Maths - MP2I

Axel Montlahuc

2024/2025

Chapitre 1

Calculs Algébriques

1.20 Somme des carrés et des cubes

— Somme des carrés :
Pour tout $n \in \mathbb{N}$, on note la proposition :

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

Démontrons-la par récurrence.

Initialisation : Pour $n = 0$, on a :

$$\sum_{k=1}^{0} k^2 = 0$$

et :

$$\frac{0 \times (0+1) \times (2 \times 0 + 1)}{6} = 0$$

Donc $P(0)$ est vraie.

Hérédité : On suppose $P(n)$ vraie pour un n fixé dans $\mathbb{N}$. On a :

$$\begin{aligned}
\sum_{k=1}^{n+1} k^2 &= \sum_{k=1}^{n} k^2 + (n+1)^2 \\
&= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\
&= \frac{n+1}{6}(n(2n+1) + 6(n+1)) \\
&= \frac{n+1}{6}(2n^2 + 7n + 6) \\
&= \frac{(n+1)(n+2)(2n+3)}{6}
\end{aligned}$$

Donc $P(n+1)$ est vraie aussi.

Conclusion : D'après le principe de récurrence,

$$\forall n \in \mathbb{N}, \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

— Somme des cubes :
Pour tout $n \in \mathbb{N}$, on note la proposition :

$$P(n) : « \sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4} »$$

Démontrons-la par récurrence.

Initialisation : Pour $n = 0$, on a :

$$\sum_{k=1}^{0} k^3 = 0$$

et :

$$\frac{0 \times (0+1)^2}{4} = 0$$

Donc $P(0)$ est vraie.

Hérédité : On suppose $P(n)$ vraie pour un n fixé dans $\mathbb{N}$. On a :

$$\begin{aligned}\sum_{k=1}^{n+1} k^3 &= \sum_{k=1}^{n} k^3 + (n+1)^3 \\ &= \frac{n^2(n+1)^2}{4} + (n+1)^3 \\ &= \frac{(n+1)^2}{4}(n^2 + 4(n+1)) \\ &= \frac{(n+1)^2}{4}(n^2 + 4n + 4) \\ &= \frac{(n+1)^2(n+2)^2}{4}\end{aligned}$$

Donc $P(n+1)$ est vraie aussi.

Conclusion : D'après le principe de récurrence,

$$\forall n \in \mathbb{N}, \sum_{k=1}^{n} k^2 = \frac{n^2(n+1)^2}{4}$$

1.39 Formule de Pascal

Démontrons pour tout $(n,p) \in (\mathbb{N}^*)^2$ la relation :

$$\text{« } \binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p} \text{ »}$$

La relation est vraie si $p > n$ (on a $0 = 0 + 0$) et si $p = n$ (qui donne $1 = 0 + 1$).

Soit $1 \leq p \leq n$:

$$\begin{aligned}\binom{n-1}{p} + \binom{n-1}{p-1} &= \frac{(n-1)!}{p!(n-1-p)!} + \frac{(n-1)!}{(p-1)!(n-p)!} \\ &= \frac{(n-1)!}{(p-1)!(n-1-p)!}\left(\frac{1}{p} + \frac{1}{n-p}\right) \\ &= \frac{(n-1)! \times n}{(p-1)!(n-1-p)! \times p(n-p)} \\ &= \frac{n!}{p!(n-p)!} \\ &= \binom{n}{p}\end{aligned}$$

1.41 Formule du capitaine

Démontrons pour n et p deux entiers tels que $1 \leq p \leq n$ la relation :

$$\text{« } n\binom{n-1}{p-1} = p\binom{n}{p} \text{ »}$$

On a :

$$n\binom{n-1}{p-1} = n \times \frac{(n-1)!}{(p-1)!(n-p)!} = p \times \frac{n!}{p!(n-p)!} = p\binom{n}{p}$$

1.42 Formule du binôme de Newton

Soit $(x,y) \in \mathbb{C}^2$. Pour tout $n \in \mathbb{N}$, on note la proposition :

$$P(n) : \text{« } (x+y)^n = \sum_{k=0}^{n} x^k y^{n-k} \text{ »}$$

Démontrons-la par récurrence.

Initialisation : Pour $n = 0$, on a :

$$(x+y)^0 = 1$$

et

$$\sum_{k=0}^{0} \binom{0}{k} x^k y^{0-k} = \binom{0}{0} x^0 y^0 = 1$$

Donc $P(0)$ est vraie.

Hérédité : On suppose $P(n)$ vraie pour un n fixé dans $\mathbb{N}$. On a :

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)(x+y)^n \\
&= (x+y) \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} && \textit{(hypothèse de récurrence)} \\
&= \sum_{k=0}^{n} \binom{n}{k} (x^{k+1} y^{n-k} + x^k y^{n+1-k}) && \textit{(linéarité)} \\
&= \sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n+1-k} \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} x^k y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n+1-k} && \textit{(translation)} \\
&= x^{n+1} + \sum_{k=1}^{n} x^k y^{n+1-k} \left(\binom{n}{k-1} + \binom{n}{k} \right) + y^{n+1} \\
&= x^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} x^k y^{n+1-k} + y^{n+1} && \textit{(formule de Pascal)} \\
&= \sum_{k=0}^{n+1} x^k y^{n+1-k}
\end{aligned}$$

Donc $P(n+1)$ est vraie aussi.

Conclusion : D'après le principe de récurrence,

$$\forall n \in \mathbb{N}, (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Chapitre 2

Logique

2.17 Equivalence logiques

2.17.1 Double négation

p	$\neg p$	$\neg(\neg p)$
V	F	V
F	V	F

On remarque que la première et la deuxième colonne sont identiques, on a donc :

$$p \iff \neg(\neg p)$$

2.17.2 Commutativité

p	q	$p \wedge q$	$q \wedge p$
V	V	V	V
V	F	F	F
F	V	F	F
F	F	F	F

On remarque que la troisième et la quatrième colonne sont identiques, on a donc :

$$p \wedge q \iff q \wedge p$$

Raisonnement analogue pour la disjonction $\vee$.

2.17.3 Associativité

p	q	r	$p \wedge q$	$(p \wedge q) \wedge r$	$q \wedge r$	$p \wedge (q \wedge r)$
V	V	V	V	V	V	V
V	V	F	V	F	F	F
V	F	V	F	F	F	F
V	F	F	F	F	F	F
F	V	V	F	F	V	F
F	V	F	F	F	F	F
F	F	V	F	F	F	F
F	F	F	F	F	F	F

On remarque que la cinquième et la septième colonne sont identiques, on a donc :

$$(p \wedge q) \wedge r \iff p \wedge (q \wedge r)$$

Raisonnement analogue pour la disjonction $\vee$.

2.17.4 Loi de Morgan

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$(\neg p) \vee (\neg q)$
V	V	V	F	F	F	F
V	F	F	V	F	V	V
F	V	F	V	V	F	V
F	F	F	V	V	V	V

On remarque que la quatrième et la septième colonne sont identiques, on a donc :

$$\neg(p \wedge q) \iff (\neg p) \vee (\neg q)$$

Raisonnement analogue pour $\neg(p \vee q) \iff (\neg p) \wedge (\neg q)$

2.17.5 Double implication

p	q	$p \Leftrightarrow q$	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$
V	V	V	V	V	V
V	F	F	F	V	F
F	V	F	V	F	F
F	F	V	V	V	V

On remarque que la troisième et la sixième colonne sont identiques, on a donc :

$$(p \Leftrightarrow q) \iff ((p \Rightarrow q) \wedge (q \Rightarrow p))$$

2.17.6 Distributivité

p	q	r	$p \wedge q$	$r \vee (p \wedge q)$	$r \vee p$	$r \vee q$	$(r \vee p) \wedge (r \vee q)$
V	V	V	V	V	V	V	V
V	V	F	V	V	V	V	V
V	F	V	F	V	V	V	V
V	F	F	F	F	V	F	F
F	V	V	F	V	V	V	V
F	V	F	F	F	F	V	F
F	F	V	F	V	V	V	V
F	F	F	F	F	F	F	F

On remarque que la cinquième et la huitième colonne sont identiques, on a donc :

$$r \vee (p \wedge q) \iff (r \vee p) \wedge (r \vee q)$$

Chapitre 3

Ensembles et applications

3.12 Propriétés du produit cartésien

Soit x et y. On a :

1.

$$\begin{aligned}(x,y) \in E \times F &\Leftrightarrow x \in E \text{ et } y \in F \\ \text{Donc } (x,y) \notin E \times F &\Leftrightarrow x \notin E \text{ ou } y \notin F\end{aligned}$$

2.

$$\begin{aligned}E \times F \neq \emptyset &\Leftrightarrow \exists (x,y) \in E \times F \\ &\Leftrightarrow \exists x \in E \text{ et } \exists y \in F \\ &\Leftrightarrow E \neq \emptyset \text{ et } F \neq \emptyset \\ &\Leftrightarrow \text{non } (E = \emptyset \text{ ou } F = \emptyset)\end{aligned}$$

3.

$$\begin{aligned}E \times F = F \times E &\Leftrightarrow \begin{cases} E \times F = F \times E \text{ et } E = \emptyset \\ E \times F = F \times E \text{ et } F = \emptyset \\ E \times F = F \times E \text{ et } E \neq \emptyset \text{ et } F \neq \emptyset \end{cases} \\ &\Leftrightarrow \begin{cases} E = \emptyset \text{ ou } F = \emptyset \\ E \neq \emptyset \text{ et } F \neq \emptyset \text{ et } \forall (x,y) \in E \times F, (x,y) \in F \times E \text{ et } \forall (a,b) \in F \times E, (a,b) \in E \times F \end{cases} \\ &\Leftrightarrow \begin{cases} E = \emptyset \text{ ou } F = \emptyset \\ E \neq \emptyset \text{ et } F \neq \emptyset \text{ et } \forall x \in E, x \in F \text{ et } \forall y \in F, y \in E \end{cases} \\ &\Leftrightarrow \begin{cases} E = \emptyset \text{ ou } F = \emptyset \\ E = F \end{cases}\end{aligned}$$

4.

$$\begin{aligned}(x,y) \in (E \times F) \cup (F \times G) &\Leftrightarrow (x,y) \in E \times F \text{ ou } (x,y) \in F \times G \\ &\Leftrightarrow (x \in E \text{ et } y \in F) \text{ ou } (x \in F \text{ et } y \in G) \\ &\Leftrightarrow x \in E \text{ et } y \in F \cup G\end{aligned}$$

5.

$$\begin{aligned}(x,y) \in (E \times F) \cap (G \times H) &\Leftrightarrow (x,y) \in E \times F \text{ et } (x,y) \in G \times H \\ &\Leftrightarrow x \in E \text{ et } y \in F \text{ et } x \in G \text{ et } y \in H \\ &\Leftrightarrow x \in E \cap G \text{ et } y \in F \cap H \\ &\Leftrightarrow (x,y) \in (E \cap G) \times (F \cap H)\end{aligned}$$

3.18 Associativité des relations

Les ensembles de départ et d'arrivée sont bien égaux (à E et H respectivement). Soit $(x,y) \in E \times H$

$$\begin{aligned}x(\mathcal{T} \circ \mathcal{S}) \circ \mathcal{R} y &\Leftrightarrow \exists z \in F, x(\mathcal{T} \circ \mathcal{S})z \text{ et } z\mathcal{R}y \\ &\Leftrightarrow \exists z \in F, \exists v \in G, (x\mathcal{T}v \text{ et } v\mathcal{S}z) \text{ et } z\mathcal{R}y \\ &\Leftrightarrow \exists z \in F, \exists v \in G, x\mathcal{T}v \text{ et } (v\mathcal{S}z \text{ et } z\mathcal{R}y) \\ &\Leftrightarrow \exists v \in G, x\mathcal{T}v \text{ et } v(\mathcal{S} \circ \mathcal{R})y \\ &\Leftrightarrow x\mathcal{T} \circ (\mathcal{S} \circ \mathcal{R})y\end{aligned}$$

3.20 Propriétés des relations réciproques

— RAF

— Les ensembles de départ sont égaux respectivement à E et à G.
Soit $(x, y) \in G \times E$. On a :

$$\begin{aligned} x\mathcal{R}^{-1} \circ \mathcal{S}^{-1} y &\Leftrightarrow \exists \alpha \in F, x\mathcal{S}^{-1}\alpha \text{ et } \alpha\mathcal{R}^{-1}y \\ &\Leftrightarrow \exists \alpha \in F, \alpha\mathcal{S}x \text{ et } y\mathcal{R}\alpha \\ &\Leftrightarrow y\mathcal{S} \circ \mathcal{R}x \\ &\Leftrightarrow x(\mathcal{R} \circ \mathcal{S})^{-1}y \end{aligned}$$

3.23 Composition de fonctions

Soit f une fonction de E vers F.
Soit g une fonction de E vers G.

$$g \circ f \text{ est une relation de } E \text{ vers } G$$

Soit $(x, y, y') \in E \times G \times G$. On suppose

$$\begin{cases} x(g \circ f)y \\ x(g \circ f)y' \end{cases}$$

Donc on choisit α dans F tel que :

$$xf\alpha \text{ et } \alpha gy$$

et β dans F tel que :

$$xf\beta \text{ et } \beta gy'$$

Or f est une fonction, donc $\alpha = \beta$.
Donc αgy et $\alpha gy'$, or g est une fonction, donc $y = y'$. Par définition, $g \circ f$ est une fonction.

3.30 Schémas de raisonnement : montrer l'injectivité/surjectivité/bijectivité

Injectivité :
Soit $(x, x') \in E^2$.
On suppose que $f(x) = f(x')$.
$\vdots$
Donc $x = x'$.

Surjectivité :
Soit $y \in F$.
$\vdots$
On choisit ... tel que :
$\vdots$
Donc$f(x) = y$

Bijectivité :
Pour la bijectivité, on montre l'injectivité et la surjectivité séparément.

3.35 Composée d'injections/surjections

Soit $f : E \to F$ et $g : F \to G$.

— On suppose que f et g sont injectives.
Soit $(x,x') \in E^2$.

$$\begin{aligned} \text{On suppose que } g\circ f(x) &= g\circ f(x') \\ \text{Donc } g(f(x)) &= g(f(x')) \\ \text{Donc } f(x) &= f(x') && \text{(g est injective)} \\ \text{Donc } x &= x' && \text{(f est injective)} \end{aligned}$$

— On suppose que f et g sont surjectives.
Soit $y \in G$.
Par surjectivité de g, on choisit $\alpha \in F$ tel que $g(\alpha) = y$.
Par surjectivité de f, on choisit $x \in E$ tel que $f(x) = \alpha$.
Donc $g \circ f(x) = y$.
Donc $g \circ f$ est surjective.

3.36 Condition nécessaire pour une composition injective/surjective

— Soit $(x,x') \in E^2$ tels que :

$$\begin{aligned} f(x) &= f(x') \\ \text{Donc } g(f(x)) &= g(f(x')) \\ \text{Donc } x &= x' \end{aligned}$$

Donc f est injective.

— On suppose $g \circ f$ surjective.
Soit $y \in G$. Soit $\alpha \in E$ tel que $g \circ f(\alpha) = y$.
On pose $x = f(\alpha) \in F$.
Donc $g(x) = y$ Donc g est surjective.

3.37 Réciproque et bijection

Soit $f : E \to F$ et f^{-1} la relation réciproque de f
— f^{-1} est une fonction si et seulement si f est injective.
— Si f^{-1} est une fonction, c'est une application.
ssi. $Def(f^{-1}) = F$
ssi. f est surjective.

3.38 Inverse d'une composée de bijections

Propositions (3.35), (3.27) et (3.20)

3.39 Condition nécessaire et suffisante de bijectivité

$\boxed{\Rightarrow}$
On suppose que f est bijective.
On pose $g = f^{-1}$ sa bijection réciproque.
On a bien $g \circ f = id_E$ et $f \circ g = id_F$.

$\boxed{\Leftarrow}$
Soit $g : F \to E$ vérifiant $g \circ f = id_E$ et $f \circ g = id_F$.
En particulier, $g \circ f$ est injective, donc f est injective.
En particulier, $f \circ g$ est surjective, donc f est surjective.
Donc f est bijective.
Or $f \circ g = id_F$.
Donc $f^{-1} \circ f \circ g = f^{-1} \circ id_F$.
Soit $g = f^{-1}$.

Chapitre 4

Généralités sur les fonctions

4.21 Exemple

On suppose que $f \geq g$. Ainsi :

$$|f-g| = f-g \Leftrightarrow \frac{f+g+|f-g|}{2} = f$$

4.23 Remarque

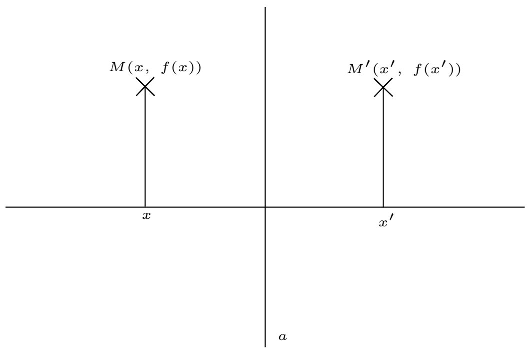
Soit $a \in \mathbb{Q}^*$. Soit $x \in \mathbb{R}$.
— Si $x \in \mathbb{Q}$, alors $x+a \in \mathbb{Q}$, donc $\mathbb{1}_{\mathbb{Q}}(x+a) = 1 = \mathbb{1}_{\mathbb{Q}}(x)$.
— Si $x \notin \mathbb{Q}$, alors $x+a \notin \mathbb{Q}$, donc $\mathbb{1}_{\mathbb{Q}}(x+a) = 0 = \mathbb{1}_{\mathbb{Q}}(x)$.

4.27 Axe de symétrie

Soit $f : I \to \mathbb{R}$ une fonction et $\mathcal{C}_f$ sa courbe représentative.
Soit $(x, x') \in I^2$.
M et M' sont symétriques par rapport $x = a$

ssi. $\begin{cases} a = \frac{x+x'}{2} \\ f(x) = f(x') \end{cases}$

ssi. $\begin{cases} x' = 2a - x \\ f(x) = f(x') \end{cases}$



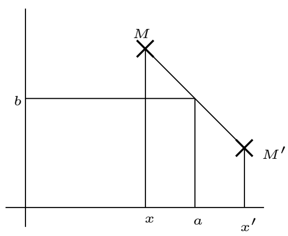
4.28 Centre de symétrie

On reprend les mêmes notations qu'à la (4.27).

M et M' sont symétriques par rapport à $A(a, b)$

ssi. $\begin{cases} a = \frac{x+x'}{2} \\ b = \frac{f(x)+f(x')}{2} \end{cases}$

ssi. $\begin{cases} x' = 2a - x \\ f(x') = 2b - f(x) \end{cases}$



4.51 Exemple

1. $f'(x) = -\frac{2x+1}{(x+x^2)^2}$
2. $f'(x) = -\frac{1}{2x\sqrt{x}} e^{\frac{1}{\sqrt{x}}}$
3. $f'(x) = -3\frac{e^x(x-1)}{x^2} \sin\left(\frac{e^x}{x}\right) \cos^2\left(\frac{e^x}{x}\right)$

4.52 Théorème de la bijection dérivable

On suppose la dérivabilité de f^{-1}. Par définition :

$$f \circ f^{-1} = \mathrm{Id}_I$$

D'après la proposition (4.48.4), on a :

$$\begin{aligned}(f^{-1})' \circ f' \times f^{-1} &= (f \circ f^{-1})' \\ &= \mathrm{Id}_I' \\ &= 1\end{aligned}$$

Comme f ne s'annule pas sur I, on a :

$$(f^{-1})' = \frac{1}{f' \circ f^{-1}}$$

4.61 Primitives d'une fonction sur un intervalle

— Si F et G sont deux primitives de f sur l'intervalle I, alors :

$$\begin{aligned} \forall n \in I, (F-G)'(x) &= F'(x) - G'(x) \\ &= f(x) - f(x) \\ &= 0 \end{aligned}$$

Comme I est un intervalle, $F - G$ est constante (4.53).
Réciproquement, pour tout $a \in \mathbb{R}$, $F + a$ est aussi une primitive de f sur I.

— Soit G une primitive de f sur I. Soit $a \in \mathbb{R}$ et $x_0 \in I$. Or pour $F = G + a - G(x_0)$, F est une primitve de f sur I et $F(x) = a$.
L'unicité est donnée par le point précédent.

4.62 Exemple

1. Sur $I = \left]-\frac{\pi}{2}; \frac{\pi}{2}\right[$.
Pour tout $x \in I$,

$$\begin{aligned} \tan x &= \frac{\sin x}{\cos x} \\ &= -\frac{-\sin x}{\cos x} \end{aligned}$$

La primitive de tan sur I est : $x \mapsto -\ln|\cos x| = \ln \cos x$.

2. Sur $I = \left]-\frac{\pi}{2}; \frac{\pi}{2}\right[$.

$$\forall x \in I, \tan^2 x = \tan^2 x + 1 - 1$$

Une primitive de $\tan^2$ sur I est : $x \mapsto \tan x - x$.

3. Sur $I = \mathbb{R}$.

$$\begin{aligned} \forall x \in \mathbb{R}, x\sqrt{1+x^2} &= x(1+x^2)^{\frac{1}{2}} \\ &= \frac{1}{2} \times 2x \times (1+x^2)^{\frac{1}{2}} \end{aligned}$$

Une primitive de $x \mapsto x(1+x^2)^{\frac{1}{2}}$ sur $\mathbb{R}$ est : $x \mapsto \frac{1}{2} \times \frac{2}{3}(1+x^2)^{\frac{3}{2}} = \frac{1}{3}(1+x^2)^{\frac{3}{2}}$.

4. Sur $I = \mathbb{R}_+^*$.

$$\forall x > 0, \frac{\ln x}{x} = \frac{1}{x} \ln x$$

Une primitive de $x \mapsto \frac{\ln x}{x}$ sur $\mathbb{R}_+^*$ est : $x \mapsto \frac{1}{2} \ln^2 x$.

4.65 Remarque

$G : y \mapsto yg(y) - F(g(y)) + \lambda, \lambda \in \mathbb{R}$.

$$\begin{aligned} G'(y) &= g(y) + yg'(y) - g'(y)f(g(y)) \\ &= g(y) + \cancel{yg'(y)} - \cancel{g'(y)y} \\ &= g(y) \end{aligned}$$

4.66 Exemple

$$\begin{aligned}
\left| \int_{-1}^{1} \frac{t^n}{1+t^2}\, dt \right| &\leq \int_{-1}^{1} \frac{|t^n|}{1+t^2}\, dt && \text{(Inégalité triangulaire)} \\
&\leq \int_{-1}^{1} |t|^n \, dt && (\forall t, \frac{|t|^n}{1+t^2} \leq |t|^n) \\
&= (-1)^n \int_{-1}^{0} t^n \, dt + \int_{0}^{1} t^n \, dt && \text{(Relation de Chasles)} \\
&= (-1)^n \left[\frac{t^{n+1}}{n+1} \right]_{-1}^{0} + \left[\frac{t^{n+1}}{n+1} \right]_{0}^{1} \\
&= -\frac{(-1)^n(-1)^{n+1}}{n+1} + \frac{1}{n+1} \\
&= \frac{2}{n+1}
\end{aligned}$$

4.69 Intégration par partie

$$\begin{aligned}
\int_a^b f'(t)g(t)\, dt + \int_a^b f(t)g'(t)\, dt &= \int_a^b (f'(t)g(t) + f(t)g'(t))\, dt \\
&= \int_a^b (fg)'(t)\, dt \\
&= [f(t)g(t)]_a^b
\end{aligned}$$

4.70 Changement de variable

Comme f est une fonction continue sur $[a,b]$, on choisit une primitive F de f sur $[a,b]$. (Théorème fondamental du calcul in
Ainsi :

$$\begin{aligned}
\int_{u(a)}^{u(b)} f(t)\, dt &= [F(t)]_{u(a)}^{u(b)} \\
&= F \circ u(b) - F \circ u(a)
\end{aligned}$$

Or :

$$\begin{aligned}
\int_a^b f(u(t))u'(t)\, dt &= \int_a^b F'(u(t)) \times u'(t)\, du(t) \\
&= [F \circ u(t)]_a^b
\end{aligned}$$

4.72 Exemple

Si $x = \sin t$, alors $dx = \cos t \, dt$.
Pour $t = 0$, $x = \sin 0 = 0$.
Pour $t = \frac{\pi}{2}$, $x = \sin \frac{\pi}{2} = 1$.
Or $t \mapsto \sin t \in \mathcal{C}^1(\left[0; \frac{\pi}{2}\right], \mathbb{R})$.

D'après le théorème de changement de variable :

$$\begin{aligned}\int_0^1 \sqrt{1-x^2}\,dx &= \int_0^{\frac{\pi}{2}} \sqrt{1-\sin^2 t}\cos t\,dt \\ &= \int_0^{\frac{\pi}{2}} \sqrt{\cos^2 t}\cos t\,dt \\ &= \int_0^{\frac{\pi}{2}} \cos^2 t\,dt \\ &= \int_0^{\frac{\pi}{2}} \frac{1+\cos 2t}{2}\,dt \\ &= \left[\frac{1}{4}\sin 2t\right]_0^{\frac{\pi}{2}} + \frac{\pi}{4} \\ &= \frac{\pi}{4}\end{aligned}$$

4.74 Méthode

Pour tout $x \in \mathbb{R}\backslash\{a;b\}$, trouver c et d tel que $\frac{\alpha x+\beta}{(x-a)(x-b)} = \frac{c}{x-a} + \frac{d}{x-b}$:

$$\begin{aligned}\frac{\alpha x+\beta}{(x-b)} &= c + \frac{d(x-a)}{(x-b)} && \text{(On multiplie par } (x-a)\text{)} \\ c &= \frac{\alpha a+\beta}{a-b} && (x=a) \\ d &= \frac{\alpha b+\beta}{b-a} && (x=b)\end{aligned}$$

4.75 Exemple

$$f : x \mapsto \frac{2x-1}{(x+1)(x-3)} = \frac{4}{3(x+1)} + \frac{4}{5(x-3)}$$

Une primitive de f sur $]-1;3[$ est : $x \mapsto \frac{3}{4}\ln|x+1| + \frac{5}{4}\ln|x-3| = \frac{3}{4}\ln(x+1) + \frac{5}{4}\ln(x-3)$

Chapitre 5

Fonctions usuelles

5.2 Propriétés du logarithme

Par définition, ln est définie et dérvable sur $\mathbb{R}_+^*$ et :

$$\forall x > 0, \ln'(x) = \frac{1}{x}$$

On montre par récurrence sur $n \geq 1$ que

$$\text{"ln est dérivable } n \text{ fois et } \forall n > 0, \ln^{(n)}(x) = \frac{(-1)^{n-1}(n-1)!}{x^n}\text{"}$$

<u>Initialisation :</u>
La propriété est vraie pour $n = 1$.

