longrightarrow \mathbb{R}$ et $T \in \mathbb{R} \setminus \{0\}$.

(a) On dit que f est *paire* si :
pour tout $x \in D$, on a $-x \in D$ et $f(-x) = f(x)$.

(b) On dit que f est *impaire* si :
pour tout $x \in D$, on a $-x \in D$ et $f(-x) = -f(x)$.

(c) On dit que f est *périodique de période* T si :
pour tout $x \in D$, on a $x + T \in D$ et $x - T \in D$ et $f(x+T) = f(x)$.

Remarque

Une variante de la définition (c) consiste à remplacer la condition « $x+T \in D$ et $x-T \in D$ » par « $x + T \in D$ » (cela permet par exemple de s'intéresser aux « suites périodiques »).

3. Fonctions rationnelles et trigonométriques

En annexe : les graphes des fonctions usuelles (dont cosh, sinh, et tanh).

Définition

(a) On dit qu'une application f de $\mathbb{R}$ dans $\mathbb{R}$ (resp. dans $\mathbb{C}$) est polynomiale s'il existe $n \in \mathbb{N}$ et $a_0, ..., a_n \in \mathbb{R}$ (resp. $\mathbb{C}$) tels que : $f(x) = a_n x^n + ... + a_1 x + a_0$ pour $x \in \mathbb{R}$.

(b) On dit qu'une fonction f de $\mathbb{R}$ dans $\mathbb{R}$ (resp. dans $\mathbb{C}$) est rationnelle s'il existe $p, q \in \mathbb{N}$, $a_0, ..., a_p \in \mathbb{R}$ (resp. $\mathbb{C}$), et $b_0, ..., b_q \in \mathbb{R}$ (resp. $\mathbb{C}$) non tous nuls, tels que : $f(x) = \frac{a_p x^p + ... + a_1 x + a_0}{b_q x^q + ... + b_1 x + b_0}$ pour tout $x \in \mathbb{R}$ vérifiant $b_q x^q + ... + b_1 x + b_0 \neq 0$.

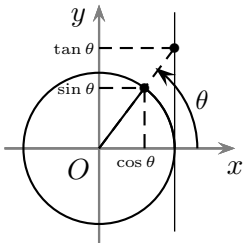
Notation

Soient $a, x, y \in \mathbb{R}$. On écrit $y \equiv x\,[a]$, ce qui se lit y *est congru à* x *modulo* a, s'il existe $k \in \mathbb{Z}$ tel que : $y = x + ka$.

Définition-Proposition

←[ln est l'unique solution $y :]0, +\infty[\to \mathbb{R}$ de : $y(1) = 0$ et $y'(x) = \frac{1}{x}$ pour $x > 0$]

(a) Les applications $\cos : \mathbb{R} \to \mathbb{R}$ et $\sin : \mathbb{R} \to \mathbb{R}$ sont les uniques applications continûment dérivables de $\mathbb{R}$ dans $\mathbb{R}$ telles que $(\cos\theta, \sin\theta)$ parcourt le cercle trigonométrique dans le sens direct en partant de $(1, 0)$ lorsque $\theta \in \mathbb{R}$, sur une longueur $\beta - \alpha$ quand θ va de α à β ($\beta > \alpha$) :



Cela implique que $\gamma = (\cos, \sin)$ est une courbe paramétrée de classe C^1 telle que $\|\gamma(\theta)\|^2 = 1$, donc $\gamma'(\theta)$ est multiple positif de $i\gamma(\theta)$ (en dérivant sachant qu'on tourne dans le sens direct), $\|\gamma'(\theta)\| = 1$ pour $\theta \in \mathbb{R}$ (dériver l'égalité $\int_0^\theta \|\gamma'(t)\|\,dt = \theta$ par rapport à θ), et $\gamma(0) = (1, 0)$. En particulier, en identifiant $\mathbb{R}^2$ à $\mathbb{C}$: $\gamma' = i\gamma$ et $\gamma(0) = 1$.

(b) Il existe un plus petit réel $\theta > 0$ tel que $\sin\theta = 0$. On le note π.

(c) L'application cos est paire et 2π périodique.
L'application sin est impaire et 2π périodique.
De plus : $\cos^2 x + \sin^2 x = 1$ pour tout $x \in \mathbb{R}$.

(d) On a : $\cos'(x) = -\sin x$ et $\sin'(x) = \cos x$ pour $x \in \mathbb{R}$; en particulier : $\frac{\sin x}{x} \underset{\substack{x \to 0 \\ x \neq 0}}{\longrightarrow} 1$.

(e) Pour tous $x, y \in \mathbb{R}$, on a : $\begin{array}{|l} \cos y = \cos x \iff \big(y \equiv x\,[2\pi] \text{ ou } y \equiv -x\,[2\pi]\big) ; \\ \sin y = \sin x \iff \big(y \equiv x\,[2\pi] \text{ ou } y \equiv \pi - x\,[2\pi]\big). \end{array}$

Proposition

(a) Pour tous $\alpha, \beta \in \mathbb{R}$, on a : $\boxed{\cos(\alpha + \beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta}$.

(Prendre la partie réelle de part et d'autre de $e^{i(\alpha+\beta)} = e^{i\alpha}e^{i\beta}$.)
En particulier, quand $\alpha \in \mathbb{R}$: $\cos(2\alpha) = 2\cos^2\alpha - 1 = 1 - 2\sin^2\alpha$.

(b) Pour tous $\alpha, \beta \in \mathbb{R}$, on a : $\boxed{\sin(\alpha + \beta) = \sin\alpha\cos\beta + \cos\alpha\sin\beta}$.

(Prendre la partie imaginaire de part et d'autre de $e^{i(\alpha+\beta)} = e^{i\alpha}e^{i\beta}$.)
En particulier, quand $\alpha \in \mathbb{R}$: $\sin(2\alpha) = 2\sin\alpha\cos\alpha$.

Définition-Proposition

(a) La fonction $\tan := \frac{\sin}{\cos}$ est définie sur $\mathbb{R}\backslash(\frac{\pi}{2}+\pi\mathbb{Z})$, où $\frac{\pi}{2}+\pi\mathbb{Z} := \{\frac{\pi}{2}+k\pi\ ;\ k\in\mathbb{Z}\}$.
L'application $\tan : \mathbb{R}\backslash(\frac{\pi}{2}+\pi\mathbb{Z}) \to \mathbb{R}$ est impaire et π-périodique.

(b) L'application $\tan : \mathbb{R}\backslash(\frac{\pi}{2}+\pi\mathbb{Z}) \to \mathbb{R}$ est dérivable et :
$$\tan'(x) = 1+\tan^2 x = \frac{1}{\cos^2 x} \text{ pour tout } x\in\mathbb{R}\backslash(\tfrac{\pi}{2}+\pi\mathbb{Z}).$$
De plus : $\tan x \underset{x\to-\frac{\pi}{2}^+}{\longrightarrow} -\infty$ et $\tan x \underset{x\to\frac{\pi}{2}^-}{\longrightarrow} +\infty$.

(c) Pour tous $x,y\in\mathbb{R}\backslash(\frac{\pi}{2}+\pi\mathbb{Z})$, on a : $\tan y = \tan x \iff y\equiv x\,[\pi]$.
(En effet, « $\tan y = \tan x$ » se traduit par « $\sin x\cos y - \sin y\cos x = \sin 0$ ».)

4. Fonctions logarithme et exponentielle

Définition-Proposition

(a) L'application $\ln\colon]0,+\infty[\to\mathbb{R}$ est définie par : $\ln x = \int_1^x \frac{\mathrm{d}t}{t}$ pour $x>0$.

(b) L'application ln est dérivable et $\ln' x = \frac{1}{x}$ pour tout $x>0$.
Elle est strictement croissante, avec : $\ln x \underset{x\to0^+}{\longrightarrow} -\infty$ et $\ln x \underset{x\to+\infty}{\longrightarrow} +\infty$.

(c) On a : $\ln(xy) = \ln x + \ln y$ et $\ln\left(\frac{x}{y}\right) = \ln x - \ln y$ pour tous $x,y>0$.

Définition-Proposition

(a) L'application $\exp\colon\mathbb{R}\to\mathbb{R}$ envoie $x\in\mathbb{R}$ sur l'unique $y\in]0,+\infty[$ tel que $x=\ln y$.
Pour tous $x,y\in\mathbb{R}$, on a donc : $y=\exp x \iff \big(y>0 \text{ et } x=\ln y\big)$.

(b) L'application exp est dérivable et $\exp' x = \exp x$ pour tout $x\in\mathbb{R}$.
Elle est strictement croissante, avec : $\exp x \underset{x\to-\infty}{\longrightarrow} 0$ et $\exp x \underset{x\to+\infty}{\longrightarrow} +\infty$.

Définition-Proposition

(a) Soit $a\in\mathbb{R}$. On note : $x^a = \exp(a\ln(x))$ pour $x>0$ (généralise le cas « $a\in\mathbb{N}\backslash\{0\}$ »).
Ainsi : $\ln(x^a) = a\ln(x)$ pour tout $x>0$

(b) On pose : $\mathrm{e} = \exp(1)$. On a donc : $\mathrm{e}^x = \exp(x)$ pour tout $x\in\mathbb{R}$.

(c) Soit $a\in\mathbb{R}$. Pour tout $x>0$, on a : $\frac{\mathrm{d}}{\mathrm{d}x}(x^a) = a\,x^{a-1}$ $\big(\text{mais } \frac{\mathrm{d}}{\mathrm{d}a}(x^a) = (\ln x)x^a\big)$.
L'application $\begin{array}{ccc}]0,+\infty[& \to & \mathbb{R} \\ x & \mapsto & x^a\end{array}$ est : constante égale à 1 lorsque $a=0$, strictement croissante de 0 à $+\infty$ quand $a>0$, et, strictement décroissante de $+\infty$ à 0 quand $a<0$.

(d) On a : $(x^a)^b = x^{ab}$, $x^{a+b} = x^a\,x^b$ et $x^{a-b} = \frac{x^a}{x^b}$ pour tous $a,b\in\mathbb{R}$ et $x>0$.

Remarques

1. Soit $a>0$. On prolonge l'application $x>0\mapsto x^a$ par continuité en 0 en posant $0^a=0$.

2. Soient $a\in\mathbb{R}\backslash\{0\}$ et $x,y>0$. On a : $x^a = y \iff x = y^{\frac{1}{a}}$.

3. Soient $n\in\mathbb{N}\backslash\{0\}$ et $x,y\in\mathbb{R}$. Si n est pair, on a : $x^n = y \iff \big(y\geq 0 \text{ et } x\in\{\pm y^{\frac{1}{n}}\}\big)$.
Si n est impair, on a : $x^n = y \iff \big((y\geq 0 \text{ et } x = y^{\frac{1}{n}}) \text{ ou } (y<0 \text{ et } x = -|y|^{\frac{1}{n}})\big)$.

Proposition (« croissances comparées »)

Soient $a>0$ et $k>0$. On a :

(i) $x^a\,|\ln x|^k \underset{x\to0^+}{\longrightarrow} 0$ et $\frac{(\ln x)^k}{x^a} \underset{x\to+\infty}{\longrightarrow} 0$;

(ii) $|x|^a\,\mathrm{e}^x \underset{x\to-\infty}{\longrightarrow} 0$ et $\frac{\mathrm{e}^x}{x^a} \underset{x\to+\infty}{\longrightarrow} +\infty$.

II. Bijection, réciproque

1. Antécédent, image d'une application

Définition

Soient $f\colon E \to F$ une application et $b \in F$.

Un antécédent de b par f est un point x de E tel que $f(x) = b$.

Définition

Soient $f\colon E \to F$ une application et $A \subseteq E$.

(a) *L'image de A par f* est la partie $f(A)$ suivante de F :

$$\underbrace{f(A)}_{\text{(image d'une partie)}} := \{\underbrace{f(x)}_{\text{(image d'un point)}} \ ; \ x \in A\} = \{y \in F \mid \exists x \in A \quad y = f(x)\}.$$

(b) *L'image de f*, notée $\operatorname{Im} f$, est la partie $f(E)$ de F.

2. Injection, surjection, bijection

Définition

Soit $f\colon E \to F$ une application.

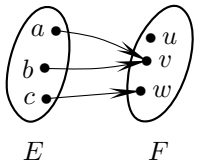
(a) On dit que f est injective (ou que « f est une injection ») si :
pour tout $y \in F$, l'équation $y = f(x)$ a au plus une solution $x \in E$.

(b) On dit que f est surjective (ou que « f est une surjection ») si :
pour tout $y \in F$, l'équation $y = f(x)$ a au moins une solution $x \in E$.

(c) On dit que f est bijective (ou que « f est une bijection ») si :
pour tout $y \in F$, l'équation $y = f(x)$ a une seule solution $x \in E$.

Remarque

Soit $f\colon E \to F$ une application (penser à :



).

(a) L'application f est injective si et seulement si tout point y de F a au plus un antécédent par f (sur le dessin on interdit que deux flèches arrivent sur le point y).

(b) L'application f est surjective si et seulement si tout point y de F a au moins un antécédent par f (sur le dessin au moins une flèche arrive sur le point y).

(c) L'application f est bijective si et seulement si tout point y de F a exactement un antécédent par f (sur le dessin exactement une flèche arrive sur le point y).

Proposition

Soit $f\colon E \to F$ une application

(a) L'application f est injective si et seulement si on a :
si $x', x'' \in E$ vérifient $f(x') = f(x'')$, alors $x' = x''$.

(b) L'application f est surjective si et seulement si $f(E) = F$.

(c) L'application f est bijective si et seulement si f est injective et surjective.

Démonstration

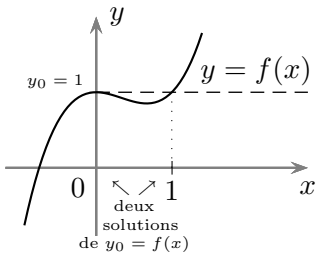
(a) ($\Longrightarrow$) On suppose f injective. Soient $x', x'' \in E$ tels que $f(x') = f(x'')$.
On pose $y := f(x')$. Comme x' et x'' sont 2 solutions de l'équation $y = f(x)$, on a $x' = x''$.
($\Longleftarrow$) Par contraposition, on suppose f non-injective.
Il existe $y_0 \in F$ tel que l'équation $y_0 = f(x)$ a 2 solutions distinctes x'_0 et x''_0.
On en déduit que l'implication « $f(x') = f(x'') \Rightarrow x' = x''$ » est fausse.

(b) Découle de la définition. □

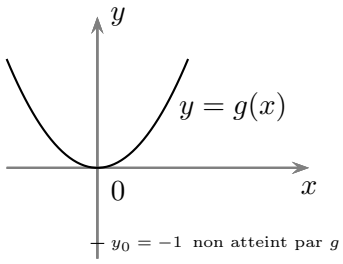
Remarque

Quand E et F sont des intervalles de $\mathbb{R}$, et f est continue, un tableau de variations permet de répondre aux questions « f est-elle injective ? » et « f est-elle surjective ? ».

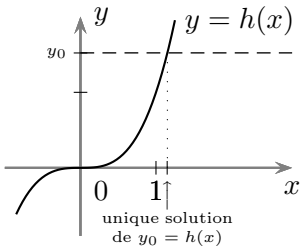
Par exemple, on considère $f\colon \begin{array}{ccc}\mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^2(x-1)+1\end{array}$, $g\colon \begin{array}{ccc}\mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^2\end{array}$, $h\colon \begin{array}{ccc}\mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^3\end{array}$.



f non injective (et surjective)



g non surjective (et non injective)



h bijective

3. Composition, réciproque

Définition

Soient E, F et G des ensembles.

(a) Soient f une application de E dans F et g une application de F dans G.
On appelle *composée de f et g* l'application $g\circ f\colon \begin{array}{ccc}E & \longrightarrow & G \\ x & \longmapsto & g(f(x))\end{array}$.

(b) Soient f une fonction de E dans F et g une fonction de F dans G.
On note D_f et D_f les ensembles de définition de f et g, et pose : $D_{g\circ f} := \{x \in D_f \mid f(x) \in D_g\}$.
On appelle *composée de f et g* la fonction $g\circ f\colon x \mapsto g(f(x))$ de E dans G d'ensemble de définition $D_{g\circ f}$.

Exemple

Pour toute application $f\colon E \to F$, on a : $f\circ \mathrm{id}_E = f = \mathrm{id}_F \circ f$.

Proposition

Soient $f\colon E \to F$, $g\colon F \to G$, et $h\colon G \to H$ des applications.
On a : $(h\circ g)\circ f = h\circ(g\circ f)$.

Démonstration

Tout d'abord, $(h\circ g)\circ f$ et $h\circ(g\circ f)$ vont toutes deux de E dans H.
Pour tout $x \in E$, on a :
$$\big((h\circ g)\circ f\big)(x) = (h\circ g)\big(f(x)\big) = h\Big(g\big(f(x)\big)\Big) = h\big((g\circ f)(x)\big) = \big(h\circ(g\circ f)\big)(x).$$
Cela donne le résultat. □

Définition-Proposition

Une application $f\colon E \to F$ est bijective si et seulement si :
il existe une application $g\colon F \to E$ telle que $g\circ f = \mathrm{id}_E$ et $f\circ g = \mathrm{id}_F$.

Dans ce cas, g est unique, appelée *réciproque de f* et notée $\underbrace{f^{-1}}$, et on a :

(i) $\forall x \in E \quad \forall y \in F \quad \big(y = f(x) \iff x = f^{-1}(y)\big)$; ne pas confondre avec $\frac{1}{f}$

(ii) f^{-1} est bijective et $(f^{-1})^{-1} = f$.

Démonstration

• ($\Longrightarrow$) On suppose f bijective.

– Soit $y_0 \in F$. On note $g(y_0)$ l'unique solution $x \in E$ de l'équation $y_0 = f(x)$.
– On construit ainsi une application $g\colon F \to E$ telle que $y = f(g(y))$ pour tout $y \in F$. Cela s'écrit : $\mathrm{id}_F = f \circ g$.
– Soit $x \in E$. On pose : $y_0 = f(x)$. Par définition de g, on a : $g(y_0) = x$, puis $g(f(x)) = x$. Cela s'écrit : $g \circ f = \mathrm{id}_E$.

($\Longleftarrow$) On suppose qu'il existe $g\colon F \to E$ telle que $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$.

Soit $y \in F$. Pour tout $x \in E$, on a :

$$y = f(x) \implies g(y) = \underbrace{g(f(x))}_{x} \implies x = g(y)$$

et aussi :

$$x = g(y) \implies f(x) = \underbrace{f(g(y))}_{y} \implies y = f(x).$$

Donc l'équation $y = f(x)$ d'inconnue $x \in E$ a pour seule solution $g(y)$.
Cela prouve que f est bijective et que g est unique.

• Il reste à vérifier (i) et (ii).

Le (i) a été obtenu au cours de la preuve du sens « ($\Longleftarrow$) ».
Il permet de résoudre à x fixé l'équation $(E)\colon\ x = \underbrace{f^{-1}}_{\text{notation pour } g}(y)$ d'inconnue y.

Donc f^{-1} est bijective, et $(f^{-1})^{-1}$ qui $\underbrace{\text{s'obtient}}_{\text{cf. (i) avec } f^{-1} \text{ au lieu de } f}$ en résolvant (E) est égale à f. □

Remarque

Lorsque f est une bijection d'une partie E de $\mathbb{R}$ sur une partie F de $\mathbb{R}$, d'après (i) le graphe de f^{-1} est le symétrique de celui de f par rapport à la 1re bissectrice (d'équation $y = x$).

Exemple

Soit $y \in \mathbb{R}_+$. Pour tout $x \in \mathbb{R}_+$, on a : $y = x^4 \iff x = \overbrace{y^{\frac{1}{4}}}^{\text{noté } \sqrt[4]{y}}$.
L'application $f\colon \begin{array}{ccc}\mathbb{R}_+ & \to & \mathbb{R}_+ \\ x & \mapsto & x^4\end{array}$ a donc pour réciproque $f^{-1}\colon \begin{array}{ccc}\mathbb{R}_+ & \to & \mathbb{R}_+ \\ y & \mapsto & \sqrt[4]{y}\end{array}$.

Proposition

Soient $f\colon E \to F$ et $g\colon F \to G$ des bijections.

L'application $g \circ f$ est bijective, et on a : $\boxed{(g \circ f)^{-1} = f^{-1} \circ g^{-1}}$.

Démonstration

Soit $z \in G$. Pour tout $x \in E$, on a grâce à la bijectivité de g et de f :

$$\begin{aligned} z = (g \circ f)(x) &\iff z = g(f(x)) &&\iff g^{-1}(z) = f(x) \\ &\iff f^{-1}(g^{-1}(z)) = x &&\iff x = (f^{-1} \circ g^{-1})(z). \end{aligned}$$

On en déduit, en tenant compte de la définition de la bijectivité, que $g \circ f$ est bijective, et, d'après le (i) de la proposition précédente, que : $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. □

4. Exemples

Définition-Proposition (« fonctions trigonométriques réciproques »)

(a) Les applications $\arcsin\colon [-1,1] \to \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$, $\arccos\colon [-1,1] \to [0,\pi]$, $\arctan\colon \mathbb{R} \to \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$ sont les réciproques (continues) des bijections continues strictement monotones suivantes :

$\left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \to [-1,1]$ qui croît, $\begin{array}{ccc} y & \mapsto & \sin y \end{array}$; $[0,\pi] \to [-1,1]$ qui décroît, $\begin{array}{ccc} y & \mapsto & \cos y \end{array}$; $\left]-\frac{\pi}{2}, \frac{\pi}{2}\right[\to \mathbb{R}$ qui croît, $\begin{array}{ccc} y & \mapsto & \tan y \end{array}$.

Par conséquent, pour tous $x, y \in \mathbb{R}$ on a :

$$\big(x \in [-1,1] \text{ et } y = \arcsin x\big) \iff \big(y \in \big[-\tfrac{\pi}{2}, \tfrac{\pi}{2}\big] \text{ et } x = \sin y\big)\,;$$
$$\big(x \in [-1,1] \text{ et } y = \arccos x\big) \iff \big(y \in [0,\pi] \text{ et } x = \cos y\big)\,;$$
$$y = \arctan x \iff \big(y \in \big]-\tfrac{\pi}{2}, \tfrac{\pi}{2}\big[\text{ et } x = \tan y\big).$$

(b) On a : $\left|\begin{array}{l} \arcsin'(x) = \frac{1}{\sqrt{1-x^2}} \text{ quand } x \in]-1,1[\,; \\ \arccos'(x) = -\frac{1}{\sqrt{1-x^2}} \text{ quand } x \in]-1,1[\,; \\ \arctan'(x) = \frac{1}{1+x^2} \text{ quand } x \in \mathbb{R}. \end{array}\right.$

On en déduit que : $\arcsin x + \arccos x = \frac{\pi}{2}$ quand $x \in [-1,1]$.

Remarques

1. Pour tout $x \in [-1,1]$, on a : $\sin(\arcsin x) = \sin|_{[-\frac{\pi}{2},\frac{\pi}{2}]}(\arcsin x) = x$.
Cependant : $\arcsin(\sin \pi) \neq \pi$ (attention !).

2. Soit $x \in [-1,1]$. On a : $\arcsin(-x) = -\arcsin x$ (éléments de $[-\frac{\pi}{2}, \frac{\pi}{2}]$ de même sinus).
On a aussi : $\arccos(-x) = \pi - \arccos x$ (éléments de $[0,\pi]$ de même cosinus).

3. Soit $x \in \mathbb{R}$. On a : $\arctan(-x) = -\arctan x$ (éléments de $\big]-\frac{\pi}{2}, \frac{\pi}{2}\big[$ de même tangente).

Bonus

On plie une feuille $ABCD$ au format A4 avec $AB = \sqrt{2}\,BC$ suivant la diagonale $[A,C]$, puis rabat vers l'intérieur (ensuite l'une dans l'autre) les deux pointes libres B et D au moyen de deux autres plis issus des pointes A ou C de façon à ce que ces plis suivent les bords de la feuille partant de ces pointes A ou C. On obtient un triangle AIC isocèle en I, qu'on pose sur la table avec (AC) horizontale. On amène la pointe A en un point du bord $[I,C]$ qu'on renomme en R ce qui fait un pli $[P,Q]$ avec P sur (l'ancien) $[A,I]$ et $[P,R]$ horizontal, et Q sur $[A,C]$. Enfin on amène symétriquement la pointe C sur le point P.

Après avoir réalisé 12 fois ce pliage et emboité les pointes dans les trous, on obtient un dodécaèdre. Est-il régulier ? Cela signifierait que chaque pliage dessine un pentagone régulier.

Le quadrilatère $APRQ$ est un losange car (AQ) est parallèle à (PR), (AP) est parallèle à (QR), et $AP = PR$. En notant α une mesure en radians de l'angle $(\overrightarrow{AQ}, \overrightarrow{AP})$, on constate que $\frac{\pi}{2} + \frac{\alpha}{2}$ est une mesure de l'angle $(\overrightarrow{PQ}, \overrightarrow{PI})$ et en cas de pentagone régulier cet angle aurait aussi comme mesure $\frac{3\pi}{5} = 1{,}884\ldots$. Mais $\tan(\frac{\alpha}{2}) > 0$ et $\tan(\alpha) = \frac{1}{\sqrt{2}}$, donc $\tan(\frac{\alpha}{2}) = \sqrt{3} - \sqrt{2}$. Comme $\frac{\pi}{2} + \arctan(\sqrt{3} - \sqrt{2}) = 1{,}878\ldots$, le pentagone n'est pas régulier.

III. Limites, asymptotes

1. Limites

Soient $f\colon \underset{\text{intervalle infini}}{I} \longrightarrow \mathbb{R}$ et $u \in \mathbb{R} \cup \{-\infty, +\infty\}$, avec $u \in I$ ou u borne de I.
On a 6 notions « $\lim\limits_{\mathcal{F}} f(x) = l$ » de limite pour que $f(x)$ tende vers l quand x lorsque vers u :
si $u \in \mathbb{R}$: $\mathcal{F} = (x \to u)$ ou $\mathcal{F} = (x \underset{x \neq u}{\longrightarrow} u)$ ou $\mathcal{F} = (x \to u^+)$ ou $\mathcal{F} = (x \to u^-)$;
si $u = -\infty$: $\mathcal{F} = (x \to -\infty)$; si $u = +\infty$: $\mathcal{F} = (x \to +\infty)$.

Définition (hors programme)

Soient $f\colon \underset{\text{partie de } \mathbb{R}}{D} \longrightarrow \mathbb{R}$ et $u, l \in \mathbb{R}$.

(a) Quand il existe $a < u < b$ vérifiant $]a,b[\subseteq D$, on écrit $f(x) \underset{x \to u}{\longrightarrow} l$ si pour tout $\epsilon > 0$, il existe $\alpha > 0$ tel que : $\forall x \in D \quad \big(|x-u| < \alpha \implies |f(x) - l| < \epsilon\big)$. Dans ce cas : $\boxed{l = f(u)}$.

(b) Quand il existe $a < u < b$ vérifiant $]a,u[\cup]u,b[\subseteq D$, on écrit $f(x) \underset{\substack{x \to u \\ x \neq u}}{\longrightarrow} l$ si pour tout $\epsilon > 0$, il existe $\alpha > 0$ tel que : $\forall x \in D \quad \big(0 < |x-u| < \alpha \implies |f(x) - l| < \epsilon\big)$.

(c) Quand il existe $b > u$ vérifiant $]u, b[\subseteq D$, on écrit $f(x) \underset{x \to u^+}{\longrightarrow} l$ si pour tout $\epsilon > 0$, il existe $\alpha > 0$ tel que : $\forall x \in D \quad \big(0 < x - u < \alpha \implies |f(x) - l| < \epsilon\big)$.

(d) Quand il existe $a < u$ vérifiant $]a, u[\subseteq D$, on écrit $f(x) \underset{x \to u^-}{\longrightarrow} l$ si pour tout $\epsilon > 0$, il existe $\alpha > 0$ tel que : $\forall x \in D \quad \big(-\alpha < x - u < 0 \implies |f(x) - l| < \epsilon\big)$.

(e) Quand il existe $b \in \mathbb{R}$ vérifiant $]-\infty, b[\subseteq D$, on écrit $f(x) \underset{x \to -\infty}{\longrightarrow} l$ si pour tout $\epsilon > 0$, il existe $\alpha > 0$ tel que : $\forall x \in D \quad \big(x < -\alpha \implies |f(x) - l| < \epsilon\big)$.

(f) Quand il existe $a \in \mathbb{R}$ vérifiant $]a, +\infty[\subseteq D$, on écrit $f(x) \underset{x \to +\infty}{\longrightarrow} l$ si pour tout $\epsilon > 0$, il existe $\alpha > 0$ tel que : $\forall x \in D \quad \big(x > \alpha \implies |f(x) - l| < \epsilon\big)$.

Définition (hors programme)

Soient $f \colon \underset{\text{partie de } \mathbb{R}}{D} \longrightarrow \mathbb{R}$ et $u \in \mathbb{R} \cup \{-\infty, +\infty\}$.

(i) On reprend chacune des 6 définitions précédentes de $f(x) \underset{\cdots}{\underset{x \to u^{\cdots}}{\longrightarrow}} l$ pour obtenir la définition de $f(x) \underset{\cdots}{\underset{x \to u^{\cdots}}{\longrightarrow}} -\infty$ en remplaçant la condition « $|f(x) - l| < \epsilon$ » par « $f(x) < -\epsilon$ ».

(ii) On reprend chacune des 6 définitions précédentes de $f(x) \underset{\cdots}{\underset{x \to u^{\cdots}}{\longrightarrow}} l$ pour obtenir la définition de $f(x) \underset{\cdots}{\underset{x \to u^{\cdots}}{\longrightarrow}} +\infty$ en remplaçant la condition « $|f(x) - l| < \epsilon$ » par « $f(x) > \epsilon$ ».

Proposition

Soient $g \colon \underset{\text{partie de } \mathbb{R}}{E} \longrightarrow \mathbb{R}$ et $f \colon \underset{\text{partie de } \mathbb{R}}{D} \longrightarrow \mathbb{R}$ telle que $f(D) \subseteq E$.

On considère une notion de limite $\mathcal{F}$ vers $u \in \mathbb{R} \cup \{-\infty, +\infty\}$ (si $u \in \mathbb{R}$: $x \to u$ ou $x \underset{x \neq u}{\longrightarrow} u$ ou $x \to u^+$ ou $x \to u^-$; si $u = -\infty$: $x \to -\infty$; si $u = +\infty$: $x \to +\infty$) et $k, l \in \mathbb{R} \cup \{-\infty, +\infty\}$.

Si $f(x) \underset{\mathcal{F}}{\longrightarrow} k$ et $g(y) \underset{y \to k}{\longrightarrow} l$, alors $g(f(x)) \underset{\mathcal{F}}{\longrightarrow} l$.

Si $k \in \mathbb{R}$ et $f(x) \underset{\mathcal{F}}{\longrightarrow} k$ avec $f(x) \underbrace{\neq k}_{\text{(resp. : } > k,\ < k)}$ pour $x \in D$ et $g(y) \underset{\substack{y \to k \\ y \neq k}}{\longrightarrow} l$ (resp. $y \to k^+$, $y \to k^-$), alors $g(f(x)) \underset{\mathcal{F}}{\longrightarrow} l$.

Démonstration

Les démonstrations se ressemblent. On se place seulement dans le cas suivant :

$$f(x) \underset{x \to u}{\longrightarrow} k \quad \text{et} \quad g(y) \underset{y \to k}{\longrightarrow} l \quad \text{avec} \quad u, k, l \in \mathbb{R}.$$

Soit $\varepsilon > 0$. Il existe $\eta > 0$ tel que : $\forall y \in \mathbb{R} \quad \big(|y - k| < \eta \implies y \in E \text{ et } |g(y) - l| < \epsilon\big)$.

Ensuite, il existe $\alpha > 0$ tel que : $\forall x \in \mathbb{R} \quad \big(|x - u| < \alpha \implies x \in D \text{ et } |f(x) - k| < \eta\big)$.

Ainsi, pour tout $x \in \mathbb{R}$, on a :

$|x - u| < \alpha \implies \big(x \in D \text{ et } |f(x) - k| < \eta\big) \implies \big(x \in D \text{ et } f(x) \in E \text{ et } |g(f(x)) - l| < \epsilon\big)$.

Conclusion : $g(f(x)) \underset{x \to u}{\longrightarrow} l$. □

Proposition

Soient $f, g \colon \underset{\text{partie de } \mathbb{R}}{D} \longrightarrow \mathbb{R}$ et $\mathcal{F}$ une notion de limite vers $u \in \mathbb{R} \cup \{-\infty, +\infty\}$.

On suppose que : $f(x) \underset{\mathcal{F}}{\longrightarrow} k$ et $g(x) \underset{\mathcal{F}}{\longrightarrow} l$ avec $k, l \in \mathbb{R} \cup \{-\infty, +\infty\}$.

On a : $f(x) + g(x) \underset{\mathcal{F}}{\longrightarrow} k + l$, $f(x)\, g(x) \underset{\mathcal{F}}{\longrightarrow} k\, l$, et, si $l \neq 0$, $\underbrace{\frac{f(x)}{g(x)}}_{\text{défini pour « } x \text{ proche de } u \text{ »}} \underset{\mathcal{F}}{\longrightarrow} \frac{k}{l}$

en interprétant ces formules correctement (*) et à condition :

(*) Soient $k, l \in \mathbb{R}$ et $\epsilon \in \{+, -\}$. On lira dans la conclusion : $\epsilon\infty + l = k + \epsilon\infty = \epsilon\infty$, $\epsilon\infty + \epsilon\infty = \epsilon\infty$; $(\epsilon\infty)l = k(\epsilon\infty) = \epsilon\infty$ si $k, l > 0$, $(\epsilon\infty)l = k(\epsilon\infty) = -\epsilon\infty$ si $k, l < 0$, $(\epsilon\infty)(\epsilon\infty) = +\infty$ et $(\epsilon\infty)(-\epsilon\infty) = -\infty$; $\frac{k}{\epsilon\infty} = 0$, $\frac{\epsilon\infty}{l} = \epsilon\infty$ si $l > 0$, $\frac{\epsilon\infty}{l} = -\epsilon\infty$ si $l < 0$, on remplacera $\frac{\epsilon\infty}{l}$ par $\epsilon\infty$ (resp. $-\epsilon\infty$) si $l = 0$ avec $g(x) > 0$ (resp. $g(x) < 0$) pour « x proche de u », on remplacera $\frac{k}{l}$ par $\epsilon\infty$ (resp. $-\epsilon\infty$) si $k \neq 0$ a pour signe ϵ et $l = 0$ avec $g(x) > 0$ (resp. $g(x) < 0$) pour « x proche de u ».

– d'écarter les formes indéterminées sous forme de sommes $\underbrace{(+\infty)+(-\infty) \text{ et } (-\infty)+(+\infty)}_{\text{« } \infty-\infty \text{ »}}$,
produits $\underbrace{0\,(+\infty) \text{ et } (+\infty)\,0 \text{ et } 0\,(-\infty) \text{ et } (-\infty)\,0}_{\text{« } 0\,\infty \text{ »}}$, et quotients $\frac{0}{0}$, $\underbrace{\frac{\pm\infty}{+\infty} \text{ et } \frac{-\infty}{-\infty} \text{ et } \frac{+\infty}{-\infty} \text{ et } \frac{-\infty}{+\infty}}_{\text{« } \frac{\infty}{\infty} \text{ »}}$;
– de n'étudier la limite en u de $\frac{f}{g}$ dans le cas $l=0$ que lorsque $\left\{\begin{array}{l}\text{ou } g(x)>0 \text{ pour « } x \text{ proche de } u \text{ »}\\ g(x)<0 \text{ pour « } x \text{ proche de } u \text{ »}\end{array}\right.$.

Démonstration

Admise : adapter la démonstration du cas des suites de réels.

Proposition

Soient $f,g,h\colon \underset{\text{partie de } \mathbb{R}}{D} \longrightarrow \mathbb{R}$ et $\mathcal{F}$ une notion de limite vers $u \in \mathbb{R}\cup\{-\infty,+\infty\}$.

(a) Si $\begin{cases} f(x)\leq h(x) \text{ pour } x\in D \\ f(x)\underset{\mathcal{F}}{\longrightarrow} k\in\mathbb{R} \text{ et } h(x)\underset{\mathcal{F}}{\longrightarrow} l\in\mathbb{R}\end{cases}$ alors $k\leq l$ « prolongement des inégalités larges ».

(b) Si $\begin{cases} f(x)\leq g(x)\leq h(x) \text{ pour } x\in D \\ l\in\mathbb{R},\ f(x)\underset{\mathcal{F}}{\longrightarrow} l \text{ et } h(x)\underset{\mathcal{F}}{\longrightarrow} l\end{cases}$ alors $g(x)\underset{\mathcal{F}}{\longrightarrow} l$ « théorème des gendarmes ».

(c) Si $\begin{cases} f(x)\leq g(x) \text{ (resp. } g(x)\leq h(x)) \text{ pour } x\in D \\ f(x)\underset{\mathcal{F}}{\longrightarrow}+\infty \text{ (resp. } h(x)\underset{\mathcal{F}}{\longrightarrow}-\infty)\end{cases}$ alors $g(x)\underset{\mathcal{F}}{\longrightarrow}+\infty$ (resp. $g(x)\underset{\mathcal{F}}{\longrightarrow}-\infty$).

Démonstration

Admise : adapter la démonstration du cas des suites de réels. □

Remarque (« *règle de (De) l'Hôpital* »)

1. On se donne $a,b\in\mathbb{R}$ avec $a<b$.
Soient $f,g\colon [a,b]\to\mathbb{R}$ deux fonctions continues sur $[a,b]$ et dérivables sur $]a,b[$.
On suppose que $g'(x)\neq 0$ pour tout $x\in]a,b[$.
Alors $g(a)\neq g(b)$ et il existe $c\in]a,b[$ tel que : $\frac{f(b)-f(a)}{g(b)-g(a)}=\frac{f'(c)}{g'(c)}$
« *théorème des accroissements finis généralisé* ».
(Cela signifie que la courbe $\gamma:=(f,g)$ admet au point c une tangente parallèle à $[\gamma(a),\gamma(b)]$.)

2. Soient $f,g\colon]a,b[\to\mathbb{R}$ avec $a,b\in\mathbb{R}\cup\{-\infty,+\infty\}$ et $a<b$.

On suppose que
(i) $\lim\limits_{\substack{x\to a^+\\(\text{resp. } x\to b^-)}} f(x)=\lim\limits_{\substack{x\to a^+\\(\text{resp. } x\to b^-)}} g(x)=0$ ou $\lim\limits_{\substack{x\to a^+\\(\text{resp. } x\to b^-)}} |f(x)|=\lim\limits_{\substack{x\to a^+\\(\text{resp. } x\to b^-)}} |g(x)|=+\infty$;
(ii) f et g sont dérivables, et g' ne s'annule pas ;
(iii) $\frac{f'(x)}{g'(x)} \underset{\substack{x\to a^+\\(\text{resp. } x\to b^-)}}{\longrightarrow} l$ pour un certain $l\in\mathbb{R}\cup\{-\infty,+\infty\}$.

Alors : $\frac{f(x)}{g(x)} \underset{\substack{x\to a^+\\(\text{resp. } x\to b^-)}}{\longrightarrow} l$.

Démonstration

1. On trouve par l'absurde que $g(a)\neq g(b)$, en utilisant le théorème de Rolle.
On obtient l'existence de c en appliquant le théorème de Rolle à l'application $\varphi\colon [a,b]\to\mathbb{R}$ définie par $\varphi(x)=f(x)-\frac{f(b)-f(a)}{g(b)-g(a)}g(x)$ pour $x\in[a,b]$.

2. Quitte à remplacer f et g par $x\mapsto f(\frac{1}{x})$ et $x\mapsto g(\frac{1}{x})$, on peut supposer que $a\neq-\infty$.

• Forme indéterminée $\frac{0}{0}$: on pose $f(a)=g(a)=0$. Pour simplifier on suppose que $l\in\mathbb{R}$ (méthode analogue dans les cas $l=-\infty$ ou $l=+\infty$).

On se donne $x \in]a,b[$. On a : $g(x) \neq 0$ (th. de Rolle entre a et x).
D'après le th. des accroissements finis généralisé, il existe $c \in]a,x[$ tel que : $\frac{f(x)}{g(x)} = \frac{f'(c)}{g'(c)}$.

Soit $\varepsilon > 0$. Il existe $\alpha > 0$ tel que $\left|\frac{f'(t)}{g'(t)} - l\right| < \varepsilon$ dès que $0 < t-a < \alpha$.
Si $0 < x-a < \alpha$, on a : $0 < c-a < \alpha$ donc $\left|\frac{f(x)}{g(x)} - l\right| = \left|\frac{f'(c)}{g'(c)} - l\right| < \varepsilon$.

En conclusion : $\frac{f(x)}{g(x)} \underset{x\to a^+}{\longrightarrow} l$. (Variante : choix de $c := c_x$ et composition de limites.)

• Forme indéterminée $\frac{\infty}{\infty}$: on va utiliser l'égalité $\frac{f(x)}{g(x)} = \left(1 - \frac{g(x_0)}{g(x)}\right)\frac{f(x)-f(x_0)}{g(x)-g(x_0)} + \frac{f(x_0)}{g(x)}$.
Pour simplifier on suppose que $l \in \mathbb{R}$ (méthode analogue dans les cas $l = -\infty$ ou $l = +\infty$).

Soit $\varepsilon > 0$. On se donne $x \in]a,b[$.

Tout d'abord, il existe $\alpha > 0$ tel que $\left|\frac{f'(t)}{g'(t)} - l\right| < \varepsilon$ dès que $0 < t-a < \alpha$.

On fixe x_0 tel que $0 < x_0 - a < \alpha$. D'après le th. des accroissements finis généralisé, il existe $c \in]x,x_0[$ tel que : $\frac{f(x)-f(x_0)}{g(x)-g(x_0)} = \frac{f'(c)}{g'(c)}$.
Il existe aussi $\beta > 0$ tel que $g(x) \neq 0$ et $\left|\frac{g(x_0)}{g(x)}\right| < \frac{\varepsilon}{|l|+\varepsilon}$ et $\left|\frac{f(x_0)}{g(x)}\right| < \varepsilon$ dès que $0 < x-a < \beta$.
Si $0 < x-a < \alpha$ et $0 < x-a < \beta$, on a : $0 < c-a < \alpha$ et $\left|\frac{g(x_0)}{g(x)}\right| < \frac{\varepsilon}{|l|+\varepsilon}$ et $\left|\frac{f(x_0)}{g(x)}\right| < \varepsilon$
puis $\left|\frac{f(x)}{g(x)} - l\right| \leq \left|\frac{f(x)-f(x_0)}{g(x)-g(x_0)} - l\right| + \left|\frac{g(x_0)}{g(x)}\right|\left|\frac{f(x)-f(x_0)}{g(x)-g(x_0)}\right| + \left|\frac{f(x_0)}{g(x)}\right| < 3\varepsilon$.

