

MATHÉMATIQUES TS

LUCAS BRAESCH

★ ★ ★

RÉSUMÉ. Sans s'éloigner du contenu, ce cours dépasse notablement les objectifs du programme. Il ne saurait toutefois se substituer à celui de votre professeur, dès lors que ses ambitions pédagogiques sont très différentes. En l'occurrence, l'accent est systématiquement porté sur les problèmes théoriques soulevés par le cours, qui sont – en général – grossièrement escamotés. Par principe, et dans la mesure du possible, tous les résultats sont démontrés. Le cas échéant, ils sont jugés élémentaires (et laissés en exercice au lecteur) ou bien ils sont admis (ce qui est signalé).

TABLE DES MATIÈRES

Algèbre	2
1. Notions de base	2
2. Dénombrement, Probabilités	4
3. Nombres complexes	7
4. Calcul vectoriel	9
5. Arithmétique	13
Analyse	16
6. Limites et Continuité	16
7. Dérivation, Primitives	20
8. Logarithmes, Exponentielles	23
9. Intégration	26
10. Equations différentielles	30

Date: 1^{er} septembre 2006.

Je remercie les contributeurs du logiciel libre L^AT_EX, sans qui ce document n'existerait pas.

Notation. Les symboles \forall , \exists et $\exists!$ signifient respectivement «pour tout», «il existe» et «il existe un unique». Ils seront assez largement utilisés par soucis de rigueur et de concision.

1. NOTIONS DE BASE

1.1. Ensembles.

1.1.1. Définitions.

- Définition 1.1.** (1) Un ensemble E est *inclus* dans un ensemble F si $\forall x \in E, x \in F$. Par convention, $\emptyset \subset E$, pour tout ensemble E .
- (2) Etant donné un ensemble E , on appelle *partie* ou *sous ensemble* de E un ensemble inclus dans E . On note $\mathcal{P}(E)$ l'ensemble des parties de E .

Exemple 1.1. L'ensemble des parties de la paire $\{0, 1\}$ est $\mathcal{P}(\{0, 1\}) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.

Définition 1.2. Soient A et B des parties d'un ensemble E . On définit :

$$\begin{aligned} A \cup B &= \{x \in E, x \in A \text{ ou } x \in B\} & A \cap B &= \{x \in E, x \in A \text{ et } x \in B\} \\ A \setminus B &= \{x \in E, x \in A \text{ et } x \notin B\} & A^C &= E \setminus A = \{x \in E, x \notin A\} \end{aligned}$$

Définition 1.3. Soit E un ensemble et $(A_i)_{i \in I}$ une famille de parties de E . On définit leur réunion et intersection *quelconques* (I peut être infini) de la façon suivante

$$\bigcup_{i \in I} A_i = \{x \in E; \exists i \in I, x \in A_i\} \qquad \bigcap_{i \in I} A_i = \{x \in E; \forall i \in I, x \in A_i\}$$

Exemple 1.2. On prends ici $E = \mathbb{R}$:

- (1) $A = \bigcup_{n \in \mathbb{Z}} [n, n + 1[= \mathbb{R}$ puisque $\forall x \in \mathbb{R}, x \in [n, n + 1[$ avec $n = [x]$.
- (2) $B = \bigcap_{n \in \mathbb{N}^*}]0, 1/n[= \emptyset$ puisque $\forall x \in \mathbb{R}_-, \forall n \in \mathbb{N}^*, x \notin]0, 1/n[$ et $\forall x \in \mathbb{R}_+, \exists N \in \mathbb{N}^*, x \notin]0, 1/N[$ (prendre $N > 1/x$).

Définition 1.4. Soient E, F deux ensembles. Le *produit cartésien* de E par F est l'ensemble

$$E \times F = \{(e, f); e \in E \text{ et } f \in F\}$$

Définition 1.5. Une famille $(A_i)_{i \in I}$ de parties non vides d'un ensemble E en est une *partition* lorsque

$$\bigcup_{i \in I} A_i = E \quad \text{et} \quad \forall (i, j) \in I^2, i \neq j \implies A_i \cap A_j = \emptyset$$

Exemple 1.3. $\{[n, n + 1[, n \in \mathbb{Z}\}$ est une partition de \mathbb{R} puisque $\bigcup_{n \in \mathbb{Z}} [n, n + 1[= \mathbb{R}$ (exemple 1.2) et $\forall (i, j) \in \mathbb{Z}^2, i \neq j \implies [i, i + 1[\cap [j, j + 1[= \emptyset$.

1.1.2. Propriétés.

Théorème 1.1 (Morgan). *Soit E un ensemble et $(A_i)_{i \in I}$ une famille de parties de E :*

$$\left(\bigcup_{i \in I} A_i \right)^C = \bigcap_{i \in I} A_i^C \qquad \left(\bigcap_{i \in I} A_i \right)^C = \bigcup_{i \in I} A_i^C$$

preuve. Il est bon de rapeller que

$$\text{non}(\forall x \in A, P(x)) = \exists x \in A, \text{non}P(x) \quad \text{et} \quad \text{non}(\exists x \in A, P(x)) = \forall x \in A, \text{non}P(x)$$

Ainsi, $\forall x \in E, x \notin \bigcup_{i \in I} A_i \iff \text{non}(\exists i \in I, x \in A_i) \iff \forall i \in I, x \notin A_i$. En appliquant la première égalité aux $(A_i^C)_{i \in I}$, on en déduit la deuxième. \square

Exemple 1.4. Dans le cadre de l'exemple 1.2, on a :

- (1) $A^C = \bigcap_{n \in \mathbb{Z}} [n, n + 1[^C = \emptyset = \mathbb{R}^C$ puisque $\forall x \in \mathbb{R}, x \notin [n, n + 1[^C$ pour $n = [x]$.
- (2) $B^C = \bigcup_{n \in \mathbb{N}^*}]0, 1/n[^C = \mathbb{R} = \emptyset^C$ (laissé au lecteur).

Proposition 1.2. \cap et \cup sont associatives, commutatives et distributives l'une sur l'autre, cad que $\forall A, B, C \in \mathcal{P}(E)$ on a :

$$\begin{aligned} (1.1) \quad A \cup (B \cap C) &= (A \cup B) \cap C & A \cap (B \cup C) &= (A \cap B) \cup C \\ (1.2) \quad A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) & A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \\ (1.3) \quad A \cup B &= B \cup A & A \cap B &= B \cap A \end{aligned}$$

preuve. L'égalité $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ se démontre en construisant une *table de vérité* où l'on envisage (à $x \in E$ fixé) toutes les valeurs de vérité du triplet $(x \in A, x \in B, x \in C)$. On notera 1 pour «vrai» et 0 pour «faux», de sorte qu'il s'agisse de compter en binaire pour ne rien oublier (cf tableau ci-contre). Bien sûr, une fois la méthode comprise, le lecteur pourra démontrer les autres résultats de la même façon (exercice fastidieux et inutile à mon goût).

A	B	C	$A \cap (B \cup C)$	$(A \cap B) \cup (A \cap C)$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	0	0
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

□

1.1.3. L'ensemble \mathbb{N} .

Proposition 1.3 (admis). *Toute partie non vide de \mathbb{N} admet un plus petit élément. Ce résultat est admis, puisqu'il découle directement de la construction de \mathbb{N} – largement hors programme.*

Théorème 1.4 (Récurrence simple). *Soit $(P(n))_{n \in \mathbb{N}}$ une famille de propositions. Si*

$$\begin{cases} P(0) \text{ est vraie} \\ \forall n \in \mathbb{N}, P(n) \implies P(n+1) \end{cases}$$

alors $\forall n \in \mathbb{N}, P(n)$ est vraie.

preuve. Soit $X = \{n \in \mathbb{N}; P(n) \text{ est fausse}\}$. Si $X \neq \emptyset$, alors X a un plus petit élément x_0 . $x_0 \neq 0$, puisque $P(0)$ est vraie, donc $x_0 - 1 \in \mathbb{N}$ et par minimalité de x_0 , $x_0 - 1 \notin X$ cad que $P(x_0 - 1)$ est vraie. Donc $P(x_0)$ est vraie, cad $x_0 \notin X$: contradiction : $X = \emptyset$.

□

Corollaire 1.5 (Récurrence forte). *Soit $(P(n))_{n \in \mathbb{N}}$ une famille de propositions. Si*

$$\begin{cases} P(0) \text{ est vraie} \\ \forall n \in \mathbb{N}, \{P(0) \text{ et } P(1) \cdots \text{ et } P(n)\} \implies P(n+1) \end{cases}$$

alors $\forall n \in \mathbb{N}, P(n)$ est vraie.

preuve. Appliquer le théorème précédent à $Q(n) = \{P(0) \text{ et } P(1) \cdots \text{ et } P(n)\}$.

□

1.1.4. L'ensemble \mathbb{Q} .

Définition 1.6. On appelle *rationnel* tout réel r tel qu' $\exists(p, q) \in \mathbb{Z} \times \mathbb{Z}^*, r = \frac{p}{q}$. On appelle *représentant irréductible* d'un rationnel $r \neq 0$ tout couple $(\alpha, \beta) \in (\mathbb{Z}^*)^2$ tel que $r = \frac{\alpha}{\beta}$ et α, β n'ont pas de diviseur commun non-trivial (on dit alors qu'ils sont *premiers entre eux*).

Proposition 1.6. *Tout rationnel non nul admet au moins un représentant irréductible. Soit $r \in \mathbb{Q}^*$ et (α, β) un représentant irréductible de r ; tout représentant de r est de la forme $(k\alpha, k\beta), k \in \mathbb{Z}^*$. Tout rationnel non nul admet exactement deux représentants irréductibles, (α, β) et $(-\alpha, -\beta)$.*

preuve. Ce résultat est démontré dans le cours d'Arithmétique, page 15.

□

1.1.5. L'ensemble \mathbb{R} .

Théorème 1.7 (admis). *Si X est une partie non vide majorée de \mathbb{R} , alors*

$$\exists! s \in \mathbb{R}, \quad \begin{cases} \forall x \in X, & x \leq s \\ \forall \varepsilon > 0, & [s - \varepsilon, s] \cap X \neq \emptyset \end{cases}$$

Ce réel s s'appelle borne supérieure (ou supremum) de X et se note $\sup X$.

preuve. L'unicité est triviale et l'existence admise (elle résulte de la construction de \mathbb{R}).