<u>Hérédité :</u>
Si elle est vraie pour $n \geq 1$, par théorème d'opérations, $\ln^{(n)}$ est encore dérivable et :

$$\begin{aligned}\forall x > 0, ln^{(n+1)}(x) &= \left[\ln^{(x)}\right](x)\\ &= (-1)^n n! x^{-n-1}\end{aligned}$$

Comme $\ln' > 0$ sur $\mathbb{R}_+^*$, alors ln est strictement croissante sur $\mathbb{R}_+^*$.

5.3 Propriété fondamentale du logarithme

On montre seulement la propriété pour $a > 0$ et $b > 0$.
On fixe $b > 0$ et on considère :

$$f : \mathbb{R}_+^* \to \mathbb{R}; x \mapsto \ln(xb)$$

Par composition, $f \in \mathcal{D}^1(\mathbb{R}_+^*, \mathbb{R})$ et :

$$\forall x > 0, f'(x) = b \times \frac{1}{xb} = \frac{1}{x}$$

Donc f est une primitive de $\frac{1}{x}$ sur $\mathbb{R}_+^*$.
On choisit $c \in \mathbb{R}$ tel que :

$$f = \ln + c$$

En particulier :

$$f(1) = \ln 1 + c$$

Soit :

$$\ln b = c$$

Ainsi :

$$\forall x > 0, \ln(xb) = \ln x + \ln b$$

On a par conséquent :

$$\begin{aligned}\forall x \in \mathbb{R}_+^*, 0 &= \ln 1\\ &= \ln(x \times \frac{1}{x})\\ &= \ln x + \ln \frac{1}{x}\end{aligned}$$

Donc pour $a > 0$ et $b > 0$, on a :

$$\begin{aligned}\ln\left(\frac{a}{b}\right) &= \ln\left(a \times \frac{1}{b}\right)\\ &= \ln a + \ln\frac{1}{b}\\ &= \ln a - \ln b\end{aligned}$$

5.4 Limites usuelles de la fonction logarithme

On commence par montrer que :

$$\ln x \underset{x\to+\infty}{\longrightarrow} +\infty$$

On sait que ln est croissante sur $\mathbb{R}_+^*$, donc d'après le théorème de la limite monotone :

$$\ln x \underset{x\to+\infty}{\longrightarrow} +\infty \qquad \text{ou} \qquad \ln x \underset{x\to+\infty}{\longrightarrow} \lambda$$

Soit $n \geq 1$. On a :

$$\begin{aligned}\ln n &= \int_1^n \frac{dt}{t}\\ &= \sum_{k=1}^{n-1}\int_k^{k+1}\frac{dt}{t}\\ &\geq \sum_{k=1}^{n-1}\int_k^{k+1}\frac{dt}{k+1}\\ &= \sum_{k=1}^{n-1}\frac{1}{k+1}\\ &= \sum_{k=1}^{n}\left(\frac{1}{k}\right) - 1\end{aligned}$$

Or :

$$\sum_{k=1}^{n}\left(\frac{1}{k}\right) - 1 \underset{n\to+\infty}{\longrightarrow} +\infty$$

Par théorème de comparaison :

$$\ln n \underset{n\to+\infty}{\longrightarrow} +\infty$$

Donc :

$$\ln x \underset{x\to+\infty}{\longrightarrow} +\infty$$

Enfin :

$$\forall x > 0, \ln x = -\ln\left(\frac{1}{x}\right)$$

Donc par composition :

$$\ln x \underset{x\to 0^+}{\longrightarrow} -\infty$$

Par taux d'accroissement, en introduisant :

$$\begin{aligned}f : \mathbb{R}_+ \to \mathbb{R}; x \mapsto \ln(1+x)\\ f \in \mathcal{D}^1(\mathbb{R}_+, \mathbb{R})\\ \frac{\ln(x+1)}{x} = \frac{f(x)-f(0)}{x-0} \underset{x\to 0}{f'(0)} = 1\end{aligned}$$

5.8 Propriétés de la fonction exponentielle

D'après les résultas précédents (5.2), (5.4), on applique le théorème de la bijection dérivable. La fonction exponentielle est dérivable sur $\mathbb{R}$ et :

$$\begin{aligned}\forall x \in \mathbb{R}, \exp' x &= \frac{1}{\ln' \circ \exp x} \\ &= \exp x\end{aligned}$$

On obtient directement que $\exp \in \mathcal{C}^{\infty}(\mathbb{R}, \mathbb{R}_+^*)$ et que $\exp^{(n)} = \exp n$ pour tout $n \in \mathbb{N}$.

5.9 Propriété fondamentale de l'exponentielle

Soit $(x, y) \in \mathbb{R}^2$. On choisit $(a, b) \in (\mathbb{R}_+^*)^2$ tel que :

$$x = \ln a \text{ et } y = \ln b$$

Ainsi :

$$\begin{aligned}\exp(x+y) &= \exp(\ln a + \ln b) \\ &= \exp(\ln(ab)) \\ &= ab \\ &= \exp x \times \exp y\end{aligned}$$

Ainsi, $\exp 0 = \exp(0+0) = \exp^2 0$.
Donc $\exp 0 \in \{0; 1\}$
Or exp est à valeur dans $\mathbb{R}_+^*$, donc $\exp 0 = 1$, donc :

$$\forall x \in \mathbb{R}_+^*, \exp 0 = \exp(x-x) = \exp x \times \exp(-x) = 1$$

5.15 Dérivée d'une fonction puissance

Soit $y > 0$. On pose $f : \mathbb{R} \to \mathbb{R}; x \mapsto y^x = \exp(x \ln y)$.
$f \in \mathcal{D}^1(\mathbb{R}, \mathbb{R})$, donc par composition :

$$\begin{aligned}\forall x \in \mathbb{R}, f'(x) &= \ln y \times \exp(x \ln y) \\ &= \ln y \times y^x\end{aligned}$$

5.21 Croissances comparées en $+\infty$

1. On commence par montrer que $\frac{\ln x}{x} \underset{x \to +\infty}{\longrightarrow} 0$.
   Soit $x \geq 1$. On a :

$$\begin{aligned}0 \leq \frac{\ln x}{x} &= \frac{1}{x} \int_1^x \frac{dt}{t} \\ &\leq \frac{1}{x} \int_1^x \frac{dt}{\sqrt{t}} \\ &= \frac{1}{x} \left[2\sqrt{t}\right]_1^x \\ &= \frac{2(\sqrt{x}-1)}{x} \\ &= 2\left(\frac{1}{\sqrt{x}} - \frac{1}{x}\right) \\ &\underset{x \to +\infty}{\longrightarrow} 0\end{aligned}$$

   D'après le théorème d'encadrement, $\frac{\ln x}{x} \underset{x \to +\infty}{\longrightarrow} 0$.
   Soit $a > 0$ et $x > 0$:

$$\frac{\ln x}{x^a} = \frac{1}{a} \times \frac{\ln x^a}{x^a} \underset{x \to +\infty}{\longrightarrow} 0 \qquad \text{(composition et théorème d'opérations)}$$

2. On utilise le changement de variable :

$$x = (\ln y)^{\frac{1}{a}}, \text{ soit } y = e^{ax}$$

Ainsi :

$$\frac{x^a}{e^x} = \frac{\ln y}{y^{\frac{1}{a}}} \underset{x\to+\infty}{\longrightarrow} \begin{cases} 0 \text{ par composition si } a > 0 \\ 0 \text{ par théorème d'opérations si } a \leq 0 \end{cases}$$

5.22 Croissances comparées en 0

On utilise la proposition (5.21.1) avec $y = \frac{1}{x}$.

5.43.2 Formule de trigonométrie hyperbolique

Soit $(a, b) \in \mathbb{R}^2$.

$$\begin{aligned} ch(a)ch(b) + sh(a)sh(b) &= \frac{(e^a + e^{-a})(e^b + e^{-b})}{4} + \frac{(e^a - e^{-a})(e^b - e^{-b})}{4} \\ &= \frac{2e^{a+b} + 2e^{-(a+b)}}{4} \\ &= ch(a + b) \end{aligned}$$

Chapitre 10

Structures algébriques

10.3 Exemple

Exemple

Soit $E =]-1;1[$. Pour $(x,y) \in E^2$, on pose : $x \star y = \frac{x+y}{1+xy}$. Montrer que l'on définit ainsi une lci dans E.

On fixe $y \in E$. On note $\varphi : [-1;1] \to \mathbb{R}; x \mapsto x \star y = \frac{x+y}{1+xy}$.
$\varphi \in \mathcal{D}^1([-1;1], \mathbb{R})$ et :

$$\begin{aligned}\forall x \in E, \varphi'(x) &= \frac{1+xy-y(x+y)}{(1+xy)^2} \\ &= \frac{1-y^2}{(1+xy)^2} \\ &> 0\end{aligned}$$

Comme E est un intervalle : φ est strictement croissante sur E et :

$$\forall x \in E, -1 = \varphi(-1) < \varphi(x) < \varphi(1) = 1$$

Donc :

$$\forall (x,y) \in E^2, x \star y \in E$$

10.6 Exemple

Exemple

Soit $E =]-1;1[$. Pour $(x,y) \in E^2$, on pose $x \star y = \frac{x+y}{1+xy}$. Montrer que $\star$ est associative et commutative.

- Commutativité : RAF
- Associativité :
  Soit $(x,y,z) \in E^3$. On a :

$$\begin{aligned}x \star (y \star z) &= x \star \left(\frac{y+z}{1+yz}\right) \\ &= \frac{x + \frac{y+z}{1+yz}}{1 + x\frac{y+z}{1+yz}} \\ &= \frac{x(1+yz)+y+z}{1+yz+xy+xz} \\ &= \frac{x+y+z+xyz}{1+yz+xy+xz}\end{aligned}$$

  C'est une expression symétrique en x, y et z donc :

$$x \star (y \star z) = (x \star y) \star z$$

Chapitre 11

Matrices

11.11 Produit matriciel

$$\begin{pmatrix} 2 & 8 & 4 \\ -1 & -1 & -1 \\ 2 & 0 & 0 \end{pmatrix}$$

$$AB = \begin{pmatrix} 1 & 2 & -1 \\ -1 & 2 & 5 \end{pmatrix} \begin{pmatrix} -2 & 6 & 2 \\ 6 & -10 & -6 \end{pmatrix}$$

11.12 Produit matriciel, lignes par colonnes

— $A = (a_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}}$ et $C_i = \begin{pmatrix} 0 \\ \vdots \\ i \\ \vdots \\ 0 \end{pmatrix} = (\delta_{ij})_{1 \leq j \leq p} \in \mathcal{M}_{p,1}(\mathbb{K})$

$$\begin{aligned} (AC_i)_{k,1} &= \sum_{l=1}^{p} a_{kl} (C_i)_{l,1} \\ &= \sum_{l=1}^{p} a_{kl} \delta_{il} \\ &= a_{ki} \end{aligned}$$

— $L_j = \begin{pmatrix} 0 & \dots & 1 & \dots & 0 \end{pmatrix} = (\delta_{ji})_{1 \leq i \leq n}$

$$\begin{aligned} (L_j A)_{1k} &= \sum_{l=1}^{n} (L_j)_{1,e} \times a_{ek} \\ &= \sum_{l=1}^{n} \delta_{je} a_{lk} \\ &= a_{jk} \end{aligned}$$

— On note $A = \begin{pmatrix} C_1 & | \dots | & C_p \end{pmatrix}$ et $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} = \sum_{k=1}^{p} x_k \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$

$$AX = \sum_{k=1}^{p} x_k A \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = \sum_{k=1}^{p} x_{kC_k}$$

11.16 Produit de deux matrices élémentaires

Soit $1 \leq k \leq n ; 1 \leq l \leq m$

$$\begin{aligned} (E_{ij} \times E_{rs})_{k,l} &= \sum_{p=1}^{t} (E_{ij})_{kp} \times (E_{rs})_{pl} \\ &= \sum_{p=1}^{t} \delta_{ik} \delta_{pj} \delta_{rp} \delta_{sl} \\ &= \delta_{rj} \delta_{ik} \delta_{sl} \\ &= \delta_{rj} (E_{is})_{kl} \end{aligned}$$

Donc $E_{ij} \times E_{rs} = \delta_{jr} E_{is}$

11.17 Propriétés du produit matriciel, matrice identité

— Soit $(A, B, C) \in \mathcal{M}_{i,p}(\mathbb{K}) \times \mathcal{M}_{q,r}(\mathbb{K})$

$$\begin{aligned}
(AB)_{ij} &= \sum_{k=1}^{p} A_{ik} B_{kj} \\
[(AB)C]_{il} &= \sum_{t=1}^{q} (AB)_{it} C_{tl} \\
&= \sum_{t=1}^{q} \sum_{k=1}^{p} A_{ik} B_{kt} C_{tl} \\
&= \sum_{k=1}^{p} A_{ik} \sum_{t=1}^{q} B_{kt} C_{tl} \\
&= \sum_{k=1}^{p} A_{ik} (BC)_{kl} \\
&= (A(BC))_{il}
\end{aligned}$$

— RAF
— RAF

11.24 Exemple

On écrit $A = I_3 + N$ avec $N = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

$$N^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Soit $k \in \mathbb{N}$. Comme I_3 et N commutent,

$$\begin{aligned}
A^k &= (I_3 + N)^k \\
&= \sum_{i=0}^{k} \binom{k}{i} N^i && \text{(Binôme de Newton)} \\
&= I_3 + \binom{k}{1} N && (N^2 = 0) \\
&= I_3 + kN \\
&= \begin{pmatrix} 1 & k & 2k \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}$$

11.25 Produit par bloc

On le fait pour un bloc. Soit $1 \leq i \leq n$ et $1 \leq j \leq s$.

$$\begin{aligned}
\left[\begin{pmatrix} A & C \\ B & D \end{pmatrix} \begin{pmatrix} A' & C' \\ B' & D' \end{pmatrix} \right]_{i,j} &= \sum_{k=1}^{p+q} \begin{pmatrix} A & C \\ B & D \end{pmatrix}_{ik} \begin{pmatrix} A' & C' \\ B' & D' \end{pmatrix}_{kj} \\
&= \sum_{k=1}^{p} \begin{pmatrix} A & C \\ B & D \end{pmatrix}_{ik} \begin{pmatrix} A' & C' \\ B' & D' \end{pmatrix}_{kj} + \sum_{k=p+1}^{p+q} \begin{pmatrix} A & C \\ B & D \end{pmatrix}_{ik} \begin{pmatrix} A' & C' \\ B' & D' \end{pmatrix}_{kj} \\
&= \sum_{k=1}^{p} A_{ik} A'_{kj} + \sum_{k=1}^{q} C_{ik} B_{kj} \\
&= (AA' + CB')_{ij}
\end{aligned}$$

11.27 Propriétés de la transposition

— RAF
— RAF
— Soit $(i,j) \in [\![1,q]\!] \times [\![1,n]\!]$

$$\begin{aligned}[^t(AB)]_{ij} &= (AB)_{ji} \\ &= \sum_{k=1}^{p} A_{jk}B_{ki} \\ &= \sum_{k=i}^{p} [^tB]_{ik}[^tA]_{kj} \\ &= [^tB^tA]_{ij}\end{aligned}$$

11.31 Forme linéaire sur $\mathcal{M}_n(\mathbb{K})$

Soit $(A,B) \in \mathcal{M}_n(\mathbb{K})^2$, $\lambda \in \mathbb{K}$.
— Trace d'une somme de matrices :

$$\begin{aligned}tr(A+B) &= \sum_{i=1}^{n}(A+B)_{ii} \\ &= \sum_{i=1}^{n} A_{ii} + B_{ii} \\ &= \sum_{i=1}^{n} A_{ii} + \sum_{i=1}^{n} B_{ii} \\ &= tr(A) + tr(B)\end{aligned}$$

— Trace d'un produit par un scalaire :

$$\begin{aligned}tr(\lambda A) &= \sum_{i=1}^{n}(\lambda A)_{ii} \\ &= \lambda \sum_{i=1}^{n} A_{ii} \\ &= \lambda tr(A)\end{aligned}$$

— Trace d'un produit de matrices :

$$\begin{aligned}tr(AB) &= \sum_{i=1}^{n}(AB)_{ii} \\ &= \sum_{i=1}^{n}\sum_{k=1}^{n} A_{ik}B_{ki} \\ &= \sum_{k=1}^{n}\sum_{i=1}^{n} B_{ki}A_{kj} \\ &= \sum_{k=1}^{n}(BA)_{kk} \\ &= tr(BA)\end{aligned}$$

11.33 Exemple

On suppose A et B solutions.
Donc $AB - BA = I_n$
Donc $tr(AB - BA) = tr(I_n) = n$
Or $tr(AB - BA) = 0$
Absurde.

11.37 Stabilité des matrices diagonales ou triangulaires

On montre le résultat pour les matrices triangulaires supérieures (ensemble noté $\mathcal{T}_n^+(\mathbb{K})$).
Soit $(A, B) \in \mathcal{T}_n^+(\mathbb{K})^2$. On a bien $A + B \in \mathcal{T}_n^+(\mathbb{K})$ et aussi $\lambda A \in \mathcal{T}_n^+(\mathbb{K})$ pour tout $\lambda \in \mathbb{K}$
Soit $i > j$, on a :

$$(AB)_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj}$$

— Si $i > j$, $A_{ik} = 0$.
— Si $i = j$, $B_{kj} = 0$.

Donc $(AB)_{ij} = 0$.
Donc $AB \in \mathcal{T}_n^+(\mathbb{K})$.

Si $(AB) \in \mathcal{T}_n^+(\mathbb{K})^2$, alors ${}^t(AB) = \underbrace{{}^tB}_{\in \mathcal{T}_n^+(\mathbb{K})} \times \underbrace{{}^tA}_{\in \mathcal{T}_n^+(\mathbb{K})} \in \mathcal{T}_n^+(\mathbb{K})$
Donc $AB \in \mathcal{T}_n^+(\mathbb{K})$

Le résultat est vrai pour les matrices diagonales, à la fois triangulaires supérieures et inférieures.

11.41 Nilpotence des matrices triangulaires

Soit $T \in \mathcal{T}_n^{++}(\mathbb{K})$.
On va montrer par récurrence sur $k \in [\![1, n]\!]$ que :

$$\text{" } T^k = \begin{pmatrix} O & - & O & - & \triangle \\ & & & & | \\ & & & & O \\ & & & & | \\ & & & & O \end{pmatrix} \text{ "}$$

C'est-à-dire que pour tout $(i, j) \in [\![1, n]\!]^2, i + k - 1 \geq j \Rightarrow T_{ij}^k = 0$.
On suppose le résultat vrai pour $k \in [\![1, n-1]\!]$.
Soit $i + k \geq j$.

$$\begin{aligned} (T^{k+1})_{ij} &= (T^k T)_{ij} \\ &= \sum_{p=1}^{n} T_{ip}^k T_{pj} \end{aligned}$$

— Si $p \leq i + k - 1$, $T_{ip}^k = 0$
— Si $p \geq i + k$, $T_{pj} = 0$

Donc $(T^{k+1})_{ij} = 0$.
Par réccurence, $P(k)$ est vrai pour tout $k \in [\![1, n]\!]$. En particulier, pour $k = n$, on obtient $T^n = 0$.

11.44 Opérations

— ${}^tA \times^t (A^{-1}) =^t (A^{-1}A) =^t I_n = I_n$
— ${}^t(A^{-1}) \times^t A =^t (AA^{-1}) =^t I_n = I_n$

Donc$({}^tA)^{-1} =^t (A^{-1})$

11.48 Caractérisation de $GL_2(\mathbb{K})$

On note $M = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ et $N = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$.

$$\begin{aligned} M.N &= \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \\ &= \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} \\ &= det(M)I_2 \end{aligned}$$

— Si $det(M) \neq 0$, alors $M \times \left(\frac{1}{det(M)}N\right) = I_2$. Donc M est inversible et $M^{-1} = \frac{1}{det(M)}N$.
— Si $det(M) = 0$, alors $M.N = 0$ donc M n'est pas inversible.

11.49 Matrices diagonales inversibles

Soit $D = Diag(\lambda_1, \dots, \lambda_n)$.

$\boxed{\Leftarrow}$
On suppose que :

$$\forall i \in [\![1, n]\!], \lambda_i \neq 0$$

$$\begin{aligned} D \times Diag(\lambda_1^{-1}, \dots, \lambda_n^{-1}) &= Diag(\lambda_1 \times \lambda_1^{-1}, \dots, \lambda_n \times \lambda_n^{-1}) \\ &= Diag(1, \dots, 1) \\ &= I_n \end{aligned}$$

Donc D est inversible et

$$D^{-1} = Diag(\lambda_1^{-1}, \dots, \lambda_n^{-1})$$

$\boxed{\Rightarrow}$
Par contraposée, soit $i \in [\![1, n]\!]$ tel que $\lambda_i = 0$.

$$D \times Diag(0, \dots, \underbrace{1}_{i^{\text{ème}} \text{ place}}, \dots, 0) = 0$$

Donc D est un diviseur de 0, donc D n'est pas inversible.

11.50 Exemple

On a :

$$\begin{pmatrix} 1 & & & a_{1n} \\ & \ddots & & \vdots \\ & & \ddots & a_{n-1,n} \\ & & & 1 \end{pmatrix} \times \begin{pmatrix} 1 & & & -a_{1n} \\ & \ddots & & \vdots \\ & & \ddots & -a_{n-1,n} \\ & & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \vdots \\ & & \ddots & 0 \\ & & & 1 \end{pmatrix}$$

11.51 Matrices triangulaires inversibles

On raisonne par récurrence forte sur $n \in \mathbb{N}^*$.
Pour $n = 1$ RAF.

Pour $n = 2$, RAS (11.48).
On suppose le résultat vrai pour $n \in \mathbb{N}^*$.
Soi $T \in \mathcal{T}_{n+1}^+(\mathbb{K})$. Donc T est de la forme :

$$T = \begin{pmatrix} \mathcal{U} & X \\ 0 & a \end{pmatrix} \qquad \text{avec } \mathcal{U} \in \mathcal{T}_n^+(\mathbb{K}),\ X \in \mathcal{M}_{n,1}(\mathbb{K}) \text{ et } a \in \mathbb{K}$$

$\boxed{\Rightarrow}$

On suppose que la diagonale de T ne contient aucun 0.
Donc $\mathcal{U}$ est inversible d'après l'hypothèse de réccurence.
On choisit $V \in \mathcal{T}_n^+(\mathbb{K})$ tel que (Hypothèse de récurrence).

$$\mathcal{U}V = I_n$$

On a :

$$\begin{aligned} T \times \begin{pmatrix} V & 0 \\ 0 & \underbrace{a^{-1}}_{a \neq 0} \end{pmatrix} &= \begin{pmatrix} \mathcal{U} & X \\ 0 & a \end{pmatrix} \begin{pmatrix} V & 0 \\ 0 & a^{-1} \end{pmatrix} \\ &= \begin{pmatrix} U_n & a^{-1}X \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Donc (11.50) :

$$T \times \begin{pmatrix} V & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} I_n & -a^{-1}X \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$$

Donc T est inversible d'inverse dans $\mathcal{T}_{n+1}^+(\mathbb{K})$.

$\boxed{\Leftarrow}$

On suppose que la diagonale de T contient un 0.

— Si $T_{11} = 0$, alors $T = \begin{pmatrix} 0 & L \\ & W \end{pmatrix}$
  Et $T \times \underbrace{E_{11}}_{\neq 0} = 0$
  Donc $T \notin GL_{n+1}(\mathbb{K})$

— On suppose que le premier 0 apparait à T_{kk} avec $k \geq 2$.
  Donc

$$T = \begin{pmatrix} A & C \\ 0 & B \end{pmatrix} \text{ avec } A = \begin{pmatrix} F & G \\ 0 & 0 \end{pmatrix},\ F \in \mathcal{T}_{k-1}^+(\mathbb{K})$$

  La diagonale de F ne contient aucun 0 donc $F \in GL_{k-1}(\mathbb{K})$ et :

$$\begin{aligned} A \times \begin{pmatrix} 0 & -F^{-1}G \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} F & G \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & -F^{-1}G \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

  Alors :

$$T \times \underbrace{\begin{pmatrix} H & 0 \\ 0 & 0 \end{pmatrix}}_{\neq 0} = 0$$

  Donc $T \notin GL_{n+1}(\mathbb{K})$.