En conclusion : $\frac{f(x)}{g(x)} \underset{x\to a^+}{\longrightarrow} l$. □

2. Asymptotes

Définition

Soient $f : \underset{\text{intervalle ouvert non vide}}{I} \to \mathbb{R}$ une application continue, u une borne de I, et $a, b \in \mathbb{R}$.

(a) On suppose que $u \in \mathbb{R}$, avec $u = \inf I$ (resp. $u = \sup I$).

On dit que f *a pour une asymptote verticale en u la droite* $D : x = u$ si :

$$\underbrace{|f(x)| \underset{x\to u^+}{\longrightarrow} +\infty}_{\text{équivaut ici à : } f(x) \underset{x\to u^+}{\longrightarrow} -\infty \text{ ou } f(x) \underset{x\to u^+}{\longrightarrow} +\infty} \qquad \left(\text{resp. } \underbrace{|f(x)| \underset{x\to u^-}{\longrightarrow} +\infty}_{\text{équivaut ici à : } f(x) \underset{x\to u^-}{\longrightarrow} -\infty \text{ ou } f(x) \underset{x\to u^-}{\longrightarrow} +\infty}\right).$$

(b) On suppose que $u = -\infty$ (resp. $u = +\infty$).

On dit que f *a pour asymptote la droite* $D : y = ax + b$ *en* $-\infty$ (resp. en $+\infty$) si :

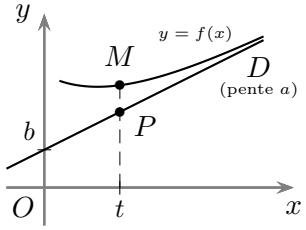
$$\boxed{f(x) - (ax+b) \underset{x\to-\infty}{\longrightarrow} 0} \quad \left(\text{resp. } \boxed{f(x) - (ax+b) \underset{x\to+\infty}{\longrightarrow} 0}\right).$$

Dans ce cas : $\boxed{\frac{f(x)}{x} \underset{x\to-\infty}{\longrightarrow} a}$ et $f(x) - ax \underset{x\to-\infty}{\longrightarrow} b$ $\left(\text{resp. } \boxed{\frac{f(x)}{x} \underset{x\to+\infty}{\longrightarrow} a} \text{ et } f(x) - ax \underset{x\to+\infty}{\longrightarrow} b\right)$.

Remarque

Dans le cas où (b) est réalisé, on peut chercher la position du graphe par rapport à D. On se place au point M du graphe de f d'abscisse t et note P le point de D d'abscisse t :

L'ordonnée du vecteur $\overrightarrow{PM}$ est $f(t) - (at+b)$. Son signe détermine la position du graphe de f par rapport à D.



IV. Continuité et dérivabilité

1. Continuité

Définition-Proposition

On considère une application $f\colon \underset{\text{intervalle infini}}{I} \longrightarrow \mathbb{R}$.

(a) Soit $x_0 \in I$. On dit que f *est continue en* x_0 si : x_0 n'est pas une borne de I et $\lim\limits_{x\to x_0} f(x) = f(x_0)$, ou $x_0 = \inf I$ et $\lim\limits_{x\to x_0^+} f(x) = f(x_0)$, ou $x_0 = \sup I$ et $\lim\limits_{x\to x_0^-} f(x) = f(x_0)$.
Cela équivaut à : $\forall \varepsilon > 0 \;\; \exists \alpha > 0 \;\; \forall x \in I \;\; \big(|x - x_0| < \alpha \implies |f(x) - f(x_0)| < \epsilon\big)$.

(b) On dit que f *est continue* si elle est continue en tout point de I.

Proposition

Soient $g\colon \underset{\text{intervalle infini}}{J} \longrightarrow \mathbb{R}$, $f\colon \underset{\text{intervalle infini}}{I} \longrightarrow \mathbb{R}$ telle que $f(I) \subseteq J$, et $x_0 \in I$.
Si f est continue en x_0 et g est continue en $f(x_0)$, alors $g \circ f$ est continue en x_0.

Démonstration

Soit $\varepsilon > 0$. Continuité de g en $f(x_0)$: $|g(y) - g(f(x_0))| < \epsilon$ si $y \in J$ et $|y - f(x_0)| < \eta$.
Ensuite, par continuité de f en x_0 on a : $|f(x) - f(x_0)| < \eta$ dès que $x \in I$ et $|x - x_0| < \alpha$.
Ainsi, pour $x \in I$ on a : $|x - x_0| < \alpha \;\Rightarrow\; |f(x) - f(x_0)| < \eta \;\Rightarrow\; |g(f(x)) - g(f(x_0))| < \epsilon$.
Conclusion : $g \circ f$ est continue en x_0. □

Exemples

1. Soit $a \in \mathbb{R}$. L'application $\begin{array}{ccc}]0,+\infty[& \to & \mathbb{R} \\ x & \mapsto & x^a := \mathrm{e}^{a \ln x} \end{array}$ est continue (cf. la proposition).
De plus, par compositions de limites, on a par exemple : $\lim\limits_{x\to 0^+} x^a = \begin{cases} 0 & \text{si } a > 0 \\ 1 & \text{si } a = 0 \\ +\infty & \text{si } a < 0 \end{cases}$ ou ou .

2. En prenant $a = \frac{1}{2}$, on en déduit la continuité de l'application $x \in \mathbb{R} \mapsto |x| = \sqrt{x^2}$.
La continuité de $x \mapsto |x|$ découle aussi facilement de la définition.

Proposition

Soient $f, g\colon \underset{\text{intervalle infini}}{I} \longrightarrow \mathbb{R}$ et $x_0 \in I$ tels que f et g sont continues en x_0.

On a : $f + g$ et fg sont continues en x_0. De plus, quand $g(x_0) \neq 0$, l'application $\frac{f}{g}$ est définie en x pour $x \in I$ avec « $|x - x_0|$ assez petit » et continue en x_0.

Démonstration

Découle des résultats sur les limites. □

Définition

Soient I un intervalle infini, $x_0 \in I$ et $f\colon I\backslash\{x_0\} \to \mathbb{R}$.
On appelle *prolongement par continuité de* f *en* x_0 toute application $\widetilde{f}\colon I \to \mathbb{R}$ continue en x_0 telle que : $\widetilde{f}(x) = f(x)$ pour tout $x \in I\backslash\{x_0\}$.

Théorème (« *théorème des valeurs intermédiaires* »)

Soit $f\colon [a,b] \to \mathbb{R}$ une application continue avec $a, b \in \mathbb{R}$ et $a < b$.
Pour tout $y_0 \in [f(a), f(b)]$, il existe $x_0 \in [a,b]$ tel que $y_0 = f(x_0)$.

Démonstration

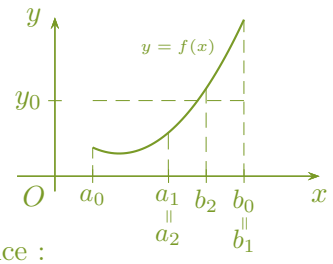
La méthode qui suit, par « dichotomie », peut être utilisée par ordinateur pour trouver une solution de l'équation $f(x) = y_0$. On suppose que $f(a) \leq f(b)$ (mêmes idées si $f(a) \geq f(b)$).

On va construire deux suites adjacentes $(a_n)_{n\geq 0}$ et $(b_n)_{n\geq 0}$ par récurrence.

On commence en notant : $(a_0, b_0) := (a, b)$.

Ensuite, à partir de (a_n, b_n) on construit :

$$(a_{n+1}, b_{n+1}) := \begin{cases} \text{ou} & (a_n, \frac{a_n+b_n}{2}) \text{ si } y_0 \leq f(\frac{a_n+b_n}{2}) \\ & (\frac{a_n+b_n}{2}, b_n) \text{ si } f(\frac{a_n+b_n}{2}) < y_0 \end{cases}.$$



On obtient $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$ et à l'aide d'une récurrence :

$$b_n - a_n = \frac{b-a}{2^n} \text{ avec } (*) \ f(a_n) \leq y_0 \leq f(b_n).$$

On note x_0 la limite commune à $(a_n)_{n\geq 0}$ et $(b_n)_{n\geq 0}$. On a : $a_n \leq x_0 \leq b_n$ pour tout $n \geq 0$. En particulier $a \leq x_0 \leq b$ (avec $n = 0$), puis $f(x_0) = y_0$ par passage à la limite dans $(*)$. □

2. Dérivabilité

Définition-Proposition

Soient $f\colon \underset{\text{intervalle infini}}{I} \longrightarrow \mathbb{R}$, $x_0 \in I$ et $l \in \mathbb{R}$.

(a) On suppose que x_0 n'est pas une borne de I.

On dit que f *est dérivable en* x_0 *et* $\underbrace{f'(x_0)}_{ou\ \frac{df(x)}{dx}\big|_{x=x_0}} = l$ si : $\frac{f(x)-f(x_0)}{x-x_0} \underset{\substack{x\to x_0 \\ x\neq x_0}}{\longrightarrow} l$.

$\leftarrow [\frac{dx^2}{dx} = 2x \ \textit{mais}\ (x^2)' = 2x]$

Cela équivaut à l'existence d'une application $\varepsilon\colon \underset{\text{intervalle ouvert contenant 0}}{J} \longrightarrow \mathbb{R}$ telle que :

$x_0 + h \in I$ et $f(x_0 + h) = f(x_0) + hl + h\varepsilon(h)$ pour tout $h \in J$, avec $\varepsilon(h) \underset{h\to 0}{\longrightarrow} 0$.

(b) On dit que f *a une dérivée à droite (resp. à gauche) en* x_0 *et* $f'_d(x_0) = l$ *(resp.* $f'_g(x_0) = l$*)* si : $\frac{f(x)-f(x_0)}{x-x_0} \underset{x\to x_0^+}{\longrightarrow} l$ (resp. $\frac{f(x)-f(x_0)}{x-x_0} \underset{x\to x_0^-}{\longrightarrow} l$).

(c) On dit que f *est dérivable* si elle est dérivable en tout point de I qui n'est pas borne de I et elle a une dérivée d'un coté, encore notée $f'(b)$, en tout point b de I qui est borne de I.

Dans ce cas, la dérivée de f est l'application $f'\colon I \to \mathbb{R}$ qui envoie x sur $f'(x)$.

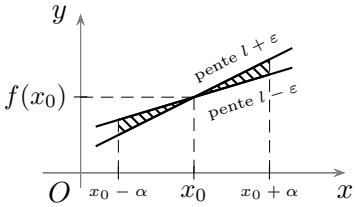
Remarques (notation ci-dessus)

1. En passant à la limite dans $f(x) = f(x_0) + (x - x_0)\frac{f(x)-f(x_0)}{x-x_0}$ $(x \neq x_0)$, on obtient :

si f est dérivable en x_0 alors f est continue en x_0.

2. Dans le cas où x_0 n'est pas borne de I, l'application f a une dérivée en x_0 avec $f'(x_0) = l$ si et seulement si :

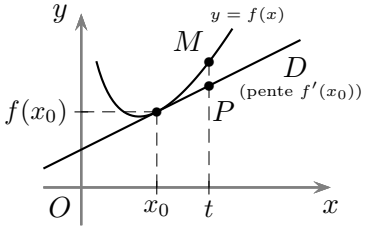
pour tout $\varepsilon > 0$, il existe $\alpha > 0$ tel que le graphe de $f_{|]x_0-\alpha, x_0+\alpha[}$ est inclus dans la partie hachurée ci-contre.



Dans ce cas $D\colon\ y = f(x_0) + f'(x_0)(x - x_0)$ s'appelle *la tangente en* x_0 *au graphe de* f.

On se place au point M du graphe de f d'abscisse t et note P le point de D d'abscisse t :

L'ordonnée de $\overrightarrow{PM}$ est $f(t) - (f(x_0) + f'(x_0)(t - x_0))$. Son signe détermine la position de M par rapport à D.



3. La définition de $f'(x_0)$ se généralise au cas d'une application $f\colon \underset{\text{intervalle infini}}{I} \longrightarrow \mathbb{C}$ en remplaçant simplement $\mathbb{R}$ par $\mathbb{C}$. Ainsi, en posant $f(x) = \underset{\mathbb{R}}{g(x)} + \mathrm{i}\,\underset{\mathbb{R}}{h(x)}$ quand $x \in I$, on a :

f est dérivable en x_0 si et seulement si g et h le sont ; dans ce cas : $f'(x_0) = g'(x_0) + \mathrm{i}\,h'(x_0)$.

Proposition

(a) Soient $f, g : \underset{\text{intervalle ouvert}}{I} \longrightarrow \mathbb{R}$ et $x_0 \in I$. On suppose que f et g sont dérivables en x_0.

On a : $\underbrace{(f+g)'(x_0)}_{\text{existe}} = f'(x_0) + g'(x_0)$, $\underbrace{(fg)'(x_0)}_{\text{existe}} = f'(x_0)\,g(x_0) + f(x_0)\,g'(x_0)$,

et $\underbrace{\left(\frac{f}{g}\right)'(x_0)}_{\text{existe}} = \frac{f'(x_0)\,g(x_0) - f(x_0)\,g'(x_0)}{g(x_0)^2}$ quand $g(x_0) \neq 0$.

(b) Soient $f : \underset{\text{intervalle ouvert}}{I} \longrightarrow \mathbb{R}$ et $g : \underset{\text{intervalle ouvert}}{J} \longrightarrow \mathbb{R}$ tels que $f(I) \subseteq J$, et $x_0 \in I$.
On suppose que : f est dérivable en x_0 et g est dérivable en $f(x_0)$.

On a : $g \circ f$ est dérivable en x_0 et $\boxed{(g \circ f)'(x_0) = g'(f(x_0)) \times f'(x_0)}$.

[À la physicienne en posant $y = f(x)$ et $z = g(y)$, on a : $\frac{\mathrm{d}z}{\mathrm{d}x} = \frac{\mathrm{d}z}{\mathrm{d}y}\,\frac{\mathrm{d}y}{\mathrm{d}x}$.]

Démonstration

(a) On a : $\left|\begin{array}{l} f(x_0+h) = f(x_0) + hf'(x_0) + h\varepsilon_1(h) \text{ avec } \varepsilon_1(h) \underset{h\to 0}{\longrightarrow} 0\,; \\ g(x_0+h) = g(x_0) + hg'(x_0) + h\varepsilon_2(h) \text{ avec } \varepsilon_2(h) \underset{h\to 0}{\longrightarrow} 0. \end{array}\right.$

Donc : $\left|\begin{array}{l} (f+g)(x_0+h) = f(x_0) + g(x_0) + h\,(f'(x_0) + g'(x_0)) + h\,\underbrace{(\varepsilon_1(h) + \varepsilon_2(h))}_{\underset{h\to 0}{\longrightarrow} 0}\,; \\ (fg)(x_0+h) = f(x_0)\,g(x_0) + h\,(f'(x_0)\,g(x_0) + f(x_0)\,g'(x_0)) + h\,\underbrace{(\cdots)}_{\underset{h\to 0}{\longrightarrow} 0}. \end{array}\right.$

Quand $g(x_0) \neq 0$, on a : $\frac{f}{g} = f \times \frac{1}{g}$ avec $\frac{\frac{1}{g(x)} - \frac{1}{g(x_0)}}{x - x_0} = -\frac{1}{g(x)\,g(x_0)}\,\frac{g(x) - g(x_0)}{x - x_0} \underset{\substack{x\to x_0 \\ x\neq x_0}}{\longrightarrow} \frac{-g'(x_0)}{g(x_0)^2}$,
en supposant x est suffisamment proche de x_0 pour que $g(x) \neq 0$.

(b) On a : $\left|\begin{array}{l} f(x_0+h) = f(x_0) + hf'(x_0) + h\varepsilon_1(h) \text{ avec } \varepsilon_1(h) \underset{h\to 0}{\longrightarrow} 0\,; \\ g(f(x_0)+k) = g(f(x_0)) + kg'(f(x_0)) + k\varepsilon_2(k) \text{ avec } \varepsilon_2(k) \underset{k\to 0}{\longrightarrow} 0. \end{array}\right.$

Donc : $(g \circ f)(x_0+h) = g(f(x_0)) + h\,g'(f(x_0)) \times f'(x_0) + h\,\varepsilon_3(h)$, où
$\varepsilon_3(h) := g'(f(x_0)) \times \varepsilon_1(h) + (f'(x_0) + \varepsilon_1(h)) \times \varepsilon_2\big(hf'(x_0) + h\varepsilon_1(h)\big) \underset{h\to 0}{\longrightarrow} 0$. □

Proposition

Soient $f : \underset{\text{intervalle infini}}{I} \longrightarrow \mathbb{R}$ dérivable.

(a) L'application f est constante si et seulement si $f' = 0$.

(b) L'application f est croissante (resp. décroissante) si et seulement si
$f'(x) \geq 0$ (resp. $f'(x) \leq 0$) pour tout $x \in I$.

(c) Si $f'(x) > 0$ (resp. $f'(x) < 0$) pour tout $x \in I$, alors l'application f est strictement croissante (resp. strictement décroissante).

Définition

Soient $f : \underset{\text{partie de } \mathbb{R}}{D} \longrightarrow \mathbb{R}$ et $x_0 \in D$.

(a) On dit que f a *un maximum* (resp. *un minimum*) *en* x_0 si :
$f(x) \leq f(x_0)$ (resp. $f(x) \geq f(x_0)$) pour tout $x \in D$.

(b) On dit que f a *un maximum local* (resp. *minimum local*) *en* x_0 s'il existe $\alpha > 0$ tel que :
$f(x) \leq f(x_0)$ (resp. $f(x) \geq f(x_0)$) pour tout $x \in]x_0 - \alpha, x_0 + \alpha[\cap D$.

(c) On dit que f a *un extremum* (resp. *extremum local*) *en* x_0 si f a un maximum ou un minimum (resp. un maximum local ou un minimum local) en x_0.

Proposition

Soient $f : \underset{\text{intervalle infini}}{I} \longrightarrow \mathbb{R}$ dérivable et $x_0 \in I$.
On suppose que I est ouvert et que f a un extremum local en x_0.
Alors : $f'(x_0) = 0$.

Démonstration

On se place dans le cas où f a un maximum local en x_0 (même méthode pour un minimum local). Il existe $\alpha > 0$ tel que $]x_0-\alpha, x_0+\alpha[\subseteq I$ et $f(x) \leq f(x_0)$ quand $x \in]x_0-\alpha, x_0+\alpha[$.

On a : $\left|\begin{array}{l} \frac{f(x)-f(x_0)}{x-x_0} \leq 0 \text{ quand } x_0 < x < x_0+\alpha \text{ donc } f'(x_0) = f'_d(x_0) \leq 0\,; \\ \frac{f(x)-f(x_0)}{x-x_0} \geq 0 \text{ quand } x_0-\alpha < x < x_0 \text{ donc } f'(x_0) = f'_g(x_0) \geq 0. \end{array}\right.$

D'où : $f'(x_0) = 0$. □

Remarque

L'application $f\colon \begin{array}{ccc} \mathbb{R}_+ & \to & \mathbb{R} \\ x & \mapsto & x \end{array}$ est dérivable et a un minimum en 0.

Mais $f'(0) \neq 0$. Explication : l'intervalle $\mathbb{R}_+$ n'est pas ouvert.

Exemple

On considère $f\colon \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^4-2x^2 \end{array}$. Variations :

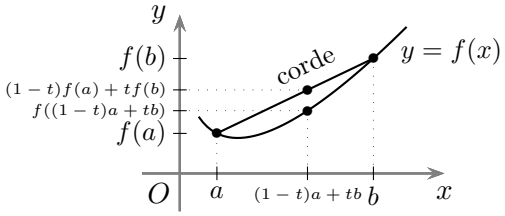
x	$-\infty$		-1		0		1		$+\infty$
$f(x)$	$+\infty$	$\searrow$	-1	$\nearrow$	0	$\searrow$	-1	$\nearrow$	$+\infty$

Donc f a un maximum local en 0 et un minimum en 1.

3. Convexité

Définition-Proposition

Soit $f\colon \underset{\text{intervalle infini}}{I} \longrightarrow \mathbb{R}$.



(a) On dit que f *est convexe* si :

$$f\big((1-t)a+tb\big) \leq (1-t)f(a)+tf(b)$$
pour tous $a, b \in I$ et $t \in [0,1]$.

(Les cordes sont au-dessus du graphe de f.)

(b) On suppose que l'application f est dérivable.
L'application f est convexe si et seulement si f' est croissante.

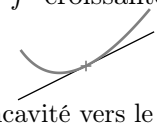
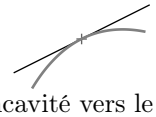
(c) On suppose que l'application f est deux fois dérivable.
L'application f est convexe si et seulement si $f'' \geq 0$.

(d) On dit que f *est concave* si $-f$ est convexe.

Remarque (penser à « l'inflexion de la courbe du chômage »)

Soient $f\colon \underset{\text{intervalle ouvert non vide}}{I} \longrightarrow \mathbb{R}$ dérivable, $x_0 \in I$ et $\alpha > 0$ tel que $]x_0-\alpha, x_0+\alpha[\subseteq I$.

Il y a quatre cas possibles lorsque les applications $f'|_{]x_0-\alpha, x_0[}$ et $f'|_{]x_0, x_0+\alpha[}$ sont monotones :

monotones dans le même sens		monotones en sens contraire	
f' croissante	f' décroissante	f' décroît puis croît	f' croît puis décroît
			
concavité vers le haut	concavité vers le bas	points d'inflexion(*)	

(*) On dit que f *a un point d'inflexion en* x_0 s'il existe $\alpha > 0$ tel que les graphes des applications $f|_{]x_0-\alpha, x_0[}$ et $f|_{]x_0, x_0+\alpha[}$ sont de part et d'autre de la tangente (l'un au-dessus et l'autre au-dessous).

4. Plan d'étude du graphe d'une fonction de $\mathbb{R}$ dans $\mathbb{R}$

Soit $f\colon \underset{\text{partie de } \mathbb{R}}{D} \longrightarrow \mathbb{R}$.

1. Ensemble d'étude

On écrit D comme réunion de $\overbrace{]u,v[\text{ ou }[u,v[\text{ ou }]u,v]\text{ ou }[u,v]}^{\text{les plus grands possibles}}$, $-\infty \leq u < v \leq +\infty$. On restreint l'étude à l'aide de la périodicité de f, ou, de la parité/imparité de f.

2. Tableau de variations

On calcule f', là où cela est possible, et étudie les variations de f.

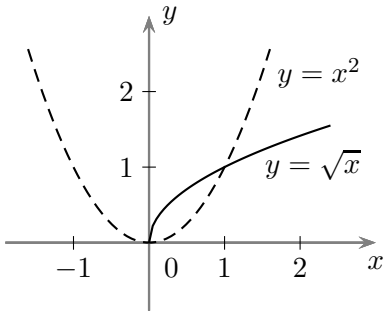
3. Études des asymptotes

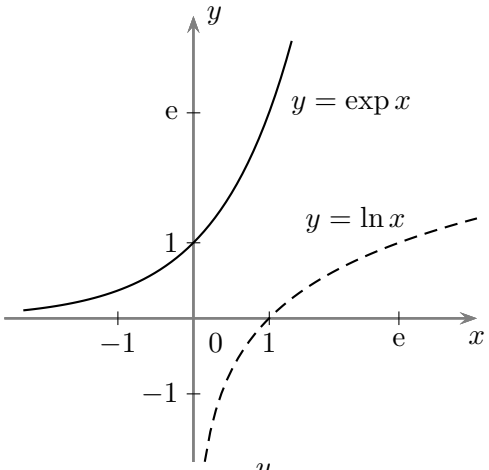
On détermine les asymptotes verticales et les asymptotes horizontales/obliques.
On peut préciser la position de la courbe par rapport à une asymptote horizontale/oblique.

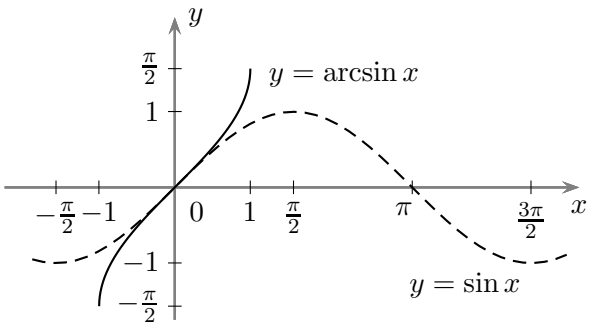
4. Tracé

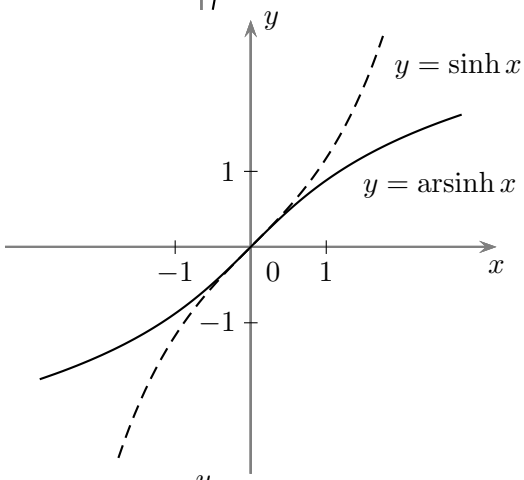
On trace la courbe, en utilisant éventuellement un tableau de valeurs.
Si f est deux fois dérivable sur un intervalle ouvert I inclus dans D et f'' s'annule en changeant de signe en $x_0 \in I$, alors le graphe de f a un point d'inflexion au point d'abscisse x_0.

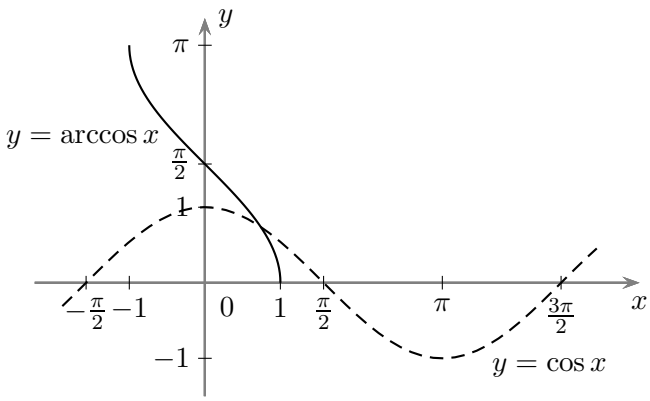
Annexe : graphes de certaines fonctions usuelles

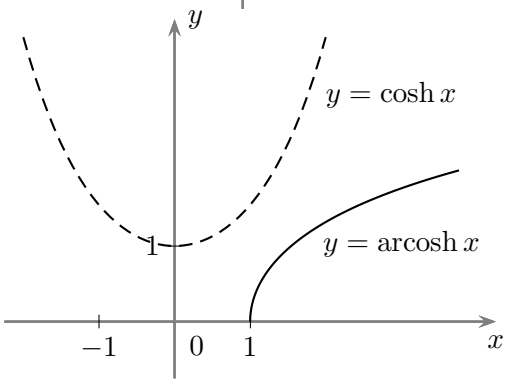


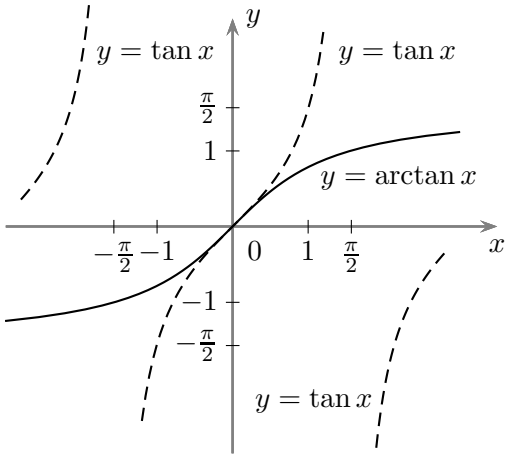


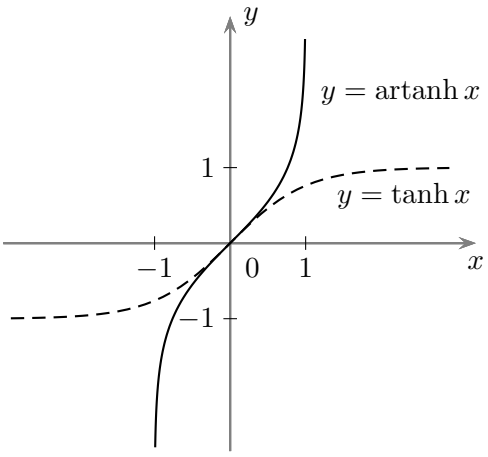












Ch. 2. Arithmétique

Plan
I. Division euclidienne dans $\mathbb{Z}$
II. Anneau $\mathbb{Z}/n\mathbb{Z}$

I. Division euclidienne dans $\mathbb{Z}$

1. Unicité du quotient et du reste

Définition

Soient $p, q \in \mathbb{Z}$.

On dit que p *divise* q (ou q *est multiple de* p), et note $p \mid q$, si :
il existe $k \in \mathbb{Z}$ tel que $q = kp$.

[Quand $p \neq 0$ et p ne divise pas q, on dispose du reste dans la division de q par p.]

Théorème

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ tel que :
$a = bq + r$ et $0 \leq r < |b|$ « division euclidienne de a par b ».

Dans ce cas, r s'appelle *le reste* et q s'appelle *le quotient*, de la division de a par b.

Démonstration

• On montre tout d'abord l'existence dans le cas où $a \geq 0$.
Récurrence sur $n \in \mathbb{N}$: (H_n) existence de $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ quand $0 \leq a \leq n$ et $b \in \mathbb{Z} \setminus \{0\}$.

(i) On suppose que $n = 0$. On a : $a = 0 = b\,0 + 0$.
Cela montre que (H_0) est vraie.

(ii) On suppose que (H_n) est vraie et $0 \leq a \leq n + 1$:
– soit $0 \leq a < |b|$ puis l'égalité $a = b\,0 + a$ fournit un couple (q, r) ;
– soit $0 < |b| \leq a \leq n + 1$ donc $0 \leq a - |b| \leq n$ puis grâce à (H_n) il existe $(q_0, r_0) \in \mathbb{Z} \times \mathbb{Z}$ tel que $a - |b| = bq_0 + r_0$ et $0 \leq r_0 < |b|$, donc $a = b(q_0 + \mathrm{sg}(b)) + r_0$ ce qui donne un couple (q, r).
On en déduit que (H_{n+1}) est vraie.

(iii) Ainsi l'existence est obtenue quand $a \geq 0$.

• On montre maintenant l'existence dans le cas où $a < 0$.
D'après le cas précédent, il existe $(q_1, r_1) \in \mathbb{Z} \times \mathbb{Z}$ tel que $-a = bq_1 + r_1$ et $0 \leq r_1 < |b|$:
– soit $r_1 = 0$ et on utilise l'égalité $a = b(-q_1)$;
– soit $r_1 \neq 0$ et on utilise l'égalité $a = b(-q_1 - \mathrm{sg}(b)) + |b| - r_1$ avec $0 \leq |b| - r_1 < |b|$.

• On montre maintenant l'unicité (dans tous les cas).
On se donne $(q, r), (q', r') \in \mathbb{Z} \times \mathbb{Z}$ tels que :

$$a = bq + r = bq' + r', \quad 0 \leq r < |b| \quad \text{et} \quad 0 \leq r' < |b|.$$

On a : $0 - (|b| - 1) \leq r' - r \leq (|b| - 1) - 0$ et $|b|\,|q - q'| = |r' - r|$ donc $|b|\,|q - q'| \leq |b| - 1$.
D'où : $q = q'$ (par l'absurde), puis $r = r'$ (car $bq + r = bq' + r'$). □

Définition-Proposition

(a) Une *loi de composition* sur un ensemble E est une application $\star : E \times E \to E$.
Suivant l'usage, on notera ici $x \star y$ l'image par $\star$ de (x, y).

(b) Un *groupe* est un couple $(G, \star)$ où G est un ensemble et $\star$ est une loi de composition sur G, vérifiant

(i) pour tous $x, y, z \in G$, on a : $(x \star y) \star z = x \star (y \star z)$ « associativité » ;
(ii) il existe $e \in G$ tel que pour tout $x \in G$, on a : $e \star x = x \star e = x$ « élément neutre » ;
(iii) pour tout $x \in G$ il existe $x' \in G$ tel que : $x \star x' = x' \star x = e$ « inverse ».

Dans ce cas, l'élément e du (ii) est unique (immédiat) appelé *élément neutre de* G, et pour chaque $x \in G$ l'élément x' de G du (iii) est unique (admis) appelé *inverse de* x et noté $\underbrace{x^{-1}}_{\text{ou } -x \text{ quand la loi est notée } +}$.

(c) On dit qu'un groupe $(G, \star)$ est *commutatif* si pour tous $x, y \in G$, on a : $x \star y = y \star x$.

(d) Un *sous-groupe* d'un groupe $(G, \star)$ comme au (b) est une partie H de G vérifiant

(i) $e \in H$;
(ii) pour tous $x, y \in H$, on a : $x \star y^{-1} \in H$.

Dans ce cas, $(H, \underbrace{\star}_{\text{en fait sa restriction à } H \times H})$ est un groupe.

Démonstration

Exercice.

Exemples

1. Le couple $(\mathbb{Z}, +)$ est un groupe commutatif avec $e = 0$ et $x' = -x$ (immédiat).

Par contre $(\mathbb{Z}, .)$ n'est pas un groupe, car sinon on aurait dans ce groupe G :
$e = 1e = 1$ d'après (b) (ii), et $e = 0.0'$ d'après (b) (iii), donc $1 = e = 0$ contradiction.

De plus $(\mathbb{Z} \setminus \{0\}, .)$ n'est pas non plus un groupe, car sinon dans ce groupe G on aurait encore $e = 1$ mais avec $x = 2$ l'équation $x.x' = 1$ d'inconnue $x' \in \mathbb{Z} \setminus \{0\}$ n'a pas de solution.

2. Soit $n \in \mathbb{Z}$. On pose : $n\mathbb{Z} = \{nk \ ; \ k \in \mathbb{Z}\}$.

L'ensemble $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ car :
(i) $0 = n0 \in n\mathbb{Z}$;
(ii) pour tous $x = nk, y = nl \in n\mathbb{Z}$, on a : $x + (-y) = n(k - l) \in n\mathbb{Z}$.

3. Les ensemble $n\mathbb{Z}$ avec $n \in \mathbb{N}$ (qui sont aussi les ensemble $n\mathbb{Z}$ avec $n \in \mathbb{Z}$ car $(-n)\mathbb{Z} = n\mathbb{Z}$) sont deux à deux distincts. En effet :
– si $n \in \mathbb{N}$ et $n\mathbb{Z} = 0\mathbb{Z}$ alors comme $n = n1 \in n\mathbb{Z}$ on a $n = 0$;
– si $p, q \in \mathbb{N} \setminus \{0\}$ et $p\mathbb{Z} = q\mathbb{Z}$, alors comme $p \in p\mathbb{Z}$ et $q \in q\mathbb{Z}$ il existe $k, l \in \mathbb{Z}$ tels que $p = kq$ et $q = lp$, donc $k, l \in \mathbb{N} \setminus \{0\}$ avec $\underbrace{k}_{\geq 1} \underbrace{l}_{\geq 1} = 1$, enfin par l'absurde $k = l = 1$ puis $p = q$.

Corollaire

Les sous-groupes de $(\mathbb{Z}, +)$ sont les ensembles distincts $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

Démonstration

On a vu que les $n\mathbb{Z}$, $n \in \mathbb{N}$, sont des sous-groupes de $(\mathbb{Z}, +)$.

Soit H un sous-groupe de $(\mathbb{Z}, +)$. On a : $0 \in H$. Si $H = \{0\}$, on a $H = 0\mathbb{Z}$.

On suppose que $H \neq \{0\}$. Il existe donc $h_0 \in H$ tel que $h_0 \neq 0$, donc $|h_0| \in H \cap (\mathbb{N} \setminus \{0\})$. On note n le plus petit élément de $\underbrace{H \cap \{1, 2, ..., |h_0|\}}_{\text{fini non-vide}}$, c-à-d le plus petit élément de $H \cap (\mathbb{N} \setminus \{0\})$.

On vérifie que $H = n\mathbb{Z}$.

($\supseteq$) On a $n \in H$ ce qui donne pour tout $k \in \mathbb{N} \setminus \{0\}$ d'une part $kn = \underbrace{n + \cdots + n}_{k \text{ termes}} \in H$ et

d'autre part $(-k)n = -kn \in H$, puis $n\mathbb{Z} \subseteq H$.

($\subseteq$) Soit $h \in H$. Par division euclidienne : $h = nq + r$ avec $q \in \mathbb{Z}$ et $0 \leq r < n$.
On a : $r = h - qn \in H \cap \mathbb{N}$ et $r < n$ donc $r = 0$, puis $h \in n\mathbb{Z}$.
Finalement $H \subseteq n\mathbb{Z}$. □

2. Algorithme d'Euclide

Définition-Proposition

Soient $a, b \in \mathbb{Z}$.

(a) Il existe un unique $d \in \mathbb{N}$ qui divise a et b, et tel que tout diviseur dans $\mathbb{Z}$ de a et b divise d. Il est caractérisé par : $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, où $a\mathbb{Z} + b\mathbb{Z} := \{au + bv \ ; \ u, v \in \mathbb{Z}\}$.

On le note : $d = \text{pgcd}(a, b)$ car, quand $a \neq 0$ et $b \neq 0$, d est le plus grand commun diviseur dans $\mathbb{N} \setminus \{0\}$ à a et b.

(b) Il existe un unique $m \in \mathbb{N}$ qui est multiple de a et b, et tel que tout multiple dans $\mathbb{Z}$ de a et b est multiple de m. Il est caractérisé par : $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

On le note : $m = \text{ppcm}(a, b)$ car, quand $a \neq 0$ et $b \neq 0$, m est le plus petit commun multiple dans $\mathbb{N} \setminus \{0\}$ à a et b.

(c) On a : $\boxed{|ab| = md}$.

Démonstration

On constate facilement que $a\mathbb{Z} + b\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z}$ sont des sous-groupes de $(\mathbb{Z}, +)$.
D'après le corollaire de la fin du 1, il existe $d, m \in \mathbb{N}$ uniques tels que :

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} \quad \text{et} \quad a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}.$$

(a) On a : $a = a1 + b0 \in d\mathbb{Z}$ et $b = a0 + b1 \in d\mathbb{Z}$ donc $d \mid a$ et $d \mid b$.
De plus, il existe $u_0, v_0 \in \mathbb{Z}$ tels que $d = au_0 + bv_0$, donc tout diviseur de a et b divise d.
Unicité : si d' et d'' conviennent, alors $d' \mid d''$ et $d'' \mid d'$ puis $d'\mathbb{Z} = d''\mathbb{Z}$ et $d' = d''$.

(b) On a : $m \in a\mathbb{Z} \cap b\mathbb{Z}$ donc m est multiple de a et b.
Tout multiple de a et b est dans $a\mathbb{Z} \cap b\mathbb{Z}$ donc dans $m\mathbb{Z}$ donc est multiple de m.
Unicité : si m' et m'' conviennent, alors $m' \in m''\mathbb{Z}$ et $m'' \in m'\mathbb{Z}$ puis $m'\mathbb{Z} = m''\mathbb{Z}$ et $m' = m''$.

(c) Il existe $a', b', u_0, v_0 \in \mathbb{Z}$ tels que : $a = a'd$, $b = b'd$, $d = au_0 + bv_0$.
On a : $a'b'd$ est multiple de a et b puis de m, donc ab qui vaut $(a'b'd)d$ est multiple de md.
On a aussi : ab divise am et bm, donc ab divise $mau_0 + mbv_0$ qui vaut md.
Sachant que $ab \in md\mathbb{Z}$ et $md \in ab\mathbb{Z}$, on a $|ab|\mathbb{Z} = md\mathbb{Z}$ donc $|ab| = md$. □

Remarques

Soient $a, b \in \mathbb{Z}$. On pose $d = \text{pgcd}(a, b)$ et $m = \text{ppcm}(a, b)$.

1. Si $n \in \mathbb{Z}$, on a : $na\mathbb{Z} + nb\mathbb{Z} = nd\mathbb{Z}$ et $na\mathbb{Z} \cap nb\mathbb{Z} = nm\mathbb{Z}$ (isoler le cas $n = 0$).
Donc $\text{pgcd}(na, nb) = |n| \ \text{pgcd}(a, b)$ et $\text{ppcm}(na, nb) = |n| \ \text{ppcm}(a, b)$.

2. On suppose que $a \neq 0$ et $b \neq 0$, donc $d \neq 0$.
On introduit $a', b' \in \mathbb{Z}$ tels que $a = da'$ et $b = db'$.
D'après 1, on a : $\text{pgcd}(a', b') = 1$.

Définition

On dit que $a, b \in \mathbb{Z}$ sont *premiers entre eux* si : $\text{pgcd}(a, b) = 1$.

Théorème

Soient $a, b \in \mathbb{Z}$. Les entiers a et b sont premiers entre eux si et seulement si il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$ « théorème de Bézout ».

Démonstration

On a, d'après la définition-proposition ci-dessus :

$$\begin{aligned}\operatorname{pgcd}(a,b)=1 &\iff \mathbb{Z}=a\mathbb{Z}+b\mathbb{Z} \iff \mathbb{Z}\subseteq a\mathbb{Z}+b\mathbb{Z}\\ &\iff 1\in a\mathbb{Z}+b\mathbb{Z} \iff \exists u,v\in\mathbb{Z}\quad au+bv=1.\end{aligned}$$

□

Proposition

Soient $a,b\in\mathbb{Z}\setminus\{0\}$. On pose $r_0=a$ et $r_1=b$. ←[sinon : $\operatorname{pgcd}(a,0)=|a|$, $\operatorname{pgcd}(0,b)=|b|$, et $\operatorname{pgcd}(0,0)=0$]

On effectue les divisions euclidiennes successives de r_k par r_{k+1} :

$a=bq_2+r_2$ avec $0<r_2<r_1$
$b=r_2q_3+r_3$ avec $0<r_3<r_2$
$\cdots$
$r_{n-2}=r_{n-1}q_n+r_n$ avec $0<r_n<r_{n-1}$
$r_{n-1}=r_nq_{n+1}+0.$ ←[on atteint 0 car les restes décroissent strictement dans $\mathbb{N}$]

Dans ce cas, on a : $\boxed{\operatorname{pgcd}(a,b)=r_n}$ « algorithme d'Euclide ».