□

Exemple 1.5. Intuitivement, il n'y a pas de «trous» dans la droite réelle, ce qui n'est pas le cas dans \mathbb{Q} . En effet, $\{x \in \mathbb{R}, x^2 < 2\}$ a une borne supérieure dans \mathbb{R} ($\sqrt{2}$), mais pas dans \mathbb{Q} .

Corollaire 1.8. *Si X est une partie non vide minorée de \mathbb{R} , alors*

$$\exists! i \in \mathbb{R}, \quad \begin{cases} \forall x \in X, & i \leq x \\ \forall \varepsilon > 0, & [i, i + \varepsilon] \cap X \neq \emptyset \end{cases}$$

Ce réel i s'appelle borne inférieure (ou infimum) de X et se note $\inf X$.

preuve. Appliquer le théorème précédent à $-X = \{-x, x \in X\}$.

□

1.2. Applications.

Définition 1.7. Soient E, F deux ensembles. On dit que $f \subset E \times F$ est une *fonction* de E vers F , et on note $f : E \longrightarrow F$, lorsque pour tout $x \in E$, il existe au plus un $y \in F$ tel que $(x, y) \in f$. L'élément x est alors un *antécédant* de son (unique) *image* y par f , ce que l'on notera $y = f(x)$ plutôt que $(x, y) \in f$. L'*ensemble de définition* de f est l'ensemble des $x \in E$ admettant une (unique) image, soit $\mathcal{D}_f = \{x \in E; \exists y \in F, (x, y) \in f\}$. Lorsque tout point a une (unique) image, on dit que f est une *application*. Enfin, signalons que l'ensemble des applications de E dans F se note F^E .

Proposition 1.9. Soient $f : E \longrightarrow F$ et $g : F \longrightarrow G$ des applications. L'ensemble

$$g \circ f = \{(x, z) \in E \times G; \exists y \in F, y = f(x) \text{ et } z = g(y)\}$$

est une application de E vers G .

Proposition 1.10 (associativité). Soient $f : E \longrightarrow F$, $g : F \longrightarrow G$, $h : G \longrightarrow H$. Alors :

$$h \circ (g \circ f) = (h \circ g) \circ f \quad \text{qu'on peut donc noter } h \circ g \circ f$$

Définition 1.8. Soit $f : E \longrightarrow F$ une fonction. Pour $X \in \mathcal{P}(E)$ et $Y \in \mathcal{P}(F)$, on note abusivement :

$$f(X) = \{f(x), x \in X \cap \mathcal{D}_f\} \qquad f^{-1}(Y) = \{x \in \mathcal{D}_f, f(x) \in Y\}$$

Définition 1.9. Une application $f : E \longrightarrow F$ est dite :

– *injective* si tout élément de l'ensemble d'arrivée a au plus un antécédant :

$$\forall (x, y) \in E^2, \quad f(x) = f(y) \implies x = y \quad \text{ou encore (contraposée)} \quad x \neq y \implies f(x) \neq f(y)$$

– *surjective* si tout élément de l'ensemble d'arrivée a au moins un antécédant :

$$\forall y \in F, \quad \exists x \in E, \quad f(x) = y \quad \text{ou encore} \quad f(E) = F$$

– *bijective* si elle est injective et surjective, cad si tout élément de l'ensemble d'arrivée a exactement un antécédant : $\forall y \in F, \quad \exists! x \in E, \quad f(x) = y$.

Exemple 1.6. (1) l'application $\mathbb{R} \longrightarrow \mathbb{R}$, $x \longmapsto \sin x$ n'est ni injective ni surjective.

(2) l'application $\mathbb{R} \longrightarrow [-1, 1]$, $x \longmapsto \sin x$ est surjective mais pas injective.

(3) l'application $[-\frac{\pi}{2}, \frac{\pi}{2}] \longrightarrow \mathbb{R}$, $x \longmapsto \sin x$ est injective mais pas surjective.

(4) l'application $[-\frac{\pi}{2}, \frac{\pi}{2}] \longrightarrow [-1, 1]$, $x \longmapsto \sin x$ est bijective.

Définition 1.10. On appelle *permutation* de E toute bijection de E dans E , et *involution* une application $f : E \longrightarrow E$ telle que $f \circ f = \text{Id}_E$.

Proposition 1.11. Soit $f : E \longrightarrow F$ une application. L'ensemble $f^{-1} = \{(y, x); (x, y) \in f\}$ est une application ssi f est bijective. Dans ce cas, $f^{-1} : F \longrightarrow E$ est une bijection qui vérifie

$$f^{-1} \circ f = \text{Id}_E \quad \text{et} \quad f \circ f^{-1} = \text{Id}_F$$

2. DÉNOMBREMENT, PROBABILITÉS

2.1. Dénombrement.

2.1.1. Applications, Permutations, Arrangements, Combinaisons.

Proposition 2.1 (rappel). Le nombre d'applications de p éléments dans n éléments est n^p .

preuve. Définir une application $\varphi : \llbracket 1, p \rrbracket \longrightarrow \llbracket 1, n \rrbracket$, c'est choisir de n façons et indépendamment, chacun des $\varphi(k)$ pour $k \in \llbracket 1, p \rrbracket$. Ainsi, $\text{Card } \llbracket 1, n \rrbracket^{\llbracket 1, p \rrbracket} = \underbrace{n \times \cdots \times n}_{p \text{ termes}} = n^p$. \square

Exemple 2.1. Un numéro de téléphone à 8 chiffres en base 10, soit $(x_1, \dots, x_8) \in \llbracket 0, 9 \rrbracket^8$, peut être considéré comme l'application de $\llbracket 1, 8 \rrbracket \longrightarrow \llbracket 0, 9 \rrbracket$, $i \longmapsto x_i$: il y en a donc 10^8 .

Définition 2.1. Soient $p \leq n$ deux entiers naturels. On note

– A_n^p le nombre d'injections de p éléments dans n éléments.

– C_n^p le nombre de parties à p éléments dans un ensemble à n éléments.

Remarque. Il revient au même de dire que A_n^p est le nombre de p -arrangements d'un ensemble à n éléments, cad le nombre de p -uplets d'éléments deux à deux distincts d'un ensemble à n éléments.

Théorème 2.2. $A_n^p = n(n-1) \cdots (n-p+1) = p!C_n^p$

preuve. Pour définir une injection $i : \llbracket 1, p \rrbracket \longrightarrow \llbracket 1, n \rrbracket$, on a n choix pour $i(1)$, $(n-1)$ pour $i(2) \neq i(1)$, \dots , $(n-p+1)$ choix pour $i(p) \notin \{i(1), \dots, i(p-1)\}$. Noter bien que le produit s'arrête à $n-p+1$ parce qu'il comporte p termes. En particulier, on note $n! = A_n^n = n(n-1) \cdots 2 \cdot 1$ le nombre de permutations de n éléments (une injection de n éléments dans n éléments est surjective, donc bijective). Etant donné une partie à p éléments d'un ensemble à n éléments, il y a donc $p!$ façons de l'ordonner en un p -arrangement, d'où $A_n^p = p!C_n^p$. \square

Exemple 2.2. Pour 17 chevaux sur la ligne de départ, il y a donc $A_{17}^3 = 17 \times 16 \times 15 = 4080$ tiercés dans l'ordre et $C_{17}^3 = \frac{4080}{3!} = 680$ tiercés dans le désordre.

2.1.2. *Propriétés algébriques des C_n^p .* En multipliant haut et bas par $(n-p)!$ nous obtenons :

$$A_n^p = \frac{n!}{(n-p)!} \qquad C_n^p = \frac{n!}{p!(n-p)!}$$

Théorème 2.3 (binôme de Newton). $\forall a, b \in \mathbb{R}, \quad (a+b)^n = \sum_{k=0}^n C_n^k a^k b^{n-k}$

preuve. Les termes du développement seront de la forme $a^k b^{n-k}$ ($0 \leq k \leq n$). Pour k fixé, il y en a C_n^k , puisqu'il s'agit de choisir k parenthèses parmi n dans lesquelles on retient a . Pour une preuve plus rigoureuse, il faut raisonner par récurrence, mais je trouve cette explication plus naturelle. \square

Corollaire 2.4. *Un ensemble à n éléments a 2^n parties.*

preuve. $\forall k \in \llbracket 0, n \rrbracket$, il y a C_n^k parties à k éléments, donc $\text{Card}(\mathcal{P}(E)) = \sum_{k=0}^n C_n^k = (1+1)^n$ \square

Exemple 2.3. $\sum_{k=0}^n (-1)^k C_n^k = (1-1)^n = 0$, d'où $\sum_{2k \leq n} C_n^{2k} = \sum_{2k+1 \leq n} C_n^{2k+1}$. Ainsi, un ensemble fini à n éléments a-t-il autant de parties de cardinal pair que de parties de cardinal impair, soit 2^{n-1} .

Définition 2.2. Le *Triangle de Pascal* est le tableau triangulaire où C_n^p figure à la ligne n et à la colonne p . Il se construit avec les 2 règles suivantes :

Proposition 2.5. $C_n^p = C_n^{n-p} \quad C_n^p + C_n^{p+1} = C_{n+1}^{p+1}$

preuve. – Autant de choix de p éléments parmi n que de non-choix des $(n-p)$ restants.

$$- C_n^p = C_{n+1}^{p+1} \frac{p+1}{n+1} \text{ et } C_n^{p+1} = C_{n+1}^{p+1} \frac{n+1-(p+1)}{n+1}, \text{ d'où le résultat. } \square$$

2.2. Probabilités.

2.2.1. Rappels.

Définition 2.3. Une *épreuve aléatoire* est une expérience pouvant être réalisée plusieurs fois dans des conditions identiques et dont le résultat ne peut pas être connu à l'avance. L'*univers* Ω est l'ensemble (supposé fini) des résultats possibles d'une épreuve. Une *éventualité* est un élément de Ω ; un *évènement* est une partie de Ω : soit $A \in \mathcal{P}(\Omega)$. Si c'est un singleton, on parle d'*évènement élémentaire*, si $A = \Omega$ c'est l'*évènement certain*, si $A = \emptyset$ c'est l'*évènement impossible*. Deux évènements $A, B \in \mathcal{P}(\Omega)$ sont dits incompatibles lorsqu'ils sont disjoints ($A \cap B = \emptyset$).

Définition 2.4. Une application $\mathbb{P} : \mathcal{P}(\Omega) \longrightarrow [0; 1]$ est une *probabilité sur* Ω lorsque $\mathbb{P}(\Omega) = 1$ et :

$$\forall A, B \in \mathcal{P}(\Omega), \quad A \cap B = \emptyset \implies \mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B)$$

Corollaire 2.6. (1) si $A \subset B$, alors $\mathbb{P}(A) \leq \mathbb{P}(B)$.