11.54 Exemple

Soit $X \in \mathbb{K}^2$.

$$\begin{aligned}
X \in \ker A &\Leftrightarrow AX = 0 \\
&\Leftrightarrow \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \\
&\Leftrightarrow \begin{cases} x + 2y = 0 \\ y = 0 \end{cases} \\
&\Leftrightarrow X = 0
\end{aligned}$$

Donc $\ker A = \{0\}$.

$$\begin{aligned}
X \in \ker B &\Leftrightarrow BX = 0 \\
&\Leftrightarrow \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \\
&\Leftrightarrow \begin{cases} x + y = 0 \\ x + y = 0 \end{cases} \\
&\Leftrightarrow x + y = 0 \\
&\Leftrightarrow X \in \left\{ \begin{pmatrix} x \\ -x \end{pmatrix},\ x \in \mathbb{K} \right\} \\
&\Leftrightarrow X \in \mathbb{K}.\begin{pmatrix} 1 \\ -1 \end{pmatrix}
\end{aligned}$$

Donc $\ker B = \mathbb{K} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

11.61 Exemple

$$\begin{aligned}
&\begin{cases} x + 2y - z = 1 \\ 2x + 5y + z = 2 \end{cases} \\
&\Leftrightarrow \begin{cases} x + 2y - z = 1 \\ 3x + 7y = 3 \end{cases} \\
&\Leftrightarrow \begin{cases} x - a = 1 - 2y \\ 3x = 3 - 7y \end{cases} \\
&\Leftrightarrow \begin{cases} -3z = y \\ x = 1 - \frac{7}{3}y \end{cases} \\
&\Leftrightarrow \begin{cases} x = 1 - \frac{7}{3}y \\ z = -\frac{1}{3}y \end{cases} \\
\Leftrightarrow X &= \begin{pmatrix} 1 - \frac{7}{3}y \\ y \\ -\frac{1}{3}y \end{pmatrix} \\
&= \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + y \begin{pmatrix} -\frac{7}{3} \\ 1 \\ -\frac{1}{3} \end{pmatrix}
\end{aligned}$$

$$\text{Donc } \mathcal{S} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \mathbb{K} \begin{pmatrix} -\frac{7}{3} \\ 1 \\ -\frac{1}{3} \end{pmatrix}$$
$$= \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \mathbb{K} \begin{pmatrix} 7 \\ -3 \\ 1 \end{pmatrix}$$

11.65 Caractérisation des matrices inversibles par les sytèmes linaires

$\boxed{\Rightarrow}$
RAF : (11.63)

$\boxed{\Leftarrow}$
Pour tout $i \in [\![1, n]\!]$, on note $Y_i \in \mathcal{M}_{n,1}(\mathbb{K})$ définie par :

$$Y_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$$

Par hypothèse, on choisit $X_i \in \mathbb{K}^n$ tel que :

$$AX_i = Y_i$$

On pose $B = \begin{pmatrix} X_1 & \dots & X_n \end{pmatrix}$ et on remarque que :

$$\begin{pmatrix} Y_1 & \dots & Y_n \end{pmatrix} = I_n$$

Par construction :

$$AB = I_n$$

11.74 Système équivalents et opérations élémentaires

Soit Σ un système et Σ' un système obtenu après avoir effectué une opération élémentaire.
Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$ la matrice du système Σ et $B \in \mathbb{K}^n$ son second membre.
Soit $X \in \mathbb{K}^p$. Effectuer une opération élémentaire revient à choisir une matrice P de la forme P_{ij}, $Q_i(\lambda)$, $R_{ij}(\lambda)$.
Ainsi :

$$\begin{aligned} X \in \mathcal{S}(\Sigma) &\Leftrightarrow AX = B \\ &\underset{P \in GL_n(\mathbb{K})}{\Leftrightarrow} PAX = PB \\ &\Leftrightarrow X \in \mathcal{S}(\Sigma') \end{aligned}$$

Donc $\boxed{\mathcal{S}(\Sigma) = \mathcal{S}(\Sigma')}$.

Chapitre 12

Arithmétique

12.1 Propriété fondamentale de $\mathbb{Z}$

Théorème 12.1

Toute partie non vide et minorée de $\mathbb{Z}$ admet un plus petit élément.

Soit A une partie non vide et minorée de $\mathbb{Z}$.
On note $\mathcal{M}$ l'ensemble des minorants de A.
Par hypothèse, $\mathcal{M} \neq \emptyset$.
Supposons par l'absurde que :

$$\forall a \in \mathbb{Z}, a \in \mathcal{M} \Rightarrow a+1 \in \mathcal{M}$$

D'après le principe de récurrence, si $a_0 \in \mathcal{M}$ est fixé :

$$\forall n \geq a_0, n \in \mathcal{M}$$

En particulier, pour $n \in A$ ($A \neq \emptyset$) on a :

$$n \geq a_0 \text{ } (a_0 \text{ est un minorant})$$

Donc $n \in \mathcal{M}$.
Donc $n+1 \in \mathcal{M}$.
Donc $n+1$ est un minorant de A.
Donc $n+1 \leq n$.
Absurde.
Ainsi, on choisit $a \in \mathbb{Z}$ avec $a \in \mathcal{M}$ et $a+1 \notin \mathcal{M}$.
On choisit donc $n \in A$ tel que :

$$a \leq n < a+1$$

Donc $n = a \in A$.
Donc $a = \min(A)$.

12.4 Division euclidienne

Théorème 12.4

Soit $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. Il existe un unique coupe $(q,r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r$$

avec $0 \leq r < |b|$. Cette égalité est appelée **division euclidienne de** a **par** b, l'entier q est alors appelé **quotient** et l'entier r le **reste**, tandis que a porte le nom de dividende et b celui de diviseur.

Existence :
On suppose dans un premier temps que $b > 0$.
Soit $a \in \mathbb{Z}$.
On note $A = \{n \in \mathbb{Z}, bn \leq a\}$.
A est un sous-ensemble non vide de $\mathbb{Z}$ et majoré.
Il admet donc un plus grand élément, noté q. On a donc $q \in A$ et $q+1 \notin A$.

$$bq \leq a < b(q+1)$$
$$\text{donc } 0 \leq a - bq < b$$

On pose alors $r = a - bq$. L'exsitence est alors prouvée pour $b > 0$.
Si $b < 0$, alors $-b > 0$ et on choisit $(q,r) \in \mathbb{Z}^2$ tel que :

$$a = -b \times q + r \text{ avec } 0 \leq r < -b$$

Le couple $(-q, r)$ convient.

Unicité :
On suppose $a = bq + r = bq' + r'$ avec $0 \leq r,' < |b|$.

Donc $b(q-q') = r'-r$.
Donc $\underbrace{|b|}_{>0} \times |q-q'| = |r'-r| < \underbrace{|b|}_{>0}$.
Donc $|q-q'| < 1$.
Donc $q = q'$.
Puis $r = r'$.

12.9 Divisibilité et multiple

Propostion 12.9

Soit a et b deux entiers. Alors a est divisble par b si et seulement si a est un multiple de b.

$\boxed{\Rightarrow}$
Si $b|a$, alors :

$$\begin{aligned} a &= bq + 0 \\ &= bq \\ &\in b\mathbb{Z} \end{aligned}$$

$\boxed{\Leftarrow}$
Si $a \in b\mathbb{Z}$, $a = b \times n = b \times n + 0$.
Par unicité de la division euclidienne, $b|a$.

12.10 Divisibilité et normes

Propostion 12.10

Soit a et b deux entiers avec $a \neq 0$ et $b|a$. Alors $|b| \leq |a|$.

Si $b|a$, alors $a = b \times n$ avec $n \neq 0$ var $a \neq 0$. Donc :

$$\begin{aligned} |a| &= |b| \times |n| \\ &\geq |b| \times 1 \end{aligned}$$

12.11 Entiers associés

Propostion 12.11

Soit a et b deux entiers. Alors

$$a\mathbb{Z} = b\mathbb{Z} \Leftrightarrow a = \pm b$$

On dit alors que a et b sont associés.

$\boxed{\Leftarrow}$
Si $a = \pm b$, alors $a\mathbb{Z} = b\mathbb{Z}$.

$\boxed{\Rightarrow}$
Si $a = 0$ et $a\mathbb{Z} = b\mathbb{Z}$, alors $b = 0$.
Si $a \neq 0$ et $a\mathbb{Z} = b\mathbb{Z}$, alors $b \neq 0$ et d'après (12.0) :

$$|a| \leq |b| \text{ et } |b| \leq |a|$$

Donc $|a| = |b|$

12.14 Intégrité de la divisibilité

Propostion 12.14

Soit a, b et c trois entiers, avec $c \neq 0$. Si $nb|na$, alors $n|a$.

Si $cb|ca$, alors $ca = ncb$.
Or c est régulier dans $\mathbb{Z}$ donc :

$$a = nb$$

Donc $b|a$.

12.20 Cas d'une divisibilité

Lemme 12.20

Si $a|b$, alors

$$\mathcal{D}_{a,b} = \mathcal{D}_a$$

Si $a|b$, si $c|a$, alors $c|b$.
Donc $\mathcal{D}_b \supset \mathcal{D}_a$.
Ainsi, $\mathcal{D}_a \cap \mathcal{D}_b = \mathcal{D}_a$

12.21 Préparation à l'algorithme d'Euclide

Lemme 12.21

Soit a, b et q trois entiers, alors

$$\mathcal{D}_{a,b} = \mathcal{D}_{a-bq,b}$$

$\boxed{\subset}$
Soit $n \in \mathcal{D}_{a,b}$, alors :

$$\begin{aligned} n|a \text{ et } n|b \\ \text{donc } n|a - bq \\ \text{donc } n \in \mathcal{D}_{a-bq,b} \end{aligned}$$

$\boxed{\supset}$
Soit $n \in \mathcal{D}_{a-bq,b}$

$$\begin{aligned} n|a - bq \text{ et } n|b \\ \text{donc } n|a - bq + bq \\ \text{soit n|a} \\ \text{donc } n \in \mathcal{D}_{a,b} \end{aligned}$$

12.23 Algorithme d'Euclide étendu ou théorème de Bézout

Lemme 12.23

Soit a et b deux entiers. Soit r le dernier reste non nul dans l'algorithme d'Euclide appliqué à a et b. Il existe deux entiers u et v tels que

$$au + bv = r$$

On utilise les notations du lemme (12.22).
On démontre par récurrence double que :

$$\forall n, \text{"}\exists (u_n, v_n) \in \mathbb{Z}^2, au_n + bv_n = r_n\text{"}$$

Initialisation :
Pour $n = 0$ il s'agit de la division euxlidienne de a par b ($u_0 =$ et $v_0 = -q$).
Pour $n = 1$:

$$\begin{aligned} a &= bq + r \\ b &= r \times q_1 + r_1 \\ \text{donc } r &= b - rq_1 \\ &= b - q_1(a - bq) \\ &= -q_1 a + b(1 + q_1 q) \end{aligned}$$

Hérédité :
On suppose le résultat vrai aux rangs n et $n + 1$.

$$\begin{aligned} a_n &= b_n q_n + r_n \\ b_n &= r_n q_{n+1} + r_{n+1} \\ r_n &= r_{n+1} q_{n+2} + r_{n+2} \end{aligned}$$

Donc :

$$\begin{aligned} r_{n+2} &= r_n - r_{n+1} q_{n+2} \\ &= au_n + bv_n - (au_{n+1} + bv_{n+1}) q_{n+2} \\ &= a \underbrace{(u_n - u_{n+1} q_{n+2})}_{\in \mathbb{Z}} + b \underbrace{(v_n - v_{n+1} q_{n+2})}_{\in \mathbb{Z}} \end{aligned}$$

On utilise le principe de récurrence avec la dernière étape de l'algorithme.

12.24 Application basique

Exemple 12.24

Appliquer l'algorithme d'Euclide aux entiers 121 et 26.

$$\begin{aligned} 121 &= 26 \times 4 + 17 \\ 26 &= 17 \times 1 + 9 \\ 17 &= 9 \times 1 + 8 \\ 9 &= 8 \times 1 + 1 \\ 8 &= 1 \times 8 + 0 \end{aligned}$$

On remonte l'algorithme :

$$\begin{aligned} 1 &= 9 - 8 \\ &= 9 - (17 - 9) \\ &= 2 \times 9 - 17 \\ &= 2 \times (26 - 17) - 17 \\ &= 2 \times 26 - 3 \times 17 \\ &= 2 \times 26 - 3 \times (121 - 4 \times 26) \\ &= 14 \times 26 - 3 \times 121 \end{aligned}$$

12.26 Théorème de Bézout

Théorème 12.26

Soit a et b deux entiers. Alors a et b sont premiers entre eux si et seulement si il existe $(u, v) \in \mathbb{Z}^2$ tel que

$$au + bv = 1$$

$\boxed{\Rightarrow}$
On suppose a et b premiers entre eux.
Donc $\mathcal{D}_{a,b} = \{\pm 1\}$.
Soit r le dernier reste non nul dans l'algorithme d'Euclide,

$$\mathcal{D}_r = \mathcal{D}_{a,b} = \{\pm 1\}$$

Donc $r = \pm 1$.
D'après le théorème de Bézout, il existe deux entiers u et v tels que :

$$au + bv = 1$$

$\boxed{\Leftarrow}$
Réciproquement, si $au + bv = 1$, alors pour tout $d \in \mathcal{D}_{a,b}$ $d|au + bv$ donc $d|1$ donc $d = \pm 1$.
Donc $\mathcal{D}_{a,b} = \{\pm 1\}$.

12.28 Proposition

Propostion 12.28

Si a est premier avec b et c, alors a est premier avec bc.

D'après le théorème de Bézout, on écrit :

$$au_1 + bv_1 = 1$$
$$au_2 + cv_2 = 1$$

avec $(u_1, u_2, v_1, v_2) \in \mathbb{Z}^4$.
Donc :

$$\begin{aligned} 1 &= (au_1 + bv_1)(au_2 + cv_2) \\ &= a\underbrace{(au_1u_2 + bv_1u_2 + cu_1v_2)}_{\in\mathbb{Z}} + \underbrace{v_1v_2}_{\in\mathbb{Z}}bc \end{aligned}$$

Donc a et bc sont premiers entre eux d'après le théorème de Bézout.

12.29 Proposition

Propostion 12.29

Si a est premier avec b, que $a|c$ et $b|c$, alors $ab|c$.

D'après le théorème de Bézout :

$$au + bv = 1,\ (u, v) \in \mathbb{Z}^2$$

Donc :

$$auc + bvc = c$$

Or $a|c$ et $b|c$, donc :

$$c = ka \text{ et } c = pb$$

Donc :

$$ab\underbrace{[pu + vk]}_{\in\mathbb{Z}} = c$$

Donc $ab|c$.

12.30 Théorème de Gauss

Théorème 12.30

Si $a|bc$ et que a est premier avec b, alors $a|c$.

D'après le théorème de Bézout :

$$au + bv = 1 \text{ avec } (u, v) \in \mathbb{Z}^2$$

Donc $auc + bvc = c$.
Or $a|bc$ donc $a|auc + bvc$.
Soit $a|c$.

12.31 Equation de Bézout

Exemple 12.31

Résoudre l'équation d'inconnue $(x, y) \in \mathbb{Z}^2, 3x - 2y = 7$.

On remarque que 3 et 2 sont premiers entre eux.

$$\begin{aligned} 3 - 2 &= 1 \\ \text{donc } 3 \times 7 - 2 \times 7 &= 7 \\ \text{donc } (7, 7) &\in \mathcal{S} \end{aligned}$$

On note (x_0, y_0) cette solution.
Soit $(x, y) \in \mathcal{S}$.
Donc :

$$\begin{aligned} 7 &= 3x - 2y \\ 7 &= 3x_0 - 2y_0 \\ \text{donc } 3(x - x_0) &= 2(y - y_0) \end{aligned}$$

Or $3|3(x - x_0)$ et 3 premier avec 2.
Donc $3|y - y_0$.
Donc $y - y_0 = 3k$, avec $k \in \mathbb{Z}$. (Théorème de Gauss)
De la même manière, $x - x_0 = 2l$, avec $l \in \mathbb{Z}$. (Théorème de Gauss)

Réciproquement, soit $x = x_0 + 2l$ et $y = y_0 + 3k$.

$$\begin{aligned} (x, y) \in \mathcal{S} &\Leftrightarrow 7 = 3x - 2y = 3x_0 - 2y_0 + 6l - 6k \\ &\Leftrightarrow 6l - 6k = 0 \\ &\Leftrightarrow k = l \end{aligned}$$

Donc $\mathcal{S} = \{(x_0 + 2k, y_0 + 3k), k \in \mathbb{Z}\}$

12.32 Proposition

Propostion 12.32

Si $ar \equiv br \mod n$ et si r et n sont premiers entre eux, alors $a \equiv b \mod n$.

Si $ar \equiv br \mod n$, alors $n|r(a - b)$.
Donc $n|a - b$ (n premier avec r et théorème de Gauss).
Donc $a \equiv b \mod n$.

12.37 Lien avec les idéaux

Propostion 12.37

Soit a et b deux entiers, alors d est le *pgcd* de a et b si et seulement si $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Soit $(a, b) \in \mathbb{Z}^2$. $a\mathbb{Z}$ et $b\mathbb{Z}$ dont des idéaux de $\mathbb{Z}$.
Donc $a\mathbb{Z} + b\mathbb{Z}$ est un idéal de $\mathbb{Z}$, donc en particulier un sous-groupe de $\mathbb{Z}$.
On choisit donc $d \geq 0$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.
Montrons que $d = pgcd(a, b) = a \wedge b$.
D'une part :

$$\begin{aligned} d &\in d\mathbb{Z} && \text{donc } d = au + bv \text{ (avec } (u, v) \in \mathbb{Z}^2 \\ &\in a\mathbb{Z} + b\mathbb{Z} && \\ \text{or } a \wedge b|a \text{ et } a \wedge b|b & && \text{donc } a \wedge b|au + bv \\ & && \text{soit } a \wedge b|d \end{aligned}$$

D'autre part, $a \wedge b$ est le dernier reste non nul de l'algorithme d'Euclide, donc (12.23) :

$$\begin{aligned} a \wedge b &= au + bv \text{ (avec } (u, v) \in \mathbb{Z}^2) \\ &\in a\mathbb{Z} + b\mathbb{Z} \\ &\in d\mathbb{Z} \end{aligned}$$

Donc $d|a \wedge b$.
Ainsi, d et $a \wedge b$ sont positifs et associés, donc égaux.

12.38 Préparation au calcul pratique d'un *pgcd*

Lemme 12.38

Si a et b sont tous les deux non nuls, alors pour tout $q \in \mathbb{Z}, pgcd(a, b) = pgcd(a - bq, b)$.

$$\begin{aligned} \mathcal{D}_{pgcd(a,b)} &= \mathcal{D}_{a,b} \\ &\underset{(12.21)}{=} \mathcal{D}_{a-bq,b} \\ &= \mathcal{D}_{pgcd(a-bq,b)} \end{aligned}$$

Les deux *pgcd* sont associés, donc égaux car positifs.

12.39 Caractérisation du *pgcd*

Propostion 12.39

Soit a et b deux entiers et $d \in \mathbb{N}$. Alors $d = pgcd(a, b)$ si et seulement si il existe $(u, v) \in \mathbb{Z}^2$ avec u et v premiers entre eux, tels que $a = du$ et $b = dv$.

$\boxed{\Rightarrow}$
On suppose que $d = a \wedge b$.
Donc $d|a$ et $d|b$.
On écrit donc $a = du$ et $b = dv$ avec $(u, v) \in \mathbb{Z}^2$.
Notons $n = u \wedge v$. On écrit $u = n \times u'$ et $v = n \times v'$ avec $(u', v') \in \mathbb{Z}^2$.
Donc $a = d \times n \times u'$ et $b = d \times n \times v'$.
Donc $dn \in \mathcal{D}_{a,b} = \mathcal{D}_d$.
Donc $dn|d$.
Donc $n = 1$.

$\boxed{\Leftarrow}$
On suppose que $a = du$ et $b = dv$ avec $u \wedge v = 1$.
D'après le théorème de Bézout :

$$uu' + vv' = 1 \text{ (avec } (u', v') \in \mathbb{Z}^2)$$

Donc $duu' + dvv' = d$.
Soit $au' + bv' = d$.
Donc $d \in a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$.
Donc $a \wedge b | d$.
Par ailleurs, $d \in \mathcal{D}_{a,b} = \mathcal{D}_{a \wedge b}$.
Donc $d | a \wedge b$.
Ainsi, $a \wedge b$ et d sont associés (et positifs) donc égaux.

12.40 Propriétés du *pgcd*

Propostion 12.40

Soit a et b deux entiers tous deux non nuls.

1. pour tout $n \in \mathbb{Z}$, si $n|a$ et $n|b$, alors $n|pgcd(a, b)$;
2. pour tout $k \in \mathbb{N}^*, pgcd(ka, kb) = kpgcd(a, b)$;
3. pour tout $n \in \mathbb{N}, pgcd(a^n, b^n) = pgcd(a, b)^n$;
4. si a et c sont premiers entre eux, alors $pgcd(a, bc) = pgcd(a, b)$.

1. RAF (définition)
2. Soit $k \in \mathbb{N}^*$. On écrit (12.39) :

$$a = (a \wedge b)u$$
$$b = (a \wedge b)v \text{ (avec } u \wedge v = 1)$$

Donc :

$$ka = [k(a \wedge b)]\, u$$
$$kb = [k(a \wedge b)]\, v$$

Donc (12.39) :

$$pgcd(ka, kb) = k(a \wedge b)$$

3. Avec une partie des notations de 2. :

$$a^n = (a \wedge b)^n u^n$$
$$b^n = (a \wedge b)^n v^n$$

Avec $(u^n) \wedge (v^n) = 1$.
Donc (12.39) :

$$pgcd(a^n, b^n) = (a \wedge b)^n$$

4.

$$a = (a \wedge b)u$$
$$b = (a \wedge b)v \text{ (avec } u \wedge v = 1)$$

Donc

$$bc = (a \wedge b) \times vc$$

Or, puisque $a \wedge c = 1$ et que $u|a$, alors :

$$u \wedge c = 1$$

Donc (12.28) :

$$u \wedge (vc) = 1$$

Donc (12.39) :

$$pgcd(a, bc) = a \wedge b$$

12.44 Définition du PPCM

Propostion 12.44

Soit a et b deux entiers non nuls. On appelle **PPCM** (plus petit commun multiple) l'unique entier $m \in \mathbb{N}$ tel que

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

Cet entier est noté $ppcm(a, b)$ ou encore $a \vee b$.

$a\mathbb{Z}$ et $b\mathbb{Z}$ ont des idéaux de $\mathbb{Z}$.
Donc $a\mathbb{Z} \cap b\mathbb{Z}$ est un idéal de $\mathbb{Z}$, donc un sous-groupe de $\mathbb{Z}$.
Donc il existe un unique entier $m \in \mathbb{N}$ tel que :

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

Comme $a \neq 0$ et $b \neq 0$, alors $m \neq 0$.

12.45 Caractérisation du *ppcm*

Propostion 12.45

Soit a et b deux entiers, et $m \in \mathbb{N}$. Alors $m = ppcm(a, b)$ si et seulement si il existe $(u, v) \in \mathbb{Z}^2$, premiers entre eux tels que $m = au = bv$.

$\boxed{\Rightarrow}$
On suppose que $m = a \vee b$.
Donc $m \in a\mathbb{Z} \cap b\mathbb{Z}$.
Donc $m = au = bv$.
On note $d = pgcd(u, v)$.
On écrit donc :

$$u = da'$$
$$v = db'$$

Donc :

$$ada' = bdb'$$

Donc :

$$aa' = bb' = m'$$

Donc :

$$\begin{aligned} m' &\in a\mathbb{Z} \cap b\mathbb{Z} \\ &\in m\mathbb{Z} \end{aligned}$$

Donc :

$$dm' = m | m'$$

Donc :

$$d = 1$$

$\boxed{\Leftarrow}$
On suppose que $m = au = bv$ avec $pgcd(u, v) = 1$.
D'une part :

$$m \in a\mathbb{Z} \cap b\mathbb{Z} = ppcm(a, b)\mathbb{Z}$$

Donc :

$$ppcm(a, b) | m$$

D'autre part, d'après le théorème de Bézout :

$$uu' + vv' = 1 \text{ avec } (u', v') \in \mathbb{Z}^2$$

Donc :

$$uu'\underbrace{ppcm(a,b)}_{ka} + vv'\underbrace{ppcm(a,b)}_{qb} = ppcm(a,b)$$

Donc :

$$m(u'k + vq') = ppcm(a,b)$$

Donc $m|ppcm(a,b)$.

12.46 Propriétés du *ppcm*

Propostion 12.46

Soit a et b deux entier non nuls, alors :

1. pour tout $n \in \mathbb{Z}$, si $a|n$ et $b|n$, alors $ppcm(a,b)|n$;
2. si a et b sont premiers entre eux, alors $ppcm(a,b) = |ab|$;
3. pour tout $k \in \mathbb{N}^*$, $ppcm(ka, kb) = kppcm(a,b)$;
4. $ppcm(a,b) \times pgcd(a,b) = |ab|$;
5. pour tout $n \in \mathbb{N}$, $ppcm(a^n, b^n) = ppcm(a,b)^n$.

1. RAF (12.44)
2. On suppose que $a > 0$ et $b > 0$.

$$ab = ba$$

avec $a \wedge b = 1$.
D'après (12.45) :

$$ppcm(a,b) = ab$$

3. On écrit (12.45) :

$$ppcm(a,b) = au = bv \text{ (avec } u \wedge v = 1)$$

Alors :

$$\begin{aligned} b \wedge ppcm(a,b) &= (ak)u \\ &= (bk)v \end{aligned}$$

Donc (12.45) :

$$ppcm(ak, bk) = kppcm(a,b)$$

5. Avec les mêmes notations :

$$\begin{aligned} ppcm(a,b)^n &= a^n u^n \\ &= b^n v^n \text{ (avec } u^n \wedge v^n = 1) \end{aligned}$$

Donc (12.45) :

$$ppcm(a^n, b^n) = ppcm(a,b)^n$$

4. D'après (12.39) (avec $a > 0$ et $b > 0$) :

$$\begin{aligned} a &= pgcd(a,b)u \\ b &= pgcd(a,b)v \text{ (avec } u \wedge v = 1) \\ pgcd(a,b) \times ppcm(a,b) &= pgcd(a,b)ppcm(pgcd(a,b)u, pgcd(a,b)v) \\ &\underset{(3.)}{=} pgcd(a,b)^2 ppcm(u,v) \\ &\underset{(2.)}{=} pgcd(a,b)^2 uv \\ &= ab \end{aligned}$$

12.50 Propriétés

Propostion 12.50

1. Si $p \in \mathbb{P}$, alors pour tout $n \in \mathbb{Z}$, soit $p|n$ soit $pgcd(n,p) = 1$.
2. Si $n \geq 2$, alors n possède au moins un diviseur premier.
3. L'ensemble $\mathbb{P}$ est infini.
4. Si $n > 1$ n'as pas de diviseur dans $[2; \sqrt{n}]$, alors n est premier.
5. Si $p \in \mathbb{P}$, alors pour tout a et b entiers, on a $(a+b)^p \equiv a^p + b^p \pmod{p}$.