Démonstration

On utilise la définition du pgcd en termes de diviseurs :

$$\operatorname{pgcd}(\underbrace{a}_{r_0},\underbrace{b}_{r_1})\underbrace{=}_{\substack{\text{mêmes}\\ \text{diviseurs communs}}}\operatorname{pgcd}(\underbrace{a-r_1q_2}_{r_2},r_1)=\operatorname{pgcd}(r_1,r_2)=\cdots=\operatorname{pgcd}(r_n,0)=r_n.$$

□

Remarque (« couple de Bézout »)

L'algorithme d'Euclide fournit aussi $(u,v)\in\mathbb{Z}^2$ tels que $au+bv=\operatorname{pgcd}(a,b)$:

$$\begin{array}{rcl|l|l}
a-bq_2 & = & \cancel{r_2} & \times(\ldots) & \text{pour équilibrer les } r_2 \text{ sur les 3 premières lignes}\\
b-\cancel{r_2}q_3 & = & \cancel{r_3} & \times(\ldots) & \text{pour équilibrer les } r_3 \text{ sur les 3 lignes suivantes}\\
 & \cdots & & & \\
\cancel{r_{n-3}}-\cancel{r_{n-2}}q_{n-1} & = & \cancel{r_{n-1}} & \times(-q_{n-1}) & \text{pour équilibrer les } r_{n-1} \text{ sur les 2 dernières lignes}\\
\cancel{r_{n-2}}-\cancel{r_{n-1}}q_n & = & r_n & & \\
\hline
au+bv & = & r_n & &
\end{array}$$

On pose : $r_0=a$ et $r_1=b$. Ainsi : $r_{i+2}=r_i-r_{i+1}\,q_{i+2}$ pour $0\le i\le n-2$.
On construit une suite $((u_i,v_i))_{0\le i\le n}$ par :
(i) $(u_0,v_0)=(1,0)$ et $(u_1,v_1)=(0,1)$;
(ii) $u_{i+2}=u_i-q_{i+2}\,u_{i+1}$ et $v_{i+2}=v_i-q_{i+2}\,v_{i+1}$ pour $0\le i\le n-2$.
On a par récurrence : $r_i=au_i+bv_i$ pour $0\le i\le n$, donc $a\,u_n+bv_n=\operatorname{pgcd}(a,b)$.

Exemple

Calcul du pgcd de 29 et 11 ? Couple de Bézout associé ?

$$\begin{aligned}
&29=11\times2+7\\
&11=7\times1+4\\
&7=4\times1+3\\
&4=3\times1+1\\
&3=1\times3+0
\end{aligned}$$

donc $\operatorname{pgcd}(29,11)=1$.

$$\begin{array}{rcl|l|l}
29-11\times2 & = & \cancel{7} & \times(-3) & \text{équilibre les 7}\\
11-\cancel{7}\times1 & = & \cancel{4} & \times2 & \text{équilibre les 4}\\
\cancel{7}-\cancel{4}\times1 & = & \cancel{3} & \times(-1) & \text{équilibre les 3}\\
\cancel{4}-\cancel{3}\times1 & = & 1 & & \\
\hline
29\times(-3)+11\times8 & = & 1 & &
\end{array}$$

D'où :

3. Décomposition en facteurs premiers

Définition

Un *nombre premier* est un élément p de $\mathbb{N}\setminus\{0\}$ différent de 1 tel que :
les éléments de $\mathbb{N}\setminus\{0\}$ qui divisent p sont 1 et p.

Proposition

(a) Soient $a, b \in \mathbb{Z}$ et p un nombre premier.
Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$ « lemme d'Euclide ».

(b) Soient $a, b, c \in \mathbb{Z}$.
Si $a \mid bc$ et $\text{pgcd}(a, b) = 1$, alors $a \mid c$ « lemme de Gauss » (généralise celui d'Euclide).

Démonstration

(a) On suppose que $p \mid ab$, et $p \nmid a$.
Comme p est premier, le seul diviseur ≥ 0 de p et a est 1. Donc $\text{pgcd}(a, p) = 1$.
Bézout : il existe $u, v \in \mathbb{Z}$ tels que $au + pv = 1$, donc $\underbrace{ba}_{\text{divisible par } p} u + bpv = b$, donc $p \mid b$.

(Variante. On suppose par l'absurde qu'il existe un nombre premier p et — quitte à changer leur signe — des entiers $a, b \in \mathbb{N}$ non multiples de p tels que ab est multiple de p.
Pour p et a fixés, on choisit b le plus petit possible (donc $b < p$ en envisageant le reste dans la division euclidienne de b par p). La division euclidienne de p par b s'écrit : $p = qb + b'$.
Donc b' n'est pas multiple de p car $0 < b' < b < p$, et $ab' = ap - qab$ est multiple de p.
Cela contredit la minimalité de b.)

(b) On suppose que $a \mid bc$ et $\text{pgcd}(a, b) = 1$.
Bézout : il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$, donc $auc + \overbrace{bc}^{\text{divisible par } a} v = c$, donc $a \mid c$. □

Remarque

Soit $x \in \mathbb{Q}^+ \setminus \{0\}$.
Il existe $a_0, b_0 \in \mathbb{N}\setminus\{0\}$ tels que $x = \frac{a_0}{b_0}$. En posant $d_0 = \text{pgcd}(a_0, b_0)$, $a = \frac{a_0}{d_0}$, $b = \frac{b_0}{d_0}$, on a :
$$x = \frac{a}{b} \in \mathbb{Q}^+ \setminus \{0\} \text{ avec } a, b \in \mathbb{N} \setminus \{0\} \text{ et } \text{pgcd}(a, b) = 1.$$
En supposant que $x = \frac{c}{d} \in \mathbb{Q}^+ \setminus \{0\}$ avec $c, d \in \mathbb{N} \setminus \{0\}$ et $\text{pgcd}(c, d) = 1$, on a : $ad = bc$ ce qui implique que $a \mid c$ et $c \mid a$ par le lemme de Gauss, puis $a = c$ et $b = d$.

Ainsi l'écriture de x sous forme de « fraction irréductible » $\frac{a}{b}$ avec $\text{pgcd}(a, b) = 1$ est unique.

Théorème

Soit $n \in \mathbb{N}\setminus\{0\}$. Il existe $k \in \mathbb{N}$, des nombres premiers $p_1 < \cdots < p_k$ et $\alpha_1, ..., \alpha_k \in \mathbb{N}\setminus\{0\}$ uniques, tels que : $n = \underbrace{p_1^{\alpha_1} \cdots p_k^{\alpha_k}}_{1 \text{ quand } k=0}$.

Dans ce cas, les diviseurs de n dans $\mathbb{N} \setminus \{0\}$ sont les nombres de la forme $p_1^{\beta_1} \cdots p_k^{\beta_k}$ avec $0 \leq \beta_1 \leq \alpha_1$, ..., $0 \leq \beta_k \leq \alpha_k$.

Démonstration

• On montre tout d'abord l'existence d'une décomposition en facteurs premiers de n.
Récurrence sur $n \geq 1$: (H_n) existence d'une décomposition en facteurs premiers pour tous les éléments de $\{1, ..., n\}$.

(i) Cas $n = 1$: $k = 0$ convient. Donc (H_1) est vraie.

(ii) On suppose que (H_n) est vraie et vérifie que $n + 1$ se décompose en facteurs premiers :
– soit $n + 1$ est premier et se décompose en $(n + 1)^1$;
– soit $n + 1$ n'est pas premier et il existe $a, b \in \{1, ..., n\}$ tels que $n + 1 = ab$, puis en appliquant (H_n) au niveau de a et de b on décompose $n + 1$ en facteurs premiers.
On en déduit que (H_{n+1}) est vraie.

(iii) Ainsi, pour chaque $n \geq 1$, (H_n) est vraie et en particulier n possède une décomposition en facteurs premiers.

• On montre l'unicité de la décomposition en partant de $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = q_1^{\beta_1} \cdots q_l^{\beta_l}$ avec $p_1 < \cdots < p_k$ premiers, $q_1 < \cdots < q_l$ premiers, et $\alpha_1, ..., \alpha_k, \beta_1, ..., \beta_l \in \mathbb{N} \setminus \{0\}$.

Le lemme d'Euclide montre que p_k divise l'un des nombres $q_1, ..., q_l$, donc $p_k \leq q_l$; de même $q_l \leq p_k$ puis $p_k = q_l$. On simplifie par le plus gros facteur de la forme p_k^{γ}, ce qui donne $p_1^{\alpha_1} \cdots p_k^{\alpha_k - \beta_l} = q_1^{\beta_1} \cdots q_{l-1}^{\beta_{l-1}}$ si $\alpha_k > \beta_l$, ou, $p_1^{\alpha_1} \cdots p_{k-1}^{\alpha_{k-1}} = q_1^{\beta_1} \cdots q_l^{\beta_l - \alpha_k}$ si $\alpha_k < \beta_l$, chacun de ces deux cas menant à une contradiction par ce qui précède. On en déduit que $\alpha_k = \beta_l$.

On obtient ensuite $p_{k-1} = q_{l-1}$ et $\alpha_{k-1} = \beta_{l-1}$... Enfin $p_1 = q_{l-k+1}$ si $k \leq l$ ou $q_1 = p_{k-l+1}$ si $l \leq k$, ce qui montre que $k = l$.

• On cherche maintenant les diviseurs de n. Ceux proposés conviennent.

Soit $b \in \mathbb{N} \setminus \{0\}$ qui divise n. Il existe $c \in \mathbb{N} \setminus \{0\}$ tel que $n = bc$.

Quitte à ajouter des q^0, on peut écrire $b = q_1^{\beta_1} \cdots q_l^{\beta_l}$ et $c = q_1^{\gamma_1} \cdots q_l^{\gamma_l}$, avec $q_1 < \cdots < q_l$ premiers et $\beta_1, ..., \beta_l, \gamma_1, ..., \gamma_l \in \mathbb{N}$ tels que $\beta_1 + \gamma_1 \neq 0$, ..., $\beta_l + \gamma_l \neq 0$.

Donc $n = q_1^{\beta_1 + \gamma_1} \cdots q_l^{\beta_l + \gamma_l}$ puis par unicité de la décomposition en facteurs premiers : $l = k$ et $q_1 = p_1$ et ... et $q_k = p_k$ et $\alpha_1 = \beta_1 + \gamma_1$ et ... et $\alpha_k = \beta_k + \gamma_k$. D'où le résultat. □

Corollaire

Soient $a, b \in \mathbb{N} \setminus \{0\}$. On peut les écrire sous la forme $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ et $b = p_1^{\beta_1} \cdots p_l^{\beta_k}$ avec $p_1 < \cdots < p_k$ premiers et $\alpha_1, ..., \alpha_k, \beta_1, ..., \beta_k \in \mathbb{N}$.

On a : $\operatorname{pgcd}(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdots p_k^{\min(\alpha_k, \beta_k)}$ et $\operatorname{ppcm}(a, b) = p_1^{\max(\alpha_1, \beta_1)} \cdots p_k^{\max(\alpha_k, \beta_k)}$.

Démonstration

D'après le théorème, le plus grand diviseur commun à a et à b est $p_1^{\min(\alpha_1, \beta_1)} \cdots p_k^{\min(\alpha_k, \beta_k)}$.
La formule pour le ppcm découle par exemple de : $ab = \operatorname{ppcm}(a, b) \operatorname{pgcd}(a, b)$. □

Remarque

Supposons, par l'absurde, que l'ensemble des nombres premiers est fini. On note p le plus grand d'entre eux. Soit q un nombre premier qui intervient dans la décomposition de $p! + 1$. On a donc : q divise $p!$ car $q \leq p$ (choix de p) et q divise $p! + 1$ (choix de q), puis q divise 1.

Cette contradiction montre qu'*il existe une infinité de nombres premiers.*

II. Anneau $\mathbb{Z}/n\mathbb{Z}$

Dans cette partie, on se donne $n \in \mathbb{N} \setminus \{0\}$.

1. Congruences

Définition

Soient $a, b \in \mathbb{Z}$.
On dit que a *est congru à* b *modulo* n, et note $a \equiv b\ [n]$, si : $a - b$ est multiple de n.

Proposition

(a) Pour tous $a, b, c \in \mathbb{Z}$, on a :
(i) $a \equiv a\ [n]$ « réflexivité » ;
(ii) si $a \equiv b\ [n]$ alors $b \equiv a\ [n]$ « symétrie » ;
(iii) si $a \equiv b\ [n]$ et $b \equiv c\ [n]$ alors $a \equiv c\ [n]$ « transitivité ».

(b) Pour tous $a, b, a', b' \in \mathbb{Z}$, on a :
si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$, alors $a + a' \equiv b + b'\ [n]$ et $aa' \equiv bb'\ [n]$.

Démonstration

(a) (i) On a : $a - a = 0n$ donc $a \equiv a\ [n]$.

(ii) On suppose que $a \equiv b\ [n]$: il existe $k \in \mathbb{Z}$ tel que $a - b = kn$.
On a : $b - a = (-k)n$ donc $b \equiv a\ [n]$.

(iii) On suppose que $a \equiv b\ [n]$ et $b \equiv c\ [n]$: il existe $k, l \in \mathbb{Z}$ tels que $a-b = kn$ et $b-c = ln$.
On a : $a - c = (a - b) + (b - c) = (k + l)n$ donc $a \equiv c\ [n]$.

(b) On suppose que $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$ et fixe $k, k' \in \mathbb{Z}$ tels que $a-b = kn$ et $a'-b' = k'n$.
On a : $(a + a') - (b + b') = (a - b) + (a' - b') = (k + k')n$ donc $a + a' \equiv b + b'\ [n]$.
On a aussi : $aa' - bb' = (a - b)a' + b(a' - b') = (ka' + bk')n$ donc $aa' \equiv bb'\ [n]$. □

Exemples

Soit $m = a_k\, 10^k + \cdots + a_1\, 10 + a_0 \in \mathbb{N}$ avec $\underbrace{a_k, ..., a_1, a_0}_{\text{chiffres dans l'écriture de } m \text{ en base } 10} \in \{0, 1, ..., 9\}$.

1. On a : $10 \equiv 0\ [2]$ puis $m \equiv a_0\ [2]$. D'où : $2 \mid m \iff a_0 \in \{0, 2, 4, 6, 8\}$.
De même : $5 \mid m \iff a_0 \in \{0, 5\}$.

2. On a : $10 \equiv 1\ [3]$ puis $m \equiv a_k + \cdots + a_1 + a_0\ [3]$. D'où : $3 \mid m \iff 3 \mid a_k + \cdots + a_1 + a_0$.
De même : $9 \mid m \iff 9 \mid a_k + \cdots + a_1 + a_0$.

3. On a : $10 \equiv -1\ [11]$ puis $m \equiv (-1)^k a_k + \cdots - a_1 + a_0\ [11]$.
D'où : $11 \mid m \iff 11 \mid (-1)^k a_k + \cdots - a_1 + a_0$.

Proposition

Soit $a \in \mathbb{Z}$.
Il existe $a' \in \mathbb{Z}$ tel que $aa' \equiv 1\ [n]$ si et seulement si a et n sont premiers entre eux.

Démonstration

On utilise le théorème de Bézout :

$$\begin{aligned} \exists a' \in \mathbb{Z} \quad aa' \equiv 1\ [n] &\iff \exists a', k \in \mathbb{Z} \quad aa' - 1 = nk \\ &\iff \exists a', k \in \mathbb{Z} \quad aa' + n(-k) = 1 \\ &\iff \exists a', k' \in \mathbb{Z} \quad aa' + nk' = 1 \\ &\iff \operatorname{pgcd}(a, n) = 1. \end{aligned}$$

D'où le résultat. □

Théorème

Soient $m \in \mathbb{N}$ tel que m et n sont premiers entre eux, et $a, b \in \mathbb{Z}$.
L'équation (E) : $x \equiv a\ [m]$ et $x \equiv b\ [n]$ d'inconnue $x \in \mathbb{Z}$ a une unique solution modulo mn « théorème des restes chinois ».

Plus précisément, en se donnant $u, v \in \mathbb{Z}$ vérifiant $mu + nv = 1$, on a :

$$(E) \iff x \equiv anv + bmu\ [mn].$$

Démonstration

On pose : $x_0 = anv + bmu$.
On a : $nv \equiv 1\ [m]$ et $mu \equiv 1\ [n]$ donc $x_0 \equiv a\ [m]$ et $x_0 \equiv b\ [n]$.
D'où :

$$\begin{aligned} (E) &\iff x \equiv x_0\ [m] \text{ et } x \equiv x_0\ [n] \\ &\iff m \mid x - x_0 \text{ et } n \mid x - x_0 \\ &\iff \operatorname{ppcm}(m, n) \mid x - x_0. \end{aligned}$$

On conclut grâce à : $\operatorname{ppcm}(m, n) = \operatorname{pgcd}(m, n) \operatorname{ppcm}(m, n) = mn$. □

Théorème

Soit p un nombre premier.

On a : $a^{p-1} \equiv 1\ [p]$ quand $a \in \mathbb{Z}$ n'est pas multiple de p
donc $a^p \equiv a\ [p]$ pour tout $a \in \mathbb{Z}$ « petit théorème de Fermat ».

Démonstration

• On fait un calcul préliminaire. Soient $x, y \in \mathbb{Z}$. On a : $(x+y)^p = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k}y^k + y^p$.
De plus, quand $1 \leq k \leq p-1$, on a aussi :
$p! = k!\,(p-k)!\,\binom{p}{k}$ donc p divise un des nombres $\underbrace{1, ..., k, 1, ..., p-k}_{\text{tous} < p}$ et $\binom{p}{k}$, puis divise $\binom{p}{k}$.
Ainsi : $(x+y)^p \equiv x^p + y^p\ [p]$.

• Soit $a \in \mathbb{Z}$. On déduit de ce qui précède que : $\underbrace{a^p}_{((a-1)+1)^p} - a \equiv (a-1)^p - (a-1) \equiv \cdots \equiv \underbrace{0}_{1^p - 1}\ [p]$.
D'où : $a^p \equiv a\ [p]$.

On suppose maintenant que $p \nmid a$. Comme $\text{pgcd}(a, p) = 1$, d'après la proposition il existe $a' \in \mathbb{Z}$ tel que $aa' \equiv 1\ [p]$. On en déduit que : $a^{p-1} \equiv a^p a' \equiv aa' \equiv 1\ [p]$. □

Exemple

Quel est le reste dans la division de 2017^{2018} par $p := 13$?
On a : $2017 = 155 \times 13 + 2$ et $2018 = 168 \times 12 + 2$.
Donc $2017^{2018} \equiv 2^{2018} \equiv (2^{12})^{168} \times 2^2 \equiv 4\ [13]$ car $2^{12} \equiv 1\ [13]$ (petit théorème de Fermat).

2. L'anneau $\mathbb{Z}/n\mathbb{Z}$

Définition

(a) Pour tout $a \in \mathbb{Z}$, on note ici $\underbrace{\overline{a}}_{\text{« classe de } a \text{ »}} := \{a + b\ ;\ b \in n\mathbb{Z}\}$.

On munit l'ensemble $\mathbb{Z}/n\mathbb{Z} := \{\overline{a}\ ;\ a \in \mathbb{Z}\}$ des lois de composition suivantes :

$$x + x' := \overline{a + a'} \quad \text{et} \quad x \times x' := \overline{aa'} \quad \text{pour} \quad x, x' \in \mathbb{Z}/n\mathbb{Z}$$

indépendamment du choix de $a, a' \in \mathbb{Z}$ tels que $x = \overline{a}$ et $x' = \overline{a'}$ (proposition du début du 1).

(b) Un *anneau* est un triplet $(A, +, \times)$, où $(A, +)$ est un groupe commutatif dont l'élément neutre sera noté $\underbrace{0}_{\text{au lieu de } e}$ et $\times$ est une loi de composition sur A, vérifiant

(i) $(x \times y) \times z = x \times (y \times z)$ pour tous $x, y, z \in A$;
(ii) $x \times (y + z) = (x \times y) + (x \times z)$ et $(x + y) \times z = (x \times z) + (y \times z)$ pour $x, y, z \in A$;
(iii) il existe $1 \in A$ tel que pour tout $x \in A$, on a : $1 \times x = x \times 1 = x$.

Dans ce cas, l'élément 1 du (iii) est unique (immédiat) et appelé *élément unité de A*.

(c) On dit qu'un anneau $(A, +, \times)$ est *commutatif* si pour tous $x, y \in A$, on a : $x \times y = y \times x$.

Proposition

(a) L'ensemble $\mathbb{Z}/n\mathbb{Z}$ a pour éléments distincts $\overline{0}$, $\overline{1}$, ..., $\overline{n-1}$.

(b) Les triplets $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs.

(c) Le triplet $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

Démonstration

(a) • Tout $a \in \mathbb{Z}$ s'écrit $a = bq + r$ avec $q \in \mathbb{Z}$ et $0 \leq r < b$.
Donc $\overline{a} = \overline{r}$ puis $\overline{a} \in \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$.
• Soient $a, b \in \{0, 1, ..., n-1\}$ tels que $\overline{a} = \overline{b}$.
On a $a - b \in n\mathbb{Z}$ avec $0 - (n-1) \leq a - b \leq (n-1) - 0$ donc $a = b$.

(b) (c) Exercice. □

Exemples

Les tables d'addition de $\mathbb{Z}/n\mathbb{Z}$ avec $n \in \{3, 4\}$ sont faciles à obtenir.

1. On a : $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$. Sa table de multiplication est :

$\overline{b}$ \ $\overline{a}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Par exemple : $\overline{2}\times\overline{2} = \overline{4} = \overline{1}$ (la notation $\overline{2}$ se réfère ici à $\mathbb{Z}/3\mathbb{Z}$.)

2. On a : $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. Sa table de multiplication est :

$\overline{b}$ \ $\overline{a}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

On remarque que : $\overline{2}\times\overline{1} = \overline{2}\times\overline{3}$ mais $\overline{1} \neq \overline{3}$ (dans $\mathbb{Z}/4\mathbb{Z}$), donc $\underbrace{\overline{2}}_{\neq \overline{0}}$ n'a pas d'inverse pour la multiplication dans $\mathbb{Z}/4\mathbb{Z}$.

Définition-Proposition (admise)

Soient $(G, \star)$ et $(G', \star')$ des groupes.

(a) Un *sous-groupe distingué de* $(G, \star)$ est un sous-groupe H de $(G, \star)$ vérifiant :
$$x \star y \star x^{-1} \in H \text{ pour tous } x \in G \text{ et } y \in H.$$
(Cette condition est automatiquement vérifiée quand G est commutatif.)

Dans ce cas, en notant $\dot{x} := \{x \star y \ ; \ y \in H\}$ pour tout $x \in G$ et $G/H := \{\dot{x} \ ; \ x \in G\}$, on munit G/H d'une structure de groupe avec la loi de composition notée aussi $\star$ définie par : $u \star v := \dot{\overbrace{x \star y}}$ pour $u, v \in G/H$ indépendamment du choix de $x, y \in G$ tels que $u = \dot{x}$ et $v = \dot{y}$.

(b) Un *morphisme* de groupes de $(G, \star)$ dans $(G', \star')$ est une application $f : G \to G'$ vérifiant : $f(x \star y) = f(x) \star' f(y)$ pour tous $x, y \in G$.

Dans ce cas, on a : $f(e_G) = e_{G'}$ en notant e_G et $e_{G'}$ les éléments neutres de G et G', $\operatorname{Ker} f := \{x \in G \mid f(x) = e_{G'}\}$ est un sous-groupe distingué de $(G, \star)$, $\operatorname{Im} f$ est un sous-groupe de G', et l'application $\begin{array}{rcl} \tilde{f} : G/\operatorname{Ker} f & \longrightarrow & \operatorname{Im} f \\ u = \dot{x} & \longmapsto & \underbrace{f(x)}_{\text{ne dépend que de } u} \end{array}$ est un morphisme de groupes qui est bijectif.

Remarque

Dans le cas où $(G, \star) = (\mathbb{Z}, +)$ et $H = n\mathbb{Z}$, on retrouve la définition du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

Proposition (variante du théorème des restes chinois)

Soit $m \in \mathbb{N} \setminus \{0\}$.

(a) L'ensemble $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ muni de l'addition $(\overline{a}, \overline{b}) + (\overline{c}, \overline{d}) := (\overline{a} + \overline{c}, \overline{b} + \overline{d})$ pour $a, b, c, d \in \mathbb{Z}$, est un groupe.

(b) L'application $\begin{array}{rcl} f : \mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto & \underbrace{(\overline{x}, \overline{x})}_{\text{les deux } \overline{x} \text{ ont des sens différents}} \end{array}$ est un morphisme de groupes pour l'addition.

(c) On suppose que m et n sont premiers entre eux.

On a : $\operatorname{Ker} f = mn\mathbb{Z}$ et l'application $\begin{array}{rcl} \tilde{f} : \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \overline{x} & \longmapsto & (\overline{x}, \overline{x}) \end{array}$ est un morphisme de groupes pour l'addition qui est bijectif.

Démonstration

(a) Exercice.

(b) Par définition de l'addition de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, f est un morphisme de groupes.

(c) • Pour tout $x \in \mathbb{Z}$, on a : $f(x) = (\overline{0},\overline{0}) \iff m \mid x$ et $n \mid x \iff \underbrace{\text{ppcm}(m,n)}_{mn \text{ ici}} \mid x$.
Donc $\operatorname{Ker} f = mn\mathbb{Z}$, ce qui permet de définir $\tilde{f}$.

• La bijectivité de $\tilde{f}$ traduit exactement le théorème des restes chinois.

Variante. Vu le (b) de la définition-proposition, on vérifie que $\operatorname{Im} f = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
Cela découle de l'injectivité de $\tilde{f}$ car elle implique que $\operatorname{Im} f$, égale à $\operatorname{Im} \tilde{f}$, est une partie à mn éléments de l'ensemble $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ qui a lui-même mn éléments. □

Remarque (réciproque du (c))

Soit $m \in \mathbb{N} \setminus \{0\}$.
On suppose qu'il existe un morphisme de groupes bijectif $\varphi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
On fixe $a, b \in \mathbb{Z}$ tels que : $\varphi(\overline{1}) = (\overline{a},\overline{b})$.
On pose : $k = \text{ppcm}(m,n)$. Donc : $\varphi(\overline{k}) = \overbrace{\varphi(\overline{1}) + \cdots + \varphi(\overline{1})}^{k \text{ fois}} = (\overline{ka},\overline{kb}) = (\overline{0},\overline{0}) = \varphi(\overline{0})$,
puis $\overline{k} = \overline{0}$ dans $\mathbb{Z}/mn\mathbb{Z}$ (par injectivité de φ), enfin $mn \mid k$. A fortiori $mn \leq \text{ppcm}(m,n)$.
Il en résulte que $mn = \text{ppcm}(m,n)$, et m et n sont donc premiers entre eux.

Définition-Proposition (admise)

Soient $(A,+,\times)$ et $(A',+',\times')$ des anneaux. On note 1_A et $1_{A'}$ leur éléments unité.

(a) Un *idéal bilatère* de $(A,+,\times)$ est un sous-groupe $\mathscr{I}$ de $(A,+)$ vérifiant :

$$x \times y \in \mathscr{I} \quad \text{et} \quad y \times x \in \mathscr{I} \quad \text{pour tous } x \in A \text{ et } y \in \mathscr{I}.$$

Dans ce cas, le groupe $(A/\mathscr{I},+)$ a une structure d'anneau avec la loi $\times$ suivante :
$u \times v := \widehat{\dot{x} \times \dot{y}}$ pour $u, v \in A/\mathscr{I}$ indépendamment du choix de $x, y \in A$ tels que $u = \dot{x}$ et $v = \dot{y}$.

(b) Un *morphisme* d'anneaux de $(A,+,\times)$ dans $(A',+',\times')$ est un morphisme de groupes f de $(A,+)$ dans $(A',+')$ vérifiant : $f(1_A) = 1_{A'}$ et $f(x \times y) = f(x) \times' f(y)$ pour tous $x, y \in A$.

Dans ce cas, on a : $\operatorname{Ker} f$ est un idéal bilatère de $(A,+,\times)$, $\operatorname{Im} f$ muni de $+$ et $\times$ est un anneau, et l'application canonique $\tilde{f} : A/\operatorname{Ker} f \to \operatorname{Im} f$ est un morphisme d'anneaux bijectif.

Remarque

On sait que les sous-groupes de $(\mathbb{Z},+)$ sont les $N\mathbb{Z}$ avec $N \in \mathbb{Z}$.
On constate que chaque $N\mathbb{Z}$ est même un idéal de $(\mathbb{Z},+,\times)$.
On retrouve ainsi la définition de l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$.

Dans le (a) de la dernière proposition, le groupe $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},+)$ a une structure d'anneau avec la loi $\times$ suivante : $(\overline{a},\overline{b}) \times (\overline{c},\overline{d}) := (\overline{a} \times \overline{c}, \overline{b} \times \overline{d})$ pour $a, b, c, d \in \mathbb{Z}$
Si $\text{pgcd}(m,n) = 1$, la bijection $\begin{array}{ccc} \tilde{f} : \mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \overline{x} & \mapsto & (\overline{x},\overline{x}) \end{array}$ est un morphisme d'anneaux.

2. Le corps $\mathbb{Z}/p\mathbb{Z}$

Définition

Soit $(A,+,\times)$ un anneau.

(a) Soit $a \in A$. On dit que a est inversible s'il existe $a' \in A$ tel que $a \times a' = a' \times a = 1$.
Dans ce cas a' est unique (admis) et noté a^{-1}.

(b) On note $A^\times$ (parfois aussi A^*) l'ensemble des éléments inversibles de A.

Exemples

On a : $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$, et $\mathbb{Z}^\times = \{-1, 1\}$.
On verra que : $(\mathfrak{M}(n,\mathbb{R}),+,\times)$ est un anneau et $\mathfrak{M}(n,\mathbb{R})^\times = GL(n,\mathbb{R})$.

Proposition

Soit $(A,+,\times)$ un anneau. On note 1 son élément unité.

Le couple $(A^\times,\times)$ est un groupe d'élément neutre 1.

Démonstration

Ici on ne fera plus apparaître le symbole de la multiplication.

Tout d'abord, le produit est une loi de composition sur $A^\times$, car pour $x,y\in A^\times$ on a : $(xy)y^{-1}x^{-1}=x(yy^{-1})x^{-1}=xx^{-1}=1$ et $y^{-1}x^{-1}(xy)=y^{-1}(x^{-1}x)y=y^{-1}y=1$, puis $xy\in A^\times$.

(i) On a : ; $(xy)z=x(yz)$; pour $x,y,z\in A^\times$.

(ii) On a : $11=1$, donc $1\in A^\times$. De plus, $1x=x1=x$ pour tout $x\in A^\times$.

(iii) Enfin, tout élément x de $A^\times$ a un inverse dans $(A^\times,\times)$ car :
$x^{-1}x=xx^{-1}=1$ puis $x^{-1}\in A^\times$ avec $(x^{-1})^{-1}=x$. □

Proposition

Un élément $\overline{a}$ de $\mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si a et n sont premiers entre eux.

Démonstration

On a : $\overline{a}\in(\mathbb{Z}/n\mathbb{Z})^\times \iff \exists\overline{a'}\in\mathbb{Z}/n\mathbb{Z}\quad \overline{a}\overline{a'}=\overline{1} \iff \exists a'\in\mathbb{Z}\quad aa'\equiv 1\ [n]$.

On applique ensuite la seconde proposition du paragraphe 1. □

Exemples

On a : $(\mathbb{Z}/3\mathbb{Z})^\times=\{\overline{1},\overline{2}\}$ et $(\mathbb{Z}/4\mathbb{Z})^\times=\{\overline{1},\overline{3}\}$.

Définition

(a) Un *corps* est un anneau $(K,+,\times)$ qui vérifie :

$$\underbrace{K\neq\{0\}\text{ et tout élément non-nul de }K\text{ est inversible}}_{\text{c'est-à-dire } K^\times=K\setminus\{0\}}.$$

(b) On dit qu'un corps $(K,+,\times)$ est *commutatif* si : $xy=yx$ pour tous $x,y\in K$.

Proposition

L'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$ est un corps si et seulement si n est premier.

Démonstration

($\Rightarrow$) Si $n=1$: $\mathbb{Z}/n\mathbb{Z}=\{\overline{0}\}$ donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps.

On suppose que $n\geq 2$ et n n'est pas premier : $n=ab$ pour certains $a,b\in\{1,...,n-1\}$. On a : $\overline{a}\neq\overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$, et, $\overline{a}\overline{b}=\overline{0}$ avec $\overline{b}\neq\overline{0}$ ce qui montre que $\overline{a}$ n'est pas inversible.

Par conséquent $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps.

($\Leftarrow$) On suppose que n est premier. Comme $n\neq 1$, on a : $\overbrace{\mathbb{Z}/n\mathbb{Z}}^{\text{ensemble à } n \text{ éléments}}\neq\{\overline{0}\}$.

Soit $a\in\{1,...,n-1\}$. Les nombres a et n sont premiers entre eux.

Donc $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ d'après la dernière proposition.

Ainsi $\mathbb{Z}/n\mathbb{Z}$ est un corps. □

Ch. 3. Nombres complexes

Plan
I. Rappels
II. Puissance et racine n^{e}

I. Rappels

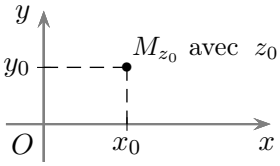
1. Coordonnées cartésiennes

Définition (Gauss, 1837)

hors programme

(a) On note $\mathbb{C}$ l'ensemble $\mathbb{R}^2$ muni de l'addition et de la multiplication suivantes :
$(a,b)+(c,d)=(a+c,b+d)$ et $(a,b)\cdot(c,d)=(ac-bd,ad+bc)$ pour $a,b,c,d\in\mathbb{R}$.
On en déduit l'inclusion $\mathbb{R}\subseteq\mathbb{C}$ en « identifiant » $x\in\mathbb{R}$ à $(x,0)$.
On pose ensuite $\mathrm{i}:=(0,1)$, donc $\mathrm{i}^2=-1$ et : $\underbrace{x}_{\text{plutôt } (x,0)} + \mathrm{i}\ \underbrace{y}_{\text{plutôt } (y,0)} = (x,y)$ quand $x,y\in\mathbb{R}$.

(b) Géométriquement :



M_{z_0} : *image de* z_0

z_0 : *affixe de* M_{z_0}

$\operatorname{Re} z_0 := x_0$ et $\operatorname{Im} z_0 := y_0$
$\overline{z_0} := x_0 - \mathrm{i}y_0$
$|z_0| := \sqrt{z_0\overline{z_0}} = \sqrt{x_0^2+y_0^2}$

(On pose $\mathbb{C}:=\mathbb{R}^2$ et $\mathbb{R}_{\text{nouveau}}:=\mathbb{R}\times\{0\}$, donc $\mathbb{R}^2_{\text{nouveau}}\subseteq\mathbb{C}$ et $\mathbb{C}$ est en bijection avec $\mathbb{R}^2_{\text{nouveau}}$.)

Proposition

Soient $z,u,v,w\in\mathbb{C}$. On dispose d'abord de règles usuelles comme sur $\mathbb{R}$.(*)

(a) On a : $\overline{\overline{z}}=z$ et $|\overline{z}|=|z|$, $\operatorname{Re} z=\frac{z+\overline{z}}{2}$ et $\operatorname{Im} z=\frac{z-\overline{z}}{2\mathrm{i}}$, $|\operatorname{Re} z|\leq|z|$ et $|\operatorname{Im} z|\leq|z|$.

(b) On a : $\overline{u+v}=\overline{u}+\overline{v}$ et $\overline{uv}=\overline{u}\,\overline{v}$.

(c) Si $z\neq 0$, on a : $\boxed{\frac{1}{z}=\frac{\overline{z}}{|z|^2}}$ et $\overline{\left(\frac{1}{z}\right)}=\frac{1}{\overline{z}}$.

D'où : $\overline{\left(\frac{u}{v}\right)}=\frac{\overline{u}}{\overline{v}}$ si $v\neq 0$.

(d) On a : $|uv|=|u||v|$ et $\boxed{|u+v|\leq|u|+|v|}$ « inégalité triangulaire ».

D'où : $\left|\frac{u}{v}\right|=\frac{|u|}{|v|}$ si $v\neq 0$.

Démonstration

(a) On pose $z=x+\mathrm{i}y$ avec $x,y\in\mathbb{R}$. On a : $\overline{\overline{z}}=\overline{x-\mathrm{i}y}=z$ et $|\overline{z}|=\sqrt{x^2+(-y)^2}=|z|$,
$\operatorname{Re} z=x=\frac{(x+\mathrm{i}y)+(x-\mathrm{i}y)}{2}=\frac{z+\overline{z}}{2}$ et $\operatorname{Im} z=y=\frac{(x+\mathrm{i}y)-(x-\mathrm{i}y)}{2}=\frac{z-\overline{z}}{2\mathrm{i}}$,
$|\operatorname{Re} z|=|x|=\sqrt{x^2}\leq\underbrace{\sqrt{x^2+y^2}}_{|z|}$ et $|\operatorname{Im} z|=|y|=\sqrt{y^2}\leq\underbrace{\sqrt{x^2+y^2}}_{|z|}$

(*) On a : (i) $(u+v)+w=u+(v+w)$ et $u+v=v+u$;
(ii) $(uv)w=u(vw)$ et $uv=vu$;
(iii) $u(v+w)=(uv)+(uw)$ et $(u+v)w=(uw)+(vw)$.
De plus : (iv) $z+0=z$ et il existe $z'\in\mathbb{C}$ tel que $z+z'=0$ (un tel z' est unique et noté $-z$) ;
(v) $z1=z$ et lorsque $z\neq 0$ il existe $z''\in\mathbb{C}$ tel que $zz''=1$ (un tel z'' est unique et noté $\frac{1}{z}$).

Il en résulte que : $\boxed{uv=0 \iff (u=0 \text{ ou } v=0)}$.

Lorsque $v\neq 0$, on note comme d'habitude : $\frac{u}{v}=u\times\frac{1}{v}$. On en déduit que : $\frac{u}{v}\times\frac{u'}{v'}=\frac{uu'}{vv'}$ et $\frac{u}{v}+\frac{u'}{v'}=\frac{uv'+vu'}{vv'}$.

(b) On pose $u = a + \mathrm{i}b$ et $v = c + \mathrm{i}d$ avec $a, b, c, d \in \mathbb{R}$. On a :
$\overline{u+v} = \overline{a + c + \mathrm{i}(b+d)} = a + c - \mathrm{i}(b+d) = (a - \mathrm{i}b) + (c - \mathrm{i}d) = \overline{u} + \overline{v}$
et $\overline{uv} = \overline{ac - bd + \mathrm{i}(ad+bc)} = ac - bd + \mathrm{i}(ad+bc) = (a - \mathrm{i}b)(c - \mathrm{i}d) = \overline{uv}$.

(c) On suppose que $z \neq 0$. On a : $z\frac{\overline{z}}{|z|^2} = \frac{z\overline{z}}{|z|^2} = 1$ (par définition de $|z|$), donc $\frac{1}{z} = \frac{\overline{z}}{|z|^2}$.

Ensuite, on a : $\overline{\left(\frac{1}{z}\right)} = \overline{\frac{1}{|z|^2}\,\overline{z}} = \frac{1}{|z|^2}\overline{\overline{z}} = \frac{\overline{\overline{z}}}{|z|^2} = \frac{\overline{\overline{z}}}{|\overline{z}|^2} = \frac{1}{\overline{z}}$.

(d) On a : $|uv| = \sqrt{uv\overline{uv}} = \sqrt{u\overline{u}}\sqrt{v\overline{v}} = |u||v|$.

Enfin : $|u+v|^2 = (u+v)(\overline{u}+\overline{v}) = |u|^2 + |v|^2 + u\overline{v} + \overline{u}v = |u|^2 + |v|^2 + 2\,\mathrm{Re}(u\overline{v})$
donc $|u+v|^2 \leq |u|^2 + |v|^2 + 2|u\overline{v}| = (|u| + |v|)^2$. □

Remarque

En appliquant le (d) de la proposition à $(u-v)+v$ et à $(v-u)+u$, on obtient aussi :

$$\boxed{||u| - |v|| \leq |u - v| \quad \text{pour } u, v \in \mathbb{C}}.$$

2. Exponentielle, coordonnées polaires

Notations

(a) Soit $z = x + \mathrm{i}y \in \mathbb{C}$ avec $x, y \in \mathbb{R}$.

On pose $\underbrace{\mathrm{e}^z}_{\text{noté aussi } \exp z} := \mathrm{e}^x(\cos y + \mathrm{i}\sin y)$ donc $\boxed{\mathrm{e}^z \in \mathbb{C}\setminus\{0\}}$.

(b) Soient $\theta, \theta' \in \mathbb{R}$. On rappelle qu'on écrit $\theta \equiv \theta'\ [2\pi]$ et lit θ *est congru à* θ' *modulo* 2π pour indiquer que $\theta - \theta' \in 2\pi\mathbb{Z}$, où $2\pi\mathbb{Z} := \{2\pi n\ ;\ n \in \mathbb{Z}\}$.

Remarque

On déduit de cette notation que : $\boxed{\mathrm{e}^{\mathrm{i}\theta} = \cos\theta + \mathrm{i}\sin\theta \quad \text{pour } \theta \in \mathbb{R}}$.

Les formules $\boxed{\cos\theta = \frac{\mathrm{e}^{\mathrm{i}\theta} + \mathrm{e}^{-\mathrm{i}\theta}}{2} \text{ et } \sin\theta = \frac{\mathrm{e}^{\mathrm{i}\theta} - \mathrm{e}^{-\mathrm{i}\theta}}{2\mathrm{i}} \text{ pour } \theta \in \mathbb{R}}$ s'appellent *les formules d'Euler*.

Proposition

Soient $z, u, v \in \mathbb{C}$ et $\alpha, \beta \in \mathbb{R}$.

(a) On a : $\overline{\mathrm{e}^z} = \mathrm{e}^{\overline{z}}$.

(b) On a : $\mathrm{e}^{u+v} = \mathrm{e}^u\,\mathrm{e}^v$ donc $\frac{1}{\mathrm{e}^u} = \mathrm{e}^{-u}$, puis $\mathrm{e}^{u-v} = \frac{\mathrm{e}^u}{\mathrm{e}^v}$.

(c) On a : $\mathrm{e}^{\mathrm{i}\alpha} = \mathrm{e}^{\mathrm{i}\beta} \iff \alpha \equiv \beta\ [2\pi]$.

En particulier : $\mathrm{e}^{\mathrm{i}\alpha} = \underbrace{1}_{\mathrm{e}^{\mathrm{i}0}} \iff \alpha \equiv 0\ [2\pi]$.