(2) si les $(A_i)_{1 \leq i \leq n}$ sont 2 à 2 disjoints, alors $\mathbb{P}(\bigcup A_i) = \sum \mathbb{P}(A_i)$.

(3) $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$.

(4) $\mathbb{P}(\Omega \setminus A) = 1 - \mathbb{P}(A)$. En particulier, $\mathbb{P}(\emptyset) = 0$.

2.2.2. Probabilité conditionnelle.

Définition 2.5. Soit une épreuve, A et B deux de ses évènements, avec $\mathbb{P}(B) > 0$. La *probabilité conditionnelle de A sachant B* est définie par $\mathbb{P}(A/B) = \mathbb{P}_B(A) = \mathbb{P}(A \cap B)/\mathbb{P}(B)$. En effet, \mathbb{P}_B est une nouvelle probabilité sur Ω (vérifiez !), ce qui justifie cette notation. Deux évènements $A, B \in \mathcal{P}(\Omega)$ sont *indépendants* si $\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$.

Proposition 2.7 (probabilités totales). *Si $(B_i)_{1 \leq i \leq n}$ est une partition de Ω alors*

$$\forall A \subset \Omega, \quad \mathbb{P}(A) = \sum \mathbb{P}(B_i)\mathbb{P}(A/B_i)$$

preuve. En effet, $(A \cap B_i)_{1 \leq i \leq n}$ est une partition de A , d'où : $\mathbb{P}(A) = \sum_{i=1}^n \mathbb{P}(A \cap B_i)$. \square

2.2.3. Variable aléatoire.

Définition 2.6. On appelle *variable aléatoire* une application $X : \Omega \longrightarrow \mathbb{R}$.

Notation. Pour $A \in \mathcal{P}(\Omega)$, on note $\{X \in A\} = X^{-1}(A) = \{\omega \in \Omega, X(\omega) \in A\}$ l'évènement $X \in A$. Pour $x \in \mathbb{R}$, on note $\{X = x\} = X^{-1}(\{x\}) = \{\omega \in \Omega, X(\omega) = x\}$ l'évènement X prend la valeur x . Cela justifie les notations $\mathbb{P}(\{X = x\})$ et $\mathbb{P}(\{X \in A\})$. En fait, on n'écrira même plus les accolades. Enfin, rappelons que Ω est fini, donc $X(\Omega)$ aussi.

Définition 2.7. La *fonction de répartition* de X est l'application $F : \mathbb{R} \longrightarrow \mathbb{R}$ définie par :

$$F(x) = \mathbb{P}(X \leq x) = \mathbb{P}(X \in]-\infty, x])$$

Définition 2.8. L'*espérance*, la *variance* et l'*écart-type* d'une variable X sont définis par :

$$\mathbb{E}(X) = \sum_{x \in X(\Omega)} x\mathbb{P}(X = x) \quad \mathbb{V}(X) = \mathbb{E}[(X - \mathbb{E}X)^2] \quad \sigma(X) = \sqrt{\mathbb{V}(X)}$$

Proposition 2.8. *L'espérance est linéaire : $\mathbb{E}(\alpha X + \beta Y) = \alpha \mathbb{E}X + \beta \mathbb{E}Y$.*

Proposition 2.9 (Formule de Kœnig). $\mathbb{V}(X) = \mathbb{E}(X^2) - (\mathbb{E}X)^2$.

preuve. $\mathbb{V}(X) = \mathbb{E}[(X - \mathbb{E}(X))^2] = \mathbb{E}[X^2 - 2X(\mathbb{E}X) + (\mathbb{E}X)^2] = \mathbb{E}(X^2) - 2(\mathbb{E}X)^2 + (\mathbb{E}X)^2$. \square

2.2.4. Variable aléatoire indépendantes.

Définition 2.9. Deux variables aléatoires $X, Y : \Omega \longrightarrow \mathbb{R}$ sont *indépendantes* – ce que l'on note $X \perp\!\!\!\perp Y$ – lorsque pour tous évènements A et B les évènements $\{X \in A\}$ et $\{Y \in B\}$ sont indépendants :

$$(2.1) \quad \forall (A, B) \in \mathcal{P}(X(\Omega)) \times \mathcal{P}(Y(\Omega)), \quad \mathbb{P}(\{X \in A\} \cap \{Y \in B\}) = \mathbb{P}(X \in A)\mathbb{P}(Y \in B)$$

Proposition 2.10. *La condition précédente (2.1) équivaut à (pour Ω fini)*

$$(2.2) \quad \forall (x, y) \in X(\Omega) \times Y(\Omega), \quad \mathbb{P}(\{X = x\} \cap \{Y = y\}) = \mathbb{P}(X = x)\mathbb{P}(Y = y)$$

preuve. (2.1) \implies (2.2), en prenant $(x, y) \in X(\Omega) \times Y(\Omega)$ et en appliquant (2.1) à $A = \{x\}$ et $B = \{y\}$.

Réciproquement, on suppose (2.2) et on prend $(A, B) \in \mathcal{P}(X(\Omega)) \times \mathcal{P}(Y(\Omega))$. En utilisant la distributivité de \cap sur \cup et le fait que les évènements $E_{a,b} = \{X = a\} \cap \{Y = b\}$ sont deux à deux disjoints (ie. $(a, b) \neq (a', b') \implies E_{a,b} \cap E_{a',b'} = \emptyset$) :

$$\begin{aligned} \mathbb{P}(\{X \in A\} \cap \{Y \in B\}) &= \mathbb{P}\left(\left(\bigcup_{a \in A} \{X = a\}\right) \cap \left(\bigcup_{b \in B} \{Y = b\}\right)\right) = \mathbb{P}\left(\bigcup_{a \in A} \bigcup_{b \in B} \{X = a\} \cap \{Y = b\}\right) \\ &= \mathbb{P}\left(\bigcup_{(a,b) \in A \times B} \{X = a\} \cap \{Y = b\}\right) = \sum_{(a,b) \in A \times B} \mathbb{P}(\{X = a\} \cap \{Y = b\}) \end{aligned}$$

On termine en développant $\mathbb{P}(X \in A)\mathbb{P}(Y \in B)$:

$$\mathbb{P}(X \in A)\mathbb{P}(Y \in B) = \left(\sum_{a \in A} \mathbb{P}(X = a)\right) \left(\sum_{b \in B} \mathbb{P}(Y = b)\right) = \sum_{(a,b) \in A \times B} \mathbb{P}(X = a)\mathbb{P}(Y = b)$$

d'où le résultat puisque $\forall (a, b) \in A \times B, \mathbb{P}(X = a)\mathbb{P}(Y = b) = \mathbb{P}(\{X = a\} \cap \{Y = b\})$ par (2.2). \square

Proposition 2.11. – *Si $X \perp\!\!\!\perp Y$, alors $\mathbb{E}(XY) = (\mathbb{E}X)(\mathbb{E}Y)$ – réciproque fausse.*

– *Si les $(X_i)_{1 \leq i \leq n}$ sont deux à deux indépendantes, alors $\mathbb{V}(\sum X_i) = \sum \mathbb{V}(X_i)$ – réciproque fausse.*

preuve. (1) On calcule $\mathbb{E}(XY)$ en utilisant $\mathbb{P}(\{X = x\} \cap \{Y = y\}) = \mathbb{P}(X = x)\mathbb{P}(Y = y)$:

$$\begin{aligned} \mathbb{E}(XY) &= \sum_{x \in X(\Omega)} \sum_{y \in Y(\Omega)} xy \mathbb{P}(\{X = x\} \cap \{Y = y\}) = \sum_{x \in X(\Omega)} \sum_{y \in Y(\Omega)} xy \mathbb{P}(X = x)\mathbb{P}(Y = y) \\ &= \sum_{x \in X(\Omega)} x \mathbb{P}(X = x) \sum_{y \in Y(\Omega)} y \mathbb{P}(Y = y) = (\mathbb{E}X)(\mathbb{E}Y) \end{aligned}$$

(2) Notons $\bar{X}_i = \mathbb{E}X_i$ et développons directement la variance de $\sum X_i$:

$$\begin{aligned} \mathbb{V}\left(\sum X_i\right) &= \mathbb{E}\left[\left(\sum X_i - \sum \bar{X}_i\right)^2\right] = \mathbb{E}\left[\left(\sum (X_i - \bar{X}_i)\right)^2\right] \\ &= \mathbb{E}\left[\sum (X_i - \bar{X}_i)^2 + \sum_{i \neq j} (X_i - \bar{X}_i)(X_j - \bar{X}_j)\right] \\ &= \sum \mathbb{E}\left[(X_i - \bar{X}_i)^2\right] + \sum_{i \neq j} \mathbb{E}\left[(X_i - \bar{X}_i)(X_j - \bar{X}_j)\right] \end{aligned}$$

Enfin $\mathbb{V}X_i = \mathbb{E}\left[(X_i - \bar{X}_i)^2\right]$ et $\mathbb{E}\left[(X_i - \bar{X}_i)(X_j - \bar{X}_j)\right] = \mathbb{E}(X_i X_j) - \bar{X}_i \bar{X}_j = 0$ puisque $X_i \perp\!\!\!\perp X_j$. \square

2.2.5. Loi binômiale.

Définition 2.10. On dit qu'une variable aléatoire X suit une *loi de Bernoulli* de paramètre $p \in [0, 1]$ quand X prend les valeurs 0 et 1, avec $\mathbb{P}(X = 1) = p$ (donc $\mathbb{P}(X = 0) = 1 - p$). La loi de Bernoulli est donc la plus simple qui soit : on note alors $X \sim \mathcal{B}(p)$.

Définition 2.11. Soit X_1, \dots, X_n des variables aléatoires indépendantes (deux à deux) et identiquement distribuées selon une loi de Bernoulli de paramètre p . La variable $S_n = X_1 + \dots + X_n$ suit alors une *loi binômiale* de paramètre (n, p) , ce que l'on note $S_n \sim \mathcal{B}(n, p)$.

Proposition 2.12. *En gardant les notations précédentes, on a*

- (1) $\forall k \in [0, n], \quad \mathbb{P}(S_n = k) = C_n^k p^k (1 - p)^{n-k}$
- (2) $\mathbb{E}(X) = np$ et $\mathbb{V}(X) = np(1 - p)$.

preuve. Loi binômiale. $\mathbb{P}(S_n = k) = \sum_{\omega \in \{S_n = k\}} \mathbb{P}(\{\omega\}) = p^k (1 - p)^{n-k} \text{Card } S_n^{-1}(k) = C_n^k p^k (1 - p)^{n-k}$

Espérance. $\mathbb{E}(S_n) = \mathbb{E}(\sum X_i) = \sum \mathbb{E}X_i = np$, par linéarité de l'espérance.