1. On suppose que $p \not| n$.
   Soit $d \in \mathcal{D}_p \cap \mathcal{D}_n$.
   $d > 0$ et $d \neq p$.
   Donc $d = 1$.
   Donc $p \wedge n = 1$.
2. On raisonne par récurrence forte $\rightarrow$ cf. (2.41).
3. On suppose par l'absurde que :
   $$\mathbb{P} = \{p_1, p_2, \ldots, p_n\}$$
   On pose :
   $$m = \prod_{i=1}^{n}(p_i) + 1$$
   Soit $p_i \in \mathbb{P}$ tel que $p_i|m$ (12.50.2).
   Donc $p_i|1$.
   Absurde.
4. On suppose $n \notin \mathbb{P}$.
   Soit $n = ab$ avec $a \geq 2$ et $b \geq 2$.
   Si $a > \sqrt{n}$ et $b > \sqrt{n}$, alors $ab = n > \sqrt{n}^2 = n$.
   Absurde.
5. D'après le binôme de Newton :
   $$\begin{aligned}(a+b)^p &= \sum_{k=0}^{p}\binom{p}{k}a^k b^{p-k} \\ &= a^p + b^p + \sum_{k=1}^{p-1}\binom{p}{k}a^k b^{p-k}\end{aligned}$$
   Or, pour $k \in [\![1; p-1]\!], p\binom{p-1}{k-1} = k\binom{p}{k}$ (formule du capitaine).
   Or $k \wedge p = 1$ et $p \left| p\binom{p-1}{k-1} \right.$ soit $p \left| \binom{p}{k} \right.$.
   Donc :
   $$p \left| \binom{p}{k} \right.$$
   Donc :
   $$(a+b)^p \equiv a^p + b^p \pmod{p}$$

12.51 Petit théorème de Fermat

Théorème 12.51

Pour tout $n \in \mathbb{Z}$ et $p \in \mathbb{P}$, on a $n^p \equiv n \pmod{p}$. En outre, si $pgcd(n,p) = 1$, alors $n^{p-1} \equiv 1 \pmod{p}$.

Soit $p \in \mathbb{P}$. On montre le résultat pour $n \geq 0$ par récurrence.
On a bien $0^p = 0 \equiv 0 \pmod{p}$. Si $n^p \equiv n \pmod{p}$, alors :

$$\begin{aligned}(n+1)^p &\equiv n^p + 1^p \pmod{p} \text{ (12.50.5).} \\ &\equiv n + 1 \pmod{p} \text{ (Hypothèse de récurrnce)}\end{aligned}$$

Soit $n \in \mathbb{N}$.

— Si $p \geq 3$ (donc p est impair), alors :

$$\begin{aligned} n^p &\equiv n \pmod p \\ (-n)^p &\underset{p \text{ impair}}{\equiv} -n^p \pmod p \\ &\equiv -n \pmod p \end{aligned}$$

— Si $p = 2$, $-1 \equiv 1 \pmod 2$.
Donc :

$$\begin{aligned} (-n)^2 &\equiv n^2 \pmod 2 \\ &\equiv n \pmod 2 \\ &\equiv -n \pmod 2 \end{aligned}$$

12.52 Décomposition en produit de facteurs premiers

Théorème 12.52

Soit $n \in \mathbb{Z} \backslash \{-1, 0, 1\}$, alors il existe des nombres premiers $p_1, \ldots, p_r$ tous distincts, et $(\alpha_1, \ldots, \alpha_r) \in (\mathbb{N}^*)^r$ et $\epsilon \in \{\pm 1\}$ tels que

$$n = \epsilon p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}$$

Cette décomposition est unique à l'ordre près.

<u>Existence :</u>
On montre l'existence par récurrence forte sur $\mathbb{N} \backslash \{0, 1\}$.

— RAF si $n = 2$.
— On suppose le résultat vrai pour tout $k \in [\![2; n]\!]$.

  — Si $n + 1 \in \mathbb{P}$: RAF
  — Si $n + 1 \notin \mathbb{P}$, on écrit :

$$n + 1 = k \times q \text{ avec } (k, q) \in [\![2, n]\!]^2$$

Donc k et q sont des produits de facteurs premiers.
Donc $n + 1 = kq$ est aussi un produit de facteurs premiers.
Le résultat est donc vrai pour tout $n \in \mathbb{N}$ et par extension pour $-n$ ($\epsilon = -1$).

<u>Unicité :</u>
On suppose que :

$$n = \epsilon p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r} = \epsilon' q_1^{\beta_1} \times \cdots \times q_s^{\beta_s}$$

Nécessairement, $\epsilon = \epsilon'$.
Soit $p_i \in \{p_1, \ldots, m_r\}$.
On a $p_i | n$ donc $p_i \left| q_1^{\beta_1} \times \cdots \times q_s^{\beta_s} \right.$.
Il existe $p_i \in \mathbb{P}$ donc $j \in [\![1; s]\!]$ tel que $p_i | q_j$.
Donc $p_i = \underbrace{q_j}_{\in \mathbb{P}}$.
Ainsi :

$$\{p_1, \ldots, p_r\} \subset \{q_1, \ldots, q_s\}$$

Par symétrie :

$$\{p_1, \ldots, p_r\} = \{q_1, \ldots, q_s\}$$

Donc $r = s$ et quitte à renommer q_j, on peut supposer que :

$$\forall i \in [\![1; r]\!], p_i = q_i$$

$$p_i^{\alpha_i} | n \text{ donc } p_i^{\alpha_i} \left| \prod_{j=1}^{r} p_j^{\beta_j} \right.$$

$$\text{donc } \alpha_i \leq \beta_i$$

Par symétrie, $\alpha_i = \beta_i$.
L'unicité est prouvée.

12.54 Caractérisation de la valuation

Théorème 12.54

Soit $n \in \mathbb{Z}^*$ et $p \in \mathbb{P}$ et $d \in \mathbb{N}$. Alors $d = v_p(n)$ si et seulement si $n = p^d u$, avec $u \wedge p = 1$.

On a :

$$\begin{aligned} d = v_p(n) &\Leftrightarrow (p^d | n \text{ et } p^{d+1} \nmid n) \\ &\Leftrightarrow \exists u \in \mathbb{Z}, n = p^d u \text{ et } p^{d+1} \nmid u \\ &\Leftrightarrow \exists u \in \mathbb{Z}, n = p^d u \text{ et } p \nmid u \\ &\underset{(p \in \mathbb{P})}{\Leftrightarrow} \exists u \in \mathbb{Z}, n = p^d u \text{ et } u \wedge p = 1 \end{aligned}$$

12.55 Valuation et décomposition en produit de facteurs premiers

Théorème 12.55

Si $p|n$, alors $v_p(n)$ est la puissance de p intervenant dans la décomposition en produit de facteurs premiers de n.

On écrit la décomposition :

$$n = \epsilon \prod_{i=1}^{r} p_i^{\alpha_i}$$

Soit $k \in [\![1, r]\!]$.

$$n = \epsilon \times p_k^{\alpha_k} \times \underbrace{\prod_{i \neq k} p_i^{\alpha_i}}_{:=u \text{ (avec } u \wedge p_k = 1)}$$

Donc (12.54) :

$$\boxed{v_{p_k}(n) = \alpha_k}$$

12.56 Propriétés de la valuation

Propostion 12.56

Pout tout $(n, m) \in \mathbb{Z}^2$ et $p \in \mathbb{P}$, on a

1. $p|n$ si et seulement si $v_p(n) > 0$;
2. $v_p(mn) = v_p(m) + v_p(n)$;
3. $v_p(n + m) \geq \min(v_p(n), v_p(m))$ avec égalité si les valuations sont distinctes ;
4. $n|m \Leftrightarrow (\forall q \in \mathbb{P}, v_q(n) \leq v_q(m))$;
5. si de plus n et m sont non nuls alors

$$v_p(n \wedge m) = \min(v_p(n), v_p(m)) \text{ et } v_p(n \vee m) = \max(v_p(n), v_p(m)).$$

1. RAF
2. On écrit $m = p^{v_p(m)} \times u$ et $n = p^{v_p(n)} \times v$ avec $u \wedge p = 1 = v \wedge p$ (12.54).
   Donc $mn = p^{v_p(m)+v_p(n)} \times uv$.
   Or $p \wedge (uv) = 1$.
   Donc (12.54) :

$$\boxed{v_p(mn) = v_p(m) + v_p(n)}$$

3. On suppose que $v_p(m) \leq v_p(n)$.
   Ainsi :

$$\begin{aligned} n + m &= p^{v_p(n)} \times v + p^{v_p(m)} \times u \\ &= p^{v_p(m)} \left[u + v_p^{v_p(n) - v_p(m)} \right] \end{aligned}$$

   Ainsi, $p^{v_p(m)} | n + m$.
   Par définition :

$$\boxed{v_p(m+n) \geq v_p(m) = \min(v_p(m), v_p(n))}$$

   .
   Si on suppose de plus que $v_p(m) \neq v_p(n)$, alors

$$p \wedge (u + v \times p^{v_p(n) - v_p(m)}) = p \wedge u = 1$$

   Donc (12.54) :

$$\boxed{v_p(n+m) = v_p(m) = \min(v_p(m), v_p(n))}$$

4. On a :

$$\begin{aligned} & n|m \text{ ssi la décomposition en produit de facteurs premiers de } n \text{ se retrouve dans celle de } m. \\ & \underset{(12.55)}{\text{ssi}} \text{ pour tout } p \in \mathbb{P} \text{ tel que } p|n, \text{ alors } v_p(n) \leq v_p(m). \\ & \underset{(\text{si } p \nmid n,\, v_p(n) = 0 \leq v_p(m))}{\text{ssi}} \text{ pour tout } \boxed{p \in \mathbb{P}, v_p(n) \leq v_p(m)}. \end{aligned}$$

5. On a $(n \wedge m)|n$ et $(n \wedge m)|m$.
   Donc (12.56.4) $\boxed{v_p(n \wedge m) \leq \min(v_p(n), v_p(m))}$.
   On suppose par exemple que $v_p(n) \leq v_p(m)$.
   Donc $p^{v_p(n)}|n$ et $p^{v_p(n)}|m$.
   Donc $p^{v_p(n)}|n \wedge m$.
   Par définition $\boxed{v_p(n \wedge m) \geq v_p(n)}$.
   Donc :

$$\boxed{v_p(n \wedge m) = \min(v_p(n), v_p(m))}$$

   On rappelle que $(n \wedge m) \times (n \vee m) = |nm|$.
   Donc $v_p((n \wedge m) \times (n \vee m)) = v_p(nm)$.
   Donc (12.56.2) :

$$\begin{aligned} v_p(n \vee m) &= v_p(n) + v_p(m) - v_p(n \wedge m) \\ &= v_p(n) + v_p(m) - \min(v_p(n), v_p(m)) \\ &= \boxed{\max(v_p(n), v_p(m))} \end{aligned}$$

Les preuves ont été rédigées avec les hypothèses $n \neq 0$ et $m \neq 0$. Si l'un des entiers est nul, on vérifie les assertions avec la convention $v_p(0) = +\infty$.

Chapitre 13

Polynômes

13.6 Produit de deux polynômes

Définition 13.6

Soit $P = (a_n)$ et $Q = (b_n)$ deux polynômes de $\mathbb{A}[X]$. Soit pour tout $n \in \mathbb{N}, c_n = \sum_{k=0}^{n} a_k b_{n-k}$. Alors la suite $(c_n)_{n\in\mathbb{N}}$ est un polynôme. On définit alors $PQ = (c_n)$. La suite $c = (c_n)$ est appelée **produit de convolution** (ou **produit de Cauchy**) des suites $a = (a_n)$ et $b = (b_n)$ et est parfois noté $c = a \star b$.

Montrons que (c_n) est un polynôme.
Soit N te M dans $\mathbb{N}$ tels que :

$$\begin{cases} \forall n \in \mathbb{N}, n \geq N, a_n = 0 \\ \forall n \in \mathbb{N}, n \geq M, b_n = 0 \end{cases}$$

Soit $n \geq M + N$, on a :

$$c_n = \sum_{k=0}^{n} a_k b_{n-k}$$

— Si $k \geq N$, $a_k = 0$.
— Si $k \leq N$, $n - k \geq M$, donc $b_{n-k} = 0$.

Donc $c_n = 0$.

13.7 Structure d'anneau de $\mathbb{A}[X]$

Théorème 13.7

La somme et le produit définis ci-dessus munissent $\mathbb{A}[X]$ d'une structure d'anneau commutatif.

— $(\mathbb{A}[X], +)$ est un sous-groupe de $(\overbrace{\mathbb{A}^{\mathbb{N}}}^{\text{suites d'éléments de } \mathbb{A}}, +)$ abélien donc est bien un sous-groupe abélien.
— Montrons que $\times$ est associative. Soit $(P, R, Q) \in \mathbb{A}[X]$.
On note $P = (p_k)_{k\in\mathbb{N}}$, $R = (r_k)_{k\in\mathbb{N}}$, $Q = (q_k)_{k\in\mathbb{N}}$.
Soit $n \in \mathbb{N}$.

$$\begin{aligned} (P \times (RQ))_n &= \sum_{k=0}^{n} p_k (RQ)_{n-k} \\ &= \sum_{i+j=n} p_i (RQ)_j \\ &= \sum_{i+j=n} \left(p_i \sum_{k+l=j} r_k q_l \right) \\ &= \sum_{i+k+l=n} p_i r_k q_l \\ &= ((PR) \times Q)_n \end{aligned}$$

— Notons $E = (1, 0, \ldots) = (\delta_{0n})_{n\in\mathbb{N}}$.
On a pour tout $n \in \mathbb{N}$:

$$\begin{aligned} (E \times P)_n &= \sum_{i+j=n} E_i \times P_j \\ &= \sum_{i+j=n} \delta_{0i} \times P_j \\ &= P_n \ (i = 0,\ j = n) \\ &= (P \times E)_n \end{aligned}$$

Donc E est l'élément neutre de $\mathbb{A}[X]$.

—

$$\begin{aligned}[P\times(R+Q)]_n &= \sum_{i+j=n} p_i(R+q)_j \\ &= \sum_{i+j=n} p_i(r_j+a_j) \\ &= \sum_{i+j=n} p_ir_j + \sum_{i+j=n} p_iq_j \\ &= (PR)_n + (PQ)_n \\ &= [PR+PQ]_n\end{aligned}$$

Donc $\times$ est distributive sur $+$.

— Comme $\mathbb{A}$ est commutatif :

$$\sum_{i+j=n} p_iq_j = \sum_{i+j=n} q_jp_i$$

Donc $\times$ est commutatif.

13.11 Monômes

Propostion 13.11

Pour tout $n\in\mathbb{N}$, on a $X^n = (\underbrace{0,\dots,0}_{n \text{ zéros}},1,0,\dots)$, le 1 est donc à l'indice n (soit $X^n = (\delta_{n,k})_{k\in\mathbb{N}}$)

Pour $n=0$, on a bien $X^0 = (1,0,\dots)$
Pour $n=1$, RAF
On suppose le résultat vrai pour $n\in\mathbb{N}$.
Soit $k\in\mathbb{N}$:

$$\begin{aligned}\left[X^{n+1}\right]_k &= [X^n\times X] \\ &= \sum_{i+j=k} [X^n]_i X_j \\ &= \sum_{i+j=k} \delta_{n,i}\times\delta_{j,1} \\ &= \delta_{k,n+1}\end{aligned}$$

13.12 Expression d'un polynôme à l'aide de l'indéterminée formelle

Corollaire 13.12

Soit $P=(a_n)$ un polynôme de $\mathbb{A}[X]$. Alors $P=\sum\limits_{k=0}^{+\infty} a_kX^k$, cette somme ayant un sens puisqu'elle est en fait finie, les a_k étant nuls à partir d'un certain rang.

$$\begin{aligned}P &= (a_n)_{n\geq 0} \\ &= (a_0,a_1,a_2,\dots \\ &= a_0(1,0,0,\dots)+a_1(0,1,0,\dots)+a_2(0,0,1,\dots)+\dots \\ &= a_0X^0+a_1X^1+a_2X^2+\dots\end{aligned}$$

13.26 Dérivée de produits

Propostion 13.26

— Soit P et Q deux polynômes à coefficients dans $\mathbb{A}$. Alors

$$(PQ)' = P'Q + Q'P.$$

— Soit $P_1, \ldots, P_n$ des polynômes à coefficients dans $\mathbb{A}$, alors

$$(P_1 \ldots P_n)' = \sum_{i=1}^{n} P_1 \ldots P_{i-1} P_i' P_{i+1} \ldots P_n.$$

— **Formule de Leibniz** : Soit P et Q deux polynômes à coefficients dans $\mathbb{A}$ et $n \in \mathbb{N}$. Alors

$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

Soit $P = \sum_{k\geq 0} a_k X^k$, $P' = \sum_{k\geq 1} k a_k X^{k-1}$ et $Q = \sum_{k\geq 0} b_k X^k$, $Q' = \sum_{k\geq 1} k b_k X^{k-1}$.
On a :

$$PQ = \sum_{k\geq 0} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) X^n$$

Donc :

$$\begin{aligned}
(PQ)' &= \sum_{n\{geq1} \left[n \sum_{k=0}^{n} a_k b_{n-k} \right] X^{n-1} \\
\text{et } P'Q &= \sum_{n\geq 0} \left[\sum_{k=0}^{n} (k+1) a_{k+1} b_{n-k} \right] X^n \\
\text{et } PQ' &= \sum_{n\geq 0} \left[\sum_{k=0}^{n} a_k (n-k+1) b_{n-k+1} \right] X^n \\
\text{donc } P'Q + Q'P &= \sum_{n\geq 0} \left[\sum_{k=0}^{n} (k+1) a_{k+1} b_{n-k} \right] X^n + \sum_{n\geq 0} \left[\sum_{k=0}^{n} (n-k+1) a_k b_{n-k+1} \right] X^n \\
&= \sum_{n\geq 0} \left[\sum_{k=1}^{n+1} k a_k b_{n-k+1} \right] X^n + \sum_{n\geq 0} \left[\sum_{k=0}^{n} (n-k+1) a_k b_{n-k+1} \right] X^n \\
&= \sum_{n\geq 0} \left[(n+1) a_{n+1} b_0 + \sum_{k=1}^{n} (n+1) a_k b_{n-k+1} + (n+1) a_0 b_{n+1} \right] X^n \\
&= \sum_{n\geq 0} \left[(n+1) \sum_{k=0}^{n+1} a_k b_{n-k+1} \right] X^n
\end{aligned}$$

13.28 Dérivée d'une composition

Propostion 13.28

Soit P et Q dans $\mathbb{A}[X]$, alors

$$(Q \circ P)' = P' \times (Q' \circ P)$$

Soit $Q = \sum_{k\geq 0} a_k X^k$.
Ainsi $Q \circ P = \sum_{k\geq 0} a_k p^k$.

Donc :

$$\begin{aligned}(Q \circ P)' &= \sum_{k \geq 0} a_k (p_k)' \ (13.24)\\ &= \sum_{k \geq 1} k a_k p' p^{k-1} \ (13.27)\\ &= P' \times \sum_{k \geq 1} k a_k p^{k-1}\\ &= P' \times Q' \circ P\end{aligned}$$

13.34 Degré d'une somme, d'un produit, d'une dérivée

Propostion 13.34

Soit P et Q deux polynômes de $\mathbb{A}[X]$ et $\lambda \in \mathbb{A}$.

1. On a $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$ avec égalité si $\deg(P) \neq \deg(Q)$.
2. Si $\mathbb{A}$ est intègre et si $\lambda \neq 0$, alors $\deg(\lambda P) = \deg(P)$.
3. Si $\mathbb{A}$ est intègre alors $\deg(PQ) = \deg(P) + \deg(Q)$.
4. On a $\deg(P') \leq \deg(P) - 1$.
5. Si $\mathbb{A}$ est intègre alors $\deg(Q \circ P) = \deg(Q) + \deg(P)$, sauf si $P = 0$ ou si $Q = 0$ et $P \in \mathbb{A}_0[X]$.

1. On note $p = \deg(P), q = \deg(Q)$.

$$P = \sum_{k=0}^{p} a_k X^k, Q = \sum_{k=0}^{q} b_k X^k$$

   Supposons $p \geq q$.
   On écrit alors :

$$\begin{aligned}Q &= \sum_{k=0}^{p} b_k X^k\\ \text{et ainsi } P+Q &= \sum_{k=0}^{p} (a_k + b_k) X^k\\ \text{et donc } \deg(P+Q) &\leq p\end{aligned}$$

   Si de plus $p > q$, alors :

$$\begin{aligned}P+Q &= a_p X^p + \sum_{k=0}^{p-1} (a_k + b_k) X^k \ (b_p = 0)\\ \text{donc } (a_p \neq 0),\ \deg(P+Q) &= p\end{aligned}$$

2.

$$\lambda P = \sum_{k=0}^{p} \lambda a_k X^k$$

   Or $\lambda a_p \neq 0$ car $a_p \neq 0$ et $\mathbb{A}$ intègre.
3.

$$P.Q = \sum_{n \geq 0} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) X^n$$

   Si $n > p + q$, alors :

$$\sum_{k=0}^{n} a_k bn - k = 0 \text{ (preuve (13.6))}$$

Or :

$$\begin{aligned}(PQ)_{p+q} &= \sum_{k=0}^{p+q} a_k b_{p+q-k} \\ &= \underbrace{a_p}_{\neq 0} \underbrace{b_q}_{\neq 0} \\ &\neq 0 \text{ car } \mathbb{A} \text{ intègre}\end{aligned}$$

4. Si $P \in \mathbb{A}_0[X]$, l'inégalité est vérifiée.
   Sinon :

$$p' = \sum_{k=0}^{p-1} (k+1) a_{k+1} X^k$$
$$\text{et } \deg(P') \leq d - 1 = \deg(P) - 1$$

5. On a :

$$Q \circ P = \sum_{k=0}^{q} b_k p_k$$

   Or, pour $k \in [\![0, q-1]\!]$, $\deg(b_k p^k) < \deg(\underbrace{b_q}_{\neq 0} p^q)$ ((13.34.2) et (13.34.3) avec $\mathbb{A}$ intègre)

   Donc :

$$\begin{aligned}deg(Q \circ P) &= \deg(b_q p^q) \\ &= q \times \deg(P) \\ &= \deg(Q) \times \deg(P)\end{aligned}$$

13.36 Théorème de permanence de l'intégrité

Corollaire 13.36

Si $\mathbb{A}$ est intègre, alors $\mathbb{A}[X]$ est intègre.

Si $P \neq 0$ et $Q \neq 0$

$$\begin{aligned}\deg(P \times Q) &= \deg(P) + \deg(Q) \ (\mathbb{A} \text{ est intègre}) \\ &\geq 0\end{aligned}$$

13.39 Propriété de stabilité

Corollaire 13.39

- $\mathbb{A}_n[X]$ est un sous-groupe additif de $\mathbb{A}[X]$.
- La dérivation $D : \mathbb{A}[X] \to \mathbb{A}[X]$ induit un homomorphisme de groupe $D_n : \mathbb{A}_n[X] \to \mathbb{A}_{n-1}[X]$.
- Si $\mathbb{K}$ est un corps de caractéristique nulle, D_n est une surjection. Autrement dit, tout polynôme de $\mathbb{K}_{n-1}[X]$ est primitivable formellement dans $\mathbb{K}_n[X]$.

- RAF
- RAF
- $\text{carac}(\mathbb{K}) = 0$. Soit $P = \sum_{k=0}^{n-1} a_k X^k \in \mathbb{K}_{n-1}[X]$.
  Pour $k \in [\![1, n]\!], k = k \times 1 \neq 0$ dans $\mathbb{K}$ car $\mathbb{K}$ est de caractéristique nulle.
  Donc k^{-1} est bien défini dans $\mathbb{K}$. On pose :

$$Q = \sum_{k=1}^{n} k^{-1} q_{k-1} X^k$$

  Alors :

$$Q' = \sum_{k=0}^{n-1} (k+1)(k+1)^{-1} a_k X^k = P.$$

13.42 Corollaire du degré d'une dérivée dans $\mathbb{K}[X]$, avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$

Corollaire 13.42

Soit $\mathbb{K}$ un corps de caractéristique nulle et soit P et Q deux polynômes de $\mathbb{K}[X]$. Alors $P' = Q'$ si et seulement si P et Q diffèrent d'une constante.

Soit $P \in \ker(D)$, où $D : \mathbb{K}[X] \to \mathbb{K}[X], P \mapsto P'$.
Donc $P' = 0$.
Si $\deg(P) > 0$, alors $\deg(P') \geq 0$ (13.41).
Donc nécessairement, $\mathbb{K}_0[X] \subset \ker(D)$.
Donc $\ker(D) = \mathbb{K}_0[X]$.

Chapitre 14

Suites numériques

14.18 Premier théorème de comparaison

Théorème 14.18

Si à partir d'un certain rang on a
$$|u_n - l| \leq v_n$$
avec $v_n \underset{n\to+\infty}{\longrightarrow} 0$, alors $u_n \underset{n\to+\infty}{\longrightarrow} l$.

Soit $u_n \in \mathbb{N}$ tel que :
$$\forall n \geq N_1, |u_n - l| \leq v_n$$
Comme $v_n \underset{n\to+\infty}{\longrightarrow} 0$, pour tout $\epsilon > 0$, on choisit $N_2 \in \mathbb{N}$ tel que :
$$\forall n \geq N_2, |v_n - 0| = |v_n| < \epsilon$$
On pose $N = \max(N_1, N_2)$. Ainsi :
$$\forall n \geq \mathbb{N}, |u_n - l| \leq v_n = |v_n| < \epsilon$$
Donc $\boxed{u_n \underset{n\to+\infty}{\longrightarrow} l}$

14.22 Unicité de la limite

Propostion 14.22

Si u admet une limite $l \in \mathbb{R}$, alors celle-ci est unique.