DÉMONSTRATION

(a) On pose : $z = x + \mathrm{i}y$ avec $x, y \in \mathbb{R}$. Donc $\overline{z} = x + \mathrm{i}(-y)$.
On a : $\overline{\mathrm{e}^z} = \overline{\mathrm{e}^x(\cos y + \mathrm{i}\sin y)} = \mathrm{e}^x(\cos y - \mathrm{i}\sin y) = \mathrm{e}^x(\cos(-y) + \mathrm{i}\sin(-y)) = \mathrm{e}^{\overline{z}}$.

(b) On pose : $u = a + \mathrm{i}b$ et $v = c + \mathrm{i}d$ avec $a, b, c, d \in \mathbb{R}$. Donc $u + v = (a+c) + \mathrm{i}(b+d)$.
On a : $\mathrm{e}^{u+v} = \mathrm{e}^{a+c}(\underbrace{\cos(b+d)}_{\cos b\cos d - \sin b\sin d} + \mathrm{i}\underbrace{\sin(b+d)}_{\sin b\cos d - \cos b\sin d}) = \mathrm{e}^a\,\mathrm{e}^c(\cos b + \mathrm{i}\sin b)(\cos d + \mathrm{i}\sin d) = \mathrm{e}^u\,\mathrm{e}^v$.

En prenant ci-dessus $-u$ à la place de v on obtient : $\underbrace{\mathrm{e}^0}_{1} = \mathrm{e}^u\,\mathrm{e}^{-u}$, donc $\frac{1}{\mathrm{e}^u} = \mathrm{e}^{-u}$.

On en déduit en combinant les deux égalités précédentes que : $\mathrm{e}^{u-v} = \mathrm{e}^u\,\mathrm{e}^{-v} = \mathrm{e}^u\,\frac{1}{\mathrm{e}^v} = \frac{\mathrm{e}^u}{\mathrm{e}^v}$.

(c) On commence par le cas particulier. On a :
$\mathrm{e}^{\mathrm{i}\alpha} = 1 \iff \cos\alpha + \mathrm{i}\sin\alpha = 1 \iff \big(\cos\alpha = 1 \text{ et } \sin\alpha = 0\big) \iff \alpha \equiv 0\ [2\pi]$.
D'où : $\mathrm{e}^{\mathrm{i}\alpha} = \mathrm{e}^{\mathrm{i}\beta} \iff \mathrm{e}^{\mathrm{i}(\alpha-\beta)} = 1 \iff \alpha - \beta \equiv 0\ [2\pi] \iff \alpha \equiv \beta\ [2\pi]$. □

Remarque

Soient $\alpha, \beta \in \mathbb{R}$. L'égalité $\mathrm{e}^{\mathrm{i}(\alpha+\beta)} = \mathrm{e}^{\mathrm{i}\alpha}\,\mathrm{e}^{\mathrm{i}\beta}$ issue du (b) permet de retrouver facilement les formules qui relient $\cos(\alpha+\beta)$ et $\sin(\alpha+\beta)$ à $\cos(\alpha)$, $\cos(\beta)$, $\sin(\alpha)$, et $\sin(\beta)$.

Définition-Proposition

Soit $z \in \mathbb{C}\setminus\{0\}$.

(a) On appelle *un argument de* z, et note par abus « $\arg z$ » (il n'y a pas unicité), tout nombre réel θ, tel que $z = |z|\,\mathrm{e}^{\mathrm{i}\theta}$.

(b) Il existe un argument θ de z. Les arguments de z sont les réels congrus à θ modulo 2π. L'unique argument de z dans $]-\pi, \pi]$ est appelé *argument principal de* z et noté $\operatorname{Arg} z$.

Démonstration

• Existence ? On pose : $\frac{z}{|z|} = a + \mathrm{i}b$ avec $a, b \in \mathbb{R}$.

On a : $\left|\frac{z}{|z|}\right| = \frac{|z|}{||z||} = \frac{|z|}{|z|} = 1$. Donc $a^2 + b^2 = 1$.

Ainsi $0 \leq a^2 \leq 1$ puis $-1 \leq a \leq 1$ et enfin il existe $\theta_0 \in \mathbb{R}$ tel que $a = \cos\theta_0$.

Ensuite, on a $b^2 = 1 - a^2 = \sin^2\theta_0$ puis $a + \mathrm{i}b \in \{\cos(-\theta_0) + \mathrm{i}\sin(-\theta_0), \cos\theta_0 + \mathrm{i}\sin(\theta_0)\}$. Cela montre que parmi $-\theta_0$ et θ_0 se trouve un argument de z.

• Unicité modulo 2π ? On se donne un argument θ de z. Donc $z = |z|\,\mathrm{e}^{\mathrm{i}\theta}$.

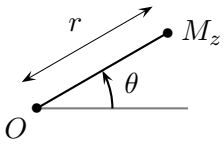
Un réel θ' est un argument de z si et seulement si $z = |z|\,\mathrm{e}^{\mathrm{i}\theta'}$, c'est-à-dire $\mathrm{e}^{\mathrm{i}\theta'} = \mathrm{e}^{\mathrm{i}\theta}$, c'est-à-dire $\theta' \equiv \theta\ [2\pi]$ □

Définition

Soient $z = x + \mathrm{i}y \in \mathbb{C}\setminus\{0\}$ d'image M_z avec $x, y \in \mathbb{R}$, $r > 0$ et $\theta \in \mathbb{R}$.

On a : $\underbrace{\begin{cases} r = |z| \\ \theta \equiv \arg z\ [2\pi] \end{cases}}_{\text{signifie que } \theta \text{ est un argument de } z} \iff \underbrace{\begin{cases} r = \sqrt{x^2+y^2} \\ \frac{z}{r} = \cos\theta + \mathrm{i}\sin\theta \end{cases}}_{\text{traduit sur la figure}} \iff \begin{cases} x = r\cos\theta \\ y = r\sin\theta \end{cases} \iff z = r\mathrm{e}^{\mathrm{i}\theta}.$

On dit que (r, θ) *est un couple de coordonnées polaires de* z (ou de M_z) quand $\boxed{z = r\mathrm{e}^{\mathrm{i}\theta}}$, c'est-à-dire quand $\boxed{(x, y) = (r\cos\theta, r\sin\theta)}$.



Proposition

Soient $u, v, z \in \mathbb{C}\setminus\{0\}$.

(a) On a : $\arg(uv) \equiv \arg(u) + \arg(v)\ [2\pi]$ et $\arg\left(\frac{u}{v}\right) \equiv \arg(u) - \arg(v)\ [2\pi]$.
On en déduit que : $\arg(-z) \equiv \arg(z) + \pi\ [2\pi]$, $\arg\left(\frac{1}{z}\right) \equiv -\arg(z)\ [2\pi]$.

(b) On a : $\arg(\overline{z}) \equiv -\arg(z)\ [2\pi]$.

Démonstration

On introduit des arguments α, β, et θ respectivement de u, v, et z.

(a) On a : $u = |u|\,\mathrm{e}^{\mathrm{i}\alpha}$ et $v = |v|\,\mathrm{e}^{\mathrm{i}\beta}$.
Donc : $uv = |u|\,\mathrm{e}^{\mathrm{i}\alpha}\,|v|\,\mathrm{e}^{\mathrm{i}\beta} = |uv|\,\mathrm{e}^{\mathrm{i}(\alpha+\beta)}$ et $\frac{u}{v} = \frac{|u|\,\mathrm{e}^{\mathrm{i}\alpha}}{|v|\,\mathrm{e}^{\mathrm{i}\beta}} = \left|\frac{u}{v}\right|\mathrm{e}^{\mathrm{i}(\alpha-\beta)}$.
D'où : $\arg(uv) \equiv \alpha+\beta \equiv \arg(u)+\arg(v)\ [2\pi]$ et $\arg\left(\frac{u}{v}\right) \equiv \alpha-\beta \equiv \arg(u)-\arg(v)\ [2\pi]$.
On en déduit que : $\arg(-z) \equiv \arg(\mathrm{e}^{\mathrm{i}\pi}z) \equiv \pi + \arg(z)\ [2\pi]$, $\arg\left(\frac{1}{z}\right) \equiv 0 - \arg(z)\ [2\pi]$.

(b) On a : $z = |z|\,\mathrm{e}^{\mathrm{i}\theta}$, puis $\overline{z} = |z|\,\mathrm{e}^{\mathrm{i}\overline{\theta}} = |z|\,\mathrm{e}^{\mathrm{i}(-\theta)}$, et enfin $\arg(\overline{z}) \equiv -\theta \equiv -\arg(z)\ [2\pi]$. □

3. Transformations géométriques du plan

Notation

Soient $U=(a,b), V=(c,d)\in\mathbb{R}^2$. On pose : $\overrightarrow{UV} \overbrace{=}^{\text{penser à } \overrightarrow{OV}-\overrightarrow{OU}} V-U=(c-a,d-b)$.

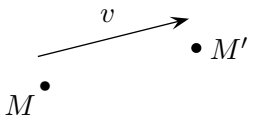
On a donc : $\|\overrightarrow{UV}\|=|u-v|$ en notant $u:=a+\mathrm{i}b$ et $v:=c+\mathrm{i}d$ les affixes de U et V.

Définition

Soient $v,\Omega\in\mathbb{R}^2$ d'affixes b,ω et $\lambda,\theta\in\mathbb{R}$.

(a) L'application $t_v\colon \mathbb{R}^2\to\mathbb{R}^2$ avec $\underbrace{\overrightarrow{MM'}=v}$ s'appelle *la translation de vecteur* v.

$\underbrace{M}_{\text{d'affixe } z}\mapsto\underbrace{M'}_{\text{d'affixe } z'}$ c'est-à-dire $\boxed{z'-z=b}$



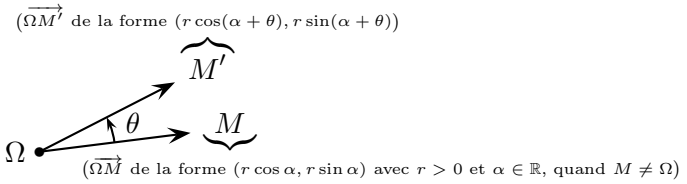
(b) L'application $h_{\Omega,\lambda}\colon \mathbb{R}^2\to\mathbb{R}^2$ avec $\underbrace{\overrightarrow{\Omega M'}=\lambda\,\overrightarrow{\Omega M}}$ s'appelle *l'homothétie de centre* Ω *et de rapport* λ .

$\underbrace{M}_{\text{d'affixe } z}\mapsto\underbrace{M'}_{\text{d'affixe } z'}$ c'est-à-dire $\boxed{z'-\omega=\lambda\,(z-\omega)}$

(c) L'application $r_{\Omega,\theta}\colon \mathbb{R}^2\to\mathbb{R}^2$ avec $\underbrace{M}_{\text{d'affixe } z}\mapsto\underbrace{M'}_{\text{d'affixe } z'}$ $\begin{cases}(u,v):=\overrightarrow{\Omega M}\\(u',v'):=\overrightarrow{\Omega M'}\end{cases}$ tels que $\underbrace{\begin{cases}u'=(\cos\theta)u-(\sin\theta)v\\v'=(\sin\theta)u+(\cos\theta)v\end{cases}}$

c'est-à-dire $\boxed{z'-\omega=\mathrm{e}^{\mathrm{i}\theta}\,(z-\omega)}$

s'appelle *la rotation de centre* Ω *et d'angle* θ.



Remarque

Soient $\Omega,A,B\in\mathbb{R}^2$ d'affixes ω,a,b tels que $A\neq\Omega$ et $B\neq\Omega$.

On appelle *mesure en radian de l'angle* $(\overrightarrow{\Omega A},\overrightarrow{\Omega B})$ et note $\mathrm{mes}(\overrightarrow{\Omega A},\overrightarrow{\Omega B})$ tout $\theta\in\mathbb{R}$ tel que : $r_{\Omega,\theta}(A_1)=B_1$, en introduisant $A_1,B_1\in\mathbb{R}^2$ tels que $\overrightarrow{\Omega A_1}=\frac{\overrightarrow{\Omega A}}{\|\overrightarrow{\Omega A}\|}$ et $\overrightarrow{\Omega B_1}=\frac{\overrightarrow{\Omega B}}{\|\overrightarrow{\Omega B}\|}$.

Ainsi, on a : $\boxed{\mathrm{mes}(\overrightarrow{\Omega A},\overrightarrow{\Omega B})\equiv\arg\left(\frac{b-\omega}{a-\omega}\right)\ [2\pi]}$.

Définition

Soient $f\colon\mathbb{R}^2\to\mathbb{R}^2$ et $M\in\mathbb{R}^2$.

On dit que M *est un point fixe de* f si $f(M)=M$.

Proposition

Soient $v,\Omega\in\mathbb{R}^2$ et $\lambda,\theta\in\mathbb{R}$. On utilise les notations de la définition précédente.

(a) On suppose que $v\neq 0$. L'application t_v n'a aucun point fixe.

(b) On suppose que $\lambda\neq 1$. L'application $h_{\Omega,\lambda}$ a pour unique point fixe Ω.

(c) On suppose que $\theta\not\equiv 0[2\pi]$. L'application $r_{\Omega,\theta}$ a pour unique point fixe Ω.

Démonstration

(a) Soit $M \in \mathbb{R}^2$. On a : $t_v(M) = M \iff \overrightarrow{MM} = \underbrace{v}_{\neq 0}$. On en déduit que $t_v(M) \neq M$.

(b) Si $M \in \mathbb{R}^2$, on a : $h_{\Omega,\lambda}(M) = M \iff \overrightarrow{\Omega M} = \lambda\overrightarrow{\Omega M} \iff \underbrace{(1-\lambda)}_{\neq 0}\overrightarrow{\Omega M} = 0 \iff M = \Omega$.

(c) Soit $M \in \mathbb{R}^2$ tel que $M \neq \Omega$. On note (r, α) un couple de coordonnées polaires de $\overrightarrow{\Omega M}$.
L'égalité $r_{\Omega,\theta}(M) = M$ équivaut au fait que $(r, \alpha+\theta)$ est un couple de coordonnées polaires de $\overrightarrow{\Omega M}$, c'est-à-dire $re^{i(\alpha+\theta)} = re^{i\alpha}$, c'est-à-dire $\underbrace{(e^{i\theta}-1)}_{\neq 0} re^{i\alpha} = 0$. Cela n'est pas réalisé. □

Proposition (exercice)

Soient $a, b \in \mathbb{C}$ avec $a \neq 0$. On note $O := (0,0)$.

(a) L'application $f : \mathbb{R}^2 \to \mathbb{R}^2$ avec $z' = z + b$ est la translation de vecteur l'image de b.
$\underbrace{M}_{\text{d'affixe } z} \mapsto \underbrace{M'}_{\text{d'affixe } z'}$

(b) L'application $g : \mathbb{R}^2 \to \mathbb{R}^2$ avec $z' = az$ s'écrit $h \circ r$ et $r \circ h$, où h est l'homothétie
$\underbrace{M}_{\text{d'affixe } z} \mapsto \underbrace{M'}_{\text{d'affixe } z'}$
de centre O et de rapport $|a|$, et, r est la rotation de centre O et d'angle $\arg a$.

(c) L'application $h : \mathbb{R}^2 \to \mathbb{R}^2$ avec $z' = \overline{z}$ est la symétrie par rapport à l'axe (Ox).
$\underbrace{M}_{\text{d'affixe } z} \mapsto \underbrace{M'}_{\text{d'affixe } z'}$

Démonstration

On se donne $M, M' \in \mathbb{R}^2$ d'affixes z et z'.

(a) On suppose que $M' = f(M)$.
On a : $z' = z + b$ donc $\overrightarrow{MM'} = v$ où v est l'image de b. Ainsi : $M' = t_v(M)$.

(b) On suppose que $M' = g(M)$. On pose $a = \lambda e^{i\theta}$ avec $\lambda > 0$ et $\theta \in \mathbb{R}$.
On a : $z' = \lambda(e^{i\theta}z)$. Cela s'écrit $M' = h_{O,\lambda}(r_{O,\theta}(M))$ car on a $\overrightarrow{OM'} = \lambda\overrightarrow{OM_0}$ où M_0 est le point d'affixe $e^{i\theta}z$. On a aussi $z' = e^{i\theta}(\lambda z)$, ce qui donne de même $M' = r_{O,\theta}(h_{O,\lambda}(M))$.

(c) On suppose que $M' = h(M)$.
On pose : $z = x + iy \in \mathbb{C}$ avec $x, y \in \mathbb{R}$. Le point 4 a donc pour affixe $x - iy$. Ainsi M' qui est égal à $(x, -y)$ est le symétrique de M qui est égal à (x, y) par rapport à (Ox). □

hors programme

Remarque (description des « similitudes du plan »)

Les applications $f : \mathbb{R}^2 \to \mathbb{R}^2$ telles qu'il existe $k > 0$ vérifiant $\|\overrightarrow{f(M)f(N)}\| = k\|\overrightarrow{MN}\|$ pour tous $M, N \in \mathbb{R}^2$ sont exactement les applications d'une des deux formes suivantes :

- $f_{\text{directe}} : \mathbb{R}^2 \to \mathbb{R}^2$ avec $z' = az + b$, où $a \in \mathbb{C}\setminus\{0\}$ et $b \in \mathbb{C}$ sont fixés ;
  $\underbrace{M}_{\text{d'affixe } z} \mapsto \underbrace{M'}_{\text{d'affixe } z'}$
- $f_{\text{indirecte}} : \mathbb{R}^2 \to \mathbb{R}^2$ avec $z' = a\overline{z} + b$, où $a \in \mathbb{C}\setminus\{0\}$ et $b \in \mathbb{C}$ sont fixés.
  $\underbrace{M}_{\text{d'affixe } z} \mapsto \underbrace{M'}_{\text{d'affixe } z'}$

Démonstration

• On constate facilement que les applications proposées conviennent.

• Soient $f : \mathbb{R}^2 \to \mathbb{R}^2$ et $k > 0$ tels que $\|\overrightarrow{f(M)f(N)}\| = k\|\overrightarrow{MN}\|$ pour tous $M, N \in \mathbb{R}^2$.

L'application $\frac{1}{k}f$ conserve les distances. Or le milieu d'un segment $[A, B]$ de $\mathbb{R}^2$ est l'unique $I \in \mathbb{R}^2$ tel que $AI = BI$ (c'est-à-dire I appartient à la médiatrice de $[A, B]$) et $AI + IB = AB$. Donc f envoie un parallélogramme $ABCD$ (c'est-à-dire un quadrilatère $ABCD$ tel que $[A, C]$ et $[B, D]$ ont un même milieu I, ce qui donne $\overrightarrow{AI} = \overrightarrow{IC}$ et $\overrightarrow{BI} = \overrightarrow{ID}$) sur un parallélogramme.

On peut définir l'application $\overrightarrow{f} : \begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ \underbrace{v}_{\text{de la forme } \overrightarrow{MN}} & \longmapsto & \underbrace{\overrightarrow{f(M)f(N)}}_{\substack{\text{indépendant des} \\ \text{choix de } M \text{ et } N}} \end{array}$. On va voir que $\overrightarrow{f}$ est linéaire.

Soient $\overrightarrow{OM}, \overrightarrow{ON} \in \mathbb{R}^2$ et $\alpha \in \mathbb{R}$. On pose : $\alpha\overrightarrow{OM} + \overrightarrow{ON} = \overrightarrow{OG}$ avec $G \in \mathbb{R}^2$. On note O', M', N', G' les images de O, M, N, G par f. On a : $\underbrace{\alpha\overrightarrow{GO} - \alpha\overrightarrow{GM} - \overrightarrow{GN} = 0}_{(G \text{ est barycentre de } ((\alpha, O), (-\alpha, M), (-1, N)))}$ puis :

$$\begin{aligned}
&\|\alpha\overrightarrow{G'O'} - \alpha\overrightarrow{G'M'} - \overrightarrow{G'N'}\|^2 \\
&= \alpha^2 G'O'^2 + \alpha^2 G'M'^2 + G'N'^2 - 2\alpha^2\overrightarrow{G'O'}\cdot\overrightarrow{G'M'} - 2\alpha\overrightarrow{G'O'}\cdot\overrightarrow{G'N'} - 2\alpha\overrightarrow{G'M'}\cdot\overrightarrow{G'N'} \\
&\overset{\text{identité de polarisation}}{=} k^2\left(\alpha^2 GO^2 + \alpha^2 GM^2 + GN^2 - 2\alpha^2\overrightarrow{GO}\cdot\overrightarrow{GM} - 2\alpha\overrightarrow{GO}\cdot\overrightarrow{GN} - 2\alpha\overrightarrow{GM}\cdot\overrightarrow{GN}\right) \\
&= k^2\|\alpha\overrightarrow{GO} - \alpha\overrightarrow{GM} - \overrightarrow{GN}\|^2 = 0.
\end{aligned}$$

On obtient $\alpha\overrightarrow{G'O'} - \alpha\overrightarrow{G'M'} - \overrightarrow{G'N'} = 0$ ce qui s'écrit comme ci-dessus $\alpha\overrightarrow{O'M'} + \overrightarrow{O'N'} = \overrightarrow{O'G'}$ autrement dit $\overrightarrow{f}(\alpha\overrightarrow{OM} + \overrightarrow{ON}) = \alpha\overrightarrow{f}(\overrightarrow{OM}) + \overrightarrow{f}(\overrightarrow{ON})$. Cela montre la linéarité de $\overrightarrow{f}$.

Comme $\frac{1}{k}\overrightarrow{f} \in O(\mathbb{R}^2)$, il existe $(u, v) \in \mathbb{R}^2\setminus\{0\}$ et $\varepsilon \in \{\pm 1\}$ tels que $\mathfrak{Mat}_{\text{base can.}}\overrightarrow{f} = \begin{pmatrix} u & -\varepsilon v \\ v & \varepsilon u \end{pmatrix}$.

On pose : $a = u + \mathrm{i}v$ et $b = f(O)$. Ainsi $f = f_{\text{directe}}$ si $\varepsilon = 1$ et $f = f_{\text{indirecte}}$ si $\varepsilon = -1$. □

II. Puissance et racine n^{e}

1. Équation du second degré

Soit $z_0 \in \mathbb{C}$. On cherche les « racines carrées de z_0 » (« racines 2^{e} de z_0 »), c'est-à-dire les solutions de l'équation $z^2 = z_0$ d'inconnue $z \in \mathbb{C}$.

Remarque

L'équation $z^2 = 0$ d'inconnue $z \in \mathbb{C}$ a pour unique solution $z = 0$

Démonstration

Il est clair que 0 est une solution.

On suppose par l'absurde que $z \neq 0$ et $z^2 = 0$. En multipliant deux fois de suite chaque membre de l'égalité $z^2 = 0$ par $\frac{1}{z}$, on en déduit que $1 = 0$. Contradiction. □

Proposition (racines carrées en coordonnées polaires)

Soit $z_0 = re^{\mathrm{i}\theta} \in \mathbb{C}\setminus\{0\}$ avec $r > 0$ et $\theta \in \mathbb{R}$.

L'équation $z^2 = z_0$ d'inconnue $z \in \mathbb{C}$ a deux solutions qui sont : $\sqrt{r}\,e^{\mathrm{i}\frac{\theta}{2}}$ et $-\sqrt{r}\,e^{\mathrm{i}\frac{\theta}{2}}$.

Démonstration

Cela découle de l'égalité suivante : $z^2 - z_0 = (z - \sqrt{r}\,e^{\mathrm{i}\frac{\theta}{2}})(z + \sqrt{r}\,e^{\mathrm{i}\frac{\theta}{2}})$. □

Exemple

On choisit $z_0 = 1 + \mathrm{i} = \sqrt{2}\,e^{\mathrm{i}\frac{\pi}{4}}$. Les racines carrées de $1 + \mathrm{i}$ sont : $2^{\frac{1}{4}}\,e^{\mathrm{i}\frac{\pi}{8}}$ et $-2^{\frac{1}{4}}\,e^{\mathrm{i}\frac{\pi}{8}}$.

Proposition (racines carrées en coordonnées cartésiennes)

Soit $z_0 = x_0 + \mathrm{i}y_0 \in \mathbb{C}$ avec $x_0, y_0 \in \mathbb{R}$.

Pour tout $z = x + \mathrm{i}y \in \mathbb{C}$ avec $x, y \in \mathbb{R}$, on a :

$$z^2 = x_0 + \mathrm{i}y_0 \iff \begin{cases} x^2 - y^2 = x_0 & \text{(égalité des parties réelles)} \\ 2xy = y_0 & \text{(égalité des parties imaginaires)} \\ \boxed{x^2 + y^2 = \sqrt{x_0^2 + y_0^2}} & \text{(égalité des modules, redondante)} \end{cases}.$$

Ce point de vue permet de résoudre l'équation $z^2 = z_0$ d'inconnue $z = x + \mathrm{i}y \in \mathbb{C}$, où $x, y \in \mathbb{R}$, en commençant par chercher x^2 et y^2 avec une condition de signe pour xy.

Démonstration

L'équivalence est immédiate. L'affirmation de la fin découle ensuite de :

$$z^2 = x_0 + \mathrm{i}y_0 \iff \begin{cases} |x| = \sqrt{\frac{1}{2}(\sqrt{x_0^2 + y_0^2} + x_0} \\ |y| = \sqrt{\frac{1}{2}(\sqrt{x_0^2 + y_0^2} - x_0} \\ \mathrm{sg}(xy) = \mathrm{sg}(y_0) \quad \text{si } y_0 \neq 0 \end{cases}.$$

Parmi les $\underbrace{2}_{\text{cas } z_0 = 0}$ ou 4 nombres complexes z déduit des deux premières égalités, seuls $\underbrace{1}_{\text{cas } z_0 = 0}$ ou 2 nombres complexes (opposés) réalisent la dernière condition. □

Exemple

On choisit $z_0 = 1 + \mathrm{i}$. Pour tout $z = x + \mathrm{i}y \in \mathbb{C}$, on a :

$$z^2 = 1+\mathrm{i} \iff \begin{cases} x^2 - y^2 = 1 \\ 2xy = 1 \\ x^2 + y^2 = \sqrt{2} \end{cases} \iff \begin{cases} x^2 = \frac{\sqrt{2}+1}{2} \in \mathbb{R} \\ y^2 = \frac{\sqrt{2}-1}{2} \in \mathbb{R} \\ 2xy = 1 \end{cases} \iff \begin{cases} x = \sqrt{\frac{\sqrt{2}+1}{2}} \text{ ou } x = -\sqrt{\frac{\sqrt{2}+1}{2}} \\ y = \sqrt{\frac{\sqrt{2}-1}{2}} \text{ ou } y = -\sqrt{\frac{\sqrt{2}-1}{2}} \\ 2xy = 1 \end{cases}.$$

Les deux racines carrées de $1+\mathrm{i}$ sont $\underbrace{\text{donc}}_{(\text{la condition } xy > 0 \text{ les impose})}$: $\sqrt{\frac{\sqrt{2}+1}{2}} + \mathrm{i}\sqrt{\frac{\sqrt{2}-1}{2}}$ et $-\left(\sqrt{\frac{\sqrt{2}+1}{2}} + \mathrm{i}\sqrt{\frac{\sqrt{2}-1}{2}}\right)$.

Proposition

Soient $a, b, c \in \mathbb{C}$ avec $a \neq 0$. On pose $\Delta := b^2 - 4ac$ et fixe $\delta \in \mathbb{C}$ tel que $\delta^2 = \Delta$.

Les solutions de l'équation $az^2 + bz + c = 0$ d'inconnue $z \in \mathbb{C}$ sont :

$$\boxed{-\tfrac{b}{2a} \text{ si } \Delta = 0, \quad \text{ou,} \quad \tfrac{-b-\delta}{2a} \text{ et } \tfrac{-b+\delta}{2a} \text{ (distinctes) si } \Delta \neq 0}.$$

Démonstration

Cela découle de l'égalité suivante : $az^2+bz+c = a\left((z+\frac{b}{2a})^2 - (\frac{\delta}{2a})^2\right)$ pour tout $z \in \mathbb{C}$. □

Remarque

Il résulte de cette démonstration que les nombres complexes obtenus par extensions quadratiques successives à partir de $\mathbb{Q}$ (« constructibles à la règle et au compas ») sont ceux dont les parties réelle et imaginaire sont obtenues à partir de $\mathbb{Q}$ en utilisant des sommes, produits, quotients et extractions de racine carrée. D'après le *théorème de Gauss-Wantzel*, le nombre complexe $\mathrm{e}^{\mathrm{i}\frac{2\pi}{n}}$ avec $n \in \mathbb{N}$ et $n \geq 2$ s'obtient ainsi si et seulement si les facteurs premiers impairs de n sont de la forme $2^{2^k} + 1$ pour un certain $k \in \mathbb{N}$.

2. Puissance n^{e}

Notation

Soient $z \in \mathbb{C}$ et $n \in \mathbb{Z}$. On pose : $z^0 = 1$ et $z^n = \overbrace{z \times \cdots \times z}^{n \text{ termes (récurrence)}}$ quand $n \geq 1$.
On note ensuite : $z^n = \frac{1}{z^{-n}}$ quand $n < 0$ et $z \neq 0$.

Lorsque $p, q \in \mathbb{N}$, ou $p, q \in \mathbb{Z}$ avec $z \neq 0$, on obtient facilement :

$$z^p\, z^q = z^{p+q} \quad \text{et} \quad (z^p)^q = z^{pq}.$$

Démonstration

Idée : on suppose que $z \neq 0$ puis on démontre séparément les deux égalités à p fixé, en commençant par la 1re, à l'aide d'une récurrence sur $|q|$. □

Remarque

Les propriétés habituelles des sommes partielles des suites arithmétiques et géométriques de nombres réels restent valables pour les suites de nombres complexes (cf. la suite du cours).

Par exemple, pour tous $n \in \mathbb{N}$ et $z \in \mathbb{C}\setminus\{1\}$, on a :

$$1 + z + \cdots + z^n = \frac{1 - z^{n+1}}{1 - z}$$

car $(1-z)(1+z+\cdots+z^n) = \underbrace{(1-z)}_{\text{à simplifier}} + \underbrace{(z-z^2)}_{\text{à simplifier}} + \cdots + \underbrace{(z^n - z^{n+1})}_{\text{à simplifier}} = 1 - z^{n+1}$.

Proposition « formule de Moivre »

Soient $\theta \in \mathbb{R}$ et $n \in \mathbb{Z}$.
On a : $(\mathrm{e}^{\mathrm{i}\theta})^n = \mathrm{e}^{\mathrm{i}n\theta}$, ce qui s'écrit aussi $\boxed{(\cos\theta + \mathrm{i}\sin\theta)^n = \cos(n\theta) + \mathrm{i}\sin(n\theta)}$.

Démonstration

On fixe $\theta \in \mathbb{R}$.

• On montre par récurrence sur $n \geq 0$ que $\mathcal{P}(n)$: $(\mathrm{e}^{\mathrm{i}\theta})^n = \mathrm{e}^{\mathrm{i}n\theta}$ est vraie pour tout $n \in \mathbb{N}$.

(i) $\mathcal{P}(0)$ est vraie, car $(\mathrm{e}^{\mathrm{i}\theta})^0 = 1 = \mathrm{e}^{\mathrm{i}0\theta}$.

(ii) Soit $n \in \mathbb{N}$ tel que $\mathcal{P}(n)$ est vraie. On a : $(\mathrm{e}^{\mathrm{i}\theta})^{n+1} = (\mathrm{e}^{\mathrm{i}\theta})^n\, \mathrm{e}^{\mathrm{i}\theta} \overset{\text{hyp. sur } n}{=} \mathrm{e}^{\mathrm{i}n\theta}\, \mathrm{e}^{\mathrm{i}\theta} = \mathrm{e}^{\mathrm{i}(n+1)\theta}$.
Donc $\mathcal{P}(n+1)$ est vraie.

Conclusion : $\mathcal{P}(n)$ est vraie pour tout $n \in \mathbb{N}$.

• On en déduit que pour tout $n \in \mathbb{Z}$ tel que $n \notin \mathbb{N}$, on a :
$(\mathrm{e}^{\mathrm{i}\theta})^n = ((\mathrm{e}^{\mathrm{i}\theta})^{-n})^{-1} \overset{-n \in \mathbb{N}}{=} (\mathrm{e}^{\mathrm{i}(-n)\theta})^{-1} = \mathrm{e}^{\mathrm{i}n\theta}$. □

Notation

(a) On note : $\boxed{0! = 1}$ et $\boxed{n! = 1 \times 2 \times \ldots \times n}$ « factorielle n », quand $n \in \mathbb{N}\setminus\{0\}$.

(b) On note : $\boxed{\binom{n}{k} = \frac{n!}{k!\,(n-k)!} \overset{\text{si } k \neq 0}{=} \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1}}$ « k parmi n », quand $n, k \in \mathbb{N}$ et $k \leq n$.

Proposition

On a : $\boxed{\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}}$ quand $n, k \in \mathbb{N}$ vérifient $1 \leq k \leq n$.

Cela donne un algorithme pour construire la table des $\binom{n}{k}$, appelée « triangle de Pascal » :

$n \backslash k$	0	1	2	3	4	5	6	7
0	1							
1	1	1						
2	1	2	1					
3	1	3	3	1				
4	1	④	⑥	4	1			
5	1	5	⑩	10	5	1		
6	1	6	15	20	15	6	1	
7	1	7	21	35	35	21	7	1

Démonstration

On a : $\binom{n}{k-1}+\binom{n}{k} = \frac{k}{k}\frac{n(n-1)\cdots(n-k+2)}{(k-1)\cdots 1}+\frac{n-k+1}{k}\frac{n(n-1)\cdots(n-k+2)}{(k-1)\cdots 1} = \frac{n+1}{k}\frac{n(n-1)\cdots(n-k+2)}{(k-1)\cdots 1}$. □

Proposition « formule du binôme de Newton »

Soient $u, v \in \mathbb{C}$ et $n \in \mathbb{N}$. On notera $\sum_{k=0}^{n} z_k := z_0 + \cdots + z_n$ lorsque $z_0, ..., z_n \in \mathbb{C}$.

On a : $\boxed{(u+v)^n = \sum_{k=0}^{n} \binom{n}{k} u^{n-k}v^k = \underbrace{\binom{n}{0}}_{1} u^n + \underbrace{\binom{n}{1}}_{n} u^{n-1}v + \binom{n}{2} u^{n-2}v^2 + \cdots + \underbrace{\binom{n}{n}}_{1} v^n}$.

Démonstration

On effectue une récurrence sur n.

• (i) On a : $(u+v)^0 = 1 = \binom{0}{0} u^0 v^0$.

• (ii) On suppose la formule vraie pour un certain $n \geq 0$. On a :

$$(u+v)^{n+1} = u\,(u+v)^n + v\,(u+v)^n = \sum_{k=0}^{n} \binom{n}{k} u^{n+1-k}v^k + \sum_{k'=0}^{n} \binom{n}{k'} u^{n-k'}v^{k'+1}$$

$$\overset{\text{CV } k=l \text{ et } k'+1=l}{=} \underbrace{\binom{n}{0}}_{\binom{n+1}{0}} u^{n+1} + \sum_{l=1}^{n} \underbrace{\left(\binom{n}{l} + \binom{n}{l-1}\right)}_{\binom{n+1}{l}} u^{n+1-l}v^l + \underbrace{\binom{n}{n}}_{\binom{n+1}{n+1}} v^{n+1}.$$

Cela signifie que la formule est vraie pour l'exposant $n+1$.

• En conclusion la formule est vraie pour tout $n \in \mathbb{N}$. □

Remarque

Soient $\theta \in \mathbb{R}$ et $n \in \mathbb{N} \setminus \{0\}$.

1. La formule du binôme permet de calculer les parties réelles $\cos(n\theta)$ et imaginaires et $\sin(n\theta)$ de $(\cos\theta + \mathrm{i}\sin\theta)^n$ à l'aide des réels $\cos^k\theta$ et $\sin^k\theta$, avec $0 \leq k \leq n$.

2. La formule du binôme permet aussi d'exprimer $\cos^n\theta$ qui vaut $\left(\frac{\mathrm{e}^{\mathrm{i}\theta}+\mathrm{e}^{\mathrm{i}\theta}}{2}\right)^n$ et $\sin^n\theta$ qui vaut $\left(\frac{\mathrm{e}^{\mathrm{i}\theta}-\mathrm{e}^{\mathrm{i}\theta}}{2\mathrm{i}}\right)^n$ à l'aide des réels $\cos(k\theta)$ et $\sin(k\theta)$, avec $0 \leq k \leq n$.

Exemple

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

1. On a : $\cos(3\theta) = \mathrm{Re}\left((\cos\theta + \mathrm{i}\sin\theta)^3\right) = \cos^3\theta - 3\cos\theta\,\sin^2\theta$.

2. On a aussi : $\cos^3\theta = \left(\frac{\mathrm{e}^{\mathrm{i}\theta}+\mathrm{e}^{\mathrm{i}\theta}}{2}\right)^3 = \frac{1}{8}\left(\mathrm{e}^{3\mathrm{i}\theta} + 3\mathrm{e}^{\mathrm{i}\theta} + 3\mathrm{e}^{-\mathrm{i}\theta} + \mathrm{e}^{3\mathrm{i}\theta}\right) = \frac{1}{4}\cos(3\theta) + \frac{3}{4}\cos\theta$.

3. Racine n^{e}

Dans ce paragraphe, on fixe $n \in \mathbb{N}\setminus\{0\}$.

Proposition

Soit $z = re^{i\theta} \in \mathbb{C}\setminus\{0\}$ avec $r > 0$ et $\theta \in \mathbb{R}$.

L'équation $Z^n = z$ d'inconnue $Z \in \mathbb{C}$ a n solutions qui sont :

$$Z_k := r^{\frac{1}{n}}\, e^{i\frac{\theta+2k\pi}{n}} \quad \text{où} \quad k \in \{0, 1, \dots, n-1\}.$$

DÉMONSTRATION

Il est clair que $Z = 0$ n'est pas solution de $Z^n = z$.

Soit $Z \in \mathbb{C}\setminus\{0\}$ de décomposition polaire $Z = Re^{i\Theta}$. On a :

$$\begin{aligned} Z^n = z &\iff R^n e^{in\Theta} = re^{i\theta} \\ &\iff R^n = r \quad \text{et} \quad n\Theta \equiv \theta\ [2\pi] \\ &\iff R = r^{\frac{1}{n}} \quad \text{et} \quad \exists k \in \mathbb{Z} \quad n\Theta = \theta + 2k\pi \\ &\iff R = r^{\frac{1}{n}} \quad \text{et} \quad \exists k \in \mathbb{Z} \quad \Theta = \tfrac{\theta+2k\pi}{n}. \end{aligned}$$

L'ensemble des solutions de l'équation $Z^n = z$ d'inconnue $Z \in \mathbb{C}$ est donc :

$$\mathscr{S} := \{Z_k\ ;\ k \in \mathbb{Z}\}, \text{ où } Z_k := r^{\frac{1}{n}}\, e^{i\frac{\theta+2k\pi}{n}}, \quad \text{avec}$$

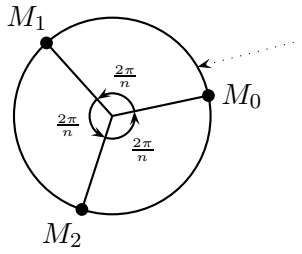
$$\forall k, l \in \mathbb{Z} \qquad Z_l = Z_k \iff (\exists p \in \mathbb{Z} \quad \tfrac{\theta+2l\pi}{n} = \tfrac{\theta+2k\pi}{n} + 2p\pi) \iff (\exists p \in \mathbb{Z} \quad l = k + pn).$$

D'où : $\mathscr{S} = \{Z_0, \dots, Z_{n-1}\}$ avec $Z_0, \dots, Z_{n-1}$ distincts. □

Remarques

1. L'équation $Z^n = 0$ d'inconnue $Z \in \mathbb{C}$ a pour unique solution 0 (clair).

2. Les images M_0, ..., M_{n-1} de Z_0, ..., Z_{n-1} (cf. la proposition) dans $\mathbb{R}^2$ sont les sommets d'un polygone régulier à n cotés inscrit dans le cercle de centre O et de rayon $r^{\frac{1}{n}}$:



cercle de centre O et de rayon $|z|^{\frac{1}{n}}$

(ici $n = 3$)

En effet, on a : $\text{mes}(\widehat{\overrightarrow{OM_k}, \overrightarrow{OM_{k+1}}}) \equiv \arg Z_{k+1} - \arg Z_k \equiv \frac{2\pi}{n}\ [2\pi]$ quand $0 \le k \le n-1$.

$\underbrace{\phantom{0 \text{ si } k = n-1}}_{0 \text{ si } k = n-1}$

[On a : $M_{k+1} = r(M_k)$ où $r : \mathbb{R}^2 \to \mathbb{R}^2$ est la rotation de centre O et d'angle $\arg\left(\frac{Z_{k+1}}{Z_k}\right)$.]

$\underbrace{M}_{\text{d'affixe } u} \mapsto \underbrace{M'}_{\text{d'affixe } \frac{Z_{k+1}}{Z_k} u}$

Définition

(a) On appelle racine n^{e} de l'unité toute solution de l'équation $z^n = 1$ d'inconnue $z \in \mathbb{C}$.

(b) On dit qu'une racine n^{e} de l'unité ζ est *une racine primitive* si le plus petit $l \in \mathbb{N}\setminus\{0\}$ tel que $\zeta^l = 1$ est égal à n.

Proposition

(a) Les racines n^{e} de l'unité sont les n nombres complexes $e^{\frac{2i\pi k}{n}}$ où $k \in \{0, 1, \dots, n-1\}$.

Leur somme, qui vaut donc $\sum_{k=0}^{n-1} \left(e^{\frac{2i\pi}{n}}\right)^k$, est égale à 0 quand $n \ge 2$.

(b) Soit $k \in \{0, 1, \dots, n-1\}$. La racine n^{e} de l'unité $e^{\frac{2i\pi k}{n}}$ est une racine n^{e} primitive de l'unité si et seulement si le seul diviseur $d \in \mathbb{N}$ commun à k et n est 1.

Démonstration

(a) Le début découle de la proposition précédente.

Ensuite, lorsque $n \geq 2$: $\displaystyle\sum_{k=0}^{n-1} \left(\mathrm{e}^{\frac{2\mathrm{i}\pi}{n}}\right)^k = \frac{1-\left(\mathrm{e}^{\frac{2\mathrm{i}\pi}{n}}\right)^{(n-1)+1}}{1-\mathrm{e}^{\frac{2\mathrm{i}\pi}{n}}} = 0.$

(b) Soit $k \in \{0, 1, \ldots, n-1\}$. Pour tout $l \in \mathbb{N} \setminus \{0\}$, on a :

$$\left(\mathrm{e}^{\frac{2\mathrm{i}\pi k}{n}}\right)^l = 1 \iff \frac{2\pi kl}{n} \equiv 0\ [2\pi] \iff n \text{ divise } kl.$$

Si le seul diviseur $d \in \mathbb{N} \setminus \{0\}$ commun à k et n est 1, alors la condition « n divise kl » implique que n divise l (décomposer n, k, et l en facteurs premiers) et a fortiori $\mathrm{e}^{\frac{2\mathrm{i}\pi k}{n}}$ est une racine n^{e} primitive de l'unité.