Variance. Les X_i sont deux à deux indépendantes, donc $\mathbb{V}(S_n) = \mathbb{V}(\sum X_i) = \sum \mathbb{V}(X_i)$. Enfin les X_i sont identiquement distribuées et $\mathbb{V}(S_n) = n\mathbb{V}(X_1) = np(1 - p)$. \square

3. NOMBRES COMPLEXES

3.1. Introduction. Le *corps* $(\mathbb{C}, +, \times)$ des *nombres complexes* est l'ensemble \mathbb{R}^2 muni des opérations suivantes : $(a, b) + (c, d) = (a + c, b + d)$ et $(a, b) \times (c, d) = (ac - bd, ad + bc)$.

Définition 3.1. Plus précisément, un ensemble \mathbb{K} muni de deux *loi de composition internes* notées $+, \times : \mathbb{K}^2 \rightarrow \mathbb{K}$ est un *corps commutatif* lorsque

- (1) $+$ et \times sont *associatives* ($\forall a, b, c \in \mathbb{K}, a + (b + c) = (a + b) + c$ et $a \times (b \times c) = (a \times b) \times c$), *commutatives* ($\forall a, b \in \mathbb{K}, a + b = b + a$ et $a \times b = b \times a$) et admettent des *éléments neutres* notés 0 et 1 ($\forall a \in \mathbb{K}, a + 0 = a$ et $a \times 1 = a$).
- (2) Tout élément admet un opposé ($\forall x \in \mathbb{K}, \exists y \in \mathbb{K}, x + y = 0$) noté $-x$ et tout élément non nul admet un inverse ($\forall x \in \mathbb{K}^*, \exists y \in \mathbb{K}, x \times y = 1$) noté x^{-1} .
- (3) \times est distributive sur $+$ ($\forall a, b, c \in \mathbb{K}, a \times (b + c) = a \times b + a \times c$).

Par exemple $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps commutatifs.

On considère que $\mathbb{R} \subset \mathbb{C}$ en identifiant le réel x au complexe $(x, 0)$. En pratique, et pour sortir de ce formalisme, on pose $i = (0, 1)$, et on peut écrire (a, b) sous la forme $a + bi$. Il suffit alors de remarquer que $i^2 = -1$, et d'user des règles de calcul usuelles (valables dans un corps commutatif). Lorsque a et b sont des réels, on les appelle respectivement *partie réelle et imaginaire* du nombre complexe $z = a + bi$,

on note $a = \operatorname{Re} z$ et $b = \operatorname{Im} z$. Attention, l'unicité de cette écriture tient au fait que a et b sont réels (ex : $(1+i) + i(3-2i) = 3+4i$).

On représente ces nombres dans le plan (muni d'un repère orthonormé $(0; \vec{u}, \vec{v})$) : le nombre $z = a+ib$ représente indifféremment le point M ou le vecteur \overrightarrow{OM} de coordonnées (a, b) . On dit alors que z est l'*affiche* de M ou que M est l'*image* de z .

3.2. Point de vue algébrique. Soient a et b deux réels.

Définition 3.2. Le nombre complexe *conjugué* de $z = a+ib$ est $\bar{z} = a-ib$. D'un point de vue géométrique la conjugaison est donc la réflexion d'axe $(O; \vec{u})$.

Remarque. On peut caractériser les réels et les *imaginaires purs* (de la forme ib) par :

$$z \in \mathbb{R} \iff z = \bar{z} \quad \text{et} \quad z \in i\mathbb{R} \iff z = -\bar{z}$$

Les parties réelle et imaginaire s'écrivent aussi : $\operatorname{Re} z = \frac{1}{2}(z + \bar{z})$ et $\operatorname{Im} z = \frac{1}{2i}(z - \bar{z})$.

Définition 3.3. Le *module* de $z = a+bi$ est $|z| = \sqrt{a^2+b^2}$. Géométriquement $|z| = OM$, distance de l'origine au point M d'affixe z .

Remarque. On a toujours $z\bar{z} = |z|^2$. Par ailleurs, on divise des complexes en multipliant haut et bas par le conjugué du dénominateur, ce qui donne :

$$\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{\beta\bar{\beta}} = \frac{\alpha\bar{\beta}}{|\beta|^2} \quad \text{par exemple :} \quad \frac{1+i}{1-i} = \frac{(1+i)^2}{2} = \frac{2i}{2} = i.$$

Proposition 3.1. La conjugaison est compatible avec $+$, \times donc avec $-$, \div . Le module est compatible avec \times donc avec \div . Autrement dit $\forall (z, z') \in \mathbb{C}^2$:

$$\begin{aligned} \overline{z+z'} &= \bar{z} + \bar{z}' & \overline{zz'} &= \bar{z}\bar{z}' & |zz'| &= |z||z'| \\ \overline{z-z'} &= \bar{z} - \bar{z}' & \overline{\left(\frac{z}{z'}\right)} &= \frac{\bar{z}}{\bar{z}'} & \left|\frac{z}{z'}\right| &= \frac{|z|}{|z'|} \quad (z' \neq 0) \end{aligned}$$

Proposition 3.2 (Inégalité triangulaire). $\forall (z, z') \in \mathbb{C}^2$, $|z+z'| \leq |z| + |z'|$.

preuve. Comparer deux réels positifs revient à comparer leur carrés :

$$|z+z'|^2 - (|z| + |z'|)^2 = (z+z')(\bar{z} + \bar{z}') - (|z| + |z'|)^2 = z\bar{z}' + z'\bar{z} - 2|zz'| = 2(\operatorname{Re}(z\bar{z}') - |z\bar{z}'|)$$

On a aussi, $\forall \gamma \in \mathbb{C}$, $|\operatorname{Re} \gamma| \leq |\gamma|$ (puisque $\forall a, b \in \mathbb{R}$, $|a| = \sqrt{a^2} \leq \sqrt{a^2+b^2}$) ; d'où le résultat. \square

3.3. Point de vue trigonométrique.

Définition 3.4. Soit $z = a+ib \neq 0$. En écrivant : $a+ib = \sqrt{a^2+b^2} \left(\frac{a}{\sqrt{a^2+b^2}} + i \frac{b}{\sqrt{a^2+b^2}} \right)$, et en remarquant que $\left(\frac{a}{\sqrt{a^2+b^2}} \right)^2 + \left(\frac{b}{\sqrt{a^2+b^2}} \right)^2 = 1$, on en déduit qu'il existe un unique réel $\theta \in]-\pi; \pi[$ tel que $\cos \theta = \frac{a}{\sqrt{a^2+b^2}}$ et $\sin \theta = \frac{b}{\sqrt{a^2+b^2}}$: on l'appelle *argument* de z et on peut écrire z sous *forme trigonométrique* :

$$z = |z|(\cos \theta + i \sin \theta), \quad \text{de fait } \theta \equiv (\vec{u}, \overrightarrow{OM}) \pmod{2\pi}$$

Remarque. Tout autre réel θ' vérifiant cette égalité s'appelle un argument de z (et $\theta' \equiv \theta \pmod{2\pi}$).

Proposition 3.3. $\forall (z, z') \in (\mathbb{C}^*)^2$, $\arg zz' = \arg z + \arg z'$ et $\arg \frac{z}{z'} = \arg z - \arg z'$.

preuve. $(\cos \theta + i \sin \theta)(\cos \varphi + i \sin \varphi) = \cos(\theta + \varphi) + i \sin(\theta + \varphi)$. Ainsi, $\arg(zz') = \arg(z) + \arg(z')$. On en déduit $\arg(z/z') = \arg(z) - \arg(z')$ en écrivant $\arg(z' \frac{z}{z'}) = \arg(z) = \arg(z') + \arg \frac{z}{z'}$. \square

Définition 3.5 (Notation exponentielle). On note aussi $e^{i\theta}$ le nombre $\cos \theta + i \sin \theta$.

Remarque. Remarquez, par exemple, que $\rho e^{i\theta} = (-\rho)e^{i(\theta+\pi)}$. Du coup, on parle de la forme trigonométrique ou exponentielle lorsque $\rho > 0$ et $\theta \in]-\pi, \pi[$. D'après la remarque précédente,

$$e^{i(\theta+\varphi)} = e^{i\theta} e^{i\varphi} \quad \text{et} \quad e^{i(\theta-\varphi)} = \frac{e^{i\theta}}{e^{i\varphi}}$$

ce qui explique l'intérêt mnémorique de cette notation.

Proposition 3.4 (Formule de Moivre). $(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta$.

preuve. Par une récurrence élémentaire, $(e^{i\theta})^n = e^{in\theta}$ (on sait déjà que $e^{i(\theta+\varphi)} = e^{i\theta} e^{i\varphi}$). \square

Proposition 3.5 (Formules d'Euler). $2 \cos \theta = e^{i\theta} + e^{-i\theta}$, $2i \sin \theta = e^{i\theta} - e^{-i\theta}$.

3.4. Applications.

3.4.1. Trinôme du second degré.

$$az^2 + bz + c = a \left(z^2 + \frac{b}{a}z + \frac{c}{a} \right) = a \left[\left(z + \frac{b}{2a} \right)^2 - \frac{b^2 - 4ac}{4a^2} \right].$$

Posons $\Delta = b^2 - 4ac$: il ne reste plus qu'à trouver un complexe δ tel que $\delta^2 = \Delta$ et de terminer la factorisation. Si Δ est réel, il suffit de savoir que $i^2 = -1$:

$$z^2 + 2 \cos \theta z + 1 = (z + \cos \theta)^2 + \sin^2 \theta = (z + \cos \theta)^2 - (i \sin \theta)^2 = (z - e^{i\theta})(z - e^{-i\theta})$$

3.4.2. *Polynômes trigonométriques.* On appelle ainsi une somme de «mônômes» de la forme $\alpha \cos^n \sin^p$. Le linéariser c'est l'écrire sous forme d'une somme de termes du type $\cos \lambda x$ ou $\sin \mu x$. Une méthode générale consiste à écrire les formules d'Euler, de développer puis de regrouper les $e^{ikx} + e^{-ikx} = 2 \cos x$ et $e^{ikx} - e^{-ikx} = 2i \sin x$:

$$\cos^4 x = 2^{-4} ((e^{i4x} + e^{-i4x}) + 4(e^{i2x} + e^{-i2x}) + 6) = 2^{-3} (\cos 4x + 4 \cos 2x + 6).$$

Si on cherche une primitive et que n ou p est impair, on s'en sort en utilisant $\cos^2 + \sin^2 = 1$:

$$\cos^3 \sin^2 = \cos(1 - \sin^2) \sin^2 = \cos \sin^2 - \cos \sin^4,$$

à ce stade il n'y a plus que des termes du type u^n .