On suppose que u admet comme limite l et l' dans $\mathbb{R}$.
Soit $\epsilon > 0$. On choisit N et N' dans $\mathbb{N}$ tels que :
$$\forall n \geq N, |u_n - l| < \epsilon$$
$$\forall n \geq N', |u_n - l'| < \epsilon$$
Pour tout $n \geq \max(N, N')$:
$$\begin{aligned} |l - l'| &= |l - u_n + u_n - l'| \\ &\leq |l - u_n| + |u_n - l'| \text{ (Inégalité triangulaire)} \\ &< l\epsilon \end{aligned}$$
Nécessairement :
$$|l - l'| = 0$$

14.23 Limite et inégalité

Propostion 14.23

Si u converge vers l et si $\alpha < l$, alors à partir d'un certain rang, $\alpha < u_n$. De la même manière, si $\beta > l$, alors à partir d'un certain rang, $u_n < \beta$.

On suppose que $u_n \underset{n\to+\infty}{\longrightarrow} l$. Soit $\alpha < l$. On pose $\epsilon = \frac{|l-\alpha|}{2}$.
D'après la définition, on choisit $N \in \mathbb{N}$ tel que :
$$\forall n \geq N, |u_n - l| < \epsilon$$
Soit :
$$\forall n \geq N, \underbrace{u_n}_{>\alpha} \in]\underbrace{l-\epsilon}_{>\alpha}, l+\epsilon[$$

14.24 Convergence et bornitude

Propostion 14.24

Une suite convergente est bornée.

Soit u une suite convergente. Notons $l = \lim\limits_{n \to +\infty} u_n$.
On pose $\epsilon =$.
Par définition, soit $N \in \mathbb{N}$ tel que :

$$\forall n \geq N, u_n \in]l-1, l+1[$$

Donc $\{u_n, n \geq N\}$ est borné. Donc $\{u_n, n \in \mathbb{N}\} = \underbrace{\{u_n, n \in [\![0, N-1]\!]\}}_{\text{ensemble fini}} \cup \underbrace{\{u_n, n \geq N\}}_{\text{borné}}$ est borné.

14.29 Minoration d'une extraction

Lemme 14.29

Soit $\sigma : \mathbb{N} \to \mathbb{N}$ une application strictement croissante, alors

$$\forall n \in \mathbb{N}, n \leq \sigma(n).$$

Par récurrence.
Comme $\sigma(0) \in \mathbb{N}$, on a bien $\sigma(0) \geq 0$.
Si $\sigma(n) \geq n$, alors $\sigma(n+1) > \sigma(n) \geq n$.
Donc $\sigma(n+1) \geq n+1$.

14.30 Extraction d'une suite convergente

Propostion 14.30

Toute suite extraite d'une suite qui tend vers $l \in \overline{\mathbb{R}}$ est une suite convergente vers l.

On suppose que $u_n \underset{n \to +\infty}{\longrightarrow} l \in \mathbb{R}$ (à adapter pour $l = \pm\infty$)
Soit $\sigma : \mathbb{N} \to \mathbb{N}$ strictement croissante.
On note $v = u \circ \sigma$.
Soit $\epsilon > 0$. Soit $N \in \mathbb{N}$ tel que :

$$\forall n \geq \mathbb{N}, |u_n - l| < \epsilon$$

Pour $n \geq N$, on a :

$$\begin{aligned} \sigma(n) &\underset{(14.29)}{\geq} n \geq N \\ \text{donc } &|u_{\sigma(n)} - l| < \epsilon \\ \text{soit } &|v_n - l| < \epsilon \\ \text{donc } &\boxed{v_n \underset{n \to +\infty}{\longrightarrow} l} \end{aligned}$$

14.32 Pair, impair et convergence

Propostion 14.32

Si $\lim u_{2n} = \lim u_{2n+1} = l \in \mathbb{R}$, alors $\lim u_n = l$

Soit $\epsilon > 0$. Soit N_1 et N_2 dans $\mathbb{N}$ telq que :

$$\forall n \geq N_1, |u_{2n} - l| \leq \epsilon$$
$$\forall n \geq N_2, |u_{2n+1} - l| \leq \epsilon$$

Or pour $N = \max(2N_1, 2N_2+1)$.
Soit $n \geq N$.

- Si $n = 2p$, alors $p \geq N_1$
$$|u_n - l| = |u_{2p} - l| \leq \epsilon$$
- Si $n = 2p+1$, alors $p \geq N_2$
$$|u_n - l| = |u_{2p+1} - l| \leq \epsilon$$

Dans tous les cas, $\boxed{|u_n - l| \leq \epsilon}$.

14.34 Opérations usuelles sur les limites

Théorème 14.34

Soit u et v deux suites qui convergent respectivement vers l et l' et soit $\lambda \in \mathbb{R}$, alors
- $u+v$ converge ver $l+l'$
- λu converge vers λl
- uv converge vers ll'
- Si $l \neq 0$, alors à partir d'un certain rang, la suite des termes u_n sont tous nuls et la suite $\frac{1}{u}$ converge vers $\frac{1}{l}$

- Soit $n \in \mathbb{N}$ tel que
$$\forall n \in \mathbb{N}, |u_n - l| \leq \epsilon \text{ et } |v_n - l'| \leq \epsilon$$
Donc :
$$\begin{aligned}\forall n \in \mathbb{N}, |u_n + v_n - (l+l')| &\leq |u_n - l| + |v_n - l'| \text{ (Inégalité triangulaire)} \\ &\leq \epsilon\end{aligned}$$
- RAS ($\lambda = 0$ et $\lambda \neq 0$)
- Comme u converge, u est bornée. Soit $M \in \mathbb{R}_+$ tel que :
$$\forall n \in N, |u_n| \leq M$$
Pour $n \in \mathbb{N}$:
$$\begin{aligned}|u_n v_n - ll'| &= |u_n v_n - u_n l' + u_n l' - ll'| \\ &\leq |M||v_n - l'| + |l'| \times |u_n - l| \\ &\leq M \times \epsilon + |l'| \times \epsilon \\ &= (M + |l'|) \times \epsilon\end{aligned}$$
Donc $\boxed{u_n v_n \underset{n\to+\infty}{\longrightarrow} ll'}$.
- On suppose $l \neq 0$. D'après (14.23), à partir d'un certain rang $u_n > 0$ (ou $u_n < 0$). Il existe en outre $N \in \mathbb{N}$ tel que :
$$0 < \frac{l}{2} < u_n \text{ et } |u_n - l| < \epsilon$$
Pour $n \geq N$:
$$\begin{aligned}\left|\frac{1}{u_n} - \frac{1}{l}\right| &= \frac{|l - u_n|}{|u_n l|} \\ &\leq 2\frac{|l-u_n|}{l^2} \\ &< \frac{2\epsilon}{l^2}\end{aligned}$$

14.35 Conservation des inégalités larges par passage à la limite

Théorème 14.35

Soit u et v deux suites réelles. Si u converge vers l et v converge vers l' et si à partir d'un certain rang $u_n \leq v_n$ alors $l \leq l'$.

On raisonne par l'absurde : $l > l'$.
On pose $\epsilon = \frac{|l'-l|}{2}$.
On choisit $N \in \mathbb{N}$ tel que :

$$\forall n \geq N, u_n \in]l-\epsilon, l+\epsilon[\text{ et } v_n \in]l'-\epsilon, l'+\epsilon[$$

En particulier :

$$\forall n \geq N, u_n > v_n$$

Absurde.

14.37 Théorème d'encadrement

Théorème 14.37

Soit u, v et w trois suites réelles. Si u et v convergent vers l et si à partir d'un certain rang, $u_n \leq w_n \leq v_n$, alors w converge vers l.

Soit $\epsilon > 0$, on choisit $N \in \mathbb{N}$ tel que :

$$\forall n \geq N, u_n \in]l-\epsilon[\text{ et } v_n \in]l-\epsilon, l+\epsilon[$$

A partir d'un certain rang M, par connexité de l'intervalle $]l-\epsilon, l+\epsilon[$:

$$\forall n \geq M, w_n \in]l-\epsilon, l+\epsilon[$$

14.38 Produit d'une suite bornée par une limite nulle

Théorème 14.38

Soit u et v deux suites réelles. Si u converge vers 0 et si v est bornée, alors w converge vers 0.

Soit $M \in \mathbb{R}_+$ telq ue :

$$\forall n \in \mathbb{N}, |v_n| \leq M$$

Alors :

$$\forall n \in \mathbb{N}, |u_n v_n| \leq M \times |u_n| \underset{n\to+\infty}{\longrightarrow} 0$$

Donc :

$$|u_n v_n| \underset{n\to+\infty}{\longrightarrow} 0$$

Soit :

$$u_n v_n \underset{n\to+\infty}{\longrightarrow} 0$$

14.39 Exemple

Exemple 14.39

Soit (u_n) une suite strictement positive et $\eta \in]0;1[$. On suppose qu'à partir d'un certain rang, on a $\frac{u_{n+1}}{u_n} \leq \eta$. Alors $\lim u_n = 0$.

On suppose que :

$$\forall n \geq n_0, \frac{u_{n+1}}{u_n} \leq 2$$

Donc ($u_n > 0$) :

$$\forall n \geq n_0, 0 < u_n < \underbrace{\eta^{n-n_0}}_{\underset{n \to +\infty}{\longrightarrow} 0} \times u_{n_0}$$

Par encadrement :

$$\boxed{u_n \underset{n \to +\infty}{\longrightarrow} 0}$$

14.40 Comparaison puissance factorielle

Théorème 14.40

$$\forall x \in \mathbb{R}, \lim_{n \to +\infty} \frac{x^n}{n!} = 0.$$

Pour $x \in \mathbb{R}$ fixé, non nul.
On note pour tout $n \in \mathbb{N}$:

$$u_n = \frac{|x|^n}{n!} > 0$$

Or :

$$\frac{u_{n+1}}{u_n} = \frac{|x|}{n+1} \underset{n \to +\infty}{\longrightarrow} 0$$

A partir d'un certain rang :

$$\frac{u_{n+1}}{u_n} \leq \frac{1}{2}$$

Donc (14.39) :

$$\boxed{u_n \underset{n \to +\infty}{\longrightarrow} 0}$$

14.41 Caractérisation séquentielle de la borne supérieure

Théorème 14.41

Soit A une partie non vide de $\mathbb{R}$ et soit $M \in \mathbb{R}$. Alors M est la borne supérieure (resp. inférieure) de A si et seulement si M majore (resp. minore) A et s'il existe une suite d'éléments de A qui converge vers M.

$\boxed{\Rightarrow}$
On suppose que $M = \sup A$. Donc M majore A.
On rappelle que :

$$\forall \epsilon > 0, \exists a \in A, M - \epsilon < a$$

Donc :

$$\forall n \in N, \exists a \in A, M - \frac{1}{n+1} < a_n \leq M \text{ (M est un majorant)}$$

D'après la suite $(a_n) \in A^{\mathbb{N}}$ étant ainsi définie, d'après le théorème d'encadrement :

$$\boxed{a_n \underset{n \to +\infty}{\longrightarrow} M}$$

$\boxed{\Leftarrow}$
On choisit $(a_n) \in A^{\mathbb{N}}$ telle que :

$$a_n \underset{n\to+\infty}{\longrightarrow} M \text{ (majorant de } A\text{)}$$

Soit $\epsilon > 0$. On choisit $a_n \in A$ tel que :

$$a_n \in]M-\epsilon, M+\epsilon[$$

Donc $M - \epsilon$ ne majore pas A.
Donc :

$$\boxed{M = \sup A}$$

14.42 Caractérisation séquentielle de la borne supérieure

Théorème 14.42

Soit A une partie non vide de $\mathbb{R}$, alors A est dense dans $\mathbb{R}$ si et seulement si pour tout $x \in \mathbb{R}$, il existe une suite d'éléments de A qui converge vers x.

$\boxed{\Rightarrow}$
On suppose que A est dense dans $\mathbb{R}$.
Soit $x \in \mathbb{R}$.

$$\forall \epsilon > 0, \exists a \in A, a \in]x-\epsilon, x+\epsilon[$$

En particulier :

$$\forall n \in \mathbb{N}, \exists a_n \in A, x - \frac{1}{n+1} < a_n < x + \frac{1}{n+1}$$

La suite $(a_n) \in A^{\mathbb{N}}$ étant fixée ainsi :

$$a_n \underset{n\to+\infty}{\longrightarrow} x \text{ (théorème d'encadrement)}$$

$\boxed{\Leftarrow}$
Soit $]x, y[$ un intervalle non vide de $\mathbb{R}$.
On pose $z = \frac{x+y}{2}$. On pose $\epsilon = \frac{|y-x|}{2}$.
On choisit $(a_n) \in A^{\mathbb{N}}$ telle que :

$$a_n \underset{n\to+\infty}{\longrightarrow} z$$

On choisit $N \in \mathbb{N}$ tel que :

$$a_n \in]z-\epsilon, z+\epsilon[=]x, y[$$

Donc :

$$\boxed{A \cap]x, y[\neq \emptyset}$$

14.48 Théorème de comparaison

Théorème 14.48

Soit u et v deux suites réelles.

1. Si $\lim u = +\infty$ et si à partir d'un certain rang on a $u_n \leq v_n$, alors $\lim v = +\infty$;
2. Si $\lim v = -\infty$ et si à partir d'un certain rang on a $u_n \leq v_n$, alors $\lim u = -\infty$;
3. Si $\lim u = +\infty$ (resp. $-\infty$) et si v est minorée (resp. majorée), alors $\lim u + v = +\infty$ (resp. $-\infty$).

1. Soit $A \geq 0$. On choisit $n \in \mathbb{N}$ tel que :
$$\forall n \geq N, A \leq u_n \text{ et } u_n \leq v_n$$
Donc :
$$\boxed{v_n \underset{n \to +\infty}{\longrightarrow} +\infty}$$
2. RAS
3. Si (v_n) est minorée, alors à partir d'un certain rang :
$$m + u_n \leq u_n + v_n$$
En adaptant le premier point ($A' = A - m$), on a :
$$\boxed{u_n + v_n \underset{n \to +\infty}{\longrightarrow} +\infty}$$

14.49 Limites infinies et opérations

Théorème 14.49

Soit u et v deux suites réelles de limites respectives l et l' dans $\overline{\mathbb{R}}$ et soit $\lambda \in \mathbb{R}$. On a
- $\lim u + v = l + l'$ (sauf si $l = +\infty$ et $l' = -\infty$ ou inversement)
- $\lim \lambda u = \lambda l$ sauf si $\lambda = 0$ auquel cas la suite λu est la suite nulle.
- $\lim u \times v = l \times l'$ sauf si $\lambda = 0$ et $l' = \pm\infty$ ou inversement
- Si à partir d'un certain rang, la suite u ne s'annule pas, alors la suite $\frac{1}{u}$:
  - si $l \in \mathbb{R}^*$, tend vers $\frac{1}{l}$;
  - si $l = \pm\infty$, tend vers 0 ;
  - si $l = 0$ et $u_n > 0$, tend vers $+\infty$;
  - si $l = 0$ et $u_n < 0$, tend vers $-\infty$;
  - n'a pas de limite dans les autre cas.

- On suppose $l' \in \mathbb{R}$ et $l = +\infty$. Donc v est bornée.
  Donc (14.48) :
$$u_n + v_n \underset{n \to +\infty}{\longrightarrow} +\infty$$
- $\lambda \neq 0, \lambda > 0$ et $l = +\infty$. Pour $A \in \mathbb{R}$, on choisit un rang à partir duquel $u_n > \frac{A}{\lambda}$.
- On suppose $l > 0$ et $l' = +\infty$.

  Comme $u_n \underset{n \to +\infty}{\longrightarrow} l$, alors à partir d'un certain rang, $u_n > m$ avec $m = \begin{cases} 1 \text{ si } l = +\infty \\ \frac{l}{2} \text{ sinon} \end{cases}$
$$u_n v_n > m v_n \underset{n \to +\infty}{\longrightarrow} +\infty$$
  Donc :
$$u_n v_n \underset{n \to +\infty}{\longrightarrow} +\infty \text{ (14.48)}$$
- $l = +\infty$.
  Soit $\epsilon > 0$, à partir d'un certain rang :
$$u_n > \frac{1}{\epsilon} > 0$$
  Donc :
$$0 < \frac{1}{u_n} < \epsilon$$
$$\frac{1}{u_n} \underset{n \to +\infty}{\longrightarrow} 0$$

Si $l = 0$ et $u_n > 0$ à partir d'un certain rang.
Pour $A \in \mathbb{R}_+^*$, à partir d'un certain rang :

$$u_n > 0 \text{ et } u_n < \frac{1}{A}$$
$$\text{donc } \frac{1}{u_n} > A$$
$$\frac{1}{u_n} \underset{n \to +\infty}{\longrightarrow} +\infty$$

14.50 Théorème de la limite monotone

Théorème 14.50

Si u est une suite croissante et majorée (resp. décroissante et minorée), alors u converge vers $\sup_{n \in \mathbb{N}}(u_n)$ (resp. vers $\inf_{n \in \mathbb{N}}(u_n)$).
Si u est une suite croissante et non majorée (resp. décroissante et non minorée) alors u tend vers $+\infty$ (resp. vers $-\infty$).

— On suppose u croissante et majorée.
L'ensemble $A = \{u_n | n \in \mathbb{N}\}$ est non vide et majoré. Cet ensemble possède une borne supérieure notée l (propriété fondamentale de $\mathbb{R}$).
Soit $\epsilon >$. Comme $l - \epsilon < u_n$ ne majore pas A, on choisit $N \in \mathbb{N}$ tel que $l - \epsilon < u_n$.
Or (u_n) est croissante donc :

$$\forall n \geq N, l - \epsilon < u_N \leq u_n \leq l$$

Donc :

$$\forall n \geq N, u_n \in]l - \epsilon, l + \epsilon[$$

Soit :

$$\boxed{u_n \underset{n \to +\infty}{\longrightarrow} l}$$

— On suppose u croissante et non majorée.
Soit $A \in \mathbb{R}_+$. Soit $N \in \mathbb{N}$ tel que :

$$u_N \geq A \ (u \text{ non majorée})$$

Donc :

$$\forall n \geq N, A \leq u_N \leq u_n \ (u \text{ croissante})$$

Soit :

$$\boxed{u_n \underset{n \to +\infty}{\longrightarrow} +\infty}$$

14.54 Exemple

Exemple 14.54

Soit u et v les suites définies par

$$\forall n \in \mathbb{N}^*, u_n = \sum_{k=0}^{n} \frac{1}{k!} \text{ et } v_n = u_n + \frac{1}{n \times n!}$$

Ces deux suites sont adjacentes.

—

$$\forall n \in \mathbb{N}^*, u_{n+1} - u_n = \frac{1}{(n+1)!} \geq 0$$

Donc (u_n) est croissante.

—

$$\begin{aligned}\forall n \in \mathbb{N}^* v_{n+1} - v_n &= u_{n+1} - u_n + \frac{1}{(n+1)(n+1)!} - \frac{1}{nn!} \\ &= \frac{1}{(n+1)!} + \frac{1}{(n+1)(n+1)!} - \frac{1}{nn!} \\ &= \frac{1}{n!}\left[\frac{1}{n+1} + \frac{1}{(n+1)^2} - \frac{1}{n}\right] \\ &= \frac{1}{n!(n+1)^2 n}[(n+1)n + n - (n+1)^2] \\ &= -\frac{1}{n!(n+1)^2 n} \\ &\leq 0\end{aligned}$$

—

$$\forall n \in \mathbb{N}^*, v_n - u_n = \frac{1}{n \times n!}$$

Donc :

$$v_n - u_n \underset{n \to +\infty}{\longrightarrow} 0$$

Donc u et v sont adjacentes et convergent alors vers une limite commune. (TCSA)

14.55 Convergence des suites adjacentes

Théorème 14.55

Deux suites adjacentes convergent vers une limite commune.

Soit u et v deux suites adjacentes avec u croissante et v décroissante.
Soit $w = v - u$. Par opération, w est décroissante.
Par hypothèse :

$$w_n \underset{n \to +\infty}{\longrightarrow} 0$$

Donc $w \leq 0$, soit $u \leq v$.
La suite u est donc majorée par v_0, et croissante donc convergente d'après le théorème de la limite monotone.
Pour les mêmes raisons, v converge.
Or, par théorème d'opérations :

$$\lim_{n \to +\infty} v_n - \lim_{n \to +\infty} u_n = \lim_{n \to +\infty} (v_n - u_n) = 0$$

14.56 Théorème de Bolzano-Weierstrass

Théorème 14.56

On peut extraire de toute suite réelle bornée une suite convergente.

Soit u une suite bornée. On note a et b un minorant et majorant de u. On construit deux suites (a_n) et (b_n) par récurrence de la manière suivante :

- On initialise $a_0 = a$ et $b_0 = b$.
- Si l'intervalle $\left[a_0, \frac{a_0+b_0}{2}\right]$ contient une infinité de valeurs de la suite (u_n), alors $a_1 = a_0$ et $b_1 = \frac{a_0+b_0}{2}$.
  Sinon, l'intervalle $\left[\frac{a_0+b_0}{2}, b_0\right]$ contient une infinité de valeurs, alors $a_1 = \frac{a_0+b_0}{2}$ et $b_1 = b_0$.
  On note $\sigma(0) = 0$ et comme $[a_1, b_1]$ contient une infinité de valeurs, on dixe $u_{n_1} \in [a_1, b_1]$ avec $n_1 > 0$.
  On pose alors $\sigma(1) = n_1$.
- Supposons construits (a_n), (b_n) et σ avec le principe précédent :

$$\forall n \in \mathbb{N}, \begin{cases} a_{n+1} = a_n \text{ et } b_{n+1} = \frac{a_n+b_n}{2} \\ \text{ou} \\ a_{n+1} = \frac{a_n+b_n}{2} \text{ et } b_{n+1} = b_n \end{cases}$$

Selon que $\left[a_n, \frac{a_n+b_n}{2}\right]$ contient une infinité de valeurs ou $\left[\frac{a_n+b_n}{2}, b_n\right]$ et $v(n+1) > v(n)$ et $u_{\sigma(n+1)} \in [a_{n+1}, b_{n+1}]$.

$$\begin{aligned}\forall n \in \mathbb{N}, a_n \leq u_{\sigma(n)} \leq b_n \\ \forall n \in \mathbb{N}, |b_{n+1} - a_{n+1}| = \frac{|b_n - a_n|}{2} \\ \forall n \in \mathbb{N}, |b_n - a_n| = \frac{|b_0 - a_0|}{2^n} \underset{n \to +\infty}{\longrightarrow} 0\end{aligned}$$

Donc (a_n) et (b_n) sont adjacentes donc convergent vers la même limite (TCSA) donc $(u_{\sigma(n)})$ converge (TE).

14.63 Exemple

Exemple 14.63

La suite (u_n) définie par $u_0 = 1$ et pour tout $n \in \mathbb{N}, u_{n+1} = u_n + e^{u_n}$ diverge vers $+\infty$.

R_+ est stable par $f : x \mapsto x + e^x$.
Comme $0 \in \mathbb{R}_+$, la suite (u_n) est bien définie.

$$\forall n \in \mathbb{N}, u_{n+1} = f(u_n) = u_n + e^{u_n} \geq u_n$$

Donc (u_n) est croissant.
Supposeons que $u_n \underset{n \to +\infty}{\longrightarrow} l \in \mathbb{R}_+$.
Par théorème d'opération, $l = l + e^l$.
Absurde.
Donc d'après le TLM :

$$u_n \underset{n \to +\infty}{\longrightarrow} +\infty$$

14.64 Exemple

Exemple 14.64

La suite (u_n) défine par $u_0 = 1$ et pour tout $n \in \mathbb{N}, u_{n+1} = \frac{u_n}{1+u_n^2}$ converge vers 0.

$[0, 1]$ est stable par $f : x \mapsto \frac{x}{x^2+1}$ et $1 \in [0, 1]$.
Donc (u_n) est bien définie et est minorée.
Or :

$$\forall n \in \mathbb{N}, u_{n+1})f(u_n) = \frac{u_n}{u_n^2 + 1} \leq u_n$$

Donc (u_n) est décroissante donc converge vers $l \in [0, 1]$ d'après le TLM.
Par théorème d'opération :

$$\begin{aligned}l = \frac{l}{l^2 + 1} \\ \text{donc } l^2 = 0 \\ \text{donc } l = 0\end{aligned}$$

14.66 Monotonie d'une suite récurrente définie par une relation $u_{n+1} = f(u_n)$

Théorème 14.66

Soit D une partie de $\mathbb{R}$, $u_0 \in D$ et $f : D \to D$ une fonction (autrement dit, D est stable par f). On note (u_n) l'unique suite définie sur $\mathbb{N}$ par $u_{n+1} = f(u_n)$.

1. Si pour tout $x \in D, f(x) \geq x$, alors (u_n) est croissante. Si pour tout $x \in D, f(x) \leq x$, alors (u_n) est décroissante. Le signe de la fonction $x \mapsto f(x) - x$ renseigne donc sur la monotonie de la suite (u_n).
2. Si f est croissante, alors (u_n) est monotone. Son sens de variation dépend alors du signe de $u_1 - u_0$.
3. Si f est décroissante, alors (u_{2n}) et (u_{2n+1}) sont monotones et de sens contraires. Leur sens de variation est entièrement déterminé par le signe de $u_2 - u_0$.

1. Si :

$$\forall n \in D, f(x) \geq x$$

Alors :

$$\forall n \in \mathbb{N}, f(u_n) = u_{n+1} > u_n$$

Donc (u_n) est croissante.

2. On suppose f croissate et $u_0 \leq u_1$. Alors :

$$u_1 = f(u_0) \leq f(u_1) = u_2$$

On termine par récurrence.

3. Si f est décroissante, alors $f^2 = f \circ f$ est croissante. Or :

$$\begin{aligned}\forall n \in \mathbb{N}, u_{2n+2} &= f^2(u_{2n}) \\ u_{2n+1} &= f^2(u_{2n-1})\end{aligned}$$

Donc (14.66.2) (u_{2n}) et (u_{2n+1}) sont monotones.
Or, si $u_2 \leq u_0$, alors $u_3 = f(u_2) \leq f(u_0) = u_1$

14.68 Exemple

Exemple 14.68

On note (u_n) la suite définie par $u_0 = 1$ et pour tout $n \in \mathbb{N}, u_{n+1} = u_n^2 + u_n$ et notons $f : x \mapsto 1 + \frac{1}{x}$.
Etudier la convergence de la suite (u_n).