Si $d \in \mathbb{N}\setminus\{1\}$ est un diviseur commun à k et n, alors $d \neq 0$ et $\left(\mathrm{e}^{\frac{2\mathrm{i}\pi k}{n}}\right)^{\frac{n}{d}} = 1$ puis $\mathrm{e}^{\frac{2\mathrm{i}\pi k}{n}}$ n'est pas une racine n^{e} primitive de l'unité. □

Exemple

Les racines 4^{e} de l'unité sont 1, i, -1, $-\mathrm{i}$.

Les racines 4^{e} primitives de l'unité sont i et $-\mathrm{i}$.

Ch. 4. Méthode de Gauss

Plan

I. Systèmes linéaires

← [idem avec $\mathbb{C}$ au lieu de $\mathbb{R}$]

1. Introduction

Deux problèmes

1. Comment passer d'une équation cartésienne (image réciproque d'un singleton par une application) d'un « sous-espace affine de $\mathbb{K}^p$ » à une équation paramétrique qui décrit les points de ce sous-espace affine ? Par exemple :

$$(E_{\text{cart}}) \begin{cases} -4x+12y-5z = 1 \\ x-3y+2z = -1 \\ 2x-6y+z = 1 \end{cases} \text{ dans } \mathbb{K}^3 \text{ détermine } \mathscr{S}_{E_{\text{cart}}} := \underbrace{\{(x,y,z)\in\mathbb{K}^3 \mid E_{\text{cart}}\}}_{\text{image réciproque de } \{(1,-1,1)\} \text{ par ...}}.$$

2. Comment passer d'une équation paramétrique (image directe d'une application) d'un « sous-espace affine de $\mathbb{K}^p$ » à une équation cartésienne de ce sous-espace affine ? Par exemple :

$$\mathscr{D}: \begin{cases} x = s-t+1 \\ y = -s+t+2 \end{cases}, \ s,t\in\mathbb{K} \text{ détermine } \mathscr{D} := \underbrace{\{(s-t+1,-s+t+2)\ ;\ s,t\in\mathbb{K}\}}_{\text{image directe de } \mathbb{K}^2 \text{ par ...}} \subseteq \mathbb{K}^2.$$

Une motivation

De nombreuses équations issues de la physique se résolvent numériquement (par « discrétisation ») en se ramenant à des « systèmes linéaires », cf. :
`http://math.nist.gov/MatrixMarket/` (cliquer sur « Search by application area »).

But

On désire « résoudre » des équations comme (E_{cart}) au sens où on écrira $\mathscr{S}_{E_{\text{cart}}}$ sous forme paramétrique, sous réserve d'avoir $\mathscr{S}_{E_{\text{cart}}} \neq 0$. On va utiliser une méthode qui permettra aussi de passer d'une forme paramétrique à une forme cartésienne. Plus précisément, on cherche :
– une forme paramétrique sans paramètre inutile (ce n'est pas le cas dans la définition de $\mathscr{D}$ où tout s'exprime avec $u := s-t$) ;
– une forme cartésienne sans égalité inutile (ce n'est pas le cas dans l'écriture de (E_{cart}) où ligne 3 = −ligne 1 − 2 ligne 2).

2. Transformation d'un système linéaire

Définition

(a) Un système *d'équations « linéaires » de n équations à p inconnues dans* $\mathbb{K}$ est du type :

$$(E) \begin{cases} a_{11}x_1+\ldots+a_{1p}x_p &= b_1 \\ \ldots & \\ a_{n1}x_1+\ldots+a_{np}x_p &= b_n \end{cases} \quad \text{d'inconnue } (x_1,\ldots,x_p)\in\mathbb{K}^p$$

où sont donnés $a_{11},\ldots,a_{1p},a_{21},\ldots,a_{2p},\ldots,a_{n1},\ldots,a_{np}\in\mathbb{K}$ et $b_1,\ldots,b_n\in\mathbb{K}$.

Dans la suite du I on fixe un tel système (E) et note $\mathscr{S}_E$ l'ensemble de ses solutions dans $\mathbb{K}^p$.

(b) Le *système d'équations linéaires homogène associé à* (E) est le système suivant :

$$(H) \begin{cases} a_{11}x_1+\ldots+a_{1p}x_p &= 0 \\ \ldots & \\ a_{n1}x_1+\ldots+a_{np}x_p &= 0 \end{cases} \quad \text{d'inconnue } (x_1,\ldots,x_p)\in\mathbb{K}^p.$$

Remarques (importantes)

1. (H) admet toujours comme solution $(0,\dots,0)$.

2. On suppose que $\mathscr{S}_E \neq \emptyset$ et fixe une solution « particulière » $(x_1^E,\dots,x_p^E)$ de (E).
Pour tout $(x_1,\dots,x_p)\in\mathbb{K}^p$, on a tout de suite :
$(x_1,\dots,x_p)$ vérifie (E) si et seulement si $(x_1-x_1^E,\dots,x_p-x_p^E)$ vérifie (H).

En résumé : $\boxed{\text{solutions de } (E) = \text{solutions de } (H) + \text{une solution particulière de } (E)}$.

Notations

(a) On utilisera les « matrices » suivantes :

$A=\begin{pmatrix} a_{11} & \dots & a_{1p} \\ & \cdots & \\ a_{n1} & \dots & a_{np} \end{pmatrix}$ *matrice de* (E), $X=\begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}\underbrace{\text{inconnue}}_{\text{identifiée à } (x_1,\dots,x_p)}$, et $B=\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ *second membre de* (E).

On écrira en abrégé $(E): AX=B$.

(b) La *matrice augmentée* de (E) est la matrice $(A|B):=\left(\begin{array}{ccc|c} a_{11} & \dots & a_{1p} & b_1 \\ & \cdots & & \vdots \\ a_{n1} & \dots & a_{np} & b_n \end{array}\right)$, où la barre verticale n'a aucune signification mathématique.

On résoudra (E) en travaillant sur les lignes de $(A|B)$ et sur les colonnes de A.

Exemples (cf. l'introduction de la partie I de ce chapitre)

1. $\underbrace{\text{L'équation}}_{\text{d'inconnue } (x,y,z)\in\mathbb{K}^3}$ $(E_{\text{cart}})\begin{cases} -4x+12y-5z=1 \\ x-3y+2z=-1 \\ 2x-6y+z=1 \end{cases}$ a pour matrice augmentée $\left(\begin{array}{ccc|c} -4 & 12 & -5 & 1 \\ 1 & -3 & 2 & -1 \\ 2 & -6 & 1 & 1 \end{array}\right)$.

2. On fixe $(x,y)\in\mathbb{K}^2$. On a : $(x,y)\in\mathscr{D} \iff \left(\exists (s,t)\in\mathbb{K}^2 \quad \begin{cases} x=s-t+1 \\ y=-s+t+2 \end{cases}\right)$.

$\underbrace{\text{L'équation}}_{\text{d'inconnue } (s,t)\in\mathbb{K}^2}$ $(E_{\text{param}})\begin{cases} s-t=x-1 \\ -s+t=y-2 \end{cases}$ a pour matrice augmentée $\left(\begin{array}{cc|c} 1 & -1 & x-1 \\ -1 & 1 & y-2 \end{array}\right)$.

Définition

Dans ce qui suit on va noter L_1, ..., L_n les lignes de $(A|B)$ et C_1, ..., C_p les colonnes de A. Étant donnés $k\in\{1,...,n\}$ et $\alpha_1,...,\alpha_n\in\mathbb{K}$, on écrira « $L_k \leftarrow \alpha_1 L_1+...+\alpha_n L_n$ » pour exprimer qu'on remplace la ligne L_k par $\alpha_1 L_1+...+\alpha_n L_n$.

(a) Une *opération élémentaire sur les lignes de* $(A|B)$ est une des transformations suivantes :
(i) $L_i \overset{\text{(échange)}}{\longleftrightarrow} L_j$ avec $i\neq j$ « permutation de deux lignes » ;
(ii) $L_i \leftarrow c\,L_i$ avec $c\neq 0$ « multiplication d'une ligne par un scalaire non-nul » ;
(iii) $L_i \leftarrow L_i + cL_j$ avec $i\neq j$ et $c\in\mathbb{K}$ « ajout à une ligne d'un multiple d'une autre ligne ».

(b) Une *permutation de deux colonnes* de A est une transformation $C_i \overset{\text{(échange)}}{\longleftrightarrow} C_j$ avec $i\neq j$.

Remarque

Pour toute opération élémentaire l sur les lignes des matrices à n lignes et p (resp. $p+1$) colonnes et toute permutation c de deux colonnes de ces matrices, on a : $c\circ l = l\circ c$.

Lemme

Soit $(A'|B')$ une matrice obtenue à partir de $(A|B)$ après avoir effectué un nombre fini d'étapes de l'un des deux types suivants :
$L_i \leftrightarrow L_j$ avec $i\neq j$;
$L_i \leftarrow c_1L_1+\dots+c_iL_i+\dots+c_nL_n$ avec $1\leq i\leq n$, $c_1,...,c_n\in\mathbb{K}$ et $\underline{\underline{c_i\neq 0}}$.
Pour tout $X=\begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}\in\mathbb{K}^p$, le système $(E): AX=B$ équivaut au système $(E'): A'X=B'$.

Démonstration (idée)

En appliquant à (E) les opérations sur les lignes qui font passer de $(A|B)$ à $(A'|B')$, on constate que : si $(x_1,\dots,x_p)$ vérifie (E), alors $(x_1,\dots,x_p)$ vérifie (E').

Chaque étape se décompose en une succession d'opérations élémentaires sur les lignes. Pour être sûr de pouvoir remonter de (E') à (E), il reste à constater que ces opérations élémentaires sont réversibles :

(i) $L_i \leftrightarrow L_j$ avec $i \neq j$ a pour réciproque $L_i \leftrightarrow L_j$;

(ii) $L_i \leftarrow c\,L_i$ avec $c \neq 0$ a pour réciproque $L_i \leftarrow \frac{1}{c} L_i$;

(iii) $L_i \leftarrow L_i + cL_j$ avec $i \neq j$ et $c \in \mathbb{K}$ a pour réciproque $L_i \leftarrow L_i - cL_j$. □

Exemple

On va écrire une suite de matrices augmentées associées à des systèmes linéaires équivalents.

On peut commencer la résolution de (E_{cart}) ainsi, en entourant le « pivot » :

$$\left(\begin{array}{ccc|c} -4 & 12 & -5 & 1 \\ \textcircled{1} & -3 & 2 & -1 \\ 2 & -6 & 1 & 1 \end{array}\right) \xrightarrow[\substack{L_1 \leftrightarrow L_2 \\ \text{(pour utiliser le pivot 1, ce qui n'est pas indispensable)}}]{} \left(\begin{array}{ccc|c} \textcircled{1} & -3 & 2 & -1 \\ -4 & 12 & -5 & 1 \\ 2 & -6 & 1 & 1 \end{array}\right) \xrightarrow[\substack{L_2 \leftarrow L_2 + 4L_1 \\ \text{puis } L_3 \leftarrow L_3 - 2L_1 \\ \text{(pour amener des 0 dans } C_1 \\ \text{strictement sous la diagonale)}}]{} \left(\begin{array}{ccc|c} 1 & -3 & 2 & -1 \\ \boxed{0} & 0 & 3 & -3 \\ \boxed{0} & 0 & -3 & 3 \end{array}\right).$$

3. Méthode du pivot de Gauss

On va travailler sur les colonnes de A dans $(A|B)$ en allant de la gauche vers la droite pour se ramener à un système triangulaire. À chaque étape on va chercher un scalaire non-nul (« pivot ») vers le bas à partir du terme diagonal, et éventuellement à droite ce qui nécessitera de faire un échange de colonnes. On amène ce pivot sur la diagonale puis des 0 sous ce pivot.

Proposition (∗)

a) On peut passer par une suite finie d'opérations élémentaires sur les lignes et d'échanges de deux colonnes, de la matrice A à une matrice de la forme

$$A' = \left(\begin{array}{ccc|ccc} d_1 & \ddots & & & & \\ 0 & \ddots & & & & \\ \vdots & \ddots & & & & \\ 0 & \cdots & 0 \; d_r & & & \\ \hline 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right) \quad \text{avec } d_1 \neq 0,\ \dots,\ d_r \neq 0.$$

b) Le système $(E) : AX = B$ d'inconnue $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$ équivaut au système $(E') : A'X' = B'$ d'inconnue $X' := \begin{pmatrix} x_{j_1} \\ \vdots \\ x_{j_p} \end{pmatrix}$, où les transformations du (a) envoient $\left(\begin{smallmatrix} x_1 \dots x_p \\ A \end{smallmatrix} \middle| B\right)$ sur $\left(\begin{smallmatrix} x_{j_1} \dots x_{j_p} \\ A' \end{smallmatrix} \middle| B'\right)$.

[Noter que les lettres qui se trouvent au-dessus de A ou de A' représentent ici les noms des variables-coordonnées d'un vecteur de $\mathbb{K}^n$ et non pas les valeurs particulières qu'elles prennent pour le vecteur X. De plus, ce sont les éventuels échanges de colonnes qui feront passer de $x_1,\dots,x_p$ à $x_{j_1},\dots,x_{j_p}$.]

c) On note $\mathscr{S}_E$ l'ensemble des solutions de (E) et $B' = \begin{pmatrix} b'_1 \\ \vdots \\ b'_n \end{pmatrix}$.

On a : $\mathscr{S}_E \neq \emptyset \iff \underbrace{b'_{r+1} = \dots = b'_n = 0}_{n-r \text{ conditions}}$.

(∗) Pour un point de vue sans échanges de colonnes, voir la fin de ce paragraphe (« matrices échelonnées »).

Les échanges de deux colonnes peuvent permettre de minimiser les erreurs d'arrondis sur ordinateur : en travaillant sur la j^{e} colonne on choisirait comme pivot a_{i_0,j_0} avec $i_0, j_0 \geq j$ tels que $|a_{i_0,j_0}| = \max_{i',j' \geq j} |a_{i',j'}|$.

Dans ce cas, on obtient une équation paramétrique de $\mathscr{S}_E$ à partir de (E') en écrivant successivement x_{j_r}, ..., x_{j_1} en fonction des paramètres $\underbrace{t_1 := x_{j_{r+1}}, ..., t_{p-r} := x_{j_p}}_{p-r \text{ paramètres}}$.

Ainsi, quand $r = n = p$ (« système de Cramer ») le système (E) a une unique solution.

Démonstration

(a) On écarte le cas $A = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}$ qui donnerait $r = 0$ et $A' = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}$. On a :

$$\left(\underbrace{A}^{x_1 \dots x_p}_{\substack{\text{a un coefficient} \\ d_1 \text{ non-nul}}} \mid B\right) \xrightarrow[\substack{\text{permutation} \\ \text{de lignes et} \\ \text{de colonnes}}]{} \left(\begin{array}{ccc|c} & \overset{x_{k_1}}{\overset{\dots}{}} & \overset{x_{k_p}}{} & \\ d_{1\neq 0} & & & \\ u_2 & & & \\ \vdots & & & \\ u_n & & & \end{array}\right) \xrightarrow[\substack{L_2 \leftarrow L_2 - \frac{u_2}{d_1}L_1 \\ \dots \\ L_n \leftarrow L_n - \frac{u_n}{d_1}L_1}]{} \left(\begin{array}{ccc|c} & \overset{x_{k_1}}{\overset{\dots}{}} & \overset{x_{k_p}}{} & \\ d_1 & & & \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{array}\right) \to \underbrace{\dots}_{\text{(récurrence)}} \to \left(\begin{array}{ccc|c} \overset{x_{j_1}}{d_1} & \overset{\dots}{} & \overset{x_{j_p}}{} & \\ 0 & \ddots & & \\ 0 \dots 0 & d_r & & \\ \hline 0 \dots 0 & & 0 \dots 0 & \\ \vdots & & \vdots & \\ 0 \dots 0 & & 0 \dots 0 & \end{array}\right)$$

$x_{k_2} \dots x_{k_p}$; on le réduit et transmet au-dessus les échanges de colonnes

où on s'arrête quand le rectangle $\left(\underbrace{\widetilde{A}}^{x_{j_1} \dots x_{j_p}} \mid \widetilde{B}\right)$ qu'on réduit par récurrence sur n vérifie $\widetilde{A} = 0$.

(b) (c) D'après le lemme du 2, et le fait qu'un échange de colonnes donne deux systèmes linéaires équivalents, (E) équivaut à :

$$(E') \begin{cases} d_1 x_{j_1} + \dots \dots \dots = b'_1 \\ \quad d_1 x_{j_2} + \dots \dots = b'_2 \\ \qquad \ddots \\ \qquad\quad d_1 x_{j_r} + \dots = b'_r \\ \qquad\qquad\quad 0 = b'_{r+1} \\ \qquad\qquad\quad \vdots \quad \vdots \\ \qquad\qquad\quad 0 = b'_n \end{cases} \quad \text{c'est-à-dire à :} \quad \begin{cases} x_{j_{r+1}} = t_1 \\ \quad \vdots \\ x_{j_p} = t_{p-r} \\ x_{j_r} = \frac{1}{d_r}(\dots) \\ \quad \vdots \\ x_{j_1} = \frac{1}{d_1}(\dots) \end{cases} \text{à exprimer avec } t_1, \dots, t_{p-r}$$

$b'_{r+1} = \dots = b'_n = 0$ et $\exists t_1, \dots, t_{p-r} \in \mathbb{K}$. □

Remarques

1. Quand (E) a strictement plus d'inconnues que d'équations (c'est-à-dire $p > n$) et $\mathscr{S}_E \neq \emptyset$ (par exemple (E) est homogène), on a : $\underbrace{p-r}_{\text{nombre de paramètres}} > n - r \geq 0$, donc $\mathscr{S}_E$ est infini.

> Tout système linéaire homogène dont le nombre d'inconnues est strictement supérieur au nombre d'équations admet une infinité de solutions.

2. La matrice $(A'|B')$ dépend des opérations sur les lignes et les colonnes qu'on a utilisées.

Cependant, on verra dans la suite du cours que :

– r ne dépend que de A, et sera appelé « le rang de A » ;

– $\mathscr{S}_E$ n'a pas d'équation paramétrique avec strictement moins que $p-r$ paramètres ;

(lorsque $\mathscr{S}_E$: $AX = B$ et $\mathscr{S}_E = \{UT+V\,;\, T \in \mathbb{K}^k\}$, on a : $k \geq \dim \overrightarrow{\mathscr{S}_E} = \dim \operatorname{Ker} A = p-r$)

– une équation cartésienne obtenue par la méthode de Gauss à partir d'une équation paramétrique a un nombre d'égalités qui est minimal.

(lorsque $\mathscr{E} = \{AT + C\,;\, T \in \mathbb{K}^p\}$ et $\mathscr{E}$: $UX = V$, on a : $\operatorname{rg} U = n - \dim \overrightarrow{\mathscr{E}} = n - r$)

Algorithme 1 (« pivot total » au sens où on cherche d_j dans n'importe quelle colonne)

On détaille la méthode de la démonstration pour construire $\left(\overset{x_{j_1} \dots x_{j_p}}{A'} \mid B'\right)$ comme au (b). On utilise une construction par récurrence. On construit la j^{e} colonne à l'étape $j \in \{1, ..., p\}$:

(i) $\left(\begin{array}{c|c} \begin{matrix} d_1 & & \\ & \ddots & \\ & & d_{j-1} \end{matrix} & \\ \hline 0 & d_j \end{array}\right)$ (ii) $\left(\begin{array}{c|c} \begin{matrix} d_1 & & \\ & \ddots & \\ & & d_{j-1} \end{matrix} & \\ \hline 0 & \textcircled{d_j} \end{array}\right)$ (iii) $\left(\begin{array}{c|c} \begin{matrix} d_1 & & \\ & \ddots & \\ & & d_{j-1} \end{matrix} & \\ \hline 0 & \begin{matrix} d_j \\ 0 \\ \vdots \\ 0 \end{matrix} \end{array}\right)$.

(i) On choisit une colonne $C_{j'}$ avec $j \leq j' \leq p$ qui a, à partir de la j^{e} ligne, au moins un coefficient $d_j \neq 0$ (s'il n'y a pas une telle colonne on arrête), puis on échange C_j et $C_{j'}$.

(ii) On échange la j^{e} ligne avec la ligne contenant d_j.

(iii) On amène des 0 strictement au-dessous de d_j par des opérations sur les lignes (composées de deux opérations élémentaires) de la forme $L_i \leftarrow c_i L_i + c_j L_j$ avec $c_i \neq 0$ quand $i > j$.

Après avoir travaillé sur toutes les colonnes en reportant les opérations sur les lignes au niveau de la colonne à droite de la barre verticale, on regarde si les membres de droite des égalités dont le membre de gauche est 0 vaut lui-même 0 (sinon le système n'a pas de solution) auquel cas on résout le système en remontant de la dernière égalité à la première égalité.

Remarques

En pratique, on exploitera la proposition précédente en allégeant la présentation :
– lorsque $B = 0$ on ne fera pas apparaître la dernière colonne (seconds membres nuls) ;
– on n'introduira les noms des variables au dessus des p premières colonnes qu'à partir du moment où un échange de colonnes aura été introduit (ce qui est rarement indispensable) ;
– on résoudra « de tête » le système triangulaire correspondant à la dernière étape de la méthode de Gauss, en partant de la dernière égalité et remontant vers la première.

Exemples (cf. l'introduction de la partie I de ce chapitre)

1. Fin de la résolution de (E_{cart}) :

$$\left(\begin{array}{ccc|c} -4 & 12 & -5 & 1 \\ 1 & -3 & 2 & -1 \\ 2 & -6 & 1 & 1 \end{array}\right) \underbrace{\rightarrow \cdots \rightarrow}_{\text{déjà vu}} \overset{\begin{matrix} x & y & z \end{matrix}}{\left(\begin{array}{ccc|c} 1 & -3 & 2 & -1 \\ 0 & 0 & \textcircled{3} & -3 \\ 0 & 0 & -3 & 3 \end{array}\right)} \xrightarrow[C_2 \leftrightarrow C_3]{} \overset{\begin{matrix} x & z & y \end{matrix}}{\left(\begin{array}{ccc|c} 1 & 2 & -3 & -1 \\ 0 & \textcircled{3} & 0 & -3 \\ 0 & -3 & 0 & 3 \end{array}\right)} \xrightarrow[L_3 \leftarrow L_3 + L_2]{} \overset{\begin{matrix} x & z & y \end{matrix}}{\left(\begin{array}{ccc|c} \boxed{1} & 2 & -3 & -1 \\ 0 & \boxed{3} & 0 & -3 \\ 0 & 0 & 0 & 0 \end{array}\right)}.$$

En renommant dans la conclusion la variable y en t, et calculant d'abord z puis ensuite x, on obtient l'équation paramétrique suivante de $\mathscr{S}_{E_{\text{cart}}}$:

$$\mathscr{S}_{E_{\text{cart}}} : \left\{\begin{array}{l} x = \frac{1}{1}(-2(-1) + 3t - 1) = 3t + 1 \\ y = t \\ z = \frac{1}{3}(-3) = -1 \end{array}\right. , \qquad t \in \mathbb{K}.$$

2. Soit $(x, y) \in \mathbb{K}^2$. Existence de $(s, t) \in \mathbb{K}^2$ vérifiant $(E_{\text{param}}) \left\{\begin{array}{r} s - t = x - 1 \\ -s + t = y - 2 \end{array}\right.$?

Calcul par la méthode de Gauss : $\left(\begin{array}{cc|c} \textcircled{1} & -1 & x-1 \\ -1 & 1 & y-2 \end{array}\right) \xrightarrow[L_2 \leftarrow L_2 + L_1]{} \left(\begin{array}{cc|c} \boxed{1} & -1 & /// \\ 0 & 0 & \underbrace{x+y-3}_{\text{est-ce égal à 0 ?}} \end{array}\right)$.

Ainsi $\mathscr{D} : \left\{\begin{array}{l} x = \ s - t + 1 \\ y = -s + t + 2 \end{array}\right.$, $s, t \in \mathbb{K}$ a pour équation cartésienne : $\mathscr{D} : x + y - 3 = 0$.

(Inutile de calculer explicitement les valeurs des paramètres s et t en fonction de x et y.)

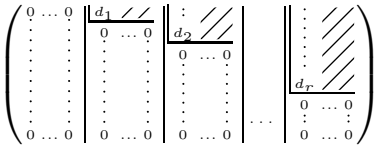
3. Le système $(E_C) \left\{\begin{array}{r} 3x + 2y = 5 \\ 2x - y = 4 \end{array}\right.$ se résout ainsi : $\left(\begin{array}{cc|c} \textcircled{3} & 2 & 5 \\ 2 & -1 & 4 \end{array}\right) \xrightarrow[L_2 \leftarrow 3L_2 - 2L_1]{} \left(\begin{array}{cc|c} \boxed{3} & 2 & 5 \\ 0 & \boxed{-7} & 2 \end{array}\right)$.

C'est un système de Cramer d'unique solution donnée par : $\left\{\begin{array}{l} x = \frac{1}{3}\big(-2(-\frac{2}{7}) + 5\big) = \frac{13}{5} \\ y = -\frac{2}{7} \end{array}\right.$.

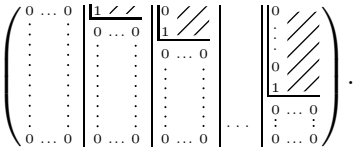
4. Un autre exemple de résolution par Gauss pour s'assurer que c'est compris : un système linéaire non-homogène à 3 lignes et 4 inconnues (L_1 choisie par un étudiant avec un 1^{er} coefficient non-nul, L_2 avec petit déterminant 2×2 nul en haut à gauche et petit déterminant 2×2 suivant non-nul, L_3 combinaison linéaire de L_1 et L_2).

Définition (« méthode de Gauss sans échange de colonnes »)

(a) Une *matrice échelonnée* — suivant les lignes — est une matrice telle que le nombre de termes nuls au début de chaque ligne augmente lorsqu'on passe d'une ligne à la suivante, et ce nombre augmente même strictement lorsqu'on passe d'une ligne non nulle à la suivante.

Il s'agit d'une matrice de la forme  avec $d_1 \neq 0$, ..., $d_r \neq 0$.

(b) Une *matrice échelonnée réduite* est une matrice échelonnée dans laquelle les premiers termes non-nuls sur chaque ligne sont des 1 au-dessus desquels se trouvent des 0. Elle s'écrit :



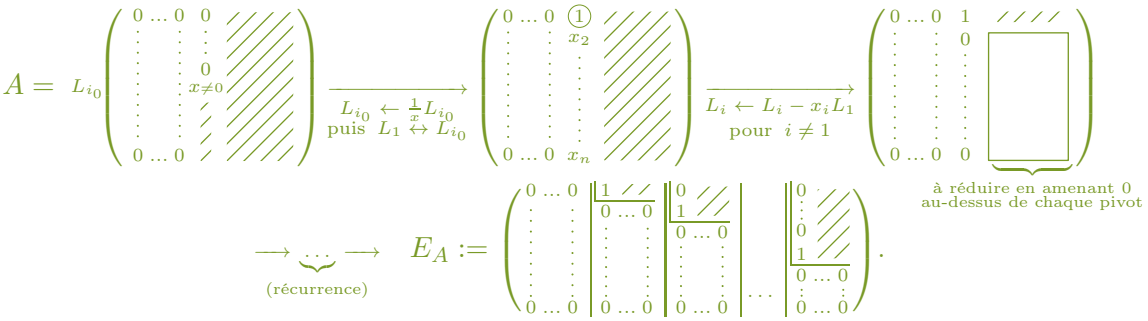
Proposition

Il existe une unique matrice échelonnée réduite E_A qui se déduit de A par des opérations élémentaires sur les lignes.

Démonstration (idées)

• Existence ?

Elle s'obtient par exemple ainsi :



• Unicité ?

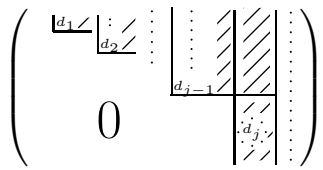
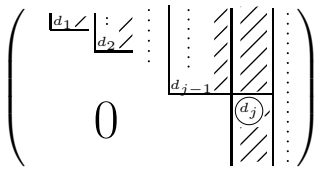
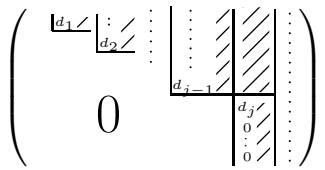
On vérifie par récurrence sur p qu'une matrice échelonnée réduite A' avec r lignes non-nulles déduite de A par des opérations élémentaires sur les lignes est déterminée par A.
On remarque tout d'abord que les relations $\alpha_1 C_1 + \cdots + \alpha_p C_p = 0$ sont vérifiées pour les mêmes $(\alpha_1, ..., \alpha_p) \in \mathbb{K}^p$ au niveau de A et de A' (il s'agit des solutions du système $(H) : AX = 0$).

Lorsque $p = 0$ la seule matrice échelonnée réduite est la matrice vide. En supposant que la proposition est vraie avec $p-1$ à la place de p, les colonnes $C_1, ..., C_{p-1}$ de A' sont déterminées par A. Il reste à constater que la colonne C_p de A' est nulle quand $A = 0$, et sinon (avec $r \neq 0$) contient :

– un seul terme non-nul égal à 1 au niveau de la r^{e} ligne si $C_p \notin \text{Vect}(C_1, ..., C_{p-1})$;
– les coordonnées de C_p suivant les r colonnes des pivots si $C_p \in \text{Vect}(C_1, ..., C_{p-1})$. □

Algorithme 2 (« pivot partiel » au sens où on cherche d_j dans la 1^{re} colonne possible)

On détaille la méthode de la démonstration pour construire $(A'|B')$ avec A' échelonnée. On utilise une construction par récurrence. On s'intéresse à la j^{e} ligne à l'étape $j \in \{1, ..., p\}$:

(i)  (ii)  (iii) 

(i) On se place dans la colonne la plus à gauche qui a, à partir de la j^{e} ligne, au moins un coefficient $d_j \neq 0$ (s'il n'y a pas une telle colonne on arrête).

(ii) On échange la j^{e} ligne avec la ligne contenant d_j.

(iii) On amène des 0 strictement au-dessous de d_j par des opérations sur les lignes (composées de deux opérations élémentaires) de la forme $L_i \leftarrow c_i L_i + c_j L_j$ avec $c_i \neq 0$ quand $i > j$.

Pour obtenir une matrice échelonnée réduite, on amènerait aussi à la j^{e} étape dans (iii) des 0 strictement au-dessus du pivot d_j par des opérations sur les lignes de la forme $L_i \leftarrow c_i L_i + c_j L_j$ avec $c_i \neq 0$ quand $i < j$, puis en fin de calcul on diviserait chacune des lignes non-nulles par son premier coefficient non-nul (noté d_j à la j^{e} étape).

Après avoir travaillé sur toutes les lignes en reportant les opérations sur les lignes au niveau de la colonne qui se trouve à droite de la barre verticale, on regarde si les membres de droite des égalités dont le membre de gauche est 0 vaut lui-même 0 (sinon le système n'a pas de solution), auquel cas on résout le système en remontant de la dernière égalité à la première égalité.

On peut adapter cet algorithme au cas des matrices à valeurs dans $\mathbb{Z}$.

Pour cela on remplace au (iii) de la j^{e} étape les opérations sur les lignes par des opérations correspondant à la multiplication à gauche par un certain $P \in \mathfrak{M}(n, \mathbb{Z})$ inversible dans $\mathfrak{M}(n, \mathbb{Z})$.

On note a_1, ..., a_n les coefficients dans la j^{e} colonne. On fixe $i > j$ tel que $a_i \neq 0$.

On pose : $d_{i,j} = \text{pgcd}(a_i, a_j) \in \mathbb{Z} \setminus \{0\}$, $b_i = \frac{a_i}{d_{i,j}}$ et $b_j = \frac{a_j}{d_{i,j}}$.

D'après le théorème de Bézout, il existe $u_i, u_j \in \mathbb{Z}$ tels que $u_i b_i + u_j b_j = 1$.

L'opération $(L_i, L_j) \leftarrow (u_i L_i + u_j L_j, -b_j L_i + b_i L_j)$ amène $d_{i,j}$ sur la j^{e} ligne et 0 sur la i^{e} ligne.

Remarques (lien entre les deux présentations de l'algorithme du pivot de Gauss)

1. En appliquant à A les opérations élémentaires sur les lignes — mais pas sur les colonnes — qui ont permis de passer de A à une matrice A' en suivant l'algorithme 1 avec à chaque étape le pivot dans la colonne la plus à gauche, on obtient une matrice échelonnée.

2. Réciproquement, à partir d'une matrice échelonnée déduite de A par des opérations élémentaires sur les lignes, en déplaçant en premières positions les colonnes contenant les termes non-nuls au début de chaque ligne, on obtient une matrice A' associée à l'algorithme 1.

II. Rappels de géométrie affine

1. Droite et plan affine : repère affine

Définition-Proposition

(a) On appelle *droite affine de* $\mathbb{R}^p$ toute partie de $\mathbb{R}^p$ de la forme

$$\mathscr{D} = \{A + sv \ ; \ s \in \mathbb{R}\} \quad \text{où} \quad A, v \in \mathbb{R}^p \text{ et } v \neq 0.$$

Dans ce cas on dit que :

– (A, v) est un « repère » de $\mathscr{D}$ et pour tout $M \in \mathscr{D}$ l'unique $s \in \mathbb{R}$ tel que $M = A + sv$ est la « coordonnée » de M dans (A, v) ;

– $\overrightarrow{\mathscr{D}} := \{\overrightarrow{MN} \ ; \ M, N \in \mathscr{D}\}$ est la « direction de $\mathscr{D}$ », telle que $\overrightarrow{\mathscr{D}} = \{sv \ ; \ s \in \mathbb{R}\}$.

La description de $\overrightarrow{\mathscr{D}}$ permet de dire que v est un *vecteur directeur de* $\mathscr{D}$.

(b) Soient $v, w \in \mathbb{R}^p$. On dit que v et w sont *colinéaires* si $v = 0$ ou w est multiple de v.

(c) On appelle *plan affine de* $\mathbb{R}^p$ toute partie de $\mathbb{R}^p$ de la forme

$$\mathscr{P} = \{A + sv + tw \ ; \ s, t \in \mathbb{R}\} \quad \text{où} \quad A, v, w \in \mathbb{R}^p \text{ et, } v \text{ et } w \text{ sont non colinéaires.}$$

Dans ce cas on dit que :

– (A, v, w) est un « repère » de $\mathscr{P}$ et pour tout $M \in \mathscr{P}$ l'unique couple $(s, t) \in \mathbb{R}^2$ tel que

$M = A + sv + tw$ est le couple des « coordonnées » de M dans (A, v, w) ;
– $\overrightarrow{\mathscr{P}} := \{\overrightarrow{MN}\ ;\ M, N \in \mathscr{P}\}$ est la « direction de $\mathscr{P}$ », telle que $\overrightarrow{\mathscr{P}} = \{sv + tw\ ;\ s, t \in \mathbb{R}\}$.
La description de $\overrightarrow{\mathscr{P}}$ permet de dire que (v, w) est une *base de la direction de* $\mathscr{P}$.

Exemples

(a) Les droites affines de $\mathbb{R}^2$ sont :

$$\mathscr{D}\colon ax + by = c \ \text{ avec } \ a, b, c \in \mathbb{R} \ \text{ et } \ (a, b) \neq (0, 0)\,;$$

Pour une telle droite $\mathscr{D}$, on a : $\overrightarrow{\mathscr{D}}\colon ax + by = 0$.

De plus, deux telles droites $\mathscr{D}_1\colon a_1x + b_1y = c_1$ et $\mathscr{D}_2\colon a_2x + b_2y = c_2$ sont égales si et seulement si (a_1, b_1, c_1) et (a_2, b_2, c_2) sont colinéaires.

(b) Les droites affines de $\mathbb{R}^3$ sont :

$\mathscr{D}\colon \begin{cases} ax + by + cz = d \\ a'x + b'y + c'z = d' \end{cases}$ avec $a, b, c, d, a', b', c', d' \in \mathbb{R}$ et, (a, b, c) et (a', b', c') non colinéaires.

Pour une telle droite $\mathscr{D}$, on a : $\overrightarrow{\mathscr{D}}\colon \begin{cases} ax + by + cz = 0 \\ a'x + b'y + c'z = 0 \end{cases}$.

(c) Les plans affines de $\mathbb{R}^3$ sont :

$$\mathscr{P}\colon ax + by + cz = d \ \text{ avec } \ a, b, c, d \in \mathbb{R} \ \text{ et } \ (a, b, c) \neq (0, 0, 0)\,;$$

Pour un tel plan $\mathscr{P}$, on a : $\overrightarrow{\mathscr{P}}\colon ax + by + cz = 0$.

De plus, deux tels plans $\mathscr{P}_1\colon a_1x + b_1y + c_1z = d_1$ et $\mathscr{P}_2\colon a_2x + b_2y + c_2z = d_2$ sont égaux si et seulement si (a_1, b_1, c_1, d_1) et (a_2, b_2, c_2, d_2) sont colinéaires.

Exemples (cf. les exemples 1 et 2 du I. 3)

1. Équation cartésienne de la droite de $\mathbb{R}^3$ de repère (A_1, v_1) avec $A_1 = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$ et $v_1 = \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}$?
Cette droite $\mathscr{D}_1$ s'écrit sous la forme paramétrique suivante :

$$\mathscr{D}_1\colon \begin{cases} x = 3t + 1 \\ y = t \\ z = -1 \end{cases}, \qquad t \in \mathbb{R}.$$

On étudie l'existence de t par la méthode de Gauss : $\left(\begin{array}{c|c} \textcircled{3} & x - 1 \\ 1 & y \\ 0 & z + 1 \end{array}\right) \xrightarrow[L_2 \leftarrow 3L_2 - L_1]{} \left(\begin{array}{c|c} \boxed{3} & /// \\ 0 & -x + 3y + 1 \\ 0 & z + 1 \end{array}\right)$.

On obtient donc l'équation cartésienne $\mathscr{D}_1\colon \begin{cases} -x + 3y + 1 = 0 \\ z + 1 = 0 \end{cases}$.

2. Repère de la droite $\mathscr{D}_2$ de $\mathbb{R}^2$ d'équation cartésienne $\mathscr{D}_2\colon\ x + y - 3 = 0$?
Résolution par la méthode de Gauss : $\left(\begin{array}{cc|c} x & y & \\ \boxed{1} & 1 & 3 \end{array}\right)$ donne $\mathscr{D}_2\colon \begin{cases} x = -s + 3 \\ y = s \end{cases}, \qquad s \in \mathbb{R}.$
Par conséquent la droite $\mathscr{D}_2$ a pour repère (A_2, v_2) avec $A_2 = \begin{pmatrix} 3 \\ 0 \end{pmatrix}$ et $v_2 = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$.

2. Droite et plans affines : repère barycentrique

Proposition

(a) Soient $A, B \in \mathbb{R}^p$ distincts.
Il existe une unique droite affine de $\mathbb{R}^p$, notée (AB), qui contient A et B.
Elle admet pour repère $(A, \overrightarrow{AB})$.

(b) Soient $A, B, C \in \mathbb{R}^p$. Les points A, B, C appartiennent à une même $\overbrace{\text{droite}}^{\text{(affine)}}$ de $\mathbb{R}^p$, ce qui se traduit en disant que « A, B, C sont alignés », si et seulement si $\overrightarrow{AB}$ et $\overrightarrow{AC}$ sont colinéaires.

(c) Soient $A, B, C \in \mathbb{R}^p$ non alignés.
Il existe un unique plan affine de $\mathbb{R}^p$, notée (ABC), qui contient A, B et C.
Il admet pour repère $(A, \overrightarrow{AB}, \overrightarrow{AC})$.

Remarque

On dit parfois que :

– (A, B) est un *repère barycentrique* de la droite $\mathscr{D} := (AB)$ du (a) ;

– (A, B, C) est un *repère barycentrique* du plan $\mathscr{P} := (ABC)$ du (c).

III. L'ESPACE VECTORIEL $\mathbb{R}^n$ ← [idem avec $\mathbb{C}$ au lieu de $\mathbb{R}$]

Dans toute cette partie on se donne $n \in \mathbb{N}$.

1. Sous-espaces vectoriels de $\mathbb{R}^n$

Notations

(a) On note $\mathbb{R}^n$ l'ensemble des n-uplets $(x_1, ..., x_n)$ de réels $x_1, ..., x_n$.
Par convention : $\mathbb{R}^0 := \{0\} \subseteq \mathbb{R}$, en « identifiant » la suite vide $()$ et 0.
On appelle « vecteur » tout élément de $\mathbb{R}^n$ et « scalaire » tout élément de $\mathbb{R}$.

(b) *Somme de deux vecteurs* : $(x_1, ..., x_n) + (y_1, ..., y_n) := (x_1 + y_1, ..., x_n + y_n)$.
Vecteur nul : $0_{\mathbb{R}^n} := (0, ..., 0)$; *opposé d'un vecteur* : $-(x_1, ..., x_n) := (-x_1, ..., -x_n)$.
Différence de deux vecteurs : $(x_1, ..., x_n) - (y_1, ..., y_n) := (x_1 - y_1, ..., x_n - y_n)$.

(c) *Multiplication d'un scalaire par un vecteur* : $\alpha\,(x_1, ..., x_n) := (\alpha x_1, ..., \alpha x_n)$.

Remarque

Pour tous $u, v, w \in \mathbb{R}^n$ et $\alpha, \beta \in \mathbb{R}$, on a :
(i) $(u + v) + w = u + (v + w)$ et $v + w = w + v$;
(ii) $v + 0_{\mathbb{R}^n} = v$ et $v + (-v) = 0_{\mathbb{R}^n}$
(iii) $\alpha\,(v + w) = (\alpha\, v) + (\alpha\, w)$ et $(\alpha + \beta)\, v = (\alpha\, v) + (\beta\, v)$;
(iv) $1\, v = v$ et $\alpha\,(\beta\, v) = (\alpha\beta)\, v$.

Dans la suite on notera plus simplement, par abus, 0 au lieu de $0_{\mathbb{R}^n}$.

Définition-Proposition

Soient $p \in \mathbb{N}$ et $v_1, \ldots, v_p, v, w \in \mathbb{R}^n$.