Remarque. L'opération inverse de la linéarisation se fait avec la formule de Moivre, en écrivant $\cos n\theta = \operatorname{Re}[(\cos \theta + i \sin \theta)^n]$ qu'on développe avec la formule du binôme.

3.4.3. *L'équation du troisième degré.* Historiquement les nombres complexes sont apparus comme un artéfact de calcul, permettant de résoudre dans \mathbb{R} l'équation du 3^e degré :

$$(3.1) \quad X^3 + \alpha X^2 + \beta X + \gamma = 0$$

Pour ce faire, on pose $Y = X + \alpha/3$, ce qui élimine le terme en Y^2 (vérifiez !) : $Y^3 + pY + q = 0$. On pose alors $Y = u + v$, avec $3uv + p = 0$. En effet, la détermination de (u, v) à partir de Y est une équation du second degré dans \mathbb{C} . L'équation en (u, v) est donc :

$$(3.2) \quad u^3 + v^3 + q = 0 \qquad 3uv + p = 0$$

On trouve alors (u^3, v^3) – réels ou complexes conjugués – comme racines de $Z^2 + qZ - p^3/27$. Si $(u^3, v^3) \in \mathbb{R}^2$, une solution réelle de $Y^3 + pY + q = 0$ est donc donnée par la *formule de Tartaglia* :

$$(3.3) \quad Y = \sqrt[3]{\frac{-q - \sqrt{\Delta}}{2}} + \sqrt[3]{\frac{-q + \sqrt{\Delta}}{2}} \qquad \Delta = q^2 + \frac{4p^3}{27}$$

Si $\Delta < 0$, alors $u^3 = \frac{-q - i\sqrt{-\Delta}}{2}$ et $v^3 = \frac{-q + i\sqrt{-\Delta}}{2}$ et une solution réelle est donnée par

$$(3.4) \quad Y = \sqrt[3]{\frac{-q - i\sqrt{-\Delta}}{2}} + \sqrt[3]{\frac{-q + i\sqrt{-\Delta}}{2}}$$

en notant $\sqrt[3]{\rho e^{i\theta}} = \sqrt[3]{\rho} e^{i\theta/3}$, pour $\rho > 0$ et $-\pi < \theta \leq +\pi$.

Remarque. L'équation $P(X) = 0$ est résoluble explicitement pour $\deg P = 1, 2, 3$ et même 4 (méthode de Ferrari non présentée ici). Plus généralement, tout polynôme à coefficients complexes a ses n racines (non nécessairement distinctes) dans \mathbb{C} (théorème de d'Alembert-Gauss). Ce résultat est étonnant : \mathbb{C} a été construit en rajoutant à \mathbb{R} une racine ad-hoc au polynôme $X^2 + 1$. Non seulement $X^2 + 1$ se factorise dans \mathbb{C} , mais il en est de même de tous les polynômes à coefficients réels et même complexes.

4. CALCUL VECTORIEL

Notation. \mathcal{V} (resp. \mathcal{E}) est un espace vectoriel réel (resp. affine dirigé par \mathcal{V}) de dimension finie $d \in \mathbb{N}^*$ (2 ou 3 si ça peut vous rassurer). Même si c'est encore l'usage au lycée, on ne mettra pas de flèches inutiles sur les vecteurs, mais uniquement sur les bipoints (on écrira $x \in \mathcal{V}$ et $\overrightarrow{AB} \in \mathcal{V}$ pour $(A, B) \in \mathcal{E}^2$). Seul le vecteur nul $\vec{0}$ se verra attribuer une flèche pour ne pas être confondu avec le scalaire $0 \in \mathbb{R}$.

4.1. Espace euclidien.

4.1.1. *Produit scalaire, Norme euclidienne.*

Définition 4.1. Une application $\varphi : \mathcal{V} \times \mathcal{V} \longrightarrow \mathbb{R}$ est un *produit scalaire* si elle est :

– *bilinéaire* : $\forall x \in \mathcal{V}$, $\varphi(x, \cdot)$ et $\varphi(\cdot, x)$ sont linéaires, cad que $\forall(x, y, z) \in \mathcal{V}^3, \forall(\alpha, \beta) \in \mathbb{R}^2$ on a :

$$\varphi(\alpha x + \beta y, z) = \alpha\varphi(x, z) + \beta\varphi(y, z) \quad \text{et} \quad \varphi(z, \alpha x + \beta y) = \alpha\varphi(z, x) + \beta\varphi(z, y)$$

– *symétrique* : $\forall x, y \in \mathcal{V}$, $\varphi(x, y) = \varphi(y, x)$

– *définie positive* : $\forall x \in \mathcal{V}$, $\varphi(x, x) \geq 0$ et $(\varphi(x, x) = 0 \implies x = \vec{0})$.

Notation. Dans toute la suite, on se fixe un produit scalaire φ sur \mathcal{V} . On dit alors que (\mathcal{V}, φ) est un *espace euclidien* et on notera $x \cdot y$ au lieu de $\varphi(x, y)$ le produit scalaire.

Définition 4.2. La *norme euclidienne* sur (\mathcal{V}, φ) (ou norme associée à φ) est l'application :

$$\|\cdot\| : \mathcal{V} \longrightarrow \mathbb{R}_+ \quad x \longmapsto \sqrt{x \cdot x}$$

Proposition 4.1. (1) $\forall x \in \mathcal{V}$, $(\|x\| = 0 \iff x = \vec{0})$

(2) Homogénéité. $\forall(x, \lambda) \in \mathcal{V} \times \mathbb{R}$, $\|\lambda x\| = |\lambda|\|x\|$ (théorème de Thalès)

(3) $\forall x, y \in \mathcal{V}$, $|x \cdot y| \leq \|x\|\|y\|$ (inégalité de Schwarz)

(4) Sous-additivité. $\forall x, y \in \mathcal{V}$, $\|x + y\| \leq \|x\| + \|y\|$ (inégalité triangulaire)

preuve. (1) et (2) sont élémentaires. Pour (3), on écrit que

$$\forall \lambda \in \mathbb{R}, \quad \|x + \lambda y\|^2 = \|x\|^2 + \lambda^2\|y\|^2 + 2\lambda(x \cdot y) \geq 0$$

donc $\Delta' = (x \cdot y)^2 - \|x\|^2\|y\|^2 \leq 0$, d'où le résultat.

(4) s'en suit immédiatement puisque $\|x + y\|^2 - (\|x\| + \|y\|)^2 = 2(x \cdot y - \|x\|\|y\|) \leq 0$. □

4.1.2. *Orthogonalité.*

Définition 4.3. Deux vecteurs $x, y \in \mathcal{V}$ sont *orthogonaux* lorsque $x \cdot y = 0$, on note alors $x \perp y$.

Théorème 4.2 (Pythagore). $\forall x, y \in \mathcal{V}$, $(\|x + y\|^2 = \|x\|^2 + \|y\|^2 \iff x \perp y)$.

preuve. $\|x + y\|^2 = \|x\|^2 + \|y\|^2 + 2(x \cdot y)$, d'où le résultat. □

Définition 4.4. On dit que $(e_i)_{1 \leq i \leq d} \in \mathcal{V}^d$ est une *base orthonormée* lorsque les e_i sont unitaires et deux à deux orthogonaux.

Proposition 4.3. Si (e_i) est orthonormée, $x = \sum x_i e_i$ et $y = \sum y_i e_i$, alors $x \cdot y = \sum x_i y_i$.

preuve. $x \cdot y = \left(\sum_{i=1}^d x_i e_i \right) \cdot \left(\sum_{i=1}^d y_i e_i \right) = \sum_{i=1}^d x_i y_i \underbrace{(e_i \cdot e_i)}_{=\|e_i\|^2=1} + \sum_{\substack{(i,j) \in \llbracket 1, n \rrbracket^2 \\ i \neq j}} x_i y_j \underbrace{(e_i \cdot e_j)}_{=0 \text{ (} i \neq j)} = \sum_{i=1}^d x_i y_i$ □

Corollaire 4.4. Si (e_i) est orthonormée et $x = \sum x_i e_i$, alors $\|x\| = \sqrt{\sum x_i^2}$ et $x_i = x \cdot e_i$.

4.1.3. *Angle géométrique.*

Définition 4.5. $\forall x, y \in \mathcal{V} \setminus \{\vec{0}\}, \exists! \theta \in [0, \pi]$, $\cos \theta = \frac{x \cdot y}{\|x\|\|y\|}$: c'est l'*angle géométrique* $(\widehat{x, y})$.

preuve. En effet, d'après l'inégalité de Schwarz, $\frac{|x \cdot y|}{\|x\|\|y\|} \leq 1$. □

Théorème 4.5 (Al-Kashi). $\forall x, y \in \mathcal{V} \setminus \{\vec{0}\}$, $\|x - y\|^2 = \|x\|^2 + \|y\|^2 - 2\|x\|\|y\| \cos(\widehat{x, y})$

preuve. $\|x - y\|^2 = \|x\|^2 + \|y\|^2 - 2(x \cdot y) = \|x\|^2 + \|y\|^2 - 2\|x\|\|y\| \cos(\widehat{x, y})$. □

Remarque. En termes affines, si $A, B, C \in \mathcal{E}$ sont distincts, alors avec $x = \overrightarrow{AC}$ $y = \overrightarrow{AB}$ on obtient (notations usuelles) $a^2 = b^2 + c^2 - 2bc \cos \widehat{A}$. Pythagore est d'ailleurs un cas particulier d'Al-Kashi.

4.2. Barycentres. On considère des *points pondérés* $(A_i, \alpha_i) \in \mathcal{E} \times \mathbb{R}$, et un *système* de points pondérés $S = \{(A_i, \alpha_i), 1 \leq i \leq n\}$. Le *poids total* de S est le réel $\alpha = \sum_{i=1}^n \alpha_i$.