$\mathbb{R}_+$ est stable par $f : x \mapsto x^2 + x$ et $1 \in \mathbb{R}_+$.
Donc (u_n) est bien définie.
Comme :

$$\forall x \in \mathbb{R}_+, f(x) - x \geq 0$$

(u_n) est croissante.
On suppose que :

$$u_n \underset{n \to +\infty}{\longrightarrow} l \geq 1 = u_0$$

Comme $f \in \mathcal{C}^\infty(\mathbb{R}_+, \mathbb{R}_+)$.
On a $f(l) = l$ donc $l^2 = 0$.
Absurde.
Donc, d'après le TLM :

$$u_n \underset{n \to +\infty}{\longrightarrow} +\infty$$

14.69 Exemple

Exemple 14.69

On note (u_n) la suite définie apr $u_0 = 1$ et pour tout $n \in \mathbb{N}, u_{n+1} = 1 + \frac{1}{u_n}$, et notons $f : x \mapsto 1 + \frac{1}{x}$.
Etudier la convergence de la suite (u_n).

$[1, 2]$ est stable par $f : x \mapsto 1 +\ frac1x$ et $1 \in [1, 2]$.
Donc (u_n) est bien définie et est bornée.
Comme f est décroissante sur $[1, 2]$, (u_{2n}) et (u_{2n+1}) sont monotones de monoties contraires.
Comme$u_0 = 1 = \min([1, 2])$, (u_{2n}) est croissante et (u_{2n+1}) décroissante, puis convergentes (TLM) vers des points fixes de f^2 (car f^2 est continue sur $[1, 2]$)
Soit $x \in [1, 2]$.

$$\begin{aligned} f^2(x) = x &\Leftrightarrow 1 + \frac{1}{1 + \frac{1}{x}} = x \\ &\Leftrightarrow x + 1 + x = x(x+1) \\ &\Leftrightarrow x^2 - x - 1 = 0 \\ &\Leftrightarrow \left(x - \underbrace{\frac{1+\sqrt{5}}{2}}_{\in[1,2]}\right)\left(x - \underbrace{\frac{1-\sqrt{5}}{2}}_{\notin[1,2]}\right) = 0 \\ &\Leftrightarrow x = \frac{1+\sqrt{5}}{2} \end{aligned}$$

Donc (u_{2n}) et (u_{2n+1}) convergent nécessairement vers $\frac{1+\sqrt{5}}{2}$.
Donc :

$$u_n \underset{n\to+\infty}{\longrightarrow} \frac{1+\sqrt{5}}{2}$$

14.72 Convergence et parties réelles et imaginaires

Théorème 14.72

Soit u une suite complexe et $l \in \mathcal{C}$. Alors la suite u converge vers l si et seulement si la suite $(Re(u_n))$ converge vers $Re(l)$ et $(Im(u_n))$ converge vers $Im(l)$.

$\boxed{\Rightarrow}$
Pour tout $n \in \mathbb{N}$:

$$|Re(u_n) - Re(l)| \leq |u_n - l| \underset{n\to+\infty}{\longrightarrow} 0$$
$$|Im(u_n) - Im(l)| \leq |u_n - l| \underset{n\to+\infty}{\longrightarrow} 0$$

Ainsi, $Im(u_n) \underset{n\to+\infty}{\longrightarrow} Im(l)$ et $Re(u_n) \underset{n\to+\infty}{\longrightarrow} Re(l)$.

$\boxed{\Leftarrow}$ On a :

$$\begin{aligned} |u_n - l| &= \sqrt{(Im(u_n) - Im(l))^2 + (Re(u_n) - Re(l))^2} \\ &\underset{n\to+\infty}{\longrightarrow} 0 \text{ (théorème d'opérations)} \end{aligned}$$

14.73 Théorème de Bolzano-Weierstrass pour les suites complexes

Remarque 14.73

Si u est bornée , on peut en extraire une suite convergente (Bolzano-Weierstrass).

$u_n = a_n + b_n$ bornée.
(a_n) et (b_n) sont bornés.
(a_n) borneé donc $(a_{\sigma(n)})$ converge.
$(b_{\sigma(n)})$ bornée donc $(b_{\sigma\circ\varphi(n)})$ converge.
$(a_{\sigma\circ\varphi(n)})$ extraite de $(a_{\sigma(n)})$ donc converge.
$(u_{\sigma\circ\varphi(n)})$ converge.

Chapitre 15

Limites et continuité

15.6 Limite en un point du domaine

Propostion 15.6

Si $a \in X$ et si $f(x)$ admet une limite finie en a, alors cette limite est nécessairement égale à $f(a)$.

Comme $f(x)$ admet une limite finie b quand $x \to a$:

$$\forall \epsilon, \exists \nu > 0, \forall x \in X, |x-a| \leq \nu \Rightarrow |f(x) - b| \leq \epsilon$$

Or pour tout $\epsilon > 0$:

$$|a-a| \leq \nu \text{ (quelque soit } \nu)$$

Donc :

$$\forall \epsilon, |f(a) - b| \leq \epsilon$$

Donc $\boxed{f(a) = b}$.

15.15 Comparaison des limites de deux fonctions coincidant au voisinage de a

Propostion 15.15

Soit f et g deux fonctions coincidant au voisinage d'un point a. Alors, si f admet une limite (finie ou infinie) en a, alors g aussi et

$$\lim_{x \to a} f(x) = \lim_{x \to a} g(x)$$

On choisit $W \in \mathcal{V}(a)$ tel que $W \cap X = W \cap Y$ et $f|_{W \cap X} = g|_{W \cap Y}$.
Soit $b \in \overline{\mathbb{R}}$ tel que $f(x)$ tend vers b quand $x \to a$.
Soit $V \in \mathcal{V}(b)$. On choisit $U \in \mathcal{V}(a)$ tel que :

$$f(U \cap X) \subset V$$

Or

$$W \cap U \in \mathcal{V}(a) \text{ et } \subset f(W \cap U \cap X)_{g(W \cap U \cap Y)} \subset V$$

Donc g admet une limite en a égale à b

15.17 Unicité de la limite, cas réel

Théorème 15.17

Soit $a \in \overline{X}$ et f une fonction réelle. Sous réserve d'existence, la limite de $f(x)$, lorsque x tend vers a est unique.

Par l'absurde. On suppose que f possède deux limites $l \neq l'$ en a.
On choisit $u \in \mathcal{V}(l)$ et $u' \in \mathcal{V}(l')$ tels que $u \cap u' = \emptyset$.
Par définition, on choisit $(W, W') \in \mathcal{V}(a)^2$ tels que $f(W \cap X) \subset U$ et $f(W' \cap X) \subset U'$.
Or $\underbrace{W \cap W'}_{\neq \emptyset} \notin \mathcal{V}(a)$ et $f(\underbrace{W \cap W' \cap X}_{\neq \emptyset}) \subset U \cap U' = \emptyset$.
Absurde.

15.23 Propostion

Propostion 15.23

Soit $a \in \overline{X}$. Soit $(Z_i)_{i \in I}$ une famille **finie** de sous-ensembles de $\mathbb{R}$ tels que $X \in \bigcup_{i \in I} Z_i$ (on dit que (Z_i) est un **recouvrement** de X). La fonction f admet au point a une limite ℓ (finie ou infinie) si et seulement si pour tout i tel que la limite de f en a sur Z_i est envisageable, cette limite existe et vaut ℓ.

$\boxed{\Rightarrow}$
On suppose que $\lim_a f = \ell$.
Soit $i \in I$ tel que $a \in \overline{X \cap Z}$.
Soit $V \in \mathcal{V}(\ell)$. On choisit $U \in \mathcal{V}(a)$ tel que $f(U \cap X) \subset V$.
EN particulier $f(\underbrace{U \cap X \cap Z_i}_{\subset U \cap X}) \subset V = f|_{X \cap Z_i}(U \cap X \cap Z_i)$.

$\boxed{\Leftarrow}$
Notons $J \subset I$ l'ensemble des indices pour lesquels la limite est envisageable en Z_i.
Soit $V \in \mathcal{V}(\ell)$. Pour tout $i \in J$, comme $\lim_{x \to a x \in Z_i} = \ell$ on choisit $U_i \in \mathcal{V}(a)$ tel que $f|_{Z_i \cap X}(U_i \cap Z_i \cap X) \subset V$.
On pose $U = \bigcap_{i \in J} U_i \in \mathcal{V}(a)$ car J est fini.
On choisit $U' \in \mathcal{V}(a)$ tel que $U' \cap \left(\bigcup_{i \in I \setminus J} Z_i \right) = \emptyset$.
$f(U \cap U' \cap X) \subset V$
Donc $\boxed{\lim_a f = \ell}$.

15.30 Composition de limites

Propostion 15.30

Soit $f : X \to \mathbb{R}$, $g : Y \to \mathbb{R}$ deux fonctions avec $f(X) \subset Y$. Soit $a \in \overline{X}$, $b \in \overline{Y}$ et $c \in \overline{\mathbb{R}}$. Si $\lim_a f = b$ et si $\lim_b g = c$, alors $\lim_a g \circ f = c$.

Soit $W \in \mathcal{V}(c)$. On choisit $V \in \mathcal{V}(b)$ tel que :

$$g(V \cap Y) \subset W$$

On choisit $U \in \mathcal{V}(a)$ tel que :

$$f(U \cap X) \subset V \cap Y \ (\lim_a f = b)$$

On a alors :

$$\boxed{g \circ f(U \cap X) \subset W}$$

15.32 Limites et inégalités strictes

Propostion 15.32

Soit $f : X \to \mathbb{R}$, $a \in \overline{X}$, $m \in \mathbb{R}$ et $M \in \mathbb{R}$.

1. Si $\lim_a f < M$ alors $f(x) < M$ au voisinage de a
2. Si $\lim_a f > m$ alors $f(x) > m$ au voisinage de a.

1. Notons $b = \lim_a f \in \overline{\mathbb{R}}$. Si $b < M$, on choisit $U \in \mathcal{V}(b)$ et $U' \in \mathcal{V}(M)$ avec $U < U'$.
   Comme $\lim_a f = b$, on choisit $W \in \mathcal{V}(a)$ tel que :

$$f(W \cap X) \subset U$$

15.33 Limite et inégalités larges

Propostion 15.33

Soit $f : X \to \mathbb{R}$ et $g : X \to \mathbb{R}$ deux fonctions et $a \in \overline{X}$. On suppose que f et g possède des limites finies en a.
Si $f(x) \leq g(x)$ au voisinage de a, alors $\lim\limits_{a} f \leq \lim\limits_{a} g$.
Ce résultat est le plus souvent utilisé lorsqu'une des deux fonctions est constante.

RAF : absurde + (15.32)

15.34 Caractérisations séquentielle de la limite d'une fonction

Théorème 15.34

Soit $f : X \to \mathbb{R}$ une fonction et $a \in \overline{X}$ et $\ell \in \overline{\mathbb{R}}$. Sont équivalentes :

1. $\lim\limits_{a} f = \ell \Leftrightarrow \forall u_n \to a, \lim f(u_n) = \ell \; (= f(\lim u_n))$
2. Pour toute suite (u_n) de limite a à valeurs dans X, la suite $(f(u_n))$ a pour limite ℓ.

$\boxed{1 \Rightarrow 2}$
On suppose que $\lim\limits_{a} f = \ell$.
Soit $(u_n) \in X^{\mathbb{N}}$ avec $u_n \underset{n\to+\infty}{\longrightarrow} a$.
Soit $V \in \mathcal{V}(\ell)$. On choisit $U \in \mathcal{V}(a)$ tel que :

$$f(U \cap X) \subset V \; (\lim_{a} f = \ell)$$

Comme $u_n \underset{n\to+\infty}{\longrightarrow} a$, on choisit $N \in \mathbb{N}$ tel que :

$$\forall n \geq N, u_n \in U \cap X$$

Donc :

$$\forall n \geq N, f(u_n) \in V$$

Donc :

$$f(u_n) \underset{n\to+\infty}{\longrightarrow} \ell$$

$\boxed{1 \Leftarrow 2}$
Par contraposée. On suppose que f n'admet pas ℓ comme limite en a. Pour tout $n \in \mathbb{N}$, on note :

$$V_n = \begin{cases}]a - \frac{1}{n+1}, a + \frac{1}{n+1}[\text{ si } a \in \mathbb{R} \\ [n, +\infty[\text{ si } a = +\infty \\ ]-\infty, -n] \text{ si } a = -\infty \end{cases}$$

Par définition, il existe $W \in \mathcal{V}(\ell)$ tel que pour tout $V \in \mathcal{V}(a)$, il existe $x \in V \cap X$ et $f(x) \neq W$.
Pour tout $n \in \mathbb{N}$, on choisit $x_n \in V_n \cap X$ tel que $f(x_n) \neq W$.
Par construction :

$$(x_n) \in X^{\mathbb{N}}, x_n \underset{n\to+\infty}{\longrightarrow} a \text{ et } f(x_n) \underset{n\to+\infty}{\not\longrightarrow} \ell$$

15.39 Théorème de la limite monotone

Théorème 15.39

Soit $a \in \mathbb{R}$ et $b \in \mathbb{R} \cup \{+\infty\}$ avec $a < b$ et $f : [a, b[\to \mathbb{R}$ une fonction croissante.

1. La limite $\lim\limits_{a^+} f$ existe et est finie. Plus précisément, on a $f(a) \leq \lim\limits_{a^+} f$.
2. Pour tout $c \in]a, b[$, $\lim\limits_{c^-} f$ et $\lim\limits_{c^+} f$ existent et sont finies. Plus précisément : $\lim\limits_{c^-} f \leq f(c) \leq \lim\limits_{c^+} f$.
3. La limite $\lim\limits_{b} f$ existe et est soit finie, soit égale à $+\infty$.

1. On note $F = f(]a, b[)$. Comme f est définie au voisinage de a, $]a, b[\neq \emptyset$ et $F \neq \emptyset$.
   Par ailleurs, comme f est croissante sur $]a, b[$, F est minorée par $f(a)$.
   D'après la propriété fondamentale de $\mathbb{R}$, F possède une borne inférieure notée α, avec $f(a) \leq \alpha$.
   Montrons par définition que $\lim\limits_{a^+} f = \alpha$.
   Soit $\epsilon > 0$, $\alpha + \epsilon$ n'est pas un minorant de F par définition de α. On choisit :
   $$\alpha \leq f(x_0) < \alpha + \epsilon$$
   Par croissance de f sur $]a, b[$:
   $$\forall x \in]a, x_0[, \alpha \leq f(x) \leq f(x_0) < \alpha + \epsilon$$
   On pose $\eta = x_0 - a > 0$, on a montré que :
   $$\boxed{\forall x \in]a - \eta[\cap]a, b[, |f(x) - \alpha| < \epsilon}$$
2. Pour $c \in]a, b[$, en appliquant (15.39.1) à $f|_{[a,b[}$, on montre que $\lim\limits_{c^+} f$ existe et $f(x) \leq \lim\limits_{x^+} f$.
   On adapte ensuite la preuve de (15.39.1) :
   $$F = f(]a, c[), \alpha = \sup(F)$$
   pour montrer que $\lim\limits_{c^-} f$ existe et
3. Par disjonction de cas.

   — Si f est majorée : on adapte la 2ème partie de (15.39.2).
   — Si f n'est pas majorée. Soit $A \in \mathbb{R}$. Comme f n'est pas majorée, on choisit $x_0 \in]a, b[$ tel que $f(x_0) > A$.
   Comme f est croissante :
   $$\forall x \geq x_0, f(x) > A$$
   Donc $\lim\limits_{b} f = +\infty$.

15.59 Théorème des valeurs intermédiaires : version 1

Théorème 15.59

Soit f une fonction continue sur un intervalle I d'extrémité a et b dans $\overline{\mathbb{R}}$ (avec existence des limites dans le cas des bornes infinies). Alors si $f(a) > 0$ et $f(b) < 0$ (ou l'inverse), il exsite $c \in]a, b[$, tel que $f(c) = 0$.

On note $A = \{x \in I, f(x) > 0\}$.

— $A \neq \emptyset$ car f est définie et strictement positive au voisinage de a (15.32).
— A est majoré car f est strictement négative au voisinage de b (et tout élément dans ce voisinage est un majorant).

D'après la propriété fondamentale de $\mathbb{R}$, A possède une borne supérieure notée $c \in]a, b[$.

— On a $c \notin A$. En effet, si $f(x) > 0$, alors f est strictement postivie sur un voisinage de c, et comme f est définie à droite de c, cela contredirait que c'est un majorant de A.
  Donc $f(c) \leq 0$.
— Si $f(c) < 0$, alors f est strictement négative au voisinage à gauche de c.
  Absurde car c est le plus petit des majorants.
  Conclusion, $\boxed{f(c) = 0}$.

15.60 Théorème des valeurs intermédiaires : version 2

Théorème 15.60

Soit f une fonction continue sur un intervalle I et soit $M = \sup_I f(x)$ et $m = \inf_I f(x)$ (éventuellement infinies).
Alors f prend toutes les valeurs de l'intervalle $]m; M[$:

$$\forall x_0 \in]m; M[, \exists c \in I, f(c) = x_0.$$

RAF : (15.59) à $f - x_0$.

15.61 Théorème des valeurs intermédiaires : version 3

Théorème 15.61

L'image d'un intervalle quelconque par une fonction continue est un intervalle.

Définition d'un intervalle par connexité.

15.65 Théorème de Heine

Théorème 15.65

Une fonction continue sur un segment est uniformément continue sur ce segment.

Rappel :

$$C^0(I) : \forall x \in I, \forall \epsilon > 0, \exists \eta > 0, \forall y \in I, |x - y| < \eta \Rightarrow |f(x) - f(y)| < \epsilon$$
$$Cu(I) : \forall \epsilon > 0, \exists \eta > 0, \forall (x, y) \in I^2, |x - y| < \eta \Rightarrow |f(x) - f(y)| < \epsilon$$

On raisonne par l'absurde. Soit f continue sur $[a, b]$ mais non uniformément continue sur $[a, b]$.
On choisit ϵ tel que :

$$\forall \eta > 0, \exists (x, y) \in [a, b]^2, |x - y| < \eta \text{ et } |f(x) - f(y)| \geq \epsilon$$

Ainsi, pour tout $b \in \mathbb{N}^*$, on choisit un couple $(x_n, y_n) \in [a, b]^2$ tel que :

$$|x_n - y_n| < \frac{1}{n} \text{ et } \underbrace{|f(x_n) - f(y_n)|}_{(*)} \geq \epsilon$$

En particulier (x_n) est bornée donc d'après le théorème de Bolzano-Weierstrass, on en extrait $(x_{\varphi(n)})$ suite convergente vers ℓ.
D'après le TCILPPL, $\ell \in [a, b]$.
Comme :

$$\forall n \in \mathbb{N}, |x_{\varphi(n)} - y_{\varphi(n)}| < \frac{1}{\varphi(n)} \underset{n \to +\infty}{\longrightarrow} 0$$

Alors :

$$y_{\varphi(n)} \underset{n \to +\infty}{\longrightarrow} \ell$$

Par continuité :

$$f(x_{\varphi(n)}) \underset{n \to +\infty}{\longrightarrow} f(\ell) \text{ et } f(y_{\varphi(n)}) \underset{n \to +\infty}{\longrightarrow} f(\ell)$$

Donc par opération :

$$|f(x_{\varphi(n)}) - f(y_{\varphi(n)})| \underset{n \to +\infty}{\longrightarrow} 0$$

Absurde d'après $(*)$.

15.67 Caractérisation des intervalles compacts

Lemme 15.67

Les intervalles compacts de $\mathbb{R}$ sont exactement les segments, c'est-à-dire les intervalles fermés bornés $[a,b]$.

Les segments sont bien compacts (BW et TCILPPL).

— Si $I =]-\infty, a[$,

$$u_n = a - n - 1 \underset{n\to+\infty}{\longrightarrow} -\infty \notin I$$
$$u_n = a - \frac{1}{n+1} \underset{n\to+\infty}{\longrightarrow} a \notin I$$

15.68 Image d'un compact par une fonction continue

Lemme 15.68

L'image continue d'un compact est compact.

Soit I un segment, donc un intervalle.
Comme f est continue sur I, $f(I)$ est un intervalle (TVI v3).
Montrons que $f(I)$ est compact.
Soit $(y_n) \in f(I)^{\mathbb{N}}$. Pour tout $n \in \mathbb{N}$, soit $x_n \in I$ tel que :

$$y_n = f(x_n)$$

Or I est compact (15.67), on choisit :

$$x_{\varphi(n)} \underset{n\to+\infty}{\longrightarrow} \ell \in I$$

$y_{\varphi(n)} \underset{n\to+\infty}{\longrightarrow} f(\ell)$ car f est continue sur I.

15.69 Image d'un segment par une fonction continue

Corollaire 15.69

Soit f continue sur un segment I, alors $f(I)$ est un segment.

(15.68) + TVI v3 + (15.67)

15.72 Théorème 15.72

Théorème 15.72

Soit I un intervalle et f une fonction continue sur I. Alors f est injective si et seulement si f est strictement monotone.

$\boxed{\Leftarrow}$
RAS

$\boxed{\Rightarrow}$
Supposons f non strictement monotone.
On peut supposer qu'il existe alors :

$$x < y < z$$

tels que $f(x) < f(y)$ et $f(z) < f(y)$.
Soit :

$$\lambda = \frac{f(y) + \max(f(y), f(z))}{2} \in]f(x), f(y)[$$
$$\in]f(z), f(y)[$$

Par continuité de f sur les intervalles $]x, y[$ et $]y, z[$, il existe $\alpha \in]x, y[$ et $\beta \in]y, z[$ tels que :

$$f(\alpha) = \lambda = f(\beta)$$

Donc f n'est pas injective.

15.73 Théorème 15.73

Théorème 15.73

Soit I un intervalle et f monotone sur I. Si $f(I)$ est un intervalle, alors f est continue sur I.

On suppose f croissante sur I.
On suppose que f n'est pas continue sur I.
On applique le TLM :

$$\forall a \in I, \lim_{a^-} f \leq f(a) \leq \lim_{a^+} f \text{ (quand tout existe)}$$

Comme f n'est pas continue sur I, on choisit $a \in I$ tel que :

$$\lim_{a^-} f < f(a) \text{ ou } f(a) < \lim_{a^+} f$$

On pose :

$$\lambda = \frac{f(a) + \lim_{a^-} f}{2} \text{ ou } \lambda = \frac{f(a) + \lim_{a^+} f}{2}$$

$f(a) \neq \lambda$ et par croissance :

$$\forall x < a, f(x) < \lambda$$
$$\forall x > a, f(x) > \lambda$$

Donc $\lambda \notin f(I)$.
Donc $f(I)$ n'est pas connexe, donc $f(I)$ n'est pas un intervalle.

15.76 Théorème de la bijection

Théorème 15.76

Soit I un intervalle d'extrémités a et b. Soit $f : I \to \mathbb{R}$ strictement monotone et continue. Soit

$$\alpha = \lim_{x \to a} f(x) \text{ et } \beta = \lim_{x \to b} f(x).$$

(ces limites existent car f et monotone). Alors $f(I)$ est un intervalle d'extrémité α et β, et f est un homémorphisme de I sur $f(I)$.
Plus précisément, la borne α de $f(I)$ est ouverte si et seulement si la borne a de I est ouverte (et de même pour β).

- $f(I)$ est un intervalle : (15.61).
- f induit une bijection de I sur $f(I)$ (15.72 $\boxed{\Leftarrow}$).
- f^{-1} est strictement monotone et définie sur $f(I)$ intervalle, d'image I intervalle donc f^{-1} est continue sur $f(I)$ (15.73 $\boxed{\Rightarrow}$).

Ainsi, f induit un homéomorphisme de I sur $f(I)$.
La nature des bornes (fermées ou ouvertes) provient de la monotonie de f.

Chapitre 16

Arithmétique des polynômes

16.1 Division euclidienne

Théorème 16.1

Soit $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$ non nul, il existe un unique couple de polynômes (Q, R) tel que $A = BQ + R$ avec $\deg R < \deg B$. Le polynôme Q est appelé **quotient** et R le **reste**.

<u>Existence :</u>
On raisonne par récurrence sur le degré de A.

- Pour $n = \deg A = 0$. Soit $A \in \mathbb{K}[X]$.
  - Si $\deg B > 0$, alors $(0, A)$ convient.
  - Si $\deg B = 0$, le couple $(B^{-1} \times A, 0)$ convient (comme B est constant et non nul), alors $B \in \mathbb{K}^*$ donc inversible).
- On suppose le résultat vrai pour tout $A \in \mathbb{K}_n[X]$.
  Soit $A \in \mathbb{K}_{n+1}[X]$ avec $\deg A = n + 1$.
  On écrit $A = \underbrace{a}_{\neq 0} X^{n+1} + A_1$ avec $A_1 \in \mathbb{K}_n[X]$.
  - Si $\deg A < \deg B$, le couple $(0, A)$ convient.
  - Si $\deg A \geq \deg B$ et on note b le coefficient dominant de B :
  $$A - ab^{-1}B \times X^{n+1-\deg B} \in \mathbb{K}_n[X]$$
  D'après l'hypothèse de récurrence, on choisit $(Q, R) \in \mathbb{K}[X]^2$ tel que $\deg R < \deg B$ et $A - ab^{-1}B \times X^{n+1-\deg B} = QB + R$.
  Donc :
  $$A = \left[Q + ab^{-1}X^{n+1-\deg A}\right] \times B + R$$

<u>Unicité :</u>
On suppose que $A = BQ + R = BQ_1 + R_1$.
Donc :

$$\begin{aligned}
B(Q - Q_1) &= R_1 - R \\
\text{donc } \underbrace{\deg(B(Q - Q_1))}_{\deg B + \deg Q - Q_1} &= \deg(R_1 - R) \\
&\leq \max(\deg R_1, \deg R) \\
&< \deg B \\
\text{donc } \deg(Q - Q_1) &< 0 \\
\text{donc } Q - Q_1 &= 0 \\
\text{puis } R_1 - R &= 0
\end{aligned}$$

16.7 Proposition 16.7

Propostion 16.7

On a :

1. Soit A et P deux polynômes non nuls. Si $A|P$ et si $P|A$, alors il existe $\alpha \in \mathbb{K}^*$ tel que $P = \alpha A$. (La relation de divisibilité n'est pas antisymétrique)
2. Si $A|B$ et si $B|C$, alors $A|C$. La relation de divisibilité est transitive.
3. Pour tout $A \in \mathbb{K}[X]$ non nul, $A|A$. La relation de divisibilité est réflexive.