(a) Une *combinaison linéaire* de $v_1, \ldots, v_p$ est un vecteur v de $\mathbb{R}^n$ de la forme
$$v = \underbrace{\alpha_1\, v_1 + \cdots + \alpha_p\, v_p}_{0 \text{ quand } p = 0} \quad \text{avec} \quad \alpha_1, \ldots, \alpha_p \in \mathbb{R}.$$

(b) On dit que v et w sont *colinéaire* (« sur une même droite ») s'il existe $\alpha \in \mathbb{R}$ tel que $v = \alpha\, w$ ou $w = \alpha\, v$. Cela équivaut à : $v = 0$ ou $\underbrace{\text{il existe } \alpha \in \mathbb{R} \text{ tel que } w = \alpha\, v}_{\text{« } w \text{ est multiple de } v \text{ »}}$.

DÉMONSTRATION

Il s'agit de prouver l'équivalence du (b).
($\Rightarrow$) Dans le cas où $v = \alpha\, w$, on a : soit $\alpha = 0$ et par suite $v = 0$, soit $\alpha \neq 0$ et $w = \frac{1}{\alpha}\, v$.
($\Leftarrow$) Lorsque $v = 0$, on a : $v = 0\, w$. □

Remarque

La notation « $\alpha_1\, v_1 + \cdots + \alpha_p\, v_p$ » avec des points de suspension est usuelle mais abusive. On pourrait la remplacer par « $\sum_{1 \leq k \leq p} \alpha_k\, v_k$ » avec la définition par récurrence suivante :
$$\sum_{1 \leq k \leq 0} u_k := 0 \quad \text{et} \quad \sum_{1 \leq k \leq p+1} u_k = \Big(\sum_{1 \leq k \leq p} u_k\Big) + u_{p+1} \quad \text{pour tous } u_1, ..., u_{p+1} \in \mathbb{R}^n.$$

Exemple

Dans $\mathbb{R}^3$, on choisit $v_1 = (0, 1, -1)$, $v_2 = (1, 0, -1)$, $v_3 = (1, -1, 0)$, et $v = (5, -2, -3)$.
Le vecteur v est combinaison linéaire de v_1, v_2, v_3 car : $v = v_1 + 2v_2 + 3v_3$.

Notation

Soient $p \in \mathbb{N}$ et $v_1, \ldots, v_p \in \mathbb{R}^n$.
On note $\mathrm{Vect}(v_1, ..., v_p)$ l'ensemble des combinaisons linéaires des vecteurs $v_1, ..., v_p$:
$$\mathrm{Vect}(v_1, ..., v_p) = \big\{\alpha_1\, v_1 + \cdots + \alpha_p\, v_p \ ;\ \alpha_1, \ldots, \alpha_p \in \mathbb{R}\big\}.$$

Définition

On dit qu'une partie E de $\mathbb{R}^n$ est un *sous-espace vectoriel de* $\mathbb{R}^n$ si :

(i) $0 \in E$;
(ii) pour tous $\alpha, \beta \in \mathbb{R}$ et $v, w \in E$, on a $\alpha\, v + \beta\, w \in E$.

Remarques

1. Il est immédiat que : $\{0_{\mathbb{R}^n}\}$ et $\mathbb{R}^n$ sont des sous-espaces vectoriels de $\mathbb{R}^n$.

2. Soient E un sous-espace vectoriel de $\mathbb{R}^n$, $p \in \mathbb{N}$ et $v_1, \ldots, v_p \in E$.
Par récurrence sur p, on constate que toute combinaison linéaire de $v_1, \ldots, v_p$ appartient à E.

On vient de voir que $\mathbb{R}^2$ admet comme sous-espaces vectoriels $\{(0,0)\}$, les droites de $\mathbb{R}^2$ passant par l'origine, et $\mathbb{R}^2$. On va vérifier géométriquement qu'il n'y a pas d'autre sous-espace vectoriel de $\mathbb{R}^2$.

Soit E un sous-espace vectoriel de $\mathbb{R}^2$ autre que $\{(0,0)\}$. Il contient un vecteur $v \neq 0$. On suppose maintenant que E n'est pas égal à $\mathbb{R}v$. Dans ce cas E contient un vecteur w non-colinéaire à v, puis E contient tout vecteur u de $\mathbb{R}^2$. En effet, on peut écrire u comme somme des vecteurs $\alpha\, v$ et $\beta\, w$ qui se trouvent aux intersections de $\mathbb{R}v$ avec la parallèle à $\mathbb{R}w$ passant par u et de $\mathbb{R}w$ avec la parallèle à $\mathbb{R}v$ passant par u. Ainsi $E = \mathbb{R}^2$. (Plus tard la notion de dimension fournira une démonstration simple.)

Exemples

1. On considère $E = \{(x,y,z) \in \mathbb{R}^3 \mid x + y + z = 0\}$.

(i) On a : $0 + 0 + 0 = 0$ donc $0 \in E$.

(ii) Soient $\alpha, \beta \in \mathbb{R}$ et $v = (x', y', z'), w = (x'', y'', z'') \in E$.
On a : $\alpha\, v + \beta\, w = (x, y, z)$ avec $x := \alpha x' + \beta x''$, $y := \alpha y' + \beta y''$, $z := \alpha z' + \beta z''$.
Or : $x + y + z = \alpha(\underbrace{x' + y' + z'}_{0 \text{ car } v \in E}) + \beta(\underbrace{x'' + y'' + z''}_{0 \text{ car } w \in E})$. D'où : $\alpha\, v + \beta\, w \in E$.

En conclusion : E est un sous-espace vectoriel de $\mathbb{R}^3$.

2. Plus généralement, l'ensemble E des solutions d'un système d'équations linéaires homogène (H) : $AX = 0$ d'inconnue $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \in \mathbb{R}^p$ est un sous-espace vectoriel de $\mathbb{R}^p$ (*) (exercice).

Définition-Proposition

Soient $p \in \mathbb{N}$ et $v_1, ..., v_p \in \mathbb{R}^n$. On a : $\mathrm{Vect}(v_1, ..., v_p)$ est l'unique sous-espace vectoriel de $\mathbb{R}^n$ qui contient $v_1, ..., v_p$ et qui est inclus dans tout sous-espace vectoriel E de $\mathbb{R}^n$ contenant $v_1, ..., v_p$ (plus petit – pour l'inclusion – sous-espace vectoriel de $\mathbb{R}^n$ contenant $v_1, ..., v_p$).

On appelle $\mathrm{Vect}(v_1, ..., v_p)$ le *sous-espace vectoriel V de $\mathbb{R}^n$ engendré par $v_1, ..., v_p$* (**).

Démonstration

On note $V = \mathrm{Vect}(v_1, ..., v_p)$.

(a) On montre que V est un sous-espace vectoriel de $\mathbb{R}^n$ contenant $v_1, ..., v_p$.
(i) On a : $0 = 0v_1 + \cdots + 0v_p$ donc $0 \in V$.
(ii) Soient $\alpha, \beta \in \mathbb{R}$ et $v = \alpha_1 v_1 + \cdots + \alpha_p v_p$, $w = \beta_1 v_1 + \cdots + \beta_p v_p \in V$, où $\alpha_1, .., \alpha_p, \beta_1, ..., \beta_p \in \mathbb{R}$.
On a : $\alpha\, v + \beta\, w = (\alpha\alpha_1 + \beta\beta_1)\, v_1 + \cdots + (\alpha\alpha_p + \beta\beta_p)\, v_p$ donc $\alpha\, v + \beta\, w \in V$.
Cela montre que V est un sous-espace vectoriel de $\mathbb{R}^n$.
De plus V contient $v_1, ..., v_p$ car : $v_1 = 1v_1 + 0v_2 + \cdots + 0v_p$ et ... et $v_p = 0v_1 + \cdots + 0v_{p-1} + 1v_p$.

(b) Soit E un sous-espace vectoriel de $\mathbb{R}^n$ contenant $v_1, ..., v_p$.
D'après la remarque 2 ci-dessus, on a : $\mathrm{Vect}(v_1, ..., v_p) \subseteq E$ ce qui donne le résultat . □

(*) On dira que E est un sous-espace vectoriel de $\mathbb{R}^p$ donné par « équation cartésienne ».
(**) On dira que V est un sous-espace vectoriel de $\mathbb{R}^n$ donné par « équation paramétrique ».

Définition

On appelle :
– *droite vectorielle de* $\mathbb{R}^n$ une partie de $\mathbb{R}^n$ de la forme $\text{Vect}(v)$ avec $v \in \mathbb{R}^n \setminus \{0\}$;
– *plan vectoriel de* $\mathbb{R}^n$ une partie de $\mathbb{R}^n$ de la forme $\text{Vect}(v, w)$ avec $v, w \in \mathbb{R}^n$ non-colinéaires.

Dans chacun de ces deux cas on reconnait un sous-espace vectoriel de $\mathbb{R}^n$.

Exemple

Soient $v_1 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$, $v_2 = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$, $v_3 = \begin{pmatrix} 1 \\ 0 \\ \lambda \end{pmatrix} \in \mathbb{R}^3$ (identifiés à des triplets) avec $\lambda \in \mathbb{R}$ fixé.

Il est « clair » que v_1 et v_2 sont non-colinéaires (car $v_2 \neq 0$ et – au vu des 1^{res} coordonnées – une égalité $v_1 = \alpha v_2$ impliquerait $1 = 0$).

(a) *A-t-on :* $v_3 \in \text{Vect}(v_1, v_2)$ *?*

On étudie par la méthode de Gauss l'existence de $\alpha_1, \alpha_2 \in \mathbb{R}$ tels que $\overbrace{\alpha_1 v_1 + \alpha_2 v_2 = v_3}^{\text{expression « paramétrique » des éléments de Vect}(v_1, v_2)}$:

$$\underbrace{\alpha_1 v_1 + \alpha_2 v_2 = v_3}_{\text{inconnues } \alpha_1, \alpha_2}$$

$$\left(\begin{array}{cc|c} 1 & 0 & 1 \\ -1 & 1 & 0 \\ 0 & -1 & \lambda \end{array}\right) \xrightarrow[L_2 \leftarrow L_2 + L_1]{} \left(\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & -1 & \lambda \end{array}\right) \xrightarrow[L_3 \leftarrow L_3 + L_2]{} \left(\begin{array}{cc|c} \boxed{1} & 0 & 1 \\ 0 & \boxed{1} & 1 \\ 0 & 0 & \lambda{+}1 \end{array}\right).$$

Donc : $v_3 \in \text{Vect}(v_1, v_2) \iff \lambda = -1$.

(b) On suppose que $\lambda \neq -1$. *A-t-on :* $\text{Vect}(v_1, v_2, v_3) = \mathbb{R}^3$ *?*

Soit $v = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3$. On étudie par la méthode de Gauss l'existence de $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$ tels que $\underbrace{\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 = v}_{\text{inconnues } \alpha_1, \alpha_2, \alpha_3}$:

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & x \\ -1 & 1 & 0 & y \\ 0 & -1 & \lambda & z \end{array}\right) \xrightarrow[\cdots]{} \text{(étapes ci-dessus)} \xrightarrow[\cdots]{} \left(\begin{array}{ccc|c} \boxed{1} & 0 & 1 & /// \\ 0 & \boxed{1} & 1 & /// \\ 0 & 0 & \boxed{\lambda{+}1} & /// \end{array}\right).$$

Donc : $v \in \text{Vect}(v_1, v_2, v_3)$.

On peut en conclure – l'inclusion $\subseteq$ étant claire – que : $\text{Vect}(v_1, v_2, v_3) = \mathbb{R}^3$.

Proposition

Soient F et G deux sous-espaces vectoriels de $\mathbb{R}^n$.
On a : $F \cap G$ est un sous-espace vectoriel de $\mathbb{R}^n$.

Démonstration

(i) On a : $0 \in F$ et $0 \in G$ donc $0 \in F \cap G$.
(ii) Soient $\alpha, \beta \in \mathbb{R}$ et $v, w \in F \cap G$.
On a : $\alpha \underset{\in F}{v} + \beta \underset{\in F}{w} \in F$ et $\alpha \underset{\in G}{v} + \beta \underset{\in G}{w} \in G$, donc $\alpha v + \beta w \in F \cap G$.
Il en résulte que $F \cap G$ est un sous-espace vectoriel de $\mathbb{R}^n$. □

Remarque

On prend ici $F = (Ox)$ et $G = (Oy)$ dans $\mathbb{R}^2$. Donc $F = \text{Vect}((1,0))$ et $G = \text{Vect}((0,1))$ sont des sous-espaces vectoriels de $\mathbb{R}^2$.

On a $F \cap G = \{(0,0)\}$, où $\{(0,0)\}$ est un sous–espace vectoriel bien connu de $\mathbb{R}^2$.

Par contre $F \cup G$ n'est pas un sous-espace vectoriel de $\mathbb{R}^2$ car : $1 \underbrace{(1,0)}_{\in F} + 1 \underbrace{(0,1)}_{\in G} = \underbrace{(1,1)}_{\notin F \cup G}$.

Exemple

Idée : des équations cartésiennes de F et G fournissent une équation cartésienne de $F \cap G$.

On considère $\Pi_1 : x + y + z = 0$ et $\Pi_2 : x + 2y = 0$ dans $\mathbb{R}^3$. Comme ensembles de solutions de systèmes d'équations homogènes, Π_1 et Π_2 sont des sous-espaces vectoriels de $\mathbb{R}^3$ (on verra

dans le prochain exemple que ce sont des plans vectoriels).
On cherche à préciser la nature du sous-espace vectoriel $\Pi_1 \cap \Pi_2$ de $\mathbb{R}^3$.

On regroupe les équations cartésiennes de Π_1 et de Π_2 : $\Pi_1 \cap \Pi_2 : \begin{cases} x+y+z=0 \\ x+2y=0 \end{cases}$.

On va exhiber une équation paramétrique de $\Pi_1 \cap \Pi_2$ en résolvant par la méthode de Gauss : $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \end{pmatrix} \xrightarrow[L_2 \leftarrow L_2 - L_1]{} \begin{pmatrix} \boxed{1} & 1 & 1 \\ 0 & \boxed{1} & -1 \end{pmatrix}$. On effectue ensuite de tête la « remontée triangulaire ».

Ainsi : $\Pi_1 \cap \Pi_2 : \begin{cases} x = -2t \\ y = t \\ z = t \end{cases}, t \in \mathbb{R}$ puis $\Pi_1 \cap \Pi_2 = \text{Vect}\left(\begin{pmatrix} -2 \\ 1 \\ 1 \end{pmatrix}\right)$ est une droite vectorielle.

Définition-Proposition

Soient F et G deux sous-espaces vectoriels de $\mathbb{R}^n$.

(a) On note : $F+G := \{v+w \ ; \ v \in F \text{ et } w \in G\}$.
On a : $F+G$ est un sous-espace vectoriel de $\mathbb{R}^n$, appelé *somme de F et de G*.

(b) On suppose que $F = \text{Vect}(v_1, ..., v_p)$ et $G = \text{Vect}(w_1, ..., w_q)$ avec $v_1, ..., v_p, w_1, ..., w_q \in \mathbb{R}^n$.
On a : $F+G = \text{Vect}(v_1, ..., v_p, w_1, ..., w_q)$.

Démonstration

(a) (i) On a : $0 = 0+0 \in F+G$.
(ii) Soient $\alpha, \alpha' \in \mathbb{R}$ et $u = \underset{\in F}{v} + \underset{\in G}{w}$, $u' = \underset{\in F}{v'} + \underset{\in G}{w'} \in F+G$.
On a : $\alpha u + \alpha' u' = \underbrace{(\alpha v + \alpha' v')}_{\in F} + \underbrace{(\alpha w + \alpha' w')}_{\in G}$, donc $\alpha u + \alpha' u' \in F+G$.

Il en résulte que $F+G$ est un sous-espace vectoriel de $\mathbb{R}^n$.

(b) On a : $F+G = \{(\alpha_1 v_1 + \cdots + \alpha_p v_p) + (\beta_1 w_1 + \cdots + \beta_p w_q) \ ; \ \alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_q \in \mathbb{R}\}$, donc en enlevant les parenthèses : $F+G = \text{Vect}(v_1, ..., v_p, w_1, ..., w_q)$. □

Exemple

Idée : des équations paramétriques de F et G donnent une équation paramétrique de $F+G$.

On reprend $\Pi_1 : x+y+z=0$ et $\Pi_2 : x+2y=0$ dans $\mathbb{R}^3$. On cherche à préciser $\Pi_1 + \Pi_2$.

• Méthode de Gauss pour aboutir à $\Pi_1 = \text{Vect}(v_1, ..., v_p)$ et $\Pi_2 = \text{Vect}(w_1, ..., w_q)$:

$\begin{pmatrix} x & y & z \\ \boxed{1} & 1 & 1 \end{pmatrix}$ donne $\Pi_1 : \begin{cases} x = -s-t \\ y = s \\ z = t \end{cases} s,t \in \mathbb{R}$, et $\begin{pmatrix} x & y & z \\ \boxed{1} & 2 & 0 \end{pmatrix}$ donne $\Pi_2 : \begin{cases} x = -2u \\ y = u \\ z = v \end{cases} u,v \in \mathbb{R}$.

En particulier $\Pi_1 = \text{Vect}\left(\begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}\right)$ et $\Pi_2 = \text{Vect}\left(\begin{pmatrix} -2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}\right)$ sont des plans vectoriels.

On a ensuite : $\Pi_1 + \Pi_2 : \begin{cases} x = -s-t-2u \\ y = s+u \\ z = t+v \end{cases} s,t,u,v \in \mathbb{R}$. On va voir que : $\Pi_1 + \Pi_2 = \mathbb{R}^3$.

• Soit $v = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3$. On étudie l'existence de $s,t,u,v \in \mathbb{R}$ permettant de s'assurer que v vérifie l'équation paramétrique précédente de $\Pi_1 + \Pi_2$, par la méthode de Gauss :

$$\left(\begin{array}{cccc|c} -1 & -1 & -2 & 0 & x \\ 1 & 0 & 1 & 0 & y \\ 0 & 1 & 0 & 1 & z \end{array}\right) \xrightarrow[L_2 \leftarrow L_2 + L_1]{} \left(\begin{array}{cccc|c} -1 & -1 & -2 & 0 & x \\ 0 & -1 & -1 & 0 & x+y \\ 0 & 1 & 0 & 1 & z \end{array}\right) \xrightarrow[L_3 \leftarrow L_3 + L_2]{} \left(\begin{array}{cccc|c} \boxed{-1} & -1 & -2 & 0 & /// \\ 0 & \boxed{-1} & -1 & 0 & /// \\ 0 & 0 & \boxed{-1} & 1 & /// \end{array}\right).$$

Donc : $v \in \Pi_1 + \Pi_2$.

En conclusion : $\Pi_1 + \Pi_2 = \mathbb{R}^3$. ⟵[variante, plus tard : extraction de base d'une famille génératrice]

2. Familles libres. Familles génératrices. Bases

Dans toute cette partie, on se donne un sous-espace vectoriel E de $\mathbb{R}^n$.

Définition ($p \in \mathbb{N}$)

(a) *Une famille formée de p vecteurs de E* est un élément $(v_1, \dots, v_p)$ de E^p.
Dans la suite de cette définition, on se donne $v_1, \dots, v_p \in E$.

(b) On dit que *la famille* $(v_1, \dots, v_p)$ *est libre* (ou « les vecteurs $v_1, \dots, v_p$ sont linéairement indépendants ») si pour tous $\alpha_1, \dots, \alpha_p \in \mathbb{R}$, on a :

$$\alpha_1 v_1 + \cdots + \alpha_p v_p = 0 \implies \alpha_1 = \cdots \alpha_p = 0 .$$

On exprimera qu'une famille de vecteurs de E n'est pas libre en disant qu'*elle est liée*, ce qui signifie donc qu'il existe $\alpha_1, ..., \alpha_p \in \mathbb{R}$ tels que $\alpha_1 v_1 + \cdots + \alpha_p v_p = 0$ et $(\alpha_1, ..., \alpha_p) \neq (0, ..., 0)$.

(c) On dit que *la famille* $(v_1, \dots, v_p)$ *est génératrice de E* (ou « les vecteurs $v_1, \dots, v_p$ engendrent E ») si pour tout $v \in E$, il existe $\alpha_1, \dots, \alpha_p \in \mathbb{R}$ tels que : $v = \alpha_1 v_1 + \cdots + \alpha_p v_p$.
Ainsi, la famille $(v_1, \dots, v_p)$ est génératrice de E si et seulement si $\mathrm{Vect}(v_1, \dots, v_p) = E$.

Exemple 1

Dans $\mathbb{R}^3$, on choisit $E : x + y + z = 0$, $v_1 = (0, 1, -1)$, $v_2 = (1, 0, -1)$, $v_3 = (1, -1, 0)$.
Donc E est un sous-espace vectoriel de $\mathbb{R}^3$ (premier exemple concret qui a été proposé pour illustrer la notion de de sous-espace vectoriel) et $v_1, v_2, v_3 \in E$.

1. Pour tous $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$, on a : $\underbrace{\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3}_{(\alpha_2 + \alpha_3, \alpha_1 - \alpha_3, -\alpha_1 - \alpha_2)} = 0 \iff \alpha_1 = -\alpha_2 = \alpha_3$.
En particulier, la famille (v_1, v_2, v_3) n'est pas libre car :
$$1v_1 + (-1)v_2 + 1v_3 = 0 \text{ bien que } (1, -1, 1) \neq (0, 0, 0).$$

2. Soit $v = (x, y, z) \in E$. Pour tous $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$, sachant que $x + y + z = 0$ on a :
$(\star)$ $v = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 \iff \alpha_2 = x - \alpha_3$ et $\alpha_1 = y + \alpha_3$.
Le choix de $(\alpha_1, \alpha_2, \alpha_3) = (y, x, 0)$ montre que l'équation $(\star)$ d'inconnue $(\alpha_1, \alpha_2, \alpha_3)$ a au moins une solution. Ainsi, la famille (v_1, v_2, v_3) est génératrice de E.

Exemple 2

Soient $u_1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$, $u_2 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$, $u_3 = \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix}$ dans $\mathbb{R}^3$.

On étudie $(\star) : \alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_3 = 0$ et $(\star\star) : \alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_3 = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ à $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3$ fixé avec comme inconnue $(\alpha_1, \alpha_2, \alpha_3)$, et obtient par la méthode de Gauss que :

– la famille (u_1, u_2, u_3) est libre, cf. $\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ 1 & 1 & 2 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \end{pmatrix} \xrightarrow[L_3 \leftarrow L_3 - L_1]{} \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ 1 & 1 & 2 \\ 0 & 2 & 1 \\ 0 & -1 & 0 \end{pmatrix} \xrightarrow[C_2 \leftrightarrow C_3]{} \underbrace{\begin{pmatrix} \alpha_1 & \alpha_3 & \alpha_2 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & -1 \end{pmatrix}}_{\text{unique solution } (0,0,0)}$;

– la famille (u_1, u_2, u_3) est génératrice de $\mathbb{R}^3$, cf. $\left(\begin{array}{ccc|c} \alpha_1 & \alpha_2 & \alpha_3 & \\ 1 & 1 & 2 & x \\ 0 & 2 & 1 & y \\ 1 & 0 & 2 & z \end{array}\right) \xrightarrow[\cdots]{} \cdots \xrightarrow[\cdots]{} \underbrace{\left(\begin{array}{ccc|c} \alpha_1 & \alpha_3 & \alpha_2 & \\ 1 & 2 & 1 & /// \\ 0 & 1 & 2 & /// \\ 0 & 0 & -1 & /// \end{array}\right)}_{\text{existence d'une solution}}$.

Remarques (exercices)

1. Dans le cas de 0, 1, ou 2 vecteurs, on constate que :
– la famille vide () est libre $\left(\text{vu la convention } \sum_{1 \leq k \leq p} \alpha_k v_k = 0 \text{ quand } p = 0\right)$;
– une famille (v_1) avec $v_1 \in E$ est libre si et seulement si $v_1 \neq 0$;
– deux vecteur de E sont linéairement indépendants si et seulement si ils sont non colinéaires.

2. Une famille $(v_1, \dots, v_p)$ de vecteurs de E est liée si et seulement si il existe un vecteur parmi $v_1, \dots, v_p$ qui est combinaison linéaire des autres.
En particulier, toute famille de vecteurs de E dans laquelle se trouve le vecteur nul ou deux vecteurs égaux, est liée.

3. On dira qu'une famille de vecteurs de E est « extraite » d'une famille $(v_1, \dots, v_p)$ de vecteurs de E si elle est de la forme $(v_{i_1}, ..., v_{i_k})$ avec $1 \leq i_1 < ... < i_k \leq p$.

Tout famille extraite d'une famille libre de vecteurs de E, est libre.

Tout famille de vecteurs de E dont une famille extraite est génératrice de E, est elle-même génératrice de E.

Proposition

Une famille $(v_1, \dots, v_p)$ de vecteurs de E est libre et génératrice de E, si et seulement si, pour tout $v \in E$ il existe $(\alpha_1, \dots, \alpha_p) \in \mathbb{R}^p$ unique tel que $v = \alpha_1 v_1 + \cdots + \alpha_p v_p$.

Démonstration

($\Rightarrow$) On suppose que $(v_1, \dots, v_p)$ est libre et génératrice de E. Soit $v \in E$.

Comme $(v_1, \dots, v_p)$ engendre E, il existe $\alpha_1, ..., \alpha_p \in \mathbb{R}$ tels que $v = \alpha_1 v_1 + \cdots + \alpha_p v_p$.

On se donne une autre décomposition $v = \beta_1 v_1 + \cdots + \beta_p v_p$ avec $\beta_1, ..., \beta_p \in \mathbb{R}$.

Par soustraction : $(\alpha_1 - \beta_1)v_1 + \cdots + (\alpha_p - \beta_p)v_p = 0$ puis, la famille $(v_1, \dots, v_p)$ étant libre, on a $\beta_1 = \alpha_1$ et ... et $\beta_p = \alpha_p$. Cela donne l'unicité de la famille $(\alpha_1, ..., \alpha_p)$.

($\Leftarrow$) On suppose que : $\forall v \in E \quad \underbrace{\exists!}_{\text{« il existe un unique »}} (\alpha_1, \dots, \alpha_p) \in \mathbb{R}^p \quad v = \alpha_1 v_1 + \cdots + \alpha_p v_p$.

L'existence de $(\alpha_1, \dots, \alpha_p)$ montre que $(v_1, \dots, v_p)$ est génératrice de E.

L'unicité de $(\alpha_1, \dots, \alpha_p)$ quand $v = 0$ montre que $(v_1, \dots, v_p)$ est libre. □

Définition

Soit $\mathscr{B} = (v_1, \dots, v_d)$ une famille de vecteurs de E.

On dit que $\mathscr{B}$ est *une base de* E si $\mathscr{B}$ est libre et génératrice de E.

Dans ce cas, pour $v \in E$ les uniques scalaires $\alpha_1, ..., \alpha_d \in \mathbb{R}$ tels que $v = \alpha_1 v_1 + \cdots + \alpha_n v_d$ s'appellent *les coordonnées de* v *suivant* $\mathscr{B}$. On le notera : $v \Big/_{\mathscr{B}} \begin{vmatrix} \alpha_1 \\ \vdots \\ \alpha_d \end{vmatrix}$.

Exemples

1. Le sous-espace vectoriel $\mathbb{R}^n$ de $\mathbb{R}^n$ a la base suivante, appelée *base canonique de* $\mathbb{R}^n$:
$\mathscr{B} := (e_1, \dots, e_n)$ avec $e_1 := (1, 0, ..., 0)$, $e_2 := (0, 1, 0, ..., 0)$, ..., $e_n := (0, ..., 0, 1)$.
Plus précisément, les coordonnées de $v = (x_1, ..., x_n) \in \mathbb{R}^n$ dans cette base sont $x_1, ..., x_n$.

2. Soit (H): $AX = 0$ avec $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \in \mathbb{R}^p$ un système d'équations linéaires homogène.
On sait que l'ensemble $\mathscr{S}_H$ de ses solutions est un sous-espace vectoriel de $\mathbb{R}^p$.

La méthode de Gauss fournit des vecteurs w_1, ..., w_{p-r} de $\mathbb{R}^p$ tels que :

– $\mathscr{S}_H = \{t_1 w_1 + \cdots + t_{p-r} w_{p-r} \ ; \ t_1, \dots, t_{p-r} \in \mathbb{R}\}$; $\longleftarrow \left[\text{cf. } \mathscr{S}_H : \begin{cases} x_{j_1} = \cdots \\ \vdots \\ x_{j_r} = \cdots \\ x_{j_{r+1}} = t_1 \\ \vdots \\ x_{j_p} = t_{p-r} \end{cases}, \ t_1, t_{p-r} \in \mathbb{R}. \right]$

– si $t_1 w_1 + \cdots + t_{p-r} w_{p-r} = 0$, alors $\begin{cases} \text{coordonnée } j_{r+1} : \ t_1 + 0 + \cdots + 0 = 0 \\ \vdots \\ \text{coordonnée } j_p \ : 0 + \cdots + 0 + t_{p-r} = 0 \end{cases}$, alors $t_1 = \cdots = t_{p-r} = 0$.

Ainsi $(w_1, ..., w_{p-r})$ est une base de $\mathscr{S}_H$.

Théorème (admis)

On a : E possède une base $(e_1, ..., e_d)$. Dans ce cas les autres bases de E ont aussi d vecteurs.

Définition

(a) On appelle *dimension de* E le nombre constant, noté $\dim E$, des vecteurs de ses bases.

(b) Soient $v_1, ..., v_p \in \mathbb{R}^n$. On appelle *rang de* $(v_1, ..., v_p)$ le nombre $\dim \mathrm{Vect}(v_1, ..., v_p)$.
On notera : $\mathrm{rg}\,(v_1, ..., v_p) := \dim \mathrm{Vect}(v_1, ..., v_p)$.

Exemples

1. Au vu de la base canonique de $\mathbb{R}^n$, on a : $\dim \mathbb{R}^n = n$.

2. On reprend certaines définitions de la sous-partie 1 :
– $E = \{0\}$ si et seulement si $\dim E = 0$;
– E est une droite vectorielle si et seulement si $\dim E = 1$;
– E est un plan vectoriel si et seulement si $\dim E = 2$.

Proposition (admise)

On note d la dimension de E.

(a) Toute famille libre de E a au plus d vecteurs ;
quand elle a d vecteurs, c'est une base de E.

(b) Toute famille génératrice de E a au moins d vecteurs ;
quand elle a d vecteurs, c'est une base de E.

Corollaire 1

Soit F un sous-espace vectoriel de $\mathbb{R}^n$ tel que $F \subseteq E$.
D'après la proposition (a), on a : $\dim F \leq \dim E$; quand $\dim F = \dim E$, on a $F = E$.

Définition

(a) On appelle *sous-espace vectoriel de* E un sous-espace vectoriel de $\mathbb{R}^n$ inclus dans E.

(b) On dit qu'un sous-espace vectoriel F de E est un *hyperplan de* E si : $\dim F = \dim E - 1$.

Corollaire 2

Soient $v_1, ..., v_p \in E$. On pose : $r = \operatorname{rg}(v_1, ..., v_p)$.

(a) La famille $(v_1, ..., v_p)$ est libre si et seulement si $r = p$.

(b) La famille $(v_1, ..., v_p)$ est génératrice de E si et seulement si $r = \dim E$.

Démonstration

(a) La famille $(v_1, ..., v_p)$, de p vecteurs, engendre $\operatorname{Vect}(v_1, ..., v_p)$ qui est de dimension r. Elle est libre si et seulement si elle est base de $\operatorname{Vect}(v_1, ..., v_p)$, ce qui équivaut (vu la proposition précédente (b)) à $r = p$.

(b) La famille $(v_1, ..., v_p)$ est génératrice de E si et seulement si $\operatorname{Vect}(v_1, ..., v_p) = E$, c'est à dire (vu le corollaire 1) $\dim \operatorname{Vect}(v_1, ..., v_p) = \dim E$, c'est à dire $r = \dim E$. □

Remarques

1. On reprend l'exemple du début de la sous-partie 2 : $u_1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$, $u_2 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$, $u_3 = \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix}$.

On a vu à l'aide d'un premier calcul que (u_1, u_2, u_3) est libre. On remarque que la base canonique de $\mathbb{R}^3$ est formée de 3 vecteurs. On peut donc utiliser le (a) de la proposition précédente pour en conclure, sans autre calcul, que (u_1, u_2, u_3) est génératrice de $\mathbb{R}^3$.

2. D'après le corollaire 1, les sous-espaces vectoriels de $\mathbb{R}^3$ ont une dimension, égale à 0 ou 1 ou 2 ou 3, le cas de la dimension 3 n'étant atteint que par $\mathbb{R}^3$ lui-même. Les sous-espaces vectoriels de $\mathbb{R}^3$ sont donc $\{0\}$, les droites vectorielles de $\mathbb{R}^3$, les plans vectoriels de $\mathbb{R}^3$, et $\mathbb{R}^3$.

3. Soit $(a_1, ..., a_n) \in \mathbb{R}^n \setminus \{0\}$. La partie $F : a_1x_1 + \cdots + a_nx_n = 0$ de $\mathbb{R}^n$ est un hyperplan vectoriel de $\mathbb{R}^n$ car on constate que la méthode de Gauss fournit une base $(w_1, ..., w_{n-1})$ de F.

Proposition

Soient $v_1 = \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix}, \ldots, v_p = \begin{pmatrix} a_{1p} \\ \vdots \\ a_{np} \end{pmatrix} \in \mathbb{R}^n$.

(a) On transforme $\overset{x_1 \ldots x_p}{A} := \begin{pmatrix} \overset{x_1 \quad \ldots \quad x_p}{a_{11} \quad \ldots \quad a_{1p}} \\ \cdots \\ a_{n1} \quad \ldots \quad a_{np} \end{pmatrix}$ en $\overset{x_{j_1} \ldots x_{j_p}}{A'} = \left(\begin{array}{ccc|ccc} \overset{x_{j_1}}{d_1} & & \overset{x_{j_r}}{} & \overset{x_{j_{r+1}} \ldots}{} & & \overset{x_{j_p}}{} \\ & \ddots & & & & \\ 0 & & & & & \\ \vdots & \ddots & \ddots & & & \\ 0 & \cdots & 0 \quad d_r & & & \\ \hline 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \ldots & 0 & 0 & \ldots & 0 \end{array}\right)$

par la méthode de Gauss, avec $d_1 \neq 0$, ..., $d_r \neq 0$.

On a : $(v_{j_1}, ..., v_{j_r})$ est une base de $\mathrm{Vect}(v_1, ..., v_p)$.

(b) En particulier : $\mathrm{rg}\,(v_1, ..., v_p) = r$ « calcul du rang par la méthode de Gauss ».
(Le nombre r est donc indépendant de la manière dont on applique la méthode de Gauss.)

Démonstration (de (a))

• On vérifie que la famille $(v_{j_1}, ..., v_{j_r})$ est libre. On montre que $(\star)$ $\alpha_1 v_{j_1} + ... + \alpha_r v_{j_r} = 0$ d'inconnue $(\alpha_1, ..., \alpha_r) \in \mathbb{R}^r$ a pour seule solution $(0, ..., 0)$.

On reprend le calcul permettant de passer de A à A' en ne prenant en compte que les colonnes qui sont sous les symboles $x_{j_1}, ..., x_{j_r}$. On constate à la fin du calcul que l'équation $(\star)$ a une unique solution : $(\alpha_1, ..., \alpha_r) = (0, ..., 0)$.

• On vérifie maintenant que $(v_{j_1}, ..., v_{j_r})$ engendre $\mathrm{Vect}(v_1, ..., v_p)$. Soit $k \in \{r+1, ..., p\}$. On montre que l'équation $(\star\star)$ $\alpha_1 v_{j_1} + ... + \alpha_r v_{j_r} = v_{j_k}$ d'inconnue $(\alpha_1, ..., \alpha_r) \in \mathbb{R}^r$ a au moins une solution. Le résultat en découlera car on aura ensuite $\underbrace{\mathrm{Vect}(v_1, ..., v_p)}_{\text{plus petit sous-espace vectoriel de } E \text{ contenant } v_1, \ ..., \ v_p} \subseteq \mathrm{Vect}(v_{j_1}, ..., v_{j_r})$.

On déplace à chaque étape de la méthode de Gauss la colonne qui est sous le symbole x_{j_k} après une barre verticale signalant le second membre, et ne garde en plus que les colonnes qui sont sous les symboles $x_{j_1}, ..., x_{j_r}$. Finalement (au vu des coefficients à droite des lignes nulles du 1er membre de la dernière étape), $(\star\star)$ a une solution. □

Remarque 1 (importante au niveau de la rédaction au cours des partiels et examens)

La proposition (a) n'est pas classique, contrairement à la proposition (b).
Dans chaque exercice on la déduira des calculs simultanés de $\mathrm{rg}\,(v_1, ..., v_r)$ et $\mathrm{rg}\,(v_{j_1}, ..., v_{j_r})$:
– on a $\mathrm{rg}\,(v_1, ..., v_r) = r$ par calcul du rang par la méthode de Gauss ;
– on a aussi $\mathrm{rg}\,(v_{j_1}, ..., v_{j_r}) = r$ en reprenant le calcul précédent et rayant à chaque étape les colonnes qui ne sont pas sous les symboles $x_{j_1}, ..., x_{j_r}$;
– ainsi $(v_{j_1}, ..., v_{j_r})$ engendre un sous-espace vectoriel de dimension r dans l'espace vectoriel $\mathrm{Vect}(v_1, ..., v_r)$ de dimension r, et il en résulte que $(v_{j_1}, ..., v_{j_r})$ est une base de $\mathrm{Vect}(v_1, ..., v_p)$.

Remarque 2

On revient sur l'exemple des 3 vecteurs $u_1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$, $u_2 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$, $u_3 = \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix} \in \mathbb{R}^3$.

La rédaction la plus rapide pour démontrer que (u_1, u_2, u_3) est une base de $\mathbb{R}^3$ consiste à prouver par la méthode de Gauss que $\mathrm{rg}\,(u_1, u_2, u_3) = 3$.

Ch. 5. Propriétés de $\mathbb{R}$ et suites numériques

Plan

I. L'ensemble ordonné $(\mathbb{R}, \leq)$

1. Majoration. Minoration

Définition-Proposition

Soient $A \subseteq \mathbb{R}$ et $m \in \mathbb{R}$.

(a) On dit que
- m est un *majorant* (resp. *minorant*) *de* A si pour tout $x \in A$ on a $m \geq x$ (resp. $m \leq x$) ;
- A est *majorée* (resp. *minorée*) s'il existe un majorant (resp. minorant) de A dans $\mathbb{R}$;
- A est *bornée* si A est majorée et minorée.

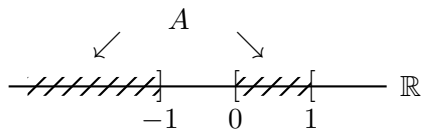
(b) On dit que
- m est *« un » plus grand* (resp. *plus petit*) *élément de* A si m est un majorant (resp. minorant) de A qui appartient à A ; dans ce cas, ce m est unique et noté $m = \max(A)$ (resp. $m = \min(A)$;
- m est *la borne supérieure* (resp. *la borne inférieure*) *de* A si m est le plus petit majorant (resp. plus grand minorant) de A ; dans ce cas, on note $m = \sup(A)$ (resp. $m = \inf(A)$).

Démonstration

Unicité d'un plus grand élément ? On suppose que m' et m'' sont plus grands éléments de A.
On a : $\underbrace{m'}_{\in A} \leq \underbrace{m''}_{\text{majorant de } A}$ et $\underbrace{m''}_{\in A} \leq \underbrace{m'}_{\text{majorant de } A}$ donc $m' = m''$.
On raisonne de même pour des plus petits éléments de A. □

Exemple

$A =]-\infty, -1] \cup [0, 1[$



Un minorant m de A vérifie : $\forall x \in]-\infty, -1] \quad m \leq x$, donc $m \leq \lim\limits_{x \to -\infty} x = -\infty$.
Cette contradiction montre que A n'a pas de minorant, pas de plus petit élément et pas de borne inférieure dans $\mathbb{R}$.

Un majorant m de A vérifie : $\forall x \in [0, 1[\quad m \geq x$, donc $m \geq \lim\limits_{x \to 1^-} x = 1$. Réciproquement, tout $m \geq 1$ est un majorant de A. L'ensemble des majorants de A est donc $[1, +\infty[$.
Comme $A \cap [1, +\infty[= \emptyset$, la partie A de $\mathbb{R}$ n'a pas de plus grand élément.
Cependant il existe un plus petit majorant de A : $\sup A = 1$.

Proposition

(a) Soient $x, y \in \mathbb{R}$. On a : $\min\{x, y\} = \begin{cases} x & \text{si } x \leq y \\ y & \text{sinon} \end{cases}$ et $\max\{x, y\} = \begin{cases} x & \text{si } x \geq y \\ y & \text{sinon} \end{cases}$.

Plus généralement, pour tous $x_1, ..., x_n \in \mathbb{R}$ avec $n \geq 1$, la partie $\{x_1, ..., x_n\}$ de $\mathbb{R}$ a un plus grand élément noté $\max(x_1, ..., x_n)$ et un plus petit élément noté $\min(x_1, ..., x_n)$.

(b) Soient $A \subseteq \mathbb{R}$ et $m \in \mathbb{R}$. On a :

- $m = \sup(A) \iff \big((\forall a \in A \quad m \geq a) \text{ et } (\forall x < m \quad \exists a \in A \quad x < a)\big)$;
- $m = \inf(A) \iff \big((\forall a \in A \quad m \leq a) \text{ et } (\forall x > m \quad \exists a \in A \quad x > a)\big)$.

(c) Soit $A \subseteq \mathbb{R}$. On a : $\sup A$ (resp. $\inf A$) existe et appartient à A si et seulement si $\max A$ (resp. $\min A$) existe. Dans ce cas : $\sup A = \max A$ (resp. $\inf A = \min A$).

Démonstration

(a) Le début est clair. Récurrence sur $n \geq 1$. Si $n = 1$: ça marche.
On suppose que c'est vrai pour un certain $n \geq 1$ et considère $x_1, ..., x_{n+1} \in \mathbb{R}$.
On pose : $m = \max(\max(x_1, ..., x_n), x_{n+1})$. Donc $m \in \{x_1, ..., x_{n+1}\}$. Comme $m \geq x_{n+1}$ et $m \geq \max(x_1, ..., x_n) \geq x_i$ pour $1 \leq i \leq n$, m est le plus grand élément de $\{x_1, ..., x_{n+1}\}$.
On raisonne de même pour obtenir l'existence de $\min(x_1, ..., x_{n+1})$.