4.2.1. *Fonction vectorielle de Leibniz.*

Définition 4.6. On appelle *fonction vectorielle de Leibniz* associée à S l'application

$$F : \mathcal{E} \longrightarrow \mathcal{V} \quad M \longmapsto \sum \alpha_i \overrightarrow{MA_i}$$

Lemme 4.6. $\forall (M, N) \in \mathcal{E}^2, F(M) - F(N) = \alpha \overrightarrow{MN}$.

preuve. En effet, $F(M) - F(N) = \sum \alpha_i (\overrightarrow{MA_i} - \overrightarrow{NA_i}) = \sum \alpha_i \overrightarrow{MN} = (\sum \alpha_i) \overrightarrow{MN}$. \square

Corollaire 4.7. Si $\alpha \neq 0$, alors F est bijective, sinon F est constante.

preuve. Supposons $\alpha \neq 0$, et fixons $O \in \mathcal{E}$. Alors $\forall (M, u) \in \mathcal{E} \times \mathcal{V}$ on a :

$$F(M) = u \iff F(O) + \alpha \overrightarrow{MO} = u \iff \overrightarrow{OM} = \frac{1}{\alpha} (F(O) - u)$$

Ainsi, l'équation $F(M) = u$, d'inconnue M et de paramètre u , a une unique solution : F est bijective. Si $\alpha = 0$, alors $\forall (M, N) \in \mathcal{E}^2, F(M) - F(N) = \vec{0}$, donc F est constante. \square

Définition 4.7. Si $\alpha \neq 0, \vec{0}$ a donc un unique antécédent par F qu'on appelle *barycentre* de S et qu'on note typiquement G . Lorsque les α_i sont tous égaux, on parle d'*isobarycentre*.

Remarque. On en déduit que $\forall M \in \mathcal{E}, F(M) = \alpha \overrightarrow{MG}$. En particulier, si O est l'origine d'un repère cartésien quelconque, la relation $\overrightarrow{OG} = \frac{1}{\alpha} \sum \alpha_i \overrightarrow{OA_i}$ fournit directement les coordonnées de G .

4.2.2. *Fonction scalaire de Leibniz.*

Définition 4.8. On appelle *fonction scalaire de Leibniz* associée à S l'application

$$\psi : \mathcal{E} \longrightarrow \mathbb{R} \quad M \longmapsto \sum \alpha_i MA_i^2.$$

Lemme 4.8. (1) $\forall (M, N) \in \mathcal{E}^2, \psi(M) - \psi(N) = \overrightarrow{MN} \cdot (F(M) + F(N))$.

(2) Si $\alpha \neq 0$, alors $\forall M \in \mathcal{E}, \psi(M) = \psi(G) + \alpha MG^2$.

preuve. (1) $\psi(M) - \psi(N) = \sum \alpha_i (\overrightarrow{MA_i}^2 - \overrightarrow{NA_i}^2) = \sum \alpha_i \overrightarrow{MN} \cdot (\overrightarrow{MA_i} + \overrightarrow{NA_i}) = \overrightarrow{MN} \cdot (\sum \alpha_i \overrightarrow{MA_i} + \sum \alpha_i \overrightarrow{NA_i})$.

(2) Avec $N = G$, on a $F(N) = \vec{0}$ et $F(M) = \alpha \overrightarrow{MG}$, d'où le résultat annoncé. \square

Remarque. Si $n = 2$ et $(\alpha_1, \alpha_2) = (1, \pm 1)$ on retrouve les deux théorèmes de la médiane.

Corollaire 4.9. Le lemme précédent permet de décrire les ensembles¹ $\{\psi = \lambda\}$ pour $\lambda \in \mathbb{R}$:

(1) Si $\alpha \neq 0$, alors $\{\psi = \lambda\}$ est la sphère de centre G et de rayon $\sqrt{\frac{1}{\alpha}(\lambda - \psi(G))}$ lorsque $\frac{1}{\alpha}(\lambda - \psi(G)) \geq 0, \emptyset$ sinon.

(2) Si $\alpha = 0$, alors $\{\psi = \lambda\}$ est un plan orthogonal au vecteur $F(M)$ (qui ne dépend pas de M , puisque $\alpha = 0$).

4.2.3. *Propriétés du barycentre ($\alpha \neq 0$).*

Théorème 4.10. (1) Si $\lambda \neq 0, G$ est le barycentre de $S' = \{(A_i, \lambda \alpha_i), 1 \leq i \leq n\}$.

(2) Si (S', S'') est une partition de S et $\alpha' \alpha'' \neq 0$, alors G est barycentre de $\{(G', \alpha'); (G'', \alpha'')\}$.

preuve. (1) *Homogénéité.* $F' = \lambda F$ avec $\lambda \neq 0$, donc $\forall M \in \mathcal{E}, F'(M) = \vec{0} \iff F(M) = \vec{0}$.

(2) *Associativité.* (S', S'') partitionne S donc $\forall M \in \mathcal{E}$

$$F(M) = \sum_{(A,\beta) \in S} \beta \overrightarrow{MA} = \sum_{(A,\beta) \in S'} \beta \overrightarrow{MA} + \sum_{(A,\beta) \in S''} \beta \overrightarrow{MA} = F'(M) + F''(M)$$

ce qui s'écrit aussi $\alpha' \overrightarrow{MG'} + \alpha'' \overrightarrow{MG''} = F(M)$, cad que S a même fonction vectorielle de Leibniz que $\{(G', \alpha'); (G'', \alpha'')\}$ donc même barycentre ($\alpha = \alpha' + \alpha'' \neq 0$). \square

Définition 4.9. $f : \mathcal{E} \longrightarrow \mathcal{E}$ est une *application affine* s'il existe une application linéaire² $L : \mathcal{V} \longrightarrow \mathcal{V}$ telle que $\forall O, M \in \mathcal{E}, f(M) = f(O) + L(\overrightarrow{OM})$. L est alors unique et s'appelle *partie linéaire* de f .

¹L'ensemble $\{\psi = \lambda\} = \psi^{-1}(\{\lambda\}) = \{M \in \mathcal{E}, \psi(M) = \lambda\}$ est appelé *ligne de niveau* λ de ψ .

²On rappelle que L est linéaire si $\forall (\alpha, \beta) \in \mathbb{R}^2, \forall (u, v) \in \mathcal{V}^2, L(\alpha u + \beta v) = \alpha L(u) + \beta L(v)$.

Théorème 4.11. *L'image d'un barycentre par une application affine est le barycentre des images affectées des mêmes coefficients.*

preuve. Soit $f : \mathcal{E} \longrightarrow \mathcal{E}$ une application affine de partie linéaire $L : \mathcal{V} \longrightarrow \mathcal{V}$. Soit $S' = \{(f(A_i), \alpha_i)\}$. $F'(f(G)) = \sum \alpha_i f(G) \overrightarrow{f(A_i)} = \sum \alpha_i L(\overrightarrow{GA_i}) = L(\sum \alpha_i \overrightarrow{GA_i}) = L(F(G)) = L(\vec{0}) = \vec{0}$. Donc $f(G)$ est le barycentre de S' . \square

4.2.4. *Applications affines usuelles.* On va voir ici que toutes les transformations vues au lycée sont affines, donc stabilisent le barycentre d'une configuration.

Définition 4.10. On appelle *similitude* de rapport $\lambda > 0$ toute application $s : \mathcal{E} \longrightarrow \mathcal{E}$ qui multiplie les distances par λ , soit : $\forall (A, B) \in \mathcal{E}^2, \quad d(s(A), s(B)) = \lambda d(A, B)$.

Théorème 4.12. *Les similitudes sont affines. Ainsi, une isométrie et une homothétie de rapport $\lambda \neq 0$, qui sont respectivement des similitudes de rapport 1 et $|\lambda|$, sont affines.*

preuve. Soit $s : \mathcal{E} \longrightarrow \mathcal{E}$ une similitude de rapport $\lambda > 0$, $O \in \mathcal{E}$ et $S : \mathcal{V} \longrightarrow \mathcal{V} \quad v \longmapsto s(O + v) - s(O)$. Soit $(u, v) \in \mathcal{V}^2$ et les points $A = O + u$, $B = A + v$. En notant $X' = s(X)$ pour tout $X \in \mathcal{E}$, on a

$$\overrightarrow{O'A'} \cdot \overrightarrow{A'B'} = S(u) \cdot S(v) = \frac{1}{2} \left(\left\| \overrightarrow{O'A'} + \overrightarrow{A'B'} \right\|^2 - \left\| \overrightarrow{O'A'} \right\|^2 - \left\| \overrightarrow{A'B'} \right\|^2 \right) = \frac{1}{2} \left(O'B'^2 - O'A'^2 - A'B'^2 \right)$$

Or s est une similitude de rapport $\lambda : \forall (X, Y) \in \mathcal{E}^2, \quad X'Y' = \lambda XY$, donc $S(u) \cdot S(v) = \lambda^2(u \cdot v)$.

On développe alors, $\forall (u, v) \in \mathcal{V}^2$ et $\forall \alpha \in \mathbb{R}$ les carrés scalaires $\|S(u + v) - S(u) - S(v)\|^2$ ainsi que $\|S(\alpha u) - \alpha S(u)\|^2$ pour s'apercevoir qu'ils sont nuls, ce qui prouve que S est linéaire :

$$\begin{aligned} \|S(u + v) - S(u) - S(v)\|^2 &= S(u + v)^2 + S(u)^2 + S(v)^2 - 2[S(u + v)S(u) + S(u + v)S(v) - S(u)S(v)] \\ &= \lambda^2 \{ (u + v)^2 + u^2 + v^2 - 2[(u + v) \cdot u + (u + v) \cdot v - u \cdot v] \} = 0 \end{aligned}$$

$$\|S(\alpha u) - \alpha S(u)\|^2 = S(\alpha u)^2 + \alpha^2 S(u)^2 - 2\alpha S(\alpha u) \cdot S(u) = \lambda^2 \{ (\alpha u)^2 + \alpha^2 u^2 - 2\alpha^2 u^2 \} = 0 \quad \square$$

Proposition 4.13. *La composée de deux applications affines est affine. Ainsi, toute composée d'isométries et d'homothéties conserve le barycentre d'une configuration.*

preuve. Soient f et g affines de parties linéaires F et G . Alors $\forall (A, B) \in \mathcal{E}^2$,

$$g(f(B)) - g(f(A)) = G(f(B) - f(A)) = G(F(B - A))$$

Enfin, $G \circ F$ est évidemment linéaire, d'où le résultat. En effet, $\forall (\alpha, \beta) \in \mathbb{R}^2, \forall (u, v) \in \mathcal{V}^2$,

$$(G \circ F)(\alpha u + \beta v) = G(\alpha F(u) + \beta F(v)) = \alpha(G \circ F)(u) + \beta(G \circ F)(v) \quad \square$$

4.3. Produit vectoriel ($d = 3$).

Définition 4.11. $u \wedge v = w$ ssi (u, v, w) est un trièdre direct (notion relative au choix arbitraire d'une base directe de référence) et $\|w\| = \|u\| \|v\| \sin(\widehat{u, v})$. Si u et v sont colinéaires, on pose $u \wedge v = \vec{0}$.