1. $P \neq 0$, $A \neq 0$. Si $A|P$ et $P|A$, alors (16.6.2) :
$$\deg A \leq \deg P \text{ et } \deg P \leq \deg A$$
Donc :
$$\deg P = \deg A$$

Or $A|P$, alors :

$$P = A \times Q$$

Puis :

$$\deg P = \deg(AQ) = \deg A + \deg Q \text{ ($\mathbb{K}$ est intègre)}$$

Donc :

$$\deg Q = 0$$

Donc :

$$Q = \alpha \in \mathbb{K}^*$$

2. RAS
3. RAS

16.15 Principalité de $\mathbb{K}[X]$

Théorème 16.15

Soit I un idéal de $\mathbb{K}[X]$ non réduit à $\{0\}$. Il existe un unique polynôme unitaire D tel que

$$I = D\mathbb{K}[X]$$

Existence :
Soit $I \neq \{0\}$ un idéal.
On note $A = \{\deg P, P \in I \backslash \{0\}\} \subset \mathbb{N}$.
$A \neq \emptyset$ ($I \neq \{0\}$), d'après la propriété fondamentale de $\mathbb{N}$, A possède un plus petit élément noté $n \geq 0$.
Comme $n \in A$, on choisit $D \in I$ tel que $\deg D = n$.
Comme I est un idéal de $\mathbb{K}[X]$ et que $\mathbb{K} = \mathbb{K}_0[X] \subset \mathbb{K}[X]$, on a :

$$\forall \alpha \in \mathbb{K}, \alpha D \in I$$

On peut donc supposer D unitaire. Comme I est un idéal de $\mathbb{K}[X]$, on a :

$$D \times \mathbb{K}[X] \subset I$$

Soit $P \in I$. On effectue la division euclidienne de P par D ($\neq 0$) :

$$P = BD + R$$

avec $\deg R \subset \deg D$.
Or :

$$R = \underbrace{P}_{\in I} - \underbrace{BD}_{\in I}$$
$$\in I$$

Par définition de $\deg D = n$, $R = 0$.

Unicité :

$$I = D\mathbb{K}[X] = J\mathbb{K}[X]$$

avec D et J unitaires.
Or ils sont associés, donc égaux.

16.17 Existence de *pgcd*

Propostion 16.17

Si A et B sont deux polynômes non nuls, de tels PGCD existent.

Soit A, B dans $\mathbb{K}[X]$, $(A, B) \neq (0,0)$.
On note $\mathcal{C} = \{\deg P, P|A \text{ et } P|B \text{ et } P \neq 0\} \subset \mathbb{N}$.
$\mathcal{C} \neq \emptyset$ car $0 \in \mathcal{C}$ et $\mathcal{C}$ est majoré par $\deg B$ ($\max(\deg A, \deg B)$).
L'existence est assurée par la propriété fondamentale de $\mathbb{N}$.

16.18 Principalité de $\mathbb{K}[X]$

Propostion 16.18

Soit A et B deux polynômes non tous deux nuls. Soit $D \in \mathbb{K}[X]$. Alors Δ est un PGCD de A et B si et seulement si

$$A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X].$$

D'après (16.15), on choisit $F \in \mathbb{K}[X]$ tel que :

$$A\mathbb{K}[X] + B\mathbb{K}[X] = F\mathbb{K}[X]$$

Soit $D \in \mathbb{K}[X]$.

$\boxed{\Rightarrow}$
On suppose que D est un PGCD.
Donc $D|A$ et $D|B$.
Donc $D|F$ (combinaison $F \in A\mathbb{K}[X] + B\mathbb{K}[X]$).
Or $F|A$ et $F|B$ ($A \in F\mathbb{K}[X]$, $B \in F\mathbb{K}[X]$).
Par maximalité de $\deg D$, on a F et D associés.

$\boxed{\Leftarrow}$

$$D\mathbb{K}[X] = A\mathbb{K}[X] + B\mathbb{K}[X] = F\mathbb{K}[X]$$

Donc $D|A$ et $D|B$.
Pour tout diviseur commun P de A et B, $P|A$ et $P|B$.
Donc $P|D$ ($D \in A\mathbb{K}[X] + B\mathbb{K}[X]$).
Donc $\deg D$ est maximal pour la divisibilité.

16.24 Lemme de préparation au calcul pratique du PGCD unitaire

Lemme 16.24

Soit A et B deux polynômes tels que $B \neq 0$. Pour tout $Q \in \mathbb{K}[X]$, on a $A \wedge B = (A - BQ) \wedge B$.
En particulier, si Q et R sont le quotient et le reste de la division euclidienne de A par B Alors $A \wedge B = B \wedge R$.

$$\begin{aligned}(A \wedge B)\mathbb{K}[X] &= A\mathbb{K}[X] + B\mathbb{K}[X] \\ &= (A - BQ)\mathbb{K}[X] + B\mathbb{K}[X] \\ &= ((A - BQ) \wedge B)\mathbb{K}[X]\end{aligned}$$

Donc $A \wedge B$ et $(A - BQ) \wedge B$ sont associés, unitaires par définition, donc égaux.

16.26 Exemple

Exemple alternatif 16.26

Trouver les PGCD de $A = X^5 + 2X$ et de $B = X^4 + 2X^3 + 4$ et une relation de Bézout.

$$\begin{aligned}
X^5 + 2X &= (X^4 + 2X^3 + 4)(X - 2) + 4X^3 - 2X + 8 \\
X^4 + 2X^3 + 4 &= (4X^3 - 2X + 8)(\frac{1}{4}X + \frac{1}{2}) + \frac{1}{2}X^2 - X \\
4X^3 - 2X + 8 &= (\frac{1}{2}X^2 - X)(8X + 16) + 14X + 8 \\
\frac{1}{2}X^2 - X &= (14X + 8)(\frac{1}{28}X - \frac{9}{14 \times 7}) + \frac{9 \times 4}{7^2} \\
A \wedge B = 1
\end{aligned}$$

$$\begin{aligned}
\frac{9 \times 4}{7^2} &= \frac{1}{2}X^2 - X - (14X + 8)(\frac{1}{28}X - \frac{9}{2 \times 7^2}) \\
&= \frac{1}{2}X^2 - X - (4X^3 - 2X + 8 - (\frac{1}{2}X^2 - X)(8X + 16))(\frac{1}{28}X - \frac{9}{2 \times 7^2})
\end{aligned}$$

16.27 Propriétés du PGCD

Propostion 16.27

L'opération $\wedge$ est commutative et associative. Par ailleurs, si C est unitaire, alors $(A \wedge B)C = (AC) \wedge (BC)$.

Soit $(A, B, C) \in \mathbb{K}[X]^3$ non tous nuls.

$$\begin{aligned}
(A \wedge B)\mathbb{K}[X] &= A\mathbb{K}[X] + B\mathbb{K}[X] \\
&= B\mathbb{K}[X] + A\mathbb{K}[X] \\
&= (B \wedge A)\mathbb{K}[X]
\end{aligned}$$

Donc $A \wedge B$ et $B \wedge A$ sont associés et unitaires donc égaux.

$$\begin{aligned}
((A \wedge B) \wedge C)\mathbb{K}[X] &= (A \wedge B)\mathbb{K}[X] + C\mathbb{K}[X] \\
&= A\mathbb{K}[X] + B\mathbb{K}[X] + C\mathbb{K}[X] \\
&= (A \wedge (B \wedge C))\mathbb{K}[X]
\end{aligned}$$

Donc $A \wedge (B \wedge C)$ et $(A \wedge B) \wedge C$ sont associés et unitaires donc égaux.
On suppose C unitaire.
On a :

$$\begin{aligned}
(A \wedge B)\mathbb{K}[X] &= A\mathbb{K}[X] + B\mathbb{K}[X] \\
\text{donc } (A \wedge B)C\mathbb{K}[X] &= AC\mathbb{K}[X] + BC\mathbb{K}[X] \\
&= ((AC) \wedge (BC))\mathbb{K}[X]
\end{aligned}$$

Ainsi $C(A \wedge B)$ et $(AC) \wedge (BC)$ sont associés et unitaires donc égaux.

16.29 Existence de PPCM

Propostion 16.29

Soit $\mathbb{K}$ un corps. Soit A et B deux polynômes non nuls de $\mathbb{K}[X]$. Alors A et B admettent des PPCM.

On note $\mathcal{D} = \{\deg P, A|P, B|P, P \neq 0\} \subset \mathbb{N}$.

$$\deg AB \in \mathcal{D} \neq \emptyset$$

On conclut avec la propriété fondamentale de $\mathbb{N}$.

16.30 Caractérisation des PPCM par les idéaux

Propostion 16.30

Soit A et B deux polynômes non nuls de $\mathbb{K}[X]$ et soit $P \in \mathbb{K}[X]$. Alors P est un PPCM de A et B si et seulement si

$$A\mathbb{K}[X] \cap B\mathbb{K}[X] = P\mathbb{K}[X].$$

$A\mathbb{K}[X] \cap B\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$, donc de la forme $M\mathbb{K}[X]$ (16.15).
Montrons que P est un PPCM de A et B si et seulement si P et M sont associés.

$\boxed{\Rightarrow}$
On a donc :

$$\begin{aligned} P &\in A\mathbb{K}[X] \cap B\mathbb{K}[X] \\ &\in M\mathbb{K}[X] \end{aligned}$$

Donc $M|P$.
Or M est un multiple commun à A et B, donc par définition de P, on a :

$$\boxed{\deg P \leq \deg M}$$

Donc P et M sont associés.

$\boxed{\Leftarrow}$
On suppose P et M associés, donc :

$$\begin{aligned} P\mathbb{K}[X] &= M\mathbb{K}[X] \\ &= A\mathbb{K}[X] \cap B\mathbb{K}[X] \end{aligned}$$

En particulier, P est un multiple commun à A et B et pour tout $Q \in A\mathbb{K}[X] \cap B\mathbb{K}[X]$, donc $P|Q$.
Donc :

$$\boxed{degP \leq \deg Q}$$

16.42 Cas d'unicité d'une relation de Bézout

Propostion 16.42

Soit A et B non constants et premiers entre eux. Il existe un unique couple $(U, V) \in \mathbb{K}[X]^2$ tel que

$$AU + BV = 1 \text{ et } \deg U < \deg B \text{ et } \deg V < \deg A.$$

<u>Existence :</u>
Soit $(C, D) \in \mathbb{K}[X]^2$ tel que (16.37 - Bézout) :

$$AC + BD = 1$$

On effectue la dviision euclidienne de C par B :

$$\begin{aligned} C &= BE + U \text{ avec } \deg U < \deg B \\ \text{donc } AU + B(\underbrace{D+AE}_{V}) &= 1 \\ \text{donc } \deg(AU+BV) &= 0 \end{aligned}$$

Si $\deg V \geq \deg A$, alors :

$$\begin{aligned} \deg B + \deg V &\geq \deg B + \deg A \\ &> \deg U + \deg B \\ &= \deg AU \end{aligned}$$

Donc $\deg(AU+BV) = \deg BV > 0$.
Absurde.
L'exsitence est prouvée.

Unicité :
Avec es hypothèses correspondantes :

$$\begin{aligned} AU_1 + BV_1 &= 1 = AU_2 + BV_2 \\ \text{donc } A(U_1 - U_2) &= B(V_2 - V_1) \\ \text{donc } A &| B(V_2 - V_1) \end{aligned}$$

Or $A \wedge B = 1$, donc $A|(V_2 - V_1)$.
Or $\deg(V_2 - V_1) < \deg A$.
Donc $V_2 - V_1 = 0$.
Puis $A(U_1 - U_2) = 0$, donc $U_1 - U_2 = 0$ car $\mathbb{K}[X]$ est intègre avec $A \neq 0$.

16.43 Corollaire

Corollaire 16.43

Soit A, B et C trois polynômes avec A et B premiers entre eux. Alors $A \wedge (BC) = A \wedge C$.

- $A \wedge C | A$ donc $A \wedge C | A \wedge (BC)$. Donc $A \wedge C | BC$.
- $A \wedge (BC) | A$. Or $A \wedge B = 1$ donc on peut écrire $AU + BV = 1$. Donc $ACU + BCV = C$.
  Or $A \wedge (BC) | ACU + BCV$ soit $A \wedge (BC) | C$. Donc $A \wedge (BC) | A \wedge C$.

Ainsi, $A \wedge C$ et $A \wedge (BC)$ sont associés et unitaires donc égaux.

16.44 Caractérisation des PGCD et PPCM

Propostion 16.44

Soit A et B deux polynômes non nuls, M et D deux polynômes. Alors

$$M = A \vee B \Leftrightarrow (M \text{ unitaire et } \exists (U,V) \in \mathbb{K}[X]^2, M = AU = BV \text{ et } U \wedge V = 1).$$

$$D = A \wedge B \Leftrightarrow (D \text{ unitaire et } \exists (U,V) \in \mathbb{K}[X]^2, A = DU \text{ et } B = DV \text{ et } U \wedge V = 1).$$

- $\boxed{\Rightarrow}$
  $M = A \vee B$. On écrit $M = AU + BV$ avec $(U,V) \in \mathbb{K}[X]^2$.
  On note $R = U \wedge V$. On écrit $U = RU_1$ et $V = RV_1$.
  Ainsi :

$$\begin{aligned} M &= RAU_1 = RBV_1 \\ \text{donc } R(AU_1 - BV_1) &= 0 \\ \text{donc } AU_1 &= BV_1 \ (\mathbb{K}[X] \text{ est intègre}) \end{aligned}$$

Donc $M_1 = AU_1 = BV_1$ est un multiple commun et par minimalité des degrés :

$$RM_1 = M|M_1 \text{ donc } R = 1$$

$\boxed{\Leftarrow}$
Par hypothèse, M est un multiple commun, donc :

$$M \in A\mathbb{K}[X] \cap B\mathbb{K}[X] = (A \vee B)\mathbb{K}[X]$$

Donc $A \vee B | M$.
Donc $M = D \times A \vee B$.
Or $A \vee B = AU_1 = BV_1$.
Donc $M = DAU_1 = DBV_1 = AU = BV$.
Donc :

$$A(DU_1 - U) = 0$$
$$B(DV_1 - V) = 0$$

Or $\mathbb{K}[X]$ est intègre donc $DU_1 = U$ et $DV_1 = V$.
Donc $D|U \wedge V = 1$.

— $\boxed{\Rightarrow}$
$D = A \wedge B$. On écrit $A = DU$ et $B = DV$.
Or pour $R = U \wedge V$, on écrit $U = RU_1$ et $V = RV_1$.
Donc $A = DRU_1$ et $B = DRV_1$.
Donc $DR|A$ et $DR|B$.
Donc $DR|D$.
Nécessairement, $R = 1$.

$\boxed{\Leftarrow}$
Par hypothèse, $D|A$ et $D|B$, donc $D|A \wedge B$.
Comme $U \wedge V = 1$, d'après le théorème de Bézout :

$$\begin{aligned} UU_1 + VV_1 &= 1 \\ \text{donc } DUU_1 + DVV_1 &= D \\ \text{soit } AU_1 + BV_1 &= D \\ \text{donc } A \wedge B &| D \end{aligned}$$

Ainsi, $A \wedge B$ et D sont associés. Or ils sont unitaires, donc égaux.

16.53 Caractérisation des racines par la divisibilité

Théorème 16.53

Soit $\mathbb{K}$ un corps, $P \in \mathbb{K}[X]$ et $r \in \mathbb{K}$. Alors r est racine de P si et seulement si $X - r$ divise P. Donc s'il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - r)Q$.

$\boxed{\Leftarrow}$
Si $P = (X - r)Q$, alors :

$$\begin{aligned} \tilde{P}(r) &= (X - r)\tilde{Q}(r) \\ &= 0 \times \tilde{Q}(r) \\ &= 0 \end{aligned}$$

$\boxed{\Rightarrow}$
On suppose r racine de P.
On effectue la division euclidienne de P par $X - r$:

$$P = (X - r)Q + R, R \in \mathbb{K}_0[X]$$

Donc $0 = \tilde{P}(r) = \tilde{R}(r)$.
Donc $R = 0$.
Donc $X - r|P$.

16.56 Formule de Taylor pour les polynômes

Théorème 16.56

Soit $\mathbb{K}$ un corps de caractéristique nulle, P un polynôme de $\mathbb{K}[X]$ de degré d et $a \in \mathbb{K}$, alors

$$P = \sum_{k=0}^{d} \frac{P^{(k)}(a)}{k!}(X-a)^k.$$

On note $E_k = X^k$, pour $k \in \mathbb{N}$.
On a, pour $i \in \mathbb{N}$:

$$E_k^{(i)} = \begin{cases} \frac{k!}{(k-i)!}X^{k-i} & \text{si } i \leq k \\ 0 & \text{si } i > k \end{cases}$$

Ainsi :

$$\begin{aligned} E_k(X+a) &= (X+a)^k \\ &= \sum_{i=0}^{k} \binom{k}{i} a^{k-i} X^i \\ &= \sum_{i=0}^{k} \frac{k!}{i!(k-i)!} a^{k-i} X^i \\ &= \sum_{i=0}^{k} \frac{E_k^{(i)}(a)}{i!} X^i \end{aligned}$$

Soit $P = \sum\limits_{k=0}^{d} a_k X^k = \sum_{k=0}^{d} a_k E_k$.
Ainsi :

$$\begin{aligned} P(x+a) &= \sum_{k=0}^{d} a_k E_k(X+a) \\ &= \sum_{k=0}^{d} a_k \sum_{i=0}^{k} \frac{E_k^{(i)}(a)}{i!} X^i \\ &= \sum_{i=0}^{d} \frac{1}{i!} \left(\sum_{k=i}^{d} a_k E_k^{(i)}(a) \right) X_i \\ &= \sum_{i=0}^{d} \frac{1}{i!} \left(\sum_{k=0}^{d} a_k E_k^{(i)}(a) \right) X_i \\ &= \sum_{i=0}^{d} \frac{1}{i!} P^{(i)}(a) X^i \end{aligned}$$

16.57 Caractérisation de la multiplicité par les dérivées

Théorème 16.57

Soit $\mathbb{K}$ un corps de caractéristique nulle, $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Le réel a est racine d'ordre multiplicité k de P si et seulement si

$$P(a) = P'(a) = \ldots = P^{(k-1)}(a) = 0 \text{ et } P^{(k)}(a) \neq 0.$$

$\Leftarrow$

D'après la formule de Taylor :

$$\begin{aligned} P &= \sum_{i=0}^{d} \frac{P^{(i)}(a)}{i!}(X-a)^i \\ &= \sum_{i=k}^{d} \frac{P^{(i)}(a)}{i!}(X-a)^i \\ &= (X-a)^k \underbrace{\sum_{i=k}^{d} \frac{P^{(i)}(a)}{i!}(X-a)^{i-k}}_{=Q} \end{aligned}$$

$$Q(a) = \frac{P^{(k)}(a)}{k!} \neq 0$$

$\boxed{\Rightarrow}$

$P = (\underbrace{X-a}_{B})^k Q$ avec $Q(a) \neq 0$.

Pour tout $i \in [\![0, k-1]\!]$:

$$\begin{aligned} P^{(i)} &= (BQ)^{(i)} \\ &= \sum_{l=0}^{i} \binom{i}{l} B^{(l)} Q^{(i-l)} \\ P^{(i)}(a) &= 0 \\ P^{(k)} &= \binom{k}{k} B^{(k)}(a) \times Q^{(k-k)}(a) \\ &= k! \times Q(a) \neq 0 \end{aligned}$$

16.59 Caractérisation de la multiplicité des racines par la divisibilité

Théorème 16.59

Soit $\mathbb{K}$ un corps. Soit $P \in \mathbb{K}[X]$ et $r_1, \dots, r_k$ des racines deux à deux distinctes de P, de multiplicités respectives $a_1, \dots, a_k$. Alors $(X - r_1)^{a_1} \dots (X - r_k)^{a_k}$ divise P et $r_1, \dots, r_k$ ne sont pas racines du quotient.

RAF :

$$(X - r_i)^{\alpha_1} \wedge (X - r_k)^{\alpha_k} = 1 \text{ si } i \neq k$$

16.63 Polynômes formels et fonctions polynomiales

Théorème 16.63

Soit $\mathbb{K}$ un corps infini. Alors l'application de $\mathbb{K}[X]$ dans $\mathbb{K}[x]$ qui à un polynôme formel associe sa fonction polynomiale est un isomorphisme d'anneaux.

RAF : $\varphi(P) = \varphi(Q)$ donc $\varphi(P - Q) = 0$

$\tilde{P} - \tilde{Q}$ s'annule sur $\mathbb{K}$ infini et on applique (16.62).

16.66 Caractérisation des polynômes interpolateurs

Lemme 16.66

Le polynôme L_i est l'unique polynôme de degré au plus n tel que pour tout $j \in [\![0, n]\!], L_i(x_j) = \delta_{ij}$.

Existence : RAF

Unicité : (16.61.3)

16.69 Corollaire

Corollaire 16.69

Soit P le polynôme d'interpolation de Lagrange associé à la famille $(x_i)_{0\leq i\leq n}$ et aux valeurs $(y_i)_{0\leq i\leq n}$ Soit $P_0 = (X-x_0)\dots(X-x_n)$. L'ensemble E des polynômes Q (sans restriction de degré) tel que pour tout $i \in [\![0,n]\!], Q(x_i) = y_i$ est décrit par

$$E = P + (P_0) = \{P + (X-x_0)\dots(X-x_n)R, R \in \mathbb{K}[X]\}$$

$\boxed{\supset}$
Si $Q = P + (X-x_0)\dots(X-x_n)R$, alors :

$$\forall i \in [\![0,n]\!], Q(x_i) = P(x_i) = y_i$$

Donc $Q \in E$.

$\boxed{\subset}$
Soit $Q \in E$, alors $x_0,\dots,x_n$ sont racines de $Q-P$.
Donc $(X-x_0)\dots(X-x_n)|Q-P$.

16.74 Proposition

Propostion 16.74 (HP)

Soit P un polynôme scindé non constant de $\mathbb{R}[X]$ à racines simples. Alors P' est scindé, et ses racines séparent celles de P.

Soit $P = \prod\limits_{k=1}^{n}(x-x_k)$ avec $x_1 < \dots < x_n$.
D'après le théroème de Rolle, comme $P(x_1) = P(x_2) = \dots = P(x_n)$ pour tout $k \in [\![1,n-1]\!]$, on choisit $y_k \in]x_k, x_{k+1}[$ tel que $P'(y_k) = 0$.
On a donc :

$$x_1 < y_1 < x_2 < y_2 < \dots < y_{n-1} < x_n$$

et $y_1,\dots,y_{n-1}$ sont $n-1$ racines distinctes de P' de degré $n-1$ ($\mathbb{R}$ de caractéristique nulle).
Donc P' est scindé (à racines simples).

16.76 Relation de Viète

Théorème 16.76

Soit $P = \sum\limits_{k=0}^{n} a_k X^k$ un polynôme de degré n, scindé, de racines (éventuellement non distinctes, apparaissant dans la liste autant de fois que sa multiplicité) $r_1,\dots,r_n$ alors pour tout $k \in [\![0,n]\!]$:

$$\sum_{1\leq i_1<\dots<i_k\leq n} r_{i_1}\dots r_{i_k} = (-1)^k \frac{a_{n-k}}{a_n}$$

$$\begin{aligned} P &= \sum_{k=0}^{n} a_k X^k \\ &= a_n \prod_{k=1}^{n}(X-r_k) \end{aligned}$$

Les relations de Viète consistent simplement à développer l'expression de droite et à identifier les mnômes de degré $n-k$.

$$a_{n-k} = (-1)^k a_n \sum_{1\leq i_1 < \ldots < i_k \leq n} r_{i_1} \ldots r_{i_k}$$

16.88 Lemme

Lemme 16.88

Soit P un polynôme irréductible de $\mathbb{K}[X]$ et A un polynôme non multiple de P. Alors A et P ont premiers entre eux.

Soit D unitaire $\in \mathcal{D}_{A,P}$.
Si $P \not| A$, alors $D \neq U(P)$.
Donc $D = 1$.
Donc $P \wedge A = 1$.

16.98 Caractérisation de la divisibilité dans $\mathbb{C}[X]$ par les racines

Théorème 16.98

Soit P et Q deux polynômes de $\mathbb{C}[X]$. Alors P divise Q si et seulement si toute racine de P est aussi une racine de Q, et que sa multiplicité dans Q est supérieure ou égale à sa multiplicité dans P.

$\boxed{\Rightarrow}$
Supposons $P|Q$.
Soit r une racine de P de multiplicité α. Donc :

$$(X-r)^\alpha | P$$
$$\text{donc } (X-r)^\alpha | Q$$

Donc r est racine de Q de multiplicité supérieure à α.

$\boxed{\Leftarrow}$
On décompose $P = \lambda \prod_{i=1}^{n} (X-r_i)^{\alpha_i}$ (P est scindé sur $\mathbb{C}$).
Par hypothèse, $\prod_{i=1}^{n} (X-r_i)^{\alpha_i} | Q$.
Donc $P|Q$.

16.99 Caractérisation des polynômes à coefficients réels

Théorème 16.99

Soit $P \in \mathbb{C}[X]$. Les propositions sont équivalents :

1. P est à coefficients réels ;
2. $P(\mathbb{R}) \subset \mathbb{R}$;
3. pour tout $z \in \mathbb{C}, \overline{P(z)} = P(\overline{z})$.

$\boxed{1 \Rightarrow 2}$
RAF

$\boxed{2 \Rightarrow 1}$
On suppose que $P(\mathbb{R}) \subset \mathbb{R}$.