(b) Par définition de $\sup A$, on a :
$m = \sup(A) \iff \big((\forall a \in A \quad m \geq a) \text{ et } (\forall x \in \mathbb{R} \ \ (\forall a \in A \quad x \geq a) \Rightarrow m \leq x \ \ )\big)$.
Il reste à contraposer l'implication qui se trouve à la fin de la ligne précédente.
De même pour la caractérisation de $\inf A$.

(c) Si $\sup A$ existe et $\sup A \in A$: $\sup A$ est un majorant de A qui appartient à A.
Si $\max A$ existe : $\max A$ est un majorant de A et comme il appartient à A il est plus petit que les autres majorants de A, donc $\sup A = \max A$.
On raisonne de même pour comparer $\inf A$ et $\min A$. □

Définition

Soit $x \in \mathbb{R}$. On pose : $|x| = \max(-x, x) = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0 \end{cases}$ ou .

Remarque

Soient $x, y \in \mathbb{R}$. En distinguant les cas $x \leq y$ et $x > y$, on obtient :
$\min(x, y) = \frac{x+y}{2} + \min\left(x - \frac{x+y}{2}, y - \frac{x+y}{2}\right) = \frac{x+y}{2} - \left|\frac{x-y}{2}\right|$
et $\max(x, y) = \frac{x+y}{2} + \max\left(x - \frac{x+y}{2}, y - \frac{x+y}{2}\right) = \frac{x+y}{2} + \left|\frac{x-y}{2}\right|$.

Proposition

On a : $|x + y| \leq |x| + |y|$ pour tous $x, y \in \mathbb{R}$ « inégalité triangulaire ».

Démonstration

Pour $x, y \in \mathbb{R}$, on a : $x + y \leq |x| + |y|$ et $-x - y \leq |x| + |y|$, donc $|x + y| \leq |x| + |y|$. □

2. Existence de la borne supérieure

Théorème (admis)

(a) Toute partie non-vide majorée de $\mathbb{R}$ a une borne supérieure dans $\mathbb{R}$. ⟵[$\sup_{\mathbb{R}} \emptyset := -\infty$]
Par convention, l'égalité « $\sup A = +\infty$ » ($A \subseteq \mathbb{R}$) signifiera que « A n'est pas majorée ».

(b) Toute partie non-vide minorée de $\mathbb{R}$ a une borne inférieure dans $\mathbb{R}$. ⟵[$\inf_{\mathbb{R}} \emptyset := +\infty$]
Par convention, l'égalité « $\inf A = -\infty$ » ($A \subseteq \mathbb{R}$) signifiera que « A n'est pas minorée ».

Corollaire

Pour tous $x \in \mathbb{R}$ et $\varepsilon > 0$, il existe $n \in \mathbb{N}$ tel que $n\varepsilon > x$ « axiome d'Archimède ».

Démonstration

On suppose par l'absurde qu'il existe $x \in \mathbb{R}$ et $\varepsilon > 0$ tels que $A := \{n\varepsilon \ ; \ n \in \mathbb{N}\}$ est majoré par x. D'après le théorème (a), on dispose de $M := \sup A \in \mathbb{R}$.

Comme $M - \varepsilon < M$, la caractérisation du sup fournit $n_0\varepsilon$ dans A tel que $M - \varepsilon < n_0\varepsilon$. On a : $n_0\varepsilon + \varepsilon > (M - \varepsilon) + \varepsilon$ donc $(n_0 + 1)\varepsilon > M$ avec $(n_0 + 1)\varepsilon \in A$; contradiction. □

Proposition

Soit $x \in \mathbb{R}$. Il existe $N \in \mathbb{Z}$ unique tel que : $N \leq x < N + 1$.
On note : $\lfloor x \rfloor = N$ *partie entière de* x.

Démonstration

• Existence ? Par l'axiome d'Archimède, il existe $n_0 \in \mathbb{N}$ tel que : $n_0\,1 > |x|$.
Comme $-n_0 \leq x$, l'ensemble $A := \big\{n \in \{-n_0, ..., -1, 0, 1, ..., n_0\} \mid n \leq x\big\}$ est fini non-vide.
On pose $N = \max A$. On a : $-n_0 \leq \boxed{N \leq x} < n_0$ puis $-n_0 \leq N + 1 \leq n_0$ $\underbrace{\text{donc}}_{\text{par maximalité}}$ $\boxed{x < N + 1}$.

• Unicité ? Soit $N' \in \mathbb{Z}$ tel que $N' \leq x < N' + 1$.
On a : $N \leq x < N' + 1$ donc $N \leq N'$. De même $N' \leq N$. D'où $N' = N$. □

Exemples

On a : $3 \leq \pi < 4$ et $-4 \leq -\pi < -3$. Donc $\lfloor \pi \rfloor = 3$ et $\lfloor -\pi \rfloor = -4$.
[Illustration : graphe de la fonction partie entière sur $[-1, 4[$.]

Définition

(a) Soit $x_0 \in \mathbb{R}$. Un *voisinage de* x_0 *(dans* $\mathbb{R}$*)* est une partie V de $\mathbb{R}$ pour laquelle il existe $\varepsilon > 0$ tel que $]x_0 - \varepsilon, x_0 + \varepsilon[\subseteq V$. Important ici : $\boxed{]x_0 - \varepsilon, x_0 + \varepsilon[= \{x \in \mathbb{R} \mid |x - x_0| < \varepsilon\}}$.

(b) Soit $A \subseteq \mathbb{R}$. On dit que A *est dense dans* $\mathbb{R}$ si pour tous $x_0 \in \mathbb{R}$ et tout voisinage V de x_0, on a $V \cap A \neq \emptyset$.

Proposition

(a) Il existe un unique $x \in \mathbb{R}_+$ tel que $x^2 = 2$. On le note $\sqrt{2}$.

(b) Le nombre réel $\sqrt{2}$ n'appartient pas à $\mathbb{Q}$.

Démonstration

(a) • Existence ? On note $A := \{x \in \mathbb{R}_+ \mid x^2 < 2\}$. On a : $0 \in A$ et la partie A est majorée par 2 car $x \notin A$ quand $x > 2$. On introduit $m := \sup A \geq 0$. On va vérifier que $m^2 = 2$.

– Si $m^2 < 2$: comme $(m + h)^2 \underset{h \to 0^+}{\longrightarrow} m^2$, on a $(m + h)^2 < m^2 + \big|m^2 - 2\big| = 2$ dès que $h > 0$ est assez petit, puis $m + h \in A$ pour un tel h fixé, enfin m ne majore pas A ; contradiction.

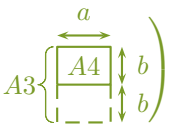
– Si $m^2 > 2$: comme $(m - h)^2 \underset{h \to 0^+}{\longrightarrow} m^2$, il existe $\alpha > 0$ tel que $(m - h)^2 > m^2 - \big|m^2 - 2\big| = 2$ dès que $0 < h < \alpha$, ce qui donne $]m - \alpha, m] \cap A = \emptyset$, et a fortiori $m - \alpha$ est un majorant de A plus petit que m ; contradiction.

On suppose que $m^2 \neq 2$ et note $\varepsilon := \big|m^2 - 2\big|$. Soit $0 < \alpha < 1$. Pour tout $k \in \mathbb{R}$, on a : $|\underbrace{(m + k)^2 - m^2}_{2mk + k^2}| \leq 2m|k| + k^2 < (2m + 1)\alpha \leq \varepsilon$ dès que $\underbrace{|k| < \alpha}_{\text{donc } k^2 \leq |k|}$ et $\alpha \leq \frac{\varepsilon}{2m+1}$.
D'où : $m^2 - \varepsilon < (m + k)^2 < m^2 + \varepsilon$ quand $\alpha = \min(1, \frac{\varepsilon}{2m+1})$ et $|k| < \alpha$.

• Unicité ? Soit $m' \in \mathbb{R}_+$ tel que $m'^2 = 2$. On a : $(m' - m)(m' + m) = m'^2 - m^2 = 0$ donc $m' \in \{\pm m\}$ avec $m, m' \in \mathbb{R}_+$ puis $m' = m$.

(b) On suppose par l'absurde que $\sqrt{2} = \frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N} \setminus \{0\}$ non tous deux pairs (sinon on simplifie) donnerait $2b^2 = a^2$, et comme le carré $4k^2 + 2k + 1$ d'un nombre impair

$2k+1$ est impair – ce qui découle aussi de la décomposition en facteurs premiers de ce nombre –, cela entrainerait que $a = 2k$ pour un certain $k \in \mathbb{Z}$ puis que $b^2 = 2k^2$ et b serait pair ; contradiction.

(Variante : On a $\sqrt{2} \notin \mathbb{Q}$, car une égalité $\sqrt{2} = \frac{a}{b}$ avec $a \in \mathbb{Z}$, et $b \in \mathbb{N}\setminus\{0\}$ minimal donnerait $\sqrt{2} = \frac{a}{b} = \frac{2b}{a} = \frac{2b-a}{a-b}$ où $0 < a-b < a$; contradiction. 

) □

En annexe : complément concernant le développement décimal.

Proposition

(a) Les parties $\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$ sont denses dans $\mathbb{R}$.

(b) La partie $]-\infty, \sqrt{2}[\cap \mathbb{Q}$ de $\mathbb{Q}$ est non-vide majorée, sans borne supérieure dans $\mathbb{Q}$.

Démonstration

(a) Soient $x_0 \in \mathbb{R}$ et $V \subseteq \mathbb{R}$ un voisinage de x_0. Il existe $\varepsilon > 0$ tel que : $V \supseteq]x_0 - \varepsilon, x_0 + \varepsilon[$.
On montre que $\mathbb{Q}$ et $\mathbb{R} \setminus \mathbb{Q}$ contiennent un point de V, par exemple dans $]x_0 - \varepsilon, x_0 + \varepsilon[$.
Idée : l'approximation décimale de x_0 à 10^{-k} près par défaut est $\frac{\lfloor 10^k x_0 \rfloor}{10^k}$ $(k \in \mathbb{N})$.

Par l'axiome d'Archimède avec $x = 1$, il existe $n \in \mathbb{N} \setminus \{0\}$ tel que $0 < \frac{1}{n} < \varepsilon$.
D'où : $\frac{\lfloor nx_0 \rfloor}{n} \leq x_0 < \frac{\lfloor nx_0 \rfloor}{n} + \frac{1}{n} < \frac{\lfloor nx_0 \rfloor}{n} + \varepsilon$ puis $x_0 - \varepsilon < \frac{\lfloor nx_0 \rfloor}{n} \leq x_0$.
De même, avec $x_0 + \sqrt{2}$ à la place de x_0, on a : $(x_0 + \sqrt{2}) - \varepsilon < \frac{\lfloor n(x_0+\sqrt{2}) \rfloor}{n} \leq (x_0 + \sqrt{2})$.
Finalement : $\frac{\lfloor nx_0 \rfloor}{n} \in]x_0 - \varepsilon, x_0 + \varepsilon[\cap \mathbb{Q}$ et $\frac{\lfloor n(x_0+\sqrt{2}) \rfloor}{n} - \sqrt{2} \in]x_0 - \varepsilon, x_0 + \varepsilon[\cap \mathbb{R} \setminus \mathbb{Q}$.

(b) On pose $A :=]-\infty, \sqrt{2}[\cap \mathbb{Q}$. Donc $0 \in A$.

L'ensemble des majorants m de A dans $\mathbb{Q}$ est égal à $[\sqrt{2}, +\infty[\cap \mathbb{Q}$. En effet un tel m vérifie $m \geq \sqrt{2}$ car $]\sqrt{2} - \varepsilon, \sqrt{2}[\cap \mathbb{Q} \neq \emptyset$ pour tout $\varepsilon > 0$ par la démonstration du (a) avec $x_0 = \sqrt{2}$.

En reprenant la démonstration du (a), on obtient aussi : $x_0 < \frac{\lfloor nx_0 \rfloor}{n} + \frac{1}{n} < x_0 + \varepsilon$.
L'ensemble $[\sqrt{2}, +\infty[\cap \mathbb{Q}$ n'a donc pas de plus petit élément m_0, car $[\sqrt{2}, \sqrt{2} + \varepsilon[\cap \mathbb{Q} \neq \emptyset$ pour tout $\varepsilon > 0$ et un tel m_0 devrait donc être égal à $\sqrt{2}$, mais $\sqrt{2} \notin \mathbb{Q}$. □

Proposition

On rappelle que les intervalles de $\mathbb{R}$ sont, par définition, les ensembles : $\emptyset$; $]a, b[$, $]a, b]$, $[a, b[$ avec $a, b \in \mathbb{R}$ et $a < b$; $[a, b]$ avec $a, b \in \mathbb{R}$ et $a \leq b$; $]a, +\infty[$, $[a, +\infty[$ avec $a \in \mathbb{R}$; $]-\infty, b[$, $]-\infty, b]$ avec $b \in \mathbb{R}$; $]-\infty, +\infty[$.

Une partie I de $\mathbb{R}$ est un intervalle si et seulement si :

$$\forall x, y \in I \quad \forall t \in \mathbb{R} \quad (x \leq t \leq y \implies t \in I).$$

Démonstration (idée)

Il est clair que tout intervalle I de $\mathbb{R}$ vérifie la condition.

Soit $I \subseteq \mathbb{R}$ non-vide qui contient tout $t \in \mathbb{R}$ pour lequel il existe $x, y \in I$ vérifiant $x \leq t \leq y$.
On distingue les cas $\inf I \in I$ et $\inf I \notin I$, et, $\sup I \in I$ et $\sup I \notin I$ (conventions du théorème).
On constate que I est égal à : $]\inf I, \sup I[$ ou $]\inf I, \sup I]$ ou $[\inf I, \sup I[$ ou $[\inf I, \sup I]$. □

II. Suites de nombres complexes

Important : tous les résultats de ce chapitre resteront valables en acceptant aussi comme « suites » les applications $n \mapsto u_n$ de $\mathbb{N}\setminus\{0, 1, ..., n_0 - 1\}$ dans $\mathbb{C}$, notées $(u_n)_{n \geq n_0}$, où $n_0 \in \mathbb{N}$.

1. Suites

Définition

(a) On appelle *suite de nombres complexes* une application $n \mapsto u_n$ de $\mathbb{N}$ dans $\mathbb{C}$. On notera $(u_n)_{n\geq 0}$ une telle suite. Elle est dite *réelle* si $u_n \in \mathbb{R}$ pour tout $n \geq 0$.

(b) Soit $r \in \mathbb{C}$. *Une suite arithmétique de raison* r est une suite $(u_n)_{n\geq 0}$ de la forme :

$$u_n = nr + c \text{ pour } n \in \mathbb{N}, \text{ avec } c \in \mathbb{C} \text{ fixé.}$$

(c) Soit $r \in \mathbb{C}$. *Une suite géométrique de raison* r est une suite $(u_n)_{n\geq 0}$ de la forme :

$$u_n = r^n\, c \text{ pour } n \in \mathbb{N}, \text{ avec } c \in \mathbb{C} \text{ fixé.}$$

Remarques

1. Soit $(u_n)_{n\geq 0} = (nr + c)_{n\geq 0}$ une suite arithmétique avec $r, c \in \mathbb{C}$.

On a : $\displaystyle\sum_{k=0}^{n} u_k = (0r + c) + \quad (1r + c) \quad + \cdots + (nr + c)$

$\displaystyle\sum_{k=0}^{n} u_k = (nr + c) + ((n-1)r + c) + \cdots + (0r + c)$

donc en additionnant : $\boxed{u_0 + \cdots + u_n \;=\; (\text{nombre de termes}) \times \frac{\text{premier terme} + \text{dernier terme}}{2}}$.

2. Soit $(u_n)_{n\geq 0} = (r^n\, c)_{n\geq 0}$ une suite géométrique avec $r, c \in \mathbb{C}$.

On a : $\displaystyle\sum_{k=0}^{n} u_k = c + rc + \cdots + r^n\, c$

$\displaystyle r\sum_{k=0}^{n} u_k = \quad rc + \cdots + r^n\, c + r^{n+1}\, c$

donc en soustrayant : $\boxed{u_0 + \cdots + u_n \;=\; \frac{\text{premier terme} - \text{dernier terme} \times \text{raison}}{1 - \text{raison}}, \text{ lorsque } r \neq 1}$.

2. Suites bornées

Définition

On se donne une suite $(u_n)_{n\geq 0}$ dans $\mathbb{C}$.

(a) On dit que $(u_n)_{n\geq 0}$ est *bornée* s'il existe $M \in \mathbb{R}_+$ tel que $|u_n| \leq M$ pour tout $n \in \mathbb{N}$.

(b) On suppose la suite $(u_n)_{n\geq 0}$ réelle. On dit que $(u_n)_{n\geq 0}$ est *majorée* (resp. *minorée*) s'il existe $M \in \mathbb{R}$ tel que $u_n \leq M$ (resp. $u_n \geq M$) pour tout $n \in \mathbb{N}$.

Ainsi : $(u_n)_{n\geq 0}$ est bornée si et seulement si elle est majorée et minorée.

Exemple

On pose $u_n = (-1)^n$ pour $n \geq 0$. La suite $(u_n)_{n\geq 0}$ est bornée car $|(-1)^n| \leq 1$ pour $n \in \mathbb{N}$.

3. Suites récurrentes

Une idée répandue est que la possibilité de construire des suites récurrentes découle immédiatement du « principe de récurrence ». Mais cette construction nécessite le résultat admis suivant, dû à Dedekind (1888). (Voir Paul R. Halmos, *Naive Set Theory*, chapitre 12.)

Proposition (« Recursion theorem »)

Soient I un intervalle, f une application de I dans $\mathbb{R}$, et $a \in \mathbb{R}$. On suppose que

($\star$) : il existe $A \subseteq I$ telle que $a \in A$ et $f(A) \subseteq A$ (donc $a \in I, f(a) \in I, f(f(a)) \in I, ...$).

Dans ce cas, il existe une unique suite $(u_n)_{n\geq 0}$ dans $\mathbb{R}$ telle que :

$$u_0 = a \text{ et } \underbrace{u_{n+1} = f(u_n)}_{\text{sous-entend que } u_n \in I} \text{ pour tout } n \in \mathbb{N}.$$

Démonstration (idée)

Une récurrence permet de montrer que pour tout $n \in \mathbb{N}$, la proposition suivante est vraie : $\mathscr{P}(n)$: il existe $(U_0, ..., U_n) \in I^{n+1}$ unique tel que $U_0 = a$ et $U_{k+1} = f(U_k)$ pour $0 \leq k \leq n-1$.
On constate que pour chaque $k \in \mathbb{N}$, le terme U_k dans $(U_0, U_1, ..., U_n)$ ne dépend pas de $n \geq k$.
On le note u_k. La suite $(u_n)_{n\geq 0}$ convient et elle est la seule à convenir. □

Remarque

Un résultat analogue permet de définir la suite $(f^n)_{n\geq 0}$ des composées de f.
On constate que $(\star)$ signifie que a est dans l'intersection des ensembles de définition des f^n.
On a ensuite : $(u_n)_{n\geq 0} = (f^n(a))_{n\geq 0}$.

III. Suites convergentes

1. Limite d'une suite

Définition-Proposition

On se donne une suite $(u_n)_{n\geq 0}$ dans $\mathbb{C}$.

(a) Soit $l \in \mathbb{C}$. On dit que $(u_n)_{n\geq 0}$ $\underbrace{\textit{a pour limite } l}_{\text{ou « tend vers } l \text{ »}}$ *quand* $n \to +\infty$ si :

$$\underbrace{\forall \varepsilon > 0}_{\text{pour tout } \varepsilon > 0} \quad \underbrace{\exists N \in \mathbb{N}}_{\text{il existe } N \in \mathbb{N} \text{ tel que}} \quad \forall n \in \mathbb{N} \quad \big(n \geq N \implies |u_n - l| < \varepsilon \big).$$

Dans ce cas, l est unique.
On note « $\lim\limits_{n\to+\infty} u_n = l$ » ou « $u_n \underset{n\to+\infty}{\longrightarrow} l$ » pour exprimer que $(u_n)_{n\geq 0}$ a pour limite l.

(b) On dit que
- $(u_n)_{n\geq 0}$ converge s'il existe $l \in \mathbb{C}$ tel que $(u_n)_{n\geq 0}$ a pour limite l ;
- $(u_n)_{n\geq 0}$ diverge si $(u_n)_{n\geq 0}$ ne converge pas.

On a : toute suite convergente de nombres complexes est bornée.

(c) On suppose la suite $(u_n)_{n\geq 0}$ réelle.
On dit que $(u_n)_{n\geq 0}$ *tend vers* $+\infty$ *quand* $n \to +\infty$ si :

$$\forall A > 0 \quad \exists N \in \mathbb{N} \quad \forall n \in \mathbb{N} \quad \big(n \geq N \implies u_n > A \big).$$

On dit que $(u_n)_{n\geq 0}$ *tend vers* $-\infty$ *quand* $n \to +\infty$ si :

$$\forall A > 0 \quad \exists N \in \mathbb{N} \quad \forall n \in \mathbb{N} \quad \big(n \geq N \implies u_n < -A \big).$$

Dans les deux cas précédents, la suite $(u_n)_{n\geq 0}$ n'est pas bornée, donc diverge (cf. (b)).
On note « $u_n \underset{n\to+\infty}{\longrightarrow} \underbrace{+\infty}_{(\text{resp. } -\infty)}$ » ou « $\lim\limits_{n\to+\infty} u_n = \underbrace{+\infty}_{(\text{resp. } -\infty)}$ » pour exprimer que $(u_n)_{n\geq 0}$ tend vers $\underbrace{+\infty}_{(\text{resp. } -\infty)}$.

Démonstration (dém. du (a) et du (b) au programme)

(a) Unicité de la limite ? Soient $k, l \in \mathbb{C}$ tels que $(u_n)_{n\geq 0}$ a pour limite k et l.
On suppose, par l'absurde, que $k \neq l$. On pose $\varepsilon = \frac{|k-l|}{2} > 0$.
Il existe donc $M, N \in \mathbb{N}$ tels que $|u_m - k| < \varepsilon$ dès que $m \geq M$ et $|u_n - l| < \varepsilon$ dès que $n \geq N$.
En choisissant $n = \max(M, N)$, on obtient la contradiction suivante :

$$\underbrace{|k-l|}_{2\varepsilon} \leq |k - u_n| + |u_n - l| < \varepsilon + \varepsilon.$$

(b) Suites convergentes bornées ? On suppose que la suite $(u_n)_{n\geq 0}$ converge vers $l \in \mathbb{C}$.
On choisit $\varepsilon = 1$ dans (a) : il existe $N \in \mathbb{N}$ tel que $|u_n - l| < 1$ dès que $n \geq N$.
Par conséquent $|u_n| \leq |u_n - l| + |l| \leq 1 + |l|$ dès que $n \geq N$.
Ainsi on a : $|u_n| \leq \max(|u_0|, ..., |u_{N-1}|, 1 + |l|)$ pour tout $n \in \mathbb{N}$.

(c) Suites de limite $+\infty$ non-bornées ? On suppose que la suite réelle $(u_n)_{n\geq 0}$ tend vers $+\infty$. Par l'absurde, on suppose aussi que $(u_n)_{n\geq 0}$ est bornée : il existe $M \geq 0$ tel que $|u_n| \leq M$ pour tout $n \in \mathbb{N}$. Il existe aussi $N \in \mathbb{N}$ tels que $u_n > M$ dès que $n \geq N$. En choisissant $n = N$, on obtient une contradiction.

On raisonne de même avec $-\infty$ à la place de $+\infty$. □

Exemple (axiome d'Archimède avec $\varepsilon = 1$)

On pose $u_n = n$ pour $n \geq 0$. La suite $(u_n)_{n\geq 0}$ a pour limite $+\infty$ car pour chaque $A > 0$, en posant $N = \lfloor A \rfloor + 1$ on a : $u_n \geq \lfloor A \rfloor + 1 > A$ dès que $n \geq N$.

Proposition

Soient $(u_n)_{n\geq 0}$ et $(v_n)_{n\geq 0}$ des suites de nombres complexes.

(a) On suppose que : $u_n \underset{n\to+\infty}{\longrightarrow} u$ et $v_n \underset{n\to+\infty}{\longrightarrow} v$ avec $u, v \in \mathbb{C}$.

On a : $u_n + v_n \underset{n\to+\infty}{\longrightarrow} u + v$, $u_n v_n \underset{n\to+\infty}{\longrightarrow} uv$, et, si $v \neq 0$, $\underbrace{\frac{u_n}{v_n}}_{v_n \neq 0 \text{ pour « } n \text{ assez grand »}} \underset{n\to+\infty}{\longrightarrow} \frac{u}{v}$.

(b) On suppose $(u_n)_{n\geq 0}$ et $(v_n)_{n\geq 0}$ réelles, $u_n \underset{n\to+\infty}{\longrightarrow} u$ et $v_n \underset{n\to+\infty}{\longrightarrow} v$ avec $u, v \in \mathbb{R} \cup \{-\infty, +\infty\}$.

Les formules du (a), interprétées correctement (*) restent valables, à condition :

– d'écarter les formes indéterminées sous forme de sommes $\underbrace{(+\infty)+(-\infty) \text{ et } (-\infty)+(+\infty)}_{\text{« } \infty-\infty \text{ »}}$, produits $\underbrace{0\,(+\infty) \text{ et } (+\infty)\,0 \text{ et } 0\,(-\infty) \text{ et } (-\infty)\,0}_{\text{« } 0\,\infty \text{ »}}$, et quotients $\frac{0}{0}$, $\underbrace{\frac{+\infty}{+\infty} \text{ et } \frac{-\infty}{-\infty} \text{ et } \frac{+\infty}{-\infty} \text{ et } \frac{-\infty}{+\infty}}_{\text{« } \frac{\infty}{\infty} \text{ »}}$;

– de n'étudier la limite de $(\frac{u_n}{v_n})_{n\geq n_0}$ dans le cas $v = 0$ que lorsque $\left\{ \text{ou } \begin{array}{l} v_n > 0 \text{ pour « } n \text{ assez grand »} \\ v_n < 0 \text{ pour « } n \text{ assez grand »} \end{array} \right.$.

Démonstration (dém. du (a) au programme)

(a) On fixe $\varepsilon > 0$.

• On a : $\underbrace{|(u_n + v_n) - (u + v)|}_{(u_n-u)+(v_n-v)} \leq \underbrace{|u_n - u|}_{<\frac{\varepsilon}{2} \text{ si } n\geq N} + \underbrace{|v_n - v|}_{<\frac{\varepsilon}{2} \text{ si } n\geq M} < \underbrace{\frac{\varepsilon}{2} + \frac{\varepsilon}{2}}_{\varepsilon}$ quand $n \geq \max(N, M)$.

Donc $u_n + v_n \underset{n\to+\infty}{\longrightarrow} u + v$.

• Sachant que $(v_n)_{n\geq 0}$ est bornée, on peut poser : $K = \max\big(\sup_{n\geq 0} |v_n|, |u|\big)$.

On a : $\underbrace{|u_n v_n - uv|}_{(u_n-u)v_n + u(v_n-v)} \leq \underbrace{|u_n - u|}_{<\frac{\varepsilon}{2K} \text{ si } n\geq N'} K + K \underbrace{|v_n - v|}_{<\frac{\varepsilon}{2K} \text{ si } n\geq M'} \underbrace{<}_{\substack{\text{clair lorsque} \\ K=0}} \varepsilon$ quand $n \geq \max(N', M')$.

Donc $u_n v_n \underset{n\to+\infty}{\longrightarrow} uv$.

• On suppose maintenant que $v \neq 0$.

On a : $\underbrace{|v|}_{(v-v_n)+v} \leq \underbrace{|v - v_n|}_{<\frac{|v|}{2} \text{ si } n\geq M_0} + |v_n| < \frac{|v|}{2} + |v_n|$ quand $n \geq M_0$.

Si $n \geq M_0$: $|v_n| > \frac{|v|}{2}$ puis $v_n \neq 0$. Enfin : $|\underbrace{\frac{1}{v_n} - \frac{1}{v}}_{-\frac{1}{v_n v}(v_n - v)}| \leq \frac{2}{|v|^2} \underbrace{|v_n - v|}_{<\frac{|v|^2}{2}\varepsilon \text{ si } n\geq M''} < \varepsilon$ quand $n \geq \max(M_0, M'')$.

Donc $\frac{1}{v_n} \underset{n\to+\infty}{\longrightarrow} \frac{1}{v}$. D'où, par ce qui précède : $\lim_{n\to+\infty} \frac{u_n}{v_n} = \lim_{n\to+\infty} u_n \frac{1}{v_n} = \frac{u}{v}$.

(b) Admis, car les méthodes sont analogues à celle de la démonstration du (a). □

(*) Soient $u, v \in \mathbb{R}$ et $\epsilon \in \{+, -\}$. On lira dans la conclusion du (a) : $\epsilon\infty + v = u + \epsilon\infty = \epsilon\infty$, $\epsilon\infty + \epsilon\infty = \epsilon\infty$; $(\epsilon\infty)v = u(\epsilon\infty) = \epsilon\infty$ si $u, v > 0$, $(\epsilon\infty)v = u(\epsilon\infty) = -\epsilon\infty$ si $u, v < 0$, $(\epsilon\infty)(\epsilon\infty) = +\infty$ et $(\epsilon\infty)(-\epsilon\infty) = -\infty$; $\frac{u}{\epsilon\infty} = 0$, $\frac{\epsilon\infty}{v} = \epsilon\infty$ si $v > 0$, $\frac{\epsilon\infty}{v} = -\epsilon\infty$ si $v < 0$, on remplacera $\frac{\epsilon\infty}{v}$ par $\epsilon\infty$ (resp. $-\epsilon\infty$) si $v = 0$ avec $v_n > 0$ (resp. $v_n < 0$) pour « n assez grand », on remplacera $\frac{u}{v}$ par $\epsilon\infty$ (resp. $-\epsilon\infty$) si $u \neq 0$ a pour signe ϵ et $v = 0$ avec $v_n > 0$ (resp. $v_n < 0$) pour « n assez grand ».

Exemples

1. On a déjà vu que $n \underset{n\to+\infty}{\longrightarrow} +\infty$. On en déduit que $\frac{1}{n} \underset{n\to+\infty}{\longrightarrow} 0$.

2. On considère une suite arithmétique $(nr+c)_{n\geq 0}$ avec $r, c \in \mathbb{R}$.

On a, avec un calcul direct quand $r=0$: $nr+c \underset{n\to+\infty}{\longrightarrow} \begin{cases} +\infty & \text{si } r>0 \\ \text{ou} \quad c & \text{si } r=0 \\ \text{ou} \quad -\infty & \text{si } r<0 \end{cases}$.

3. Attention aux formes indéterminées, par exemple avec $u_n := n^2$ et $v_n := -n$, $n \in \mathbb{N}$.
On a : $u_n = n \times n \underset{n\to+\infty}{\longrightarrow} +\infty$ et $v_n = (-1)\times n \underset{n\to+\infty}{\longrightarrow} -\infty$. Mais : $u_n + v_n = n^2\,(1-\frac{1}{n}) \underset{n\to+\infty}{\longrightarrow} \underbrace{+\infty}_{\neq 0}$.

Remarque

Il découle immédiatement des définitions que :
si $f\colon [0,+\infty[\, \to \mathbb{R}$ et $l \in \mathbb{R}\cup\{-\infty,+\infty\}$ vérifient $f(x) \underset{x\in\mathbb{R},\, x\to+\infty}{\longrightarrow} l$, alors $f(n) \underset{n\in\mathbb{N},\, n\to+\infty}{\longrightarrow} l$.
Cela permettra d'utiliser les résultats concernant les « croissances comparées ».

2. Composition des limites

Définition

On se donne une suite $(u_n)_{n\geq 0}$ de nombres complexes.

On appelle *suite extraite* de $(u_n)_{n\geq 0}$ toute suite de la forme $(u_{n_k})_{k\geq 0}$ avec :
$0 \leq n_0 < n_1 < n_2 < \ldots$ dans $\mathbb{N}$ (c-à-d $(n_k)_{k\geq 0}$ est une suite strictement croissante dans $\mathbb{N}$).

Proposition $\longleftarrow$[l'hypothèse « $n_k \underset{k\to+\infty}{\longrightarrow} +\infty$ » sur $(n_k)_{k\geq 0}$ suffit]

On se donne une suite $(u_n)_{n\geq 0}$ dans $\mathbb{C}$ et une suite extraite $(u_{n_k})_{k\geq 0}$ de $(u_n)_{n\geq 0}$.

(a) Soit $l \in \mathbb{C}$. Si $u_n \underset{n\to+\infty}{\longrightarrow} l$, alors $u_{n_k} \underset{k\to+\infty}{\longrightarrow} l$.

(b) On suppose que la suite $(u_n)_{n\geq 0}$ réelle.
Si $u_n \underset{n\to+\infty}{\longrightarrow} \underbrace{+\infty}_{(\text{resp. } -\infty)}$, alors $u_{n_k} \underset{k\to+\infty}{\longrightarrow} \underbrace{+\infty}_{(\text{resp. } -\infty)}$.

Démonstration (idée : $n_k \geq k$)

(a) Hypothèse : $u_n \underset{n\to+\infty}{\longrightarrow} l$. Soit $\varepsilon > 0$. Il existe $N \in \mathbb{N}$ tel que : $|u_n - l| < \varepsilon$ dès que $n \geq N$.
Or par récurrence sur $k \in \mathbb{N}$, on trouve que : $n_k \geq k$ pour tout $k \in \mathbb{N}$.
Donc $|u_{n_k} - l| < \varepsilon$ dès que $k \geq N$, car dans ce cas on a $n_k \geq N$.

(b) Hypothèse : $u_n \underset{n\to+\infty}{\longrightarrow} \underbrace{+\infty}_{(\text{resp. } -\infty)}$. Soit $A > 0$. On reprend la démonstration du (a) en remplaçant l'inégalité « $|u_n - l| < \varepsilon$ » par l'inégalité « $u_n > A$ » (resp. « $u_n < -A$ »). □

Exemple (important)

On pose $u_n = (-1)^n$ pour $n \geq 0$.

Les suites $(v_n)_{n\geq 0} := (1)_{n\geq 0}$ et $(w_n)_{n\geq 0} := (-1)_{n\geq 0}$ sont extraites de $(u_n)_{n\geq 0}$ car :
$v_k = u_{2k}$ et $w_k = u_{2k+1}$ avec $0 \leq 2\times 0 < 2\times 1 < \ldots$ et $0 \leq 2\times 0 + 1 < 2\times 1 + 1 < \ldots$.

Soit $l \in \mathbb{R}\cup\{-\infty,+\infty\}$. Si $u_n \underset{n\to+\infty}{\longrightarrow} l$, alors $l = \lim\limits_{n\to+\infty} v_n = 1$ et $l = \lim\limits_{n\to+\infty} w_n = -1$.
Cette contradiction montre que : la suite $((-1)^n)_{n\geq 0}$ n'a pas de limite dans $\mathbb{R}\cup\{-\infty,+\infty\}$.

Proposition

On se donne une application $g\colon \underset{\text{partie de } \mathbb{R}}{E} \longrightarrow \mathbb{R}$ et une suite $(u_n)_{n\geq 0}$ d'éléments de E.

On considère $k, l \in \mathbb{R}\cup\{-\infty,+\infty\}$.
Si $u_n \underset{n\to+\infty}{\longrightarrow} k$ et $g(y) \underset{y\to k}{\longrightarrow} l$, alors $g(u_n) \underset{n\to+\infty}{\longrightarrow} l$.
Si $k \in \mathbb{R}$ et $u_n \underset{n\to+\infty}{\longrightarrow} k$ avec $u_n \underbrace{\neq k}_{(\text{resp. } : \,>k,\, <k)}$ pour $n \in \mathbb{N}$ et $g(y) \underset{\substack{y\to k \\ y\neq k}}{\longrightarrow} l$ $(\text{resp. } y\to k^+,\, y\to k^-)$, alors $g(u_n) \underset{n\to+\infty}{\longrightarrow} l$.

Démonstration

Admise : s'inspirer du cas de la composée de deux fonctions de la variable réelle. □

Exemple (important)

On montre par l'absurde, en utilisant la proposition, que $x \mapsto \sin x$ n'a pas de limite quand $x \to +\infty$. Sinon, en supposant que $\sin x \underset{x\in\mathbb{R},\, x\to+\infty}{\longrightarrow} l \in \mathbb{R} \cup \{-\infty, +\infty\}$, on aurait :

$l = \lim\limits_{n\in\mathbb{N},\, n\to+\infty} \sin(2\pi n) = 0$ et $l = \lim\limits_{n\in\mathbb{N},\, n\to+\infty} \sin(2\pi n + \frac{\pi}{2}\, n) = 1$ contradiction.

3. Utilisation d'inégalités

Proposition

Soient $(u_n)_{n\geq 0}$, $(v_n)_{n\geq 0}$, $(w_n)_{n\geq 0}$ des suites dans $\mathbb{R}$.

(a) Si $\begin{cases} u_n \leq w_n \text{ pour tout } n \in \mathbb{N} \\ u_n \underset{n\to+\infty}{\longrightarrow} u \in \mathbb{R} \text{ et } w_n \underset{n\to+\infty}{\longrightarrow} w \in \mathbb{R} \end{cases}$ alors $u \leq w$ « prolongement des inégalités larges ».

(b) Si $\begin{cases} u_n \leq v_n \leq w_n \text{ pour tout } n \in \mathbb{N} \\ l \in \mathbb{R},\, u_n \underset{n\to+\infty}{\longrightarrow} l \text{ et } w_n \underset{n\to+\infty}{\longrightarrow} l \end{cases}$ alors $v_n \underset{n\to+\infty}{\longrightarrow} l$ « théorème des gendarmes ».

si deux gendarmes encadrent un bandit et vont en prison alors le bandit va en prison

(c) Si $\begin{cases} u_n \leq v_n \text{ (resp. } v_n \leq w_n) \text{ pour tout } n \in \mathbb{N} \\ u_n \underset{n\to+\infty}{\longrightarrow} +\infty \text{ (resp. } w_n \underset{n\to+\infty}{\longrightarrow} -\infty) \end{cases}$ alors $v_n \underset{n\to+\infty}{\longrightarrow} +\infty$ (resp. $v_n \underset{n\to+\infty}{\longrightarrow} -\infty$).

Démonstration (dém. du (b) au programme)

(a) On suppose par l'absurde que $u - w > 0$. Vu que $x \leq |x|$ pour tout $x \in \mathbb{R}$, on a :

$$\underbrace{u-w}_{-(u_n-u)+(u_n-w_n)+(w_n-w)} \leq \underbrace{|u_n-u|}_{<\frac{u-w}{2} \text{ dès que } n\geq N} + \underbrace{(u_n-w_n)}_{\leq 0} + \underbrace{|w_n-w|}_{<\frac{u-w}{2} \text{ dès que } n\geq M} < u-w \quad \text{quand } n \geq \max(N, M).$$

D'où une contradiction.

(b) Soit $\varepsilon > 0$. On a : $v_n - l \leq w_n - l \leq \underbrace{|w_n - l|}_{<\varepsilon \text{ dès que } n\geq M}$ et $-(v_n - l) \leq -(u_n - l) \leq \underbrace{|u_n - l|}_{<\varepsilon \text{ dès que } n\geq N}$

donc $|v_n - l| < \varepsilon$ quand $n \geq \max(N, M)$. Cela donne le résultat.

(c) Admis, car les méthodes sont analogues à celle de la démonstration du (b). □

Remarque

Le « prolongement des inégalités strictes » pose un problème.

Par exemple, on a $-\frac{1}{n} < \frac{1}{n}$ pour tout $n \geq 1$, mais $\lim\limits_{n\to+\infty} -\frac{1}{n} \not< \lim\limits_{n\to+\infty} \frac{1}{n}$.

Corollaire

On se donne une suite $(u_n)_{n\geq 0}$ dans $\mathbb{C}$ et $u \in \mathbb{C}$.

On pose $u_n = a_n + \mathrm{i}b_n$ avec $a_n, b_n \in \mathbb{R}$ pour $n \in \mathbb{N}$, et $u = a + \mathrm{i}b \in \mathbb{C}$ avec $a, b \in \mathbb{R}$.

On a : $u_n \underset{n\to+\infty}{\longrightarrow} u \iff |u_n - u| \underset{n\to+\infty}{\longrightarrow} 0 \iff a_n \underset{n\to+\infty}{\longrightarrow} a$ et $b_n \underset{n\to+\infty}{\longrightarrow} b$.

En particulier une suite de nombres réels qui converge dans $\mathbb{C}$ a une limite réelle.

Démonstration

La 1re équivalence découle tout de suite de la définition de la limite. On montre la seconde.

($\Rightarrow$) On applique le théorème des gendarmes à partir des inégalités :

$$0 \leq |a_n - a| \leq |u_n - u| \text{ et } 0 \leq |b_n - b| \leq |u_n - u| \text{ pour } n \in \mathbb{N}.$$

($\Leftarrow$) On utilise les égalités $u_n = a_n + \mathrm{i}b_n$ pour $n \in \mathbb{N}$, et les résultats sur la limite d'une somme et d'un produit. □

Exemple

On considère une suite géométrique $(r^n)_{n\geq 0}$ avec $r \in \mathbb{C}$ (choix de $c = 1$).

On a vu à la fin du paragraphe 2 que cette suite diverge lorsque $r = -1$. Cas général :

– si $|r| > 1$: $|r^n| = |r|^n = \big(1 + \underbrace{(|r| - 1)}_{\text{noté } h}\big)^n \underbrace{\geq}_{\text{formule du binôme}} 1 + nh$ avec $1 + nh \underset{n\to+\infty}{\longrightarrow} +\infty$,

donc $\boxed{|r^n| \underset{n\to+\infty}{\longrightarrow} +\infty \text{ quand } |r| > 1}$ en particulier la suite non-bornée $(r^n)_{n\geq 0}$ diverge ;

– si $|r| = 1$: $|r|^n = \underbrace{1}_{\underset{n\to+\infty}{\not\to} 0}$ donc $r^n \underset{n\to+\infty}{\not\to} 0$, puis $r = \frac{\lim\limits_{n\to+\infty} r^{n+1}}{\lim\limits_{n\to+\infty} r^n} = 1$ quand $(r^n)_{n\geq 0}$ converge,

donc $\boxed{(r^n)_{n\geq 0} \text{ diverge quand } |r| = 1 \text{ et } r \neq 1}$ et bien sûr $r^n \underset{n\to+\infty}{\longrightarrow} 1$ quand $r = 1$;

– si $|r| < 1$: $|r^n| = \frac{1}{\left|\left(\frac{1}{r}\right)^n\right|}$ avec $\left|\frac{1}{r}\right| > 1$, donc $\boxed{r^n \underset{n\to+\infty}{\longrightarrow} 0 \text{ quand } |r| < 1}$ vu le premier cas.