Corollaire 4.14. $\|u \wedge v\|$ mesure l'aire d'un parallélogramme construit sur les vecteurs u et v . On en déduit que l'aire d'un triangle ABC est donnée par $S = \frac{1}{2} \|\overrightarrow{AB} \wedge \overrightarrow{AC}\|$.

Proposition 4.15. *Le produit vectoriel est bilinéaire et antisymétrique (ie. $\forall u, v \in \mathcal{V} \quad v \wedge u = -u \wedge v$). Attention, il n'est ni associatif ni commutatif.*

Corollaire 4.16. *Soit une base orthonormée directe (i, j, k) , et $u(x, y, z)$, $v(x', y', z')$. Alors $u \wedge v$ a pour coordonnées $\left(\begin{array}{c|c|c} y & y' & | & z & z' & | & x & x' \\ z & z' & | & x & x' & | & y & y' \end{array} \right)$.*

preuve. Commençons par remarquer que $i \wedge j = k$ et (permutations circulaires) $j \wedge k = i$, $k \wedge i = j$. A partir de là, il suffit de développer le produit $u \wedge v$ (par bilinéarité antisymétrique) :

$$(xi + yj + zk) \wedge (x'i + y'j + z'k) = (yz' - zy')i + (zx' - xz')j + (xy' - yx')k. \quad \square$$

Proposition 4.17 (Quelques applications). (1) Equation du plan $(A; u, v) : \overrightarrow{AM} \cdot (u \wedge v) = 0$.

(2) Distance du point M à la droite $(A, u) : \frac{\|\overrightarrow{AM} \wedge u\|}{\|u\|}$.

(3) Distance du point M au plan $(A; u, v) : \frac{|\overrightarrow{AM} \cdot (u \wedge v)|}{\|u \wedge v\|}$.

preuve. (1) $u \wedge v \neq 0$ et normal au plan, donc $M \in (A; u, v)$ ssi $\overrightarrow{AM} \perp (u \wedge v)$.

(2) Si H est le projeté orthogonal de M sur (A, u) , alors $\overrightarrow{AM} \wedge u = (\overrightarrow{AH} + \overrightarrow{HM}) \wedge u = \overrightarrow{AH} \wedge u + \overrightarrow{HM} \wedge u$. Le premier terme est nul et le deuxième a pour norme $d\|u\|$.

(3) $n = \frac{u \wedge v}{\|u \wedge v\|}$ est unitaire et normal au plan, d'où le résultat. \square

5. ARITHMÉTIQUE

5.1. Divisibilité.

Définition 5.1. Soit $(a, b) \in \mathbb{Z}^2$. On dit que a *divise* b ou que b est *multiple* de a , et on note $a \mid b$, s'il existe $\lambda \in \mathbb{Z}$ tel que $b = \lambda a$.

Notation. On note $\mathcal{D}(a)$ l'ensemble des diviseurs de a et $\mathcal{D}(a_1, \dots, a_n) = \bigcap_{i=1}^n \mathcal{D}(a_i)$ l'ensemble des diviseurs communs des $(a_i)_{1 \leq i \leq n}$. On note aussi $a\mathbb{Z} = \{\lambda a, \lambda \in \mathbb{Z}\}$ l'ensemble des multiples de a , et $\mathcal{M}(a_1, \dots, a_n) = \bigcap_{i=1}^n a_i\mathbb{Z}$ l'ensemble des multiples communs des (a_i) .

Remarque. $\mathcal{D}(a) \neq \emptyset$, car il contient $\{-a, -1, 1, a\}$; $\mathcal{D}(a_1, \dots, a_n) \neq \emptyset$ car il contient $\{-1, 1\}$.

Proposition 5.1. (1) $\forall (a, d) \in (\mathbb{Z}^*)^2, \quad d \mid a \implies |d| \leq |a|$

(2) $\forall (a, b) \in \mathbb{Z}^2, \quad (a \mid b \text{ et } b \mid a) \implies |a| = |b|$

(3) $\forall (a, b, c) \in \mathbb{Z}^3, \quad (a \mid b \text{ et } b \mid c) \implies a \mid c$

Proposition 5.2. (1) $\forall (a, b, c) \in \mathbb{Z}^3, \quad a \mid b \implies a \mid bc$

(2) $\forall (a, b, c) \in \mathbb{Z}^3, \quad (a \mid b \text{ et } a \mid c) \implies a \mid b + c$

(3) $\forall (a, b, \alpha, \beta) \in \mathbb{Z}^4, \quad (a \mid b \text{ et } \alpha \mid \beta) \implies a\alpha \mid b\beta$

(4) $\forall (a, b, n) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}^*, \quad a \mid b \implies a^n \mid b^n$

Définition 5.2. Soit $n \in \mathbb{N}^*$ et $(a, b) \in \mathbb{Z}^2$; on dit que a est *congru à b modulo n* , et on note $a \equiv b [n]$ si $n \mid a - b$, cad si a et b sont égaux à un multiple de n près.

Proposition 5.3. $\equiv [n]$ est une relation d'équivalence sur \mathbb{Z} , cad qu'elle est

- réflexive : $\forall a \in \mathbb{Z}, \quad a \equiv a [n]$

- symétrique : $\forall (a, b) \in \mathbb{Z}^2, \quad a \equiv b [n] \implies b \equiv a [n]$

- transitive : $\forall (a, b, c) \in \mathbb{Z}^3, \quad (a \equiv b [n] \text{ et } b \equiv c [n]) \implies a \equiv c [n]$

Proposition 5.4. Si $a \equiv b [n]$ et $c \equiv d [n]$, alors $a + c \equiv b + d [n]$ et $ac \equiv bd [n]$.

Corollaire 5.5. $\forall (a, b) \in \mathbb{Z}^2, \forall k \in \mathbb{N}^*, \quad a \equiv b [n] \implies a^k \equiv b^k [n]$.

Théorème 5.6 (Division euclidienne). $\forall (a, b) \in \mathbb{Z} \times \mathbb{N}^*, \exists!(q, r) \in \mathbb{Z} \times \llbracket 0, b \llbracket, \quad a = bq + r$. Les entiers a, b, q et r s'appellent *dividende*, *diviseur*, *quotient* et *reste* de la division euclidienne de a par b .

preuve. Existence. Soit $X = \{q \in \mathbb{Z}, bq \leq a\}$. C'est une partie non vide ($-|a| \in X$) majorée (par $|a|$) de \mathbb{Z} , donc elle admet un plus grand élément q . Soit $r = a - bq \geq 0$; si $r \geq b$, alors $q + 1 \in X$: contradiction avec la définition de q ; donc $r < b$.

Unicité. Si (q', r') est une autre solution, alors $b \mid r - r'$ avec $|r - r'| < b$, donc $r - r' = 0$. On en déduit $q = q'$, comme $b \neq 0$. \square

Définition 5.3. On dit que $\emptyset \subsetneq A \subset \mathbb{Z}$ est un *sous-groupe* de \mathbb{Z} , et on note $A \leq \mathbb{Z}$ lorsqu'il est «stable par soustraction» : $\forall (a, b) \in A^2, \quad a - b \in A$.

Proposition 5.7. Si $A \leq \mathbb{Z}$, alors $\exists! d \in \mathbb{N}, \quad A = d\mathbb{Z}$.

preuve. Si $A = \{0\}$, $d = 0$. Sinon, $A \cap \mathbb{N}^*$ est une partie non vide de \mathbb{N}^* , soit $d > 0$ son plus petit élément. $d \in A$ et $A \leq \mathbb{Z}$, donc $d\mathbb{Z} \subset A$ (laissé en exercice³).

Pour l'inclusion réciproque, soit $a \in A, (q, r) \in \mathbb{Z} \times \llbracket 0, d \llbracket, \quad a = dq + r$: on veut montrer que $r = 0$. Remarquons que $r = a - dq \in A$ (car $A \leq \mathbb{Z}$ et $a, d \in A$). Or $r \in \llbracket 0, d \llbracket$, donc par définition de d , $r = 0$. L'unicité est triviale, car si $d\mathbb{Z} = d'\mathbb{Z}$, alors $d \mid d'$ et $d' \mid d$, d'où $|d| = |d'|$. \square

³Indication : vérifier que $A \leq \mathbb{Z} \iff \{0 \in A; \forall a \in A, -a \in A \text{ et } \forall (a, b) \in A^2, a + b \in A\}$.

5.2. **pgcd, ppcm.** Soient $n \geq 1$, $(a_i)_{1 \leq i \leq n} \in (\mathbb{Z}^*)^n$.

Définition 5.4. – $\mathcal{D}(a_1, \dots, a_n)$ est fini et non vide. Il admet donc un plus grand élément, appelé *plus grand diviseur commun* des (a_i) est noté $\text{pgcd}(a_1, \dots, a_n)$.
– $\mathcal{M}(a_1, \dots, a_n) \cap \mathbb{N}^*$ est une partie non vide de \mathbb{N}^* dont le plus petit élément, appelé *plus petit multiple commun* des (a_i) est noté $\text{ppcm}(a_1, \dots, a_n)$.

preuve. – $\{-1, 1\} \subset \mathcal{D}(a_1, \dots, a_n) = \bigcap_{i=1}^n \mathcal{D}(a_i) \subset \mathcal{D}(a_1) \subset \llbracket -|a_1|, +|a_1| \rrbracket$.