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

$$\begin{aligned} P &= \sum_{k=0}^{n} a_k X^k \\ \overline{P(z)} &= \overline{\sum_{k=0}^{n} a_k z^k} \\ &= \sum_{k=0}^{n} \overline{a_k} (\overline{z})^k \end{aligned}$$

Par hypothèse, pour $z \in \mathbb{R}$, $P(z) \in \mathbb{R}$, soit $\overline{P(z)} = P(z)$.
Ainsi, pour $z \in \mathbb{R}$:

$$\sum_{k=0}^{n} \overline{a_k} z^k = \sum_{k=0}^{n} a_k z^k$$

Les deux polynômes $\sum\limits_{k=0}^{n} \overline{a_k} X^k$ et $\sum\limits_{k=0}^{n} a_k X^k$ coincident sur une infinité de valeurs, donc (théorème de rigidité) ils sont égaux.
Donc :

$$\forall k \in [\![0, n]\!], a_k = \overline{a_k}$$

Donc $P \in \mathbb{R}[X]$.

$\boxed{1 \Rightarrow 3}$
RAF

$\boxed{3 \Rightarrow 2}$
Si $\overline{P(z)} = P(\overline{z})$ pour tout $z \in \mathbb{C}$, alors en particulier pour $z \in \mathbb{R}$, $\overline{P(z)} = P(z)$ soit $P(z) \in \mathbb{R}$.

16.100 Racine complexe d'un polynôme réel

Corollaire 16.100

Soit P un polynôme à coefficients réels et r une racine de P dans $\mathbb{C}$. Si $r \notin \mathbb{R}$, alors $\overline{r}$ est aussi une racine de P et elles ont la même multiplicité.

Soit r une racine complexe de P.
Donc $P(r) = 0$.
Donc $\overline{P(r)} = 0$.
Donc (16.99.3) $P(\overline{r}) = 0$.
Donc $\overline{r}$ est aussi une racine de P.
Donc $(X - \overline{r})(X - r) | P$.
Donc $P = (X - \overline{r})(X - r)Q$ et si r est une racine de Q, $\overline{r}$ également, ce qui justifie que $\overline{r}$ ala même multiplicité que r.

16.101 Polynômes irréductibles de $\mathbb{R}[X]$

Théorème 16.101

1. Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif.
2. Ainsi, tout polynôme $P \in \mathbb{R}[X]$ peut être factorisé en produit de polynômes de $\mathbb{R}[X]$ de degré 1 ou de degré 2, de discriminant strictement négatif.

1. Les polynômes annoncés sont bien les seuls irréductibles dans $\mathbb{R}_2[X]$.
   Soit $P \in \mathbb{R}[X]$, avec $\deg P \geq 3$. Dans $\mathbb{C}[X]$, P est scindé.
   Si P admet une racine dans $\mathbb{R}$, P est réductible.
   Supposons maintenant que toutes les racines de P sont complexes. Soit r l'une d'entre elles.
   Alors $\overline{r} \neq r$ est aussi une racine de P.
   Donc $(X - r)(X - \overline{r})|P$.
   Donc :
   $$\begin{aligned} P &= (X - r)(X - \overline{r})Q \text{ avec } Q \in \mathbb{C}[X] \\ &= \underbrace{(x^2 - 2Re(r)X + |r|^2)}_{:=R \in \mathbb{R}[X]}Q \end{aligned}$$
   Donc $P = RQ$ est la division euclidienne de P par R dans $\mathbb{C}[X]$ et aussi dans $\mathbb{R}[X]$.
   Par unicité, on a donc $Q \in \mathbb{R}[X]$ et P est réductible dans $\mathbb{R}[X]$.
2. RAF

Chapitre 17

Fractions rationnelles

17.2 Addition, multiplication et produit par un scalaire

Définition 17.2

Soit $\frac{P}{Q}$ et $\frac{R}{S}$ deux fractions rationnelles et soit $\lambda \in \mathbb{K}$. On pose

$$\frac{P}{Q} + \frac{R}{S} = \frac{PS + QR}{QS}, \ \frac{P}{Q} \times \frac{R}{S} = \frac{PR}{QS} \text{ et } \lambda \times \frac{P}{Q} = \frac{\lambda P}{Q}.$$

Montrons que l'addition est bien définie.
Soit $\frac{P_1}{Q_1} = \frac{P}{Q}$ et $\frac{R}{S}$ dans $\mathbb{K}(X)$.
Montrons que :

$$\frac{PS + QR}{QS} = \frac{P_1S + Q_1R}{Q_1S}$$

On a :

$$\begin{aligned}(PS + QR)Q_1S - (P_1S + Q_1R)QS &= S^2(\underbrace{PQ_1 - P_1Q}_{=0}) + RS(\underbrace{QQ_1 - Q_1Q}_{=0}) \\ &= 0\end{aligned}$$

On raisonne de la même manière pour $\frac{R}{S} = \frac{R_1}{S_1}$ et ainsi, l'opération est bien définie.

17.10 Degré d'une fraction

Définition 17.10

Soit $F = \frac{P}{Q}$ une fraction. On pose $\deg(F) = -\infty$ si $F = 0$ et $\deg(F) = \deg(P) - \deg(Q)$ sinon. Le degré d'une fraction est donc un élément de $\mathbb{Z} \cup \{-\infty\}$.

Si $\frac{P_1}{Q_1} = \frac{P}{Q}$, alors :

$$\begin{aligned} P_1Q &= PQ_1 \\ \text{donc } \deg(P_1Q) &= \deg(PQ_1) \\ \text{donc } \deg(P_1) + \deg(Q) &= \deg(P) + \deg(Q_1) \ (\mathbb{K} \text{ intègre}) \\ \text{donc } \deg(P_1) - \deg Q_1 &= \deg(P) - \deg(Q)\end{aligned}$$

17.13 Propriété du degré

Théorème 17.13

Soit F et G deux fractions rationnelles. On a

$$\deg(F + G) \leq \max(\deg(F), \deg(G)) \text{ et } \deg(F \times G) = \deg(F) + \deg(G).$$

On retrouve les mêmes propriétés que pour les polynômes.

Soit $F = \frac{P}{Q}$ et $G = \frac{R}{S}$.

—

$$\begin{aligned}\deg(F + G) &= \deg(\frac{PS + QR}{QS}) \\ &= \deg(PS + QR) - \deg(QS) \\ &\leq \max(\deg(PS), \deg(QR)) - \deg(QS) \\ &= \max(\deg(PS) - \deg(QS), \deg(QR) - \deg(QS)) \\ &= \max\left(\deg\left(\frac{P}{Q}\right), \deg\left(\frac{R}{Q}\right)\right) \\ &= \max(\deg(F), \deg(G))\end{aligned}$$

— RAS

17.19 Théorème

Théorème 17.19

Soit F et G deux fractions rationnelles. Si les fonctions rationnelles $\tilde{F}$ et $\tilde{G}$ sont égales sur une partie infinie $\mathcal{D}_F \cap \mathcal{D}_G$ alors les fractions rationnelles sont égales, i.e. $F = G$.

On note $F = \frac{P}{Q}$ et $G = \frac{R}{S}$ avec $P \wedge Q = 1$ et $R \wedge S = 1$.
On a :

$$\forall x \in \mathcal{D} \subset \mathcal{D}_F \cap \mathcal{D}_G, \tilde{F}(x) = \tilde{G}(x)$$

Soit :

$$\forall x \in \mathcal{D}, P\tilde{(x)} \times S\tilde{(x)} = R\tilde{(x)} \times Q\tilde{(x)}$$

Comme $\mathcal{D}$ est infini, d'après le théorème de rigidité, $PS = RQ$, donc $F = G$.

17.20 Fraction dérivée

Définition 17.20

Soit $F = \frac{P}{Q} \in \mathbb{K}(X)$. On appelle **fraction dérivée** de F la fraction notée F' (ou $\frac{dF}{dX}$) définie par

$$F' = \frac{P'Q - PQ'}{Q^2}.$$

Le résultat ne dépend pas du représentant de F choisi. On définit également les dérivées successives de F en posant $F^(0) = F$ et pour tout $n \in \mathbb{N}, F^{(n+1)} = (F^{(n)})'$.

On écrit $F = \frac{P}{Q} = \frac{R}{S}$.
Montrons que $\frac{P'Q - Q'P}{Q^2} = \frac{R'S - RS'}{S^2}$.
Comme $\frac{P}{Q} = \frac{R}{S}$, on a $PS = RQ$.
Donc $P'S + S'P = R'Q + Q'R$.
Ainsi :

$$\begin{aligned}
[P'Q - PQ']S^2 - [R'S - RS']Q^2 &= P'SQ^2 + S'PQ^2 - R'QS^2 - Q'RS^2 \\
&= QS(P'S - R'Q) + Q^2RS' - S^2Q'P \\
&= QS(Q'R - S'P) + PSQS' - SQRQ' \\
&= 0
\end{aligned}$$

17.24 Dérivée logarithmique d'un produit

Théorème 17.24

Si F est une fraction non nulle qui se facotorise en $F = F_1 \times \ldots \times F_n$ dans $\mathbb{K}(X)$ avec $n \in \mathbb{N}$ alors

$$\frac{F'}{F} = \frac{F_1'}{F_1} + \ldots + \frac{F_n'}{F_n}.$$

Pour $n = 2$ seulement.

$$F = F_1 \times F_2 \neq 0$$

Donc :

$$F' = F_1'F_2 + F_1F_2'$$

Donc :

$$\frac{F'}{F} = \frac{F_1'F_2}{F_1F_2} + \frac{F_1F_2'}{F_1F_2} = \frac{F_1'}{F_1} + \frac{F_2'}{F_2}$$

17.25 Partie entière

Théorème 17.25

Soit $F \in \mathbb{K}(X)$. Il existe un unique polynôme Q tel que $\deg(F - Q) < 0$. Celui-ci est appelé **partie entière** de F, c'est le quotient dans la division euclidienne du numérateur de F par le dénominateur.

Existence :
Soit $F = \frac{A}{B}$ avec $A \wedge B = 1$.
Soit la division euclidiene de A par B :

$$A = BQ + R \text{ avec } \deg(R) < \deg(B)$$

Donc :

$$F = \frac{A}{B} = \frac{BQ + R}{B} = Q + \frac{R}{B}$$

Donc :

$$\deg(F - Q) = \deg\left(\frac{R}{B}\right) = \deg(R) - \deg(B) < 0$$

Unicité :
On suppose que :

$$F = Q + G = Q_1 + G_1 \text{ avec } (Q_1, G_1) \in \mathbb{K}[X]^2 \text{ et } \deg(G), \deg(G_1) < 0$$

Donc :

$$\begin{aligned} Q - Q_1 &= G_1 - G \\ \text{donc } \deg(Q - Q_1) &= \deg(G_1 - G) \\ &\leq \max(\deg(G_1), \deg(G)) \\ &< 0 \end{aligned}$$

Or $Q - Q_1 \in \mathbb{K}[X]$, donc $Q = Q_1$.

17.31 Existence d'une décomposition

Théorème 17.31

Si T et S sont deux polynômes premiers entre eux et si $\deg\left(\frac{A}{TS}\right) < 0$, alors il existe deux polynômes U et V tels que

$$\frac{A}{TS} = \frac{U}{T} + \frac{V}{S}, \text{ avec } \deg(U) < \deg(T) \text{ et } \deg(V) < \deg(S).$$

Comme $T \wedge S = 1$, d'après le théormème de Bézout, on écrit :

$$CT + DS = 1$$

Donc :

$$ACT + DSA = A$$

Donc :

$$\begin{aligned} \frac{A}{TS} &= \frac{ACT + DSA}{TS} \\ &= \frac{DA}{T} + \frac{AC}{S} \end{aligned}$$

On écrit la division euclidienne de DA par T et de AC par S :

$$\begin{aligned} DA &= TQ + U \text{ avec } \deg(U) < \deg(T) \\ AC &= SH + V \text{ avec } \deg(V) < \deg(S) \end{aligned}$$

Donc :

$$\frac{A}{TS} = \frac{U}{T} + \frac{V}{S} + Q + H$$

Ainsi :

$$\begin{aligned}\deg(Q+H) &= \deg\left(\frac{A}{TS} - \frac{U}{T} - \frac{V}{S}\right)\\ &\leq \max(\ldots, \ldots, \ldots)\\ &< 0\end{aligned}$$

Donc $Q + H = 0$.

17.32 Théorème

Théorème 17.33

Si T est un polynôme irréductible unitaire et si $\deg\left(\frac{A}{T^n}\right) < 0$ (avec $n \geq 1$), alors il existe des polynômes $V_1, \ldots, V_n$ tels que

$$\frac{A}{T^n} = \sum_{k=1}^{n} \frac{V_k}{T^k}, \text{ avec } \deg(V_k) < \deg(T).$$

C'est une **décomposition en éléments simples**.

Par récurrence sur n.

- Pour $n = 1$, RAF.
- On suppose le résultat vrai pour $n \geq 1$ fixé.
  On écrit la division euclidienne de A par T :

  $$A = BT + V_{n+1} \text{ avec } \deg(V_{n+1}) < \deg(T)$$

  Ainsi :

  $$\begin{aligned}\frac{A}{T^{n+1}} &= \frac{BT + V_{n+1}}{T^{n+1}}\\ &= \frac{B}{T^n} + \frac{V_{n+1}}{T^{n+1}}\\ &= \sum_{k=1} \frac{V_k}{T^k} + \frac{V_{n+1}}{T^{n+1}} \text{ (Hypothèse de récurrence)}\end{aligned}$$

17.38 Cas d'un pôle simple

Propostion 17.38

Si a est un pôle simple de $F = \frac{A}{B}$, alors la partie polaire de F relative à a est

$$P_F(a) = \frac{c}{X-a} \text{ avec } c = \frac{A(a)}{B'(a)} = \frac{A(a)}{Q(a)} \text{ où } B = (X-a)Q.$$

D'après le théorème d'existence de la DES :

$$\frac{A}{B} = F = E + \frac{c}{X-a} + G$$

Donc :

$$\begin{aligned}c &= \frac{(X-a)A}{B} - (X-a)E - (X-a)G\\ &= \frac{A}{Q} - (X-a)E - (X-a)G\end{aligned}$$

Donc $c = \frac{A(a)}{Q(a)}$.
Si $B = (X-a)Q$, alors $B'(a) = Q(a)$.

17.39 Exemple

Exemple 17.39

Décomposer en éléments simples dan $\mathbb{C}(X)$ la fraction raitonnelle $F = \frac{1}{X^n - 1}$ avec $n \geq 1$.

— $\deg F = -n < 0$.

— F possède n pôles simples. $e^{\frac{2ik\pi}{n}} = \omega_k$.
— D'après le théorème de DES :

$$F = \sum_{k=0}^{n-1} \frac{c_k}{X - \omega_k}$$

Or, pour tout $k \in [\![0, n-1]\!]$, $c_k = \frac{1}{nw_k^{n-1}} = \frac{\omega_k}{n}$.

$$F = \frac{1}{n} \sum_{k=0}^{n-1} \frac{\omega_k}{X - \omega_k}$$

17.40 Cas d'un pôle double

Propostion 17.40

Si a est un pôle double de $F = \frac{A}{B}$, alors la partie polaire de F relative à a est

$$P_F(a) = \frac{\alpha}{X - a} + \frac{\beta}{(X-a)^2} \text{ avec } \beta = H(a) \text{ et } \alpha = H'(a) \text{ en posant } H = (X-a)^2 F.$$

On a (notations 17.38) :

$$F = E + \frac{\alpha}{X-a} + \frac{\beta}{(X-a)^2} + G$$
$$\beta + (X-a)\alpha = \underbrace{(X-a)^2 F}_{:=H} - (X-a)^2 E - (X-a)^2 G$$

En évaluant en a : $\beta = H(a)$.
On dérive et on évalue en a : $\alpha = H'(a)$.

17.42 Exemple

Exemple 17.42

Décomposer $F = \frac{X^6}{(X-1)^2(X^3+1)}$ en éléments simples dans $\mathbb{C}(X)$.

— $\deg F = 1 \geq 0$
—

$$X^6 = (X-1)^2(X^3+1)(X+2) + R \text{ avec } \deg R < 5$$

— D'après le théorème DES :

$$\begin{aligned}
F &= \frac{X^6}{(X-1)^2(X+1)(X+j)(X+j^2)} \\
&= X + 2 + \frac{a}{X-1} + \frac{b}{(X-1)^2} + \frac{c}{X+1} + \frac{d}{X+j} + \frac{e}{x+j^2} \\
c &= (x+1)\tilde{F}(-1) = \frac{1}{4} \\
d &= (x+j)\tilde{F}(-j) \\
&= \frac{1}{(j+1)^2(1-j)(-j+j^2)} \\
&= \frac{1}{(1+j)(1-j^2)(j-1)j} \\
&= \frac{-1}{(1-j^2)^2 j} \\
&= \frac{-1}{j(-3j^2)} \\
&= \frac{1}{3} \\
e &= (x+j^2)\tilde{F}(-j^2) = \frac{1}{3} \\
H &= (X-1)^2 F = \frac{X^6}{X^3+1} \\
b &= H(1) = \frac{1}{2} \\
a = H'(1) &= \frac{9}{4}
\end{aligned}$$

17.44 Parties polaires conjuguées d'une fraction réelle

Propostion 17.44

Si F est à coefficients réels, alors les parties polaires relatives aux pôles conjugués sont conjuguées.

Soit $F \in \mathbb{R}(X) \subset \mathbb{C}(X)$.
On écrit $F = \frac{A}{B}$ avec $A, B \in \mathbb{R}(X)^2$.
Soit r un pôle de multiplicité m.
Comme $F \in \mathbb{R}(X)$, $\overline{r}$ est un pôle de multiplicité m. On suppose que $r \neq \overline{r}$
D'après le théorème de DES, on écrit :

$$F = E + P_F(r) + G \text{ avec } (E, r) \in \mathbb{R}(X)^2, G \in \mathbb{C}(X)$$

r n'est pas un pôle de G ($\overline{r}$ oui).
Ainsi :

$$\begin{aligned}
F &= \overline{F} \\
&= \overline{E + P_F(r) + G} \\
&= \overline{E} + P_F(\overline{r}) + \overline{G} \\
&= E + \overline{P_F(r)} + \overline{G}
\end{aligned}$$

Or r n'est pas un pôle de $\overline{P_F(r)}$ mais $\overline{r}$ est un pôle de $\overline{P_F(r)}$.
De la même manière, comme r n'est pas un pôle de G, $\overline{r}$ n'est pas un pôle de $\overline{G}$.
Donc $P_F(\overline{r}) = \overline{P_F(r)}$.

17.45 Exemple

Exemple 17.45

Décomposer en éléments simples $F = \frac{1}{(X^2+X+1)^2}$ dans $\mathbb{C}(X)$.

$F = \overline{(x^2+x+1)^2}, \deg(F) = -4 < 0$.
Les pôles de F sont j et j^2 (de multiplicité 2).
D'après le théorème de DES :

$$F = \frac{a}{X-j} + \frac{b}{(X-j)^2} + \frac{c}{X-j^2} + \frac{d}{(X-j^2)^2} \text{ car } F \in \mathbb{R}(X)$$

On pose $H = (X-j)^2 F = \frac{1}{(x-j^2)^2}$.
On trouve $b = H(j) = \frac{j}{(1-j)}$ et $a = H'(j) = \frac{-2}{(1-j)^3} = \frac{-2j^2}{3(1-j)j}$.

17.46 Exemple

Exemple 17.47

Décomposer en éléments simples $F = \frac{X^4+1}{X(X^2-1)^2}$ dans $\mathbb{R}(X)$.

$F = \frac{X^4+1}{X(X^2-1)^2}, \deg F = -1 < 0$. Donc :

$$F = \frac{a}{X} + \frac{b}{X-1} + \frac{c}{(X-1)^2} + \frac{d}{X+1} + \frac{e}{(X+1)^2}$$

F est impaire donc :

$$\begin{aligned}
F(-X) &= -\frac{a}{X} + \frac{b}{-X-1} + \frac{c}{(-X-1)^2} + \frac{d}{-X+1} + \frac{e}{(-X+1)^2} \\
&= -\frac{a}{X} - \frac{b}{X+1} + \frac{c}{(X+1)^2} - \frac{d}{X-1} + \frac{e}{(X-1)^2} \\
&= -F \\
&= -\frac{a}{X} - \frac{b}{X-1} - \frac{c}{(X-1)^2} - \frac{d}{X+1} - \frac{e}{(X+1)^2}
\end{aligned}$$

Par unicité :

$$\begin{cases} a = a \\ -b = -d \\ -c = e \end{cases} \quad \text{soit} \quad \begin{cases} b = d \\ e = -c \end{cases}$$

On a : $a = X\tilde{F}(0) = 1$.
On pose :

$$\begin{aligned}
H &= (X-1)^2 F = \frac{X^4+1}{X(X+1)^2} \\
c &= H(1) = \frac{1}{2} \\
b &= H'(1) \\
&= \frac{4 \times 4 - 2 \times (3+4+1)}{4} \\
&= 0
\end{aligned}$$

17.51 Exemple - Calcul de la dérivée n-ième d'une fraction

Exemple 17.51

Soit $f(x) = \frac{1}{x^2+1}$. Calculer $f^{(n)}(x)$.

Soit $f : \mathbb{R} \to \mathbb{R}; x \mapsto \frac{1}{x^2+1} \in \mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$.
On définit :

$$\begin{aligned} F = \frac{1}{X^2+1} &\in \mathbb{R}(X) \\ &\in \mathbb{C}(X) \end{aligned}$$

D'après le théorème de DES, car les pôles de F sont simples, égaux à i et $-i$:

$$\begin{aligned} F &= \frac{\frac{1}{-2i}}{X+i} + \frac{\frac{1}{2i}}{X-i} \\ F^{(n)} &= \frac{\frac{i}{2}(-1)^n n!}{(X+i)^{n+1}} + \frac{\frac{-i}{2}(-1)^n n!}{(X-i)^{n+1}} \\ &= \frac{(-1)^n n!}{(X^2+i)^{n+1}} \frac{i}{2} \left[(X-i)^{n+i} - (X+i)^{n+i} \right] \\ &= \frac{(-1)^n n!}{(X^2+1)^{n+1}} \frac{i}{2} \sum_{k=0}^{n+1} \binom{n+1}{k} [(-i)^k - i^k] X^{n+1-k} \\ &= \frac{(-1)^n n!}{(X^2+1)^{n+1}} \sum_{0 \leq 2k+1 \leq n+1} \binom{n+1}{2k+1} (-i)^{k+1} X^{n-2k} \end{aligned}$$

Donc :

$$f^{(n)}(x) = \frac{(-1)^n n!}{(x^2+1)^{n+1}} \sum_{0 \leq 2k+1 \leq n+1} \binom{n+1}{2k+1} (-i)^{k+1} x^{n-2k}$$

Chapitre 18

Dérivabilité

18.43 Théorème de prolongement de classe $\mathcal{C}^n$ - HP

Théorème 18.43 - HP

Soit I un intervalle et $x_0 \in I$. Soit f une fonction définie de classe $\mathcal{C}^n$ sur $I \backslash \{x_0\}$. Si $f^{(n)}$ admet une limite finie en x_0, alors f est prolongeable en une fonction de classe $\mathcal{C}^n$ sur I.

— On prouve le théorème pour $n = 1$. On suppose $f \in \mathcal{C}^1(I \backslash \{x_0\}, \mathbb{R})$ et que f' admet une limite finie en x_0.
On prolonge f' en une fonction g par continuité en x_0. Ainsi, $g \in \mathcal{C}^0(I, \mathbb{R})$.
On remarque que pour tout $x \neq x_0$:

$$f(x) = f(a) + \int_a^x f'(t)\,dt$$

où $a \in I \backslash \{x_0\}$ quelconque.

$$f(x) = \underbrace{f(a) + \int_a^x g(t)\,dt}_{\text{Admet une limite finie quand } x \to x_0}$$

Donc $f(x)$ admet également une limite finie quand $x \to x_0$.
On prolonge alors f par continuité en $\tilde{f}$, de classe $\mathcal{C}^1$ sur I.

— On raisonne par récurrence. Pour $n \in \mathbb{N}$, on pose :

$P(n)$: "Pour tout $f \in \mathcal{C}^n(I \backslash \{x_0\}, \mathbb{R})$, si $f^{(n)}$ admet une limite finie en x_0, alors f se prolonge en $\tilde{f} \in \mathcal{C}^n(I, \mathbb{R})$".

Pour $n = 0$, c'est le prolongement par continuité.
Pour $n = 1$, c'est fait.
On suppose $P(n)$ vraie pour $n \geq 1$.
Soit $f \in \mathcal{C}^{n+1}(I \backslash \{x_0\}, \mathbb{R})$, etc...
Donc $f' \in \mathcal{C}^n(I \backslash \{x_0\}, \mathbb{R})$ et $f^{(n)}$ admet une limite finie en x_0.
D'après $P(n)$, on prolonge f' en $g \in \mathcal{C}^n(I, \mathbb{R})$.
En particulier, g est continue sur I.
Donc f' admet une limite finie en x_0.
On applique $P(1)$. On prolonge f en $\tilde{f} \in \mathcal{C}^{n+1}(I, \mathbb{R})$.
Or $\tilde{f}' = g \in \mathcal{C}^n(I, \mathbb{R})$.
Donc $\tilde{f} \in \mathcal{C}^{n+1}(I, \mathbb{R})$.

18.45 IAF pour les fonctions à valeurs dans $\mathbb{C}$

Théorème 18.45

Soit $f \in \mathcal{C}^1([a, b], \mathbb{C})$ et M un réel tel que $|f'| \leq M$ sur $]a, b[$. Alors

$$|f(b) - f(a)| \leq M|b - a|$$

Si $f \in C^1([a, b], \mathbb{R})$, alors :

$$f(b) - f(a) = \int_a^b f'(t)\,dt$$

D'après l'inégalité triangulaire intégrale :

$$
\begin{aligned}
|f(b) - f(a)| &= \left| \int_a^b f'(t)\, dt \right| \\
&\leq \int_a^b |f'(t)|\, dt \\
&\leq \int_a^b M\, dt \\
&= M|b-a|
\end{aligned}
$$

Chapitre 19

Convexité