4. Suites de Cauchy

Définition

On dit qu'une suite $(u_n)_{n\geq 0}$ de nombres complexes est *une suite de Cauchy* si :

$$\underbrace{\forall \varepsilon > 0 \quad \exists N \in \mathbb{N} \quad \forall p, q \in \mathbb{N} \quad \big(\, p \geq q \geq N \implies |u_p - u_q| < \varepsilon \,\big)}_{\text{s'écrit en abrégé : } u_p - u_q \underset{p\geq q,\ q\to+\infty}{\longrightarrow} 0}.$$

Exemple

On pose $u_n = \sum_{k=0}^{n} \frac{1}{k!}$ pour $n \geq 0$.

Pour tous $p, q \in \mathbb{N}$ tels que $p \geq q$, on a :

$|u_p - u_q| = \frac{1}{(q+1)!} + \frac{1}{(q+2)!} + \frac{1}{(q+3)!} + \cdots + \frac{1}{p!} \leq \frac{1}{(q+1)!}\big(1 + \frac{1}{q+2} + \frac{1}{(q+2)^2} + \cdots + \frac{1}{(q+2)^{p-q-1}}\big)$

donc $0 \leq |u_p - u_q| \leq \frac{1}{q+1}\big(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^{p-q-1}}\big) \leq \frac{1}{q+1}\left(\frac{1-\frac{1}{2^{p-q}}}{1-\frac{1}{2}}\right) \leq \frac{2}{q+1}$.

Comme $\frac{2}{q+1} \underset{q\to+\infty}{\longrightarrow} 0$, on en déduit que la suite $(u_n)_{n\geq 0}$ est de Cauchy.

IV. Suites croissantes majorées

En annexe : complément concernant les suites récurrentes.

1. Suites monotones

Définition-Proposition

Soit $(u_n)_{n\geq 0}$ une suite dans $\mathbb{R}$. On dit que $(u_n)_{n\geq 0}$ est *croissante* (resp. *décroissante*) si elle vérifie l'une des deux propriétés équivalentes suivantes :

(i) $u_p \leq u_q$ (resp. $u_p \geq u_q$) pour tous $p, q \in \mathbb{N}$ tels que $p \leq q$;

(ii) $u_n \leq u_{n+1}$ (resp. $u_n \geq u_{n+1}$) pour tout $n \in \mathbb{N}$.

Démonstration

La propriété (ii) est un cas particulier de (i).

L'implication ((ii) $\Rightarrow$ (i)) vient de : $u_p \leq u_{p+1} \leq \ldots \leq u_q$ (récurrence cachée sur $q - p$). □

2. Toute suite croissante majorée converge

En annexe : complément concernant concernant la construction de $\mathbb{R}$.

Théorème (« théorème des suites monotones »)

Une suite $(u_n)_{n\geq 0}$ croissante (resp. décroissante) dans $\mathbb{R}$ est :

– convergente de limite $\sup\limits_{n\geq 0} u_n$ (resp. $\inf\limits_{n\geq 0} u_n$) lorsqu'elle est majorée (resp. minorée) ;

– divergente de limite $+\infty$ (resp. $-\infty$) lorsqu'elle n'est pas majorée (resp. pas minorée).

Démonstration (dém. au programme)

On se place dans le cas où $(u_n)_{n\geq 0}$ est croissante et majorée. On pose $l = \sup\limits_{n\geq 0} u_n$.

Soit $\varepsilon > 0$. Par définition du sup, il existe $N \in \mathbb{N}$ tel que : $u_N > l - \varepsilon$. Comme la suite $(u_n)_{n\geq 0}$ croît, on a : $l - \varepsilon < u_N \leq u_n \leq l$ pour $n \geq N$. Donc $|u_n - l| < \varepsilon$ pour $n \geq N$.

En conclusion : $u_n \underset{n\to+\infty}{\longrightarrow} l$.

Les 3 autres cas se traitent de façon analogue. □

Théorème (« théorème des suites adjacentes »)

Soient $(u_n)_{n\geq 0}$ et $(v_n)_{n\geq 0}$ deux suites dans $\mathbb{R}$ telles que :
$(u_n)_{n\geq 0}$ est croissante, $(v_n)_{n\geq 0}$ est décroissante, et $v_n - u_n \underset{n\to+\infty}{\longrightarrow} 0$ « suites adjacentes ».
Alors il existe $l \in \mathbb{R}$ tel que : $u_n \underset{n\to+\infty}{\longrightarrow} l$, $v_n \underset{n\to+\infty}{\longrightarrow} l$, et $u_n \leq l \leq v_n$ pour tout $n \in \mathbb{N}$.

Démonstration

Par définition de la limite, il existe $N \in \mathbb{N}$ tel que : $|v_n - u_n| < 1$ dès que $n \geq N$.
Si $n \geq N$, on a : $u_n < v_n + 1 \leq v_0 + 1$ et $v_n > u_n - 1 \geq u_0 - 1$.

D'après le théorème précédent, il existe $u, v \in \mathbb{R}$ tels que $u_n \underset{n\to+\infty}{\longrightarrow} u$ et $v_n \underset{n\to+\infty}{\longrightarrow} v$.
On a : $v - u = \lim\limits_{n\to+\infty} (v_n - u_n) = 0$. On pose $l = u = v$.

Si $n \in \mathbb{N}$, on a : $u_n \leq u_{n+k}$ pour $k \geq 0$, donc $u_n \leq \lim\limits_{k\to+\infty} u_{n+k} = l$; de même : $l \leq v_n$.

[*Variante.* Si $n \in \mathbb{N}$, on a d'après (a) : $u_n \leq \sup\limits_{n\geq 0} u_n = l = \inf\limits_{n\geq 0} v_n \leq v_n$.] □

Proposition

Une suite $(u_n)_{n\geq 0}$ de nombres complexes converge si et seulement si elle est de Cauchy.

Démonstration

($\Rightarrow$) On suppose que la suite $(u_n)_{n\geq 0}$ converge vers $l \in \mathbb{C}$.

Soit $\varepsilon > 0$. Il existe $N \in \mathbb{N}$ tel que $|u_n - l| < \frac{\varepsilon}{2}$ dès que $n \geq N$.
Donc $|u_p - u_q| = |(u_p - l) + (-(u_q - l))| \leq |u_p - l| + |u_q - l| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2}$ dès que $p \geq q \geq N$.
Cela montre que la suite $(u_n)_{n\geq 0}$ est de Cauchy.

($\Leftarrow$) On suppose que la suite $(u_n)_{n\geq 0}$ est de Cauchy.
Les inégalités $|\mathrm{Re}(u_p - u_q)| \leq |u_p - u_q|$ et $|\mathrm{Im}(u_p - u_q)| \leq |u_p - u_q|$ montrent que les suites $(\mathrm{Re}\, u_n)_{n\geq 0}$ et $(\mathrm{Im}\, u_n)_{n\geq 0}$ sont de Cauchy. On peut donc supposer que la suite $(u_n)_{n\geq 0}$ est réelle.

Par choix de $\varepsilon = 1$, il existe $N_0 \in \mathbb{N}$ tel que $|u_p - u_q| < 1$ dès que $p \geq q \geq N_0$.
D'où, en prenant $q = N_0$: $|u_p| \leq \max\big(\max\limits_{0\leq i\leq N_0-1} |u_i|, |u_{N_0}| + 1\big)$ pour tout $p \in \mathbb{N}$.
Ainsi la suite réelle $(u_n)_{n\geq 0}$ est bornée. On pose : $v_n = \inf\limits_{k\geq n} u_k$ et $w_n = \sup\limits_{k\geq n} u_k$ pour $n \geq 0$.

On constate que : $(v_n)_{n\geq 0}$ croît, $(w_n)_{n\geq 0}$ décroît, et $v_n \leq u_n \leq w_n$ pour tout $n \geq 0$.
Compte tenu du (b) du théorème précédent, il reste à vérifier que $w_n - v_n \underset{n\to+\infty}{\longrightarrow} 0$.

Soit $\varepsilon > 0$. On fixe $N \in \mathbb{N}$ tel que $|u_p - u_q| < \frac{\varepsilon}{3}$ dès que $p \geq N$ et $q \geq N$.
Soit $n \geq N$. Comme $v_n + \frac{\varepsilon}{3}$ ne minore pas $\{u_k\}_{k\geq n}$ et $w_n - \frac{\varepsilon}{3}$ ne majore pas $\{u_k\}_{k\geq n}$, il existe $p \geq n$ et $q \geq n$ tels que $v_n + \frac{\varepsilon}{3} > u_p$ et $w_n - \frac{\varepsilon}{3} < u_q$.
On a : $0 \leq w_n - v_n < (u_q + \frac{\varepsilon}{3}) - (u_p - \frac{\varepsilon}{3}) \leq |u_p - u_q| + 2\frac{\varepsilon}{3} < \varepsilon$.

Ainsi : $w_n - v_n \underset{n\to+\infty}{\longrightarrow} 0$. □

3. Théorème de Bolzano-Weierstrass

Proposition (« théorème de Bolzano-Weierstrass »)
Toute suite bornée de nombres réels admet une suite extraite convergente. ← pas $(\inf_{k\geq n} u_k)_{n\geq 0}$

Démonstration (dém. au programme)
Soit $(u_n)_{n\geq 0}$ une suite bornée dans $\mathbb{R}$.
On va construire une suite extraite convergente $(u_{n_k})_{k\geq 0}$ par récurrence.
On commence en notant : $[a_0, b_0] := [\inf_{n\geq 0} u_n, \sup_{n\geq 0} u_n]$ et $n_0 := 0$, donc $u_{n_0} \in [a_0, b_0]$.
On suppose construit (a_k, b_k, n_k) tel que :

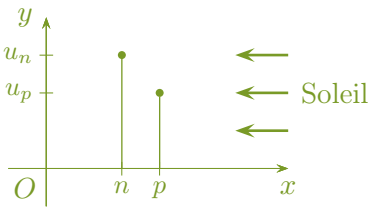
$$a_k \leq b_k,\ b_k - a_k = \frac{b_0 - a_0}{2^k},\ u_{n_k} \in [a_k, b_k] \text{ et } \{n \in \mathbb{N} \mid u_n \in [a_k, b_k]\} \text{ est infini.}$$

On note : $[a_{k+1}, b_{k+1}] := \begin{cases} [a_k, \frac{a_k+b_k}{2}] & \text{si } [a_k, \frac{a_k+b_k}{2}] \text{ contient } u_n \text{ pour une infinité de } n \\ \text{ou} \\ [\frac{a_k+b_k}{2}, b_k] & \text{sinon (donc cet intervalle contient } u_n \text{ pour une infinité de } n) \end{cases}$

et n_{k+1} le plus petit entier $n > n_k$ pour lequel $u_n \in [a_{k+1}, b_{k+1}]$.
Les suites $(a_k)_{k\geq 0}$ qui croît, et $(b_k)_{k\geq 0}$ qui décroît, sont adjacentes car $b_k - a_k = \frac{b_0-a_0}{2^k} \underset{k\to+\infty}{\longrightarrow} 0$.
On note : $l = \lim_{k\to+\infty} a_k = \lim_{k\to+\infty} b_k$. Comme $a_k \leq u_{n_k} \leq b_k$, on obtient : $u_{n_k} \underset{k\to+\infty}{\longrightarrow} l$.

(Variante : on tente de construire par récurrence une suite extraite croissante $(u_{n_k})_{k\geq 0}$ de $(u_n)_{n\geq 0}$.

On note : $B_{\text{ronzé}} := \{n \in \mathbb{N} \mid \underbrace{\forall p > n \quad u_p < u_n}_{\text{condition à éviter pour } n = n_k}\}$.



• Si $B_{\text{ronzé}}$ est fini, il existe $n_0 \in \mathbb{N}$ tel que $B_{\text{ronzé}} \subseteq \{0, 1, ..., n_0 - 1\}$.
Comme $n_0 \notin B_{\text{ronzé}}$: $u_{n_0} \leq u_{n_1}$ pour un certain $n_1 > n_0$ minimal.
Comme $n_1 \notin B_{\text{ronzé}}$: $u_{n_1} \leq u_{n_2}$ pour un certain $n_2 > n_1$ minimal. ...
La suite $(u_{n_k})_{k\geq 0}$ est croissante et majorée, donc converge.

• Si $B_{\text{ronzé}}$ est infini, on note $n_0 < n_1 < ...$ ses éléments.
La suite $(u_{n_k})_{k\geq 0}$ est décroissante et minorée, donc converge.)

Conclusion : $(u_n)_{n\geq 0}$ a une suite extraite convergente. □

Exemple
La suite $((-1)^n)_{n\geq 0}$ admet pour suite extraite convergente la suite $(1)_{n\geq 0}$ (avec $n_k = 2k$).

Annexe 1 : développement décimal

Proposition (« *représentation d'un nombre entier en base* 10 »)

Pour tout $a \in \mathbb{N}$, il existe une unique suite $(c_k)_{k\in\mathbb{N}}$ d'éléments de $\{0,...,9\}$ nuls au-delà d'un certain $s \in \mathbb{N}$, telle que : $a = c_s 10^s + ... + c_1 10 + c_0$. On notera : $a = \underbrace{c_s c_{s-1} ... c_0}_{\text{mot concaténé des chiffres } c_s, c_{s-1}, ..., c_0}$.

Démonstration

Récurrence sur a. C'est vrai pour $a = 0$. On suppose que $a \geq 1$ et que c'est acquis pour les nombres dans $\{0,...,a-1\}$. On utilise la division euclidienne de a par 10 : $a = 10q + r$.
Si $q = 0$: $a > q$; si $q \neq 0$: $a \geq 10q > q$. Dans tous les cas, on a : $q \in \{0,...,a-1\}$.
On peut donc appliquer l'hypothèse de récurrence à q

Existence ? On pose d'abord : $c_0 = r$. L'existence pour q fournit une décomposition de la forme $q = d_t 10^t + ... + d_1 10 + d_0$. D'où : $a = d_t 10^{t+1} + ... + d_1 10^2 + d_0 10 + c_0$.

Unicité ? On se place dans le cas où $a = c_s 10^s + ... + c_1 10 + c_0$ et $a = c'_{s'} 10^{s'} + ... + c'_1 10 + c'_0$.
On complète par des 0 pour obtenir les suites $(c_k)_{k\in\mathbb{N}}$ et $(c'_k)_{k\in\mathbb{N}}$.
Nécessairement $r = c_0$ et $r = c'_0$. Ensuite $q = c_s 10^{s-1} + ... + c_1$ et $q = c'_{s'} 10^{s'-1} + ... + c'_1$
puis $(c_k)_{k\geq 1} = (c'_k)_{k\geq 1}$ par l'unicité pour q. Ainsi $(c_k)_{k\in\mathbb{N}} = (c'_k)_{k\in\mathbb{N}}$. □

On déduit de la proposition précédente que les *nombres décimaux positifs* (c'est à dire les réels $\frac{a}{10^n}$ avec $a \in \mathbb{N}$ et $n \in \mathbb{N}$) sont les nombres réels de la forme $c_0 + \frac{c_1}{10} + ... + \frac{c_n}{10^n}$ avec $c_0 \in \mathbb{N}$, $n \in \mathbb{N}$ et $c_1, ..., c_n \in \{0,...,9\}$.

Définition-Proposition

(a) Soit $(c_n)_{n\in\mathbb{Z}}$ une famille d'éléments de $\{0,...,9\}$ indexée par $\mathbb{Z}$ telle qu'il existe $k \in \mathbb{N}$ vérifiant $c_n = 0$ quand $n < -k$.

La suite $(u_n)_{n\geq -k}$ définie par $u_n := 10^k\, c_{-k} + ... + 10^{-n}\, c_n$ converge vers un élément x de $\mathbb{R}_+$.
On dit que $(c_n)_{n\in\mathbb{Z}}$ est *un développement décimal de* x et note : $x = \underbrace{c_{-k} \,...\, c_{-1} c_0 \,,\, c_1 c_2 \,...}_{\text{deux mots infinis (0 avant } c_{-k})}$.

Par exemple on a : $1 = 1{,}000...$ et $1 = 0{,}999....$

(b) Soit $x \in \mathbb{R}_+$. Il existe un unique développement décimal $(c_n)_{n\in\mathbb{Z}}$ de x qui ne devient pas constamment égal à 9 à partir d'un certain rang.

Il s'écrit : $c_n = \lfloor 10^n x \rfloor - 10 \lfloor 10^{n-1} x \rfloor$ pour $n \in \mathbb{Z}$.

On dit que $(c_n)_{n\in\mathbb{Z}}$ est *le développement décimal propre de* x.
Tout autre développement décimal de x est appelé *un développement décimal impropre de* x.

(c) Les $x \in \mathbb{R}_+$ qui ont un développement décimal impropre $(c'_n)_{n\in\mathbb{Z}}$ sont les décimaux non-nuls : $x = \sum_{i=p}^{q} 10^{-i} c_i$ avec $p, q \in \mathbb{Z}$, $p \leq q$, $c_n \in \{0,...,9\}$ pour $p \leq n \leq q$, $c_p \neq 0$ et $c_q \neq 0$. (*)
Celui-ci est alors unique : $c'_n = 0$ si $n < p$, $c'_n = c_n$ si $p \leq n < q$, $c'_q = c_q - 1$, $c'_n = 9$ si $n > q$.

Démonstration

(a) Si $n \geq -k$, on a : $u_n \leq 9{\times}10^k + ... + 9{\times}10^{-n} = 10^{k+1} - 10^{-n} \leq 10^{k+1}$.
La suite $(u_n)_{n\geq -k}$ est croissante majorée à termes positifs, donc converge dans $\mathbb{R}_+$.

(b) (Unicité) On suppose que $(c_n)_{n\in\mathbb{Z}}$ convient. On introduit la suite $(u_n)_{n\geq -k}$ du (a).

Soit $n \geq -k$. Comme la suite $(u_n)_{n\geq -k}$ croît, on a d'abord : $u_n \leq x$.
Par hypothèse, il existe – et on fixe – un $p > n$ tel que $c_p \leq 8$. Si $q \geq p$, on a :
$u_q \leq 10^k c_{-k} + \cdots + 10^0 c_0 + \cdots + 10^{-n} c_n + (9{\times}10^{-n-1} + ... + 9{\times}10^{-q}) - 10^{-p}$
$\leq 10^k c_{-k} + \cdots + 10^0 c_0 + \cdots + 10^{-n} c_n + 10^{-n} - 10^{-p}$.

(*) Il est clair que le développement décimal propre d'un tel réel x est la suite $(c_n)_{n\in\mathbb{Z}}$ obtenue en complétant la suite finie $(c_p, ..., c_q)$, indexée par $\{p, ..., q\}$, par $c_n = 0$ quand $n < p$ ou $n > q$.

Un passage à $q \to +\infty$ donne : $x \leq u_n + 10^{-n} - 10^{-p} < u_n + 10^{-n}$.
Le choix de $n = -k$ dans l'inégalité $x < u_n + 10^{-n}$ montre que $0 \leq 10^{-k}x < c_{-k} + 1$.

Ainsi : $10^n u_n \leq 10^n x < 10^n u_n + 1$ avec $10^n u_n \in \mathbb{N}$ ce qui signifie que $10^n u_n = \lfloor 10^n x \rfloor$.
On a donc, en posant $u_{-k-1} = 0$: $c_n = 10^n(u_n - u_{n-1}) = \lfloor 10^n x \rfloor - 10\lfloor 10^{n-1} x \rfloor$.
Soit $n' < -k$. On a : $c_{n'} = \lfloor 10^{n'} x \rfloor - 10 \lfloor 10^{n'-1} x \rfloor$ car $c_{n'} = 0$ et $0 \leq 10^{n'-1}x \leq 10^{n'}x < 1$.

(Existence) On pose : $c_n = \lfloor 10^n x \rfloor - 10 \lfloor 10^{n-1} x \rfloor$ quand $n \in \mathbb{Z}$.
On a : $10^n x - 1 < \lfloor 10^n x \rfloor \leq 10^n x$ et $-10{\times}10^{n-1}x \leq -10{\times}\lfloor 10^{n-1} x \rfloor < -10{\times}(10^{n-1}x - 1)$.
En additionnant ces inégalités, on obtient : $-1 < c_n < 10$ puis $c_n \in \{0, ..., 9\}$.

On choisit $k \in \mathbb{N}$ minimal pour que $10^{-k-1}x < 1$. On a donc $c_n = 0$ quand $n < -k$.
On introduit à nouveau la suite $(u_n)_{n \geq -k}$ du (a).

Si $n \geq -k$: $u_n = 10^k(\lfloor 10^{-k} x \rfloor - 0) + \cdots + 10^{-n}(\lfloor 10^n x \rfloor - 10 \lfloor 10^{n-1} x \rfloor) = 10^{-n} \lfloor 10^n x \rfloor$ donc $10^n u_n \leq 10^n x < 10^n u_n + 1$. Le théorème des gendarmes appliqué aux inégalités $x - 10^{-n} < u_n \leq x$ donne $x = c_{-k} \ldots c_{-1} c_0 \, , c_1 c_2 \ldots$.

De plus, les coefficients c_n ne peuvent être égaux à 9 pour $n > p$ ($p \geq -k$), car sinon on aurait : $x - 10^{-p} = \lim\limits_{\substack{n>p \\ n \to +\infty}} u_n - 10^{-p} = \lim\limits_{\substack{n>p \\ n \to +\infty}} u_p + (9{\times}10^{-p-1} + ... + 9{\times}10^{-n}) - 10^{-p} = u_p \not< u_p$.

(c) (Condition suffisante) Soit $x = 10^{-p}c_p + \cdots + 10^{-q}c_q$ comme dans l'énoncé.
On pose : $c'_n = 0$ si $n < p$, $c'_n = c_n$ si $p \leq n < q$, $c'_q = c_q - 1$, $c'_n = 9$ si $n > q$.

Lorsque $n \geq q$, on a :
$10^{-p}c'_p + ... + 10^{-n}c'_n = 10^{-p}c'_p + ... + 10^{-q}c'_q + (9{\times}10^{-q-1} + ... + 9{\times}10^{-n}) = 10^{-p}c_p + ... + 10^{-q}c_q - 10^{-n}$.
D'où : $\lim\limits_{n \to +\infty} 10^{-p}c'_p + \cdots + 10^{-n}c'_n = x$. Ainsi x admet une représentation décimale impropre.

(Condition nécessaire) Soit $x \in \mathbb{R}_+$ qui a une représentation décimale $(c'_n)_{n \in \mathbb{Z}}$ impropre.
On note p (resp. q) le plus grand (resp. plus petit) élément de $\mathbb{Z}$ tel que $c'_n = 0$ pour tout $n < p$ (resp. $c'_n = 9$ pour tout $n > q$). On a obtient à l'aide du calcul pour la condition suffisante :
$x = \lim\limits_{n \to +\infty} 10^{-p}c'_p + \cdots + 10^{-n}c'_n = 10^{-p}c'_p + \cdots + 10^{-q}(c'_q + 1)$ avec $c'_q \leq 8$.
Donc x est le nombre décimal dont l'unique représentation décimale propre $(c_n)_{n \in \mathbb{N}}$ est :
$c_n = 0$ si $n < p$, $c_n = c'_n$ si $p \leq n < q$, $c_q = c'_q + 1$, $c_n = 0$ si $n > q$.
En particulier la suite $(c'_n)_{n \in \mathbb{N}}$ est unique. □

Remarque

Soit $x \in \mathbb{R}_+$. On note $(c_n)_{n \in \mathbb{Z}}$ le développement décimal propre de x.
On pose : $u_n = \sum\limits_{i \leq n} 10^{-i} c_i$ pour $n \in \mathbb{Z}$, où la somme contient un nombre fini de termes non-nuls.

D'après (b) : $u_n = 10^{-n} \lfloor 10^n x \rfloor$, donc $u_n \leq x < u_n + 10^{-n}$ avec $u_n \in 10^{-n}\,\mathbb{N}$.
Les nombres u_n et $u_n + 10^{-n}$ s'appellent *la valeur décimale approchée par défaut de x à 10^{-n} près* et *la valeur décimale approchée strictement par excès de x à 10^{-n} près*.
Par un calcul immédiat : les suites $(u_n)_{n \geq 0}$ et $(u_n + 10^{-n})_{n \geq 0}$ sont adjacentes de limite x.

Annexe 2 : suites récurrentes [cas général hors programme]

On considère une application continue $f : \underset{\text{intervalle infini}}{I} \longrightarrow \mathbb{R}$ et $a \in \mathbb{R}$ tels que :
$\underbrace{a \in I, f(a) \in I, f(f(a)) \in I, ...}_{\substack{a \text{ est dans l'intersection des ensembles} \\ \text{de définition des fonctions } f,\ f\circ f,\ f\circ f\circ f,\ ...}}$ (signifie qu'il existe $A \subseteq I$ telle que $a \in A$ et $f(A) \subseteq A$).

Proposition 1 (« *suite définie par une relation de récurrence* »)
Il existe une unique suite $(u_n)_{n\geq 0}$ dans $\mathbb{R}$ telle que : $u_0 = a$ et $\underbrace{u_{n+1} = f(u_n)}_{\text{sous-entend que } u_n \in I}$ pour $n \in \mathbb{N}$.

Démonstration (idée)

Une récurrence permet de montrer que pour tout $n \in \mathbb{N}$, la proposition suivante est vraie :
$\mathscr{P}(n)$: il existe $(U_0, ..., U_n) \in I^{n+1}$ unique tel que $U_0 = a$ et $U_{k+1} = f(U_k)$ pour $0 \leq k \leq n-1$.
On constate que pour chaque $k \in \mathbb{N}$, le terme U_k dans $(U_0, U_1, ..., U_n)$ ne dépend pas de $n \geq k$.
On le note u_k. La suite $(u_n)_{n\geq 0}$ convient et elle est la seule à convenir. □

Proposition 2

On suppose que la suite $(u_n)_{n\geq 0}$ converge vers un point l de I. Alors : $\boxed{f(l) = l}$.

Démonstration

On va passer à la limite dans l'égalité $u_{n+1} = f(u_n)$.
Comme $(u_{n+1})_{n\geq 0}$ est extraite de $(u_n)_{n\geq 0}$, on a : $u_{n+1} \underset{n\to+\infty}{\longrightarrow} l$.
De plus, la continuité de f assure que : $f(u_n) \underset{n\to+\infty}{\longrightarrow} f(l)$. D'où le résultat . □

Début de l'étude (cas simples)

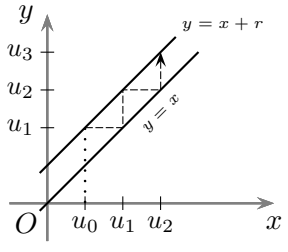
(1) On résout l'équation $f(x) = x$ et étudie les variations de f.
Le signe de $f(x) - x$ fournit la position de la courbe $\mathscr{C} : y = f(x)$ par rapport à la première bissectrice.

(2) On fait une brève étude graphique de la suite $(u_n)_{n\geq 0}$ au brouillon :
– on place (u_0, u_1) sur la courbe $\mathscr{C}$;
– on place (u_1, u_1) sur la 1re bissectrice, puis (u_1, u_2) sur la courbe $\mathscr{C}$;
– on place de même les points (u_2, u_2) et (u_2, u_3) d'abscisse u_2 ;
– ....

Exemples

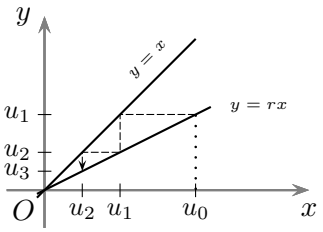
(1) Suite arithmétique de raison r $(r > 0)$:
$u_0 = c$ et $u_{n+1} = u_n + r$ pour $n \geq 0$.

Le dessin est en accord avec : $u_n \underset{n\to+\infty}{\longrightarrow} +\infty$.



(2) Suite géométrique de raison r $(0 < r < 1)$:
$u_0 = c$ et $u_{n+1} = ru_n$ pour $n \geq 0$.

Le dessin est en accord avec : $u_n \underset{n\to+\infty}{\longrightarrow} 0$.



Discussion

(1) On suppose que f est croissante et que $\alpha \in I$ vérifie $f(\alpha) = \alpha$.

(a) On a : $u_{n+1} - u_n = f(u_n) - f(u_{n-1})$ pour $n \geq 1$.

Donc : – si $f(a) - a \geq 0$ alors $(u_n)_{n\geq 0}$ est croissante ;
– si $f(a) - a \leq 0$ alors $(u_n)_{n\geq 0}$ est décroissante.

(b) On a aussi : $u_{n+1} - \alpha = f(u_n) - f(\alpha)$ pour $n \geq 0$.

Donc : – si $a \leq \alpha$ alors $(u_n)_{n\geq 0}$ est majorée par α ;
– si $a \geq \alpha$ alors $(u_n)_{n\geq 0}$ est minorée par α.

(2) On suppose que f est décroissante et que $\beta \in I$ vérifie $f(\beta) = \beta$.

On note $g := f \circ f$ (définie sur une partie de I), $v_n := u_{2n}$ et $w_n := u_{2n+1}$ pour $n \in \mathbb{N}$. Les suites $(v_n)_{n\geq 0}$ et $(w_n)_{n\geq 0}$ vérifient $v_{n+1} = g(v_n)$ et $w_{n+1} = g(w_n)$ pour tout $n \geq 0$.

Comme g est croissante et $g(\beta) = \beta$, on est ramené au cas (1).

De plus : si $g(a) - a \geq 0$ alors $g(f(a)) - f(a) \leq 0$; si $g(a) - a \leq 0$ alors $g(f(a)) - f(a) \geq 0$. Ainsi : les suites $(v_n)_{n\geq 0}$ et $(w_n)_{n\geq 0}$ varient en sens contraire.

On pourra utiliser : si $(v_n)_{n\geq 0}$ et $(w_n)_{n\geq 0}$ convergent vers β, alors $(u_n)_{n\geq 0}$ converge vers β.

(On suppose que : $\lim\limits_{p\to+\infty} v_p = \lim\limits_{q\to+\infty} w_q = \beta$. Soit $\varepsilon > 0$. Il existe $P, Q \in \mathbb{N}$ tels que $|v_p - \beta| < \varepsilon$ et $|w_q - \beta| < \varepsilon$ dès que $p \geq P$ et $q \geq Q$. D'où : $|u_n - \beta| < \varepsilon$ dès que $n \geq \max(2P, 2Q+1)$.)

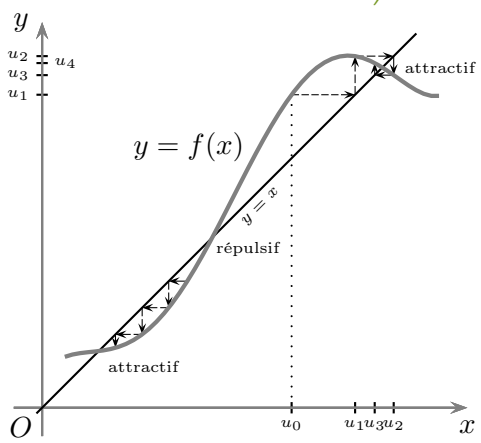
Précisions

On suppose que f est dérivable, et que $l \in I$ vérifie $f(l) = l$.

(a) S'il existe $k \in [0, 1[$ tel que $|f'(x)| \leq k$ pour tout $x \in I$, alors $u_n \underset{n\to+\infty}{\longrightarrow} l$.

(On utilise l'inégalité des accroissements finis :
$\underbrace{|u_n - l|}_{|f(u_{n-1})-f(l)|} \leq k \underbrace{|u_{n-1} - l|}_{|f(u_{n-2})-f(l)|} \leq k^2 |u_{n-2} - l| \leq \cdots \leq k^n |u_0 - l|$ puis $|u_n - l| \underset{n\to+\infty}{\longrightarrow} 0$.)

(b) On suppose en outre que I est ouvert.



– Si $|f'(l)| < 1$:
on dit que l est « un point attractif » (cf. dessin).

– Si $|f'(l)| = 1$:
cas à étudier plus précisément.

– Si $|f'(l)| > 1$:
on dit que l est « un point répulsif » (cf. dessin).

Les mots « attractif » et « répulsif » font référence à ce qui suit.

– Si $|f'(l)| < 1$: il existe $\eta > 0$ tel que la condition $|u_0 - l| < \eta$ implique que $u_n \underset{n\to+\infty}{\longrightarrow} l$;

(On pose : $k = |f'(l)| + \frac{1-|f'(l)|}{2} = \frac{|f'(l)|+1}{2} < 1$. On a : $\frac{|f(x)-f(l)|}{|x-l|} \underset{x\to l,\, x\in I \text{ et } x\neq l}{\longrightarrow} |f'(l)|$.
Il existe donc $\eta > 0$ tel que : $x \in I$ et $\frac{|f(x)-f(l)|}{|x-l|} < k$ dès que $0 < |x - l| < \eta$.
On obtient : $|u_n - l| \leq k |u_{n-1} - l| \leq \cdots \leq k^n |u_0 - l|$ puis $|u_n - l| \underset{n\to+\infty}{\longrightarrow} 0$.)

– Si $|f'(l)| > 1$: il existe $\eta > 0$ tel que la condition $0 < |u_0 - l| < \eta$ implique qu'un des termes de la suite $(u_n)_{n\geq 0}$ sort de $]l - \eta, l + \eta[$.

(On pose : $k = |f'(l)| - \frac{|f'(l)|-1}{2} = \frac{|f'(l)|+1}{2} > 1$. On a encore : $\frac{|f(x)-f(l)|}{|x-l|} \underset{x\to l,\, x\in I \text{ et } x\neq l}{\longrightarrow} |f'(l)|$.
Il existe donc $\eta > 0$ tel que : $x \in I$ et $\frac{|f(x)-f(l)|}{|x-l|} > k$ dès que $0 < |x - l| < \eta$.
On suppose par l'absurde que $|u_n - l| < \eta$ pour tout $n \geq 0$.
On a : $|u_n - l| \geq k |u_{n-1} - l| \geq \cdots \geq k^n \underbrace{|u_0 - l|}_{\neq 0}$ puis $|u_n - l| \underset{n\to+\infty}{\longrightarrow} +\infty$. Contradiction.)

Annexe 3 : construction de $\mathbb{R}$ (complément hors programme)

Ce complément explique pourquoi diverses constructions de $\mathbb{R}$ (dont celle par les « coupures de Dedekind » évoquée à la fin) qui aboutissent à des descriptions différentes, fournissent néanmoins des objets « comparables » (au sens de la seconde partie du théorème ci-dessous).

Remarques

Il est possible de construire $\mathbb{N}$, $\mathbb{Z}$, et $\mathbb{Q}$. Par exemple en tenant compte des idées qui suivent.

Tout d'abord (« axiome de l'infini »), il existe un ensemble A vérifiant :

$$(\star) \qquad \emptyset \in A \quad \text{et} \quad \forall x \in A \quad x \cup \{x\} \in A.$$

Avec cet axiome on peut démontrer qu'il existe un plus petit ensemble A vérifiant $(\star)$. On le note $\mathbb{N}$. On construit par récurrence l'addition sur $\mathbb{N}$, puis la multiplication sur $\mathbb{N}$.

On obtient ensuite $\mathbb{Z}$ comme quotient de $\mathbb{N}^2$, en cherchant à représenter $p-q$ par (p,q) :

$$\mathbb{Z} := \mathbb{N}^2/\sim \quad \text{où} \quad (p,q) \sim (p',q') \iff p+q' = p'+q.$$

On obtient finalement $\mathbb{Q}$ comme quotient de $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, en assimilant $\frac{p}{q}$ à (p,q) :

$$\mathbb{Q} := (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/\sim \quad \text{où} \quad (p,q) \sim (p',q') \iff pq' = p'q.$$

Définition 1

Soient E un ensemble et Γ une partie de $E \times E$. On note « $x \leq y$ » pour « $(x,y) \in \Gamma$ ».
On dit que $\leq$ est une relation d'ordre si :

(i) $\forall x \in E \quad x \leq x$;
(ii) $\forall x,y \in E \quad \big((x \leq y \text{ et } y \leq x) \implies x = y\big)$;
(iii) $\forall x,y,z \in E \quad \big((x \leq y \text{ et } y \leq z) \implies x \leq z\big)$.

Dans ce cas, l'ordre $\leq$ est dit total si :

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

Définition 2

Un corps commutatif est un ensemble $\mathbb{K}$ muni de deux applications

$$\begin{array}{ccc} \mathbb{K}\times\mathbb{K} & \longrightarrow & \mathbb{K} \\ (x,y) & \longmapsto & x+y \end{array} \quad \text{et} \quad \begin{array}{ccc} \mathbb{K}\times\mathbb{K} & \longrightarrow & \mathbb{K} \\ (x,y) & \longmapsto & x\cdot y \end{array} \quad \text{telles que :}$$

(i) on a $(x+y)+z = x+(y+z)$ et $x+y = y+x$ pour tous $x,y,z \in \mathbb{K}$;
(ii) il existe un élément 0 de $\mathbb{K}$ tel que $x+0 = x$ pour tout $x \in \mathbb{K}$ (dans ce cas, cet élément 0 est unique) ;
(iii) pour tout $x \in \mathbb{K}$, il existe un élément $-x$ de $\mathbb{K}$ tel que $x+(-x) = 0$ (dans ce cas, cet élément $-x$ est unique) ;
(iv) on a $(x\cdot y)\cdot z = x\cdot(y\cdot z)$ et $x\cdot y = y\cdot x$ pour tous $x,y,z \in \mathbb{K}$;
(v) il existe un élément 1 de $\mathbb{K}\setminus\{0\}$ tel que $x\cdot 1 = x$ pour tout $x \in \mathbb{K}$ (dans ce cas, cet élément 1 est unique) ;
(vi) pour tout $x \in \mathbb{K}\setminus\{0\}$, il existe un élément x^{-1} de $\mathbb{K}$ tel que $x\cdot x^{-1} = 1$ (dans ce cas, cet élément x^{-1} est unique) ;
(vii) on a $x\cdot(y+z) = (x\cdot y)+(x\cdot z)$ pour tous $x,y,z \in \mathbb{K}$.

Définition 3

On appelle corps des nombres réels tout corps commutatif $(\mathbb{R},+,\cdot)$ muni d'une relation d'ordre total $\leq$ telle que :

(i) $\forall x,y,z \in \mathbb{R} \quad \big(x \leq y \implies x+z \leq y+z\big)$;
(ii) $\forall x,y \in \mathbb{R} \quad \big((0 \leq x \text{ et } 0 \leq y) \implies 0 \leq x\cdot y\big)$;
(iii) toute partie non-vide majorée de $\mathbb{R}$ a une borne supérieure.

Théorème (⋆)

a) Il existe un corps des nombres réels $(\mathbb{R}, +, \cdot, \leq)$.

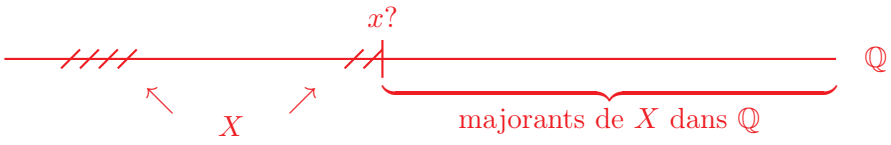
b) Pour tout autre corps des nombres réels $(\widetilde{\mathbb{R}}, \widetilde{+}, \widetilde{\cdot}, \widetilde{\leq})$, il existe une unique bijection $\varphi : \mathbb{R} \to \widetilde{\mathbb{R}}$ telle que :

(i) $\forall x, y \in \mathbb{R} \quad \varphi(x+y) = \varphi(x) \mathbin{\widetilde{+}} \varphi(y)$; $\quad \leftarrow$(donc $\varphi(0) = \widetilde{0}$)
(ii) $\forall x, y \in \mathbb{R} \quad \varphi(x \cdot y) = \varphi(x) \mathbin{\widetilde{\cdot}} \varphi(y)$; $\quad \leftarrow$(donc $\varphi(1) = \widetilde{1}$, car φ est injective)
(iii) $\forall x, y \in \mathbb{R} \quad \big(x \leq y \iff \varphi(x) \mathbin{\widetilde{\leq}} \varphi(y)\big)$.

Exemple de construction

On note : Majorées$(\mathbb{Q}) = \{X \subseteq \mathbb{Q} \mid X \neq \emptyset$ et X est majorée dans $\mathbb{Q}\}$.

Idée :



(ici en deux morceaux)

Un élément de $\mathbb{R}$ est un ensemble x de parties de $\mathbb{Q}$ tel qu'il existe $X \in$ Majorées$(\mathbb{Q})$ avec : $x = \big\{X' \in \text{Majorées}(\mathbb{Q}) \mid \{\text{majorants de } X' \text{ dans } \mathbb{Q}\} = \{\text{majorants de } X \text{ dans } \mathbb{Q}\}\big\}$.

On note : $x = \dot{0}$ quand $X = \mathbb{Q}^-$.

Quand $x \in \mathbb{R}$ est associé à X et $y \in \mathbb{R}$ est associé à Y, on définit :
$x \leq y \iff \{\text{majorants de } Y \text{ dans } \mathbb{Q}\} \subseteq \{\text{majorants de } X \text{ dans } \mathbb{Q}\}$;
$x + y = u$, où u est associé à $U := \{t \in \mathbb{Q} \mid \exists r \in X \ \exists s \in Y \ t = r + s\}$;
$xy = v$ si $x > \dot{0}$ et $y > \dot{0}$, où v est associé à $V := \{t \in \mathbb{Q} \mid \exists r \in X \cap \mathbb{Q}^+ \ \exists s \in Y \cap \mathbb{Q}^+ \ t = rs\}$.

On admet que ces définitions de « $x \leq y$ », « $x + y$ » et « xy » ne dépendent pas des choix de $X, Y \in$ Majorées$(\mathbb{Q})$ associés à x et y. On prolonge le produit par la règle des signes.

On peut montrer, laborieusement, que ce triplet $(\mathbb{R}, +, \cdot, \leq)$ est un corps des nombres réels.

Remarque

On « identifie » $\mathbb{N}$ à son image par l'injection $\begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{R} \\ n & \longmapsto & \underbrace{1 + \cdots + 1}_{n \text{ fois}} \end{array}$.

On constate que les lois $+$ et $\cdot$ et la relation $\leq$ dans $\mathbb{N}$, sont correctement traduites dans $\mathbb{R}$.

On posera dorénavant (changements de notations) :
$\mathbb{Z} = \{x \in \mathbb{R} \mid x \in \mathbb{N}$ ou $-x \in \mathbb{N}\}$ puis $\mathbb{Q} = \{x \in \mathbb{R} \mid \exists p \in \mathbb{Z} \quad \exists q \in \mathbb{N} \setminus \{0\} \quad x = \frac{p}{q}\}$.

(⋆) Démonstration dans le tome 3 du « Cours de mathématiques spéciales » de Ramis, Deschamps, Odoux.