– Remarquer que $\llbracket \prod a_i \rrbracket \in \mathcal{M}(a_1, \dots, a_n) \cap \mathbb{N}^*$. □

Notation. Pour $(a, b) \in \mathbb{Z}^2$, on note souvent $a \wedge b = \text{pgcd}(a, b)$ et $a \vee b = \text{ppcm}(a, b)$. Enfin, on définit

$$\sum a_i \mathbb{Z} = a_1 \mathbb{Z} + \dots + a_n \mathbb{Z} = \{\lambda_1 a_1 + \dots + \lambda_n a_n, (\lambda_1, \dots, \lambda_n) \in \mathbb{Z}^n\}$$

Théorème 5.8. Si $\delta = \text{pgcd}(a_1, \dots, a_n)$ et $\mu = \text{ppcm}(a_1, \dots, a_n)$, alors $\sum a_i \mathbb{Z} = \delta \mathbb{Z}$ et $\bigcap a_i \mathbb{Z} = \mu \mathbb{Z}$. En d'autres termes, les «combinaisons linéaires» à coefficients entiers sont les multiples du pgcd, et les multiples communs sont les multiples du ppcm.

preuve. $\sum a_i \mathbb{Z} \leq \mathbb{Z}$, donc $\exists d \in \mathbb{N}$, $\sum a_i \mathbb{Z} = d \mathbb{Z}$. On a déjà, $\forall i$, $a_i \in \sum a_i \mathbb{Z} = d \mathbb{Z}$, cad $d \mid a_i$ donc $d \leq \delta$. Par ailleurs, $d \mathbb{Z} = \sum a_i \mathbb{Z} \subset \delta \mathbb{Z}$, puisque δ divise les a_i . Donc $\delta \mid d$, en particulier, $\delta \leq d$.

$\bigcap a_i \mathbb{Z} \leq \mathbb{Z}$, donc il existe $m \geq 0$ tel que $\bigcap a_i \mathbb{Z} = m \mathbb{Z}$. Or $\mu \in \bigcap a_i \mathbb{Z}$, donc $m \mid \mu$. En particulier, $m \leq \mu$, donc $m = \mu$ ($m, \mu \in \bigcap a_i \mathbb{Z}$ dont μ est le plus petit élément). □

Proposition 5.9. $\forall \lambda \in \mathbb{Z}$, $\text{pgcd}(\lambda a_i)_{1 \leq i \leq n} = |\lambda| \text{pgcd}(a_i)_{1 \leq i \leq n}$ et $\text{ppcm}(\lambda a_i)_{1 \leq i \leq n} = |\lambda| \text{ppcm}(a_i)_{1 \leq i \leq n}$.

preuve. $\sum \lambda a_i \mathbb{Z} = \lambda(\sum a_i \mathbb{Z})$, cad (théorème 5.8) $\text{pgcd}(\lambda a_1, \dots, \lambda a_n) \mathbb{Z} = \lambda \text{pgcd}(a_1, \dots, a_n) \mathbb{Z}$. Enfin, remarquez que $\forall (\alpha, \beta) \in \mathbb{Z}$, $\alpha \mathbb{Z} = \beta \mathbb{Z} \iff (\alpha \in \beta \mathbb{Z} \text{ et } \beta \in \alpha \mathbb{Z}) \iff (\alpha \mid \beta \text{ et } \beta \mid \alpha) \iff |\alpha| = |\beta|$.

$\bigcap \lambda a_i \mathbb{Z} = \lambda(\bigcap a_i \mathbb{Z})$ cad (théorème 5.8) $\text{ppcm}(\lambda a_1, \dots, \lambda a_n) \mathbb{Z} = \lambda \text{ppcm}(a_1, \dots, a_n) \mathbb{Z}$. □

Proposition 5.10. Soient $\delta = \text{pgcd}(a_i)_{1 \leq i \leq n}$ et $\mu = \text{ppcm}(a_i)_{1 \leq i \leq n}$ et $x \in \mathbb{Z}$

$$(\forall i, x \mid a_i) \iff x \mid \delta \quad \text{et} \quad (\forall i, a_i \mid x) \iff \mu \mid x$$

preuve. $x \mid \delta \iff \delta \mathbb{Z} = \sum a_i \mathbb{Z} \subset x \mathbb{Z} \iff x \in \mathcal{D}(a_1, \dots, a_n)$

$(\forall i, a_i \mid x) \iff x \in \bigcap a_i \mathbb{Z} = \mu \mathbb{Z} \iff \mu \mid x$ □

Théorème 5.11 (Algorithme d'Euclide). Soit $(a, b) \in \mathbb{Z}^2$ tel que $1 \leq b \leq a$. Le pgcd de a et b est, dans les divisions euclidiennes successives, le dernier reste non nul :

$$\left\{ \begin{array}{l} a = bq_1 + r_1 \\ 0 < r_1 < b \end{array} \right\}, \left\{ \begin{array}{l} b = r_1q_2 + r_2 \\ 0 < r_2 < r_1 \end{array} \right\}, \dots, \left\{ \begin{array}{l} r_{n-2} = r_{n-1}q_n + r_n \\ 0 < r_n < r_{n-1} \end{array} \right\}, \quad \begin{array}{l} r_n \mid r_{n-1} \\ a \wedge b = r_n \end{array}$$

preuve. (r_k) est une suite strictement décroissante d'entiers naturels tant qu'elle ne s'annule pas, donc il existe un unique entier n tel que $r_k > 0$ si $k \leq n$ et $r_k = 0$ si $k > n$.

De manière générale, si $(a, b, q, r) \in \mathbb{Z}^4$ vérifie $a = bq + r$, alors $\mathcal{D}(a, b) = \mathcal{D}(b, r)$ (double inclusion triviale) donc $a \wedge b = b \wedge r$. Ainsi $a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \dots = r_{n-1} \wedge r_n = r_n$. □

5.3. **Nombres premiers entre eux.** Soient $n \geq 1$, $(a_1, \dots, a_n) \in \mathbb{Z}^n$.

Définition 5.5. Les (a_i) sont *premiers entre eux dans leur ensemble* si $\text{pgcd}(a_1, \dots, a_n) = 1$.

Remarque. A ne pas confondre avec *deux à deux premiers entre eux* qui signifie que

$$\forall (i, j) \in \llbracket 1, n \rrbracket^2, \quad i \neq j \implies a_i \wedge a_j = 1$$

Proposition 5.12. $\forall (a, b, c) \in \mathbb{Z}^3$, $(a \wedge b = 1 \text{ et } c \mid b) \implies a \wedge c = 1$

preuve. Si $c \mid b$, alors $\mathcal{D}(c) \subset \mathcal{D}(b)$, donc $\mathcal{D}(a, c) \subset \mathcal{D}(a, b) = \mathcal{D}(1) = \{-1, 1\}$. □

Théorème 5.13 (Bezout). $\text{pgcd}(a_1, \dots, a_n) = 1 \iff \exists (u_1, \dots, u_n) \in \mathbb{Z}^n$, $\sum u_i a_i = 1$

preuve. $\text{pgcd}(a_1, \dots, a_n) = 1 \iff \sum a_i \mathbb{Z} = \mathbb{Z} \iff 1 \in \sum a_i \mathbb{Z}$ □

Théorème 5.14 (Gauss). $\forall (a, b, c) \in \mathbb{Z}^3$, $(a \mid bc \text{ et } a \wedge b = 1) \implies a \mid c$

preuve. $a \mid bc$, donc $\exists \lambda \in \mathbb{Z}$, $\lambda a = bc$ et $a \wedge b = 1$, donc (Bezout) $\exists (u, v) \in \mathbb{Z}^2$, $au + bv = 1$. On en déduit $a \lambda v = bvc$, puis avec $bv = 1 - au$, $a \lambda v = (1 - au)c$, d'où $c = a(\lambda v + cu)$ et $a \mid c$. □

Proposition 5.15. *L'équation diophantienne $au + bv = 1$ d'inconnue $(u, v) \in \mathbb{Z}^2$ et de paramètre $(a, b) \in (\mathbb{Z}^*)^2$ admet des solutions ssi $a \wedge b = 1$ (puisque $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$). Dans ce cas, si on note (u_0, v_0) un solution particulière, la solution générale est donnée par :*

$$u = u_0 + b\lambda, \quad v = v_0 - a\lambda, \quad \text{pour } \lambda \in \mathbb{Z}$$

preuve. Soit $(u, v) \in \mathbb{Z}^2$, $au + bv = 1$. En soustrayant $au_0 + bv_0 = 1$ on trouve $(*) : a(u - u_0) = b(v_0 - v)$. Ainsi, $a \mid b(v_0 - v)$. Or $a \wedge b = 1$, donc (théorème de Gauss) $a \mid v_0 - v$, cad qu' $\exists \lambda \in \mathbb{Z}$, $v_0 - v = \lambda a$. En remplaçant dans $(*)$, on en déduit que $u - u_0 = b\lambda$, d'où la condition nécessaire. Pour la condition suffisante, on vérifie que $\forall \lambda \in \mathbb{Z}$, $(u_0 + b\lambda, v_0 - a\lambda)$ est solution. \square

Remarque. Concrètement, pour trouver une solution particulière (u_0, v_0) , on peut appliquer l'algorithme d'Euclide à (a, b) et procéder par substitution ou combinaison des équations : faites le sur un exemple !

Corollaire 5.16. *Soit $(a, b) \in \mathbb{Z}^2$ tel que $a \wedge b = 1$. Il existe $(u, v) \in \mathbb{Z}^2$ tel que*

$$au + bv = 1 \quad \text{avec} \quad |u| \leq |b| \quad \text{et} \quad |v| \leq |a|$$

Proposition 5.17. *Soit $x \in \mathbb{Z}$. On a $(\forall i, x \wedge a_i = 1) \iff x \wedge \prod a_i = 1$*

preuve. Si $x \wedge \prod a_i = 1$, alors $\exists (u, v) \in \mathbb{Z}^2$, $ux + v \prod a_i = 1$, donc $\forall i, x \wedge a_i = 1$. Réciproquement, si $\forall i, x \wedge a_i = 1$, alors $\forall i, \exists (u_i, v_i) \in \mathbb{Z}^2$, $u_i x + v_i a_i = 1$. En multipliant ces n lignes, on obtient une égalité de Bezout en $(x, \prod a_i)$. \square

Corollaire 5.18. $\forall (a, b) \in \mathbb{Z}^2, \forall (k, l) \in (\mathbb{N}^*)^2, \quad a \wedge b = 1 \iff a^k \wedge b^l = 1$

Corollaire 5.19. $\forall (a, b) \in \mathbb{Z}^2, \forall k \in \mathbb{N}^*, \quad a^k \wedge b^k = (a \wedge b)^k$

preuve. Soit $\delta = a \wedge b$, de sorte que $a = \delta\alpha$, $b = \delta\beta$ avec $\alpha \wedge \beta = 1$. Alors $a^k \wedge b^k = (\delta^k \alpha^k \wedge \delta^k \beta^k) = \delta^k (\alpha^k \wedge \beta^k)$. On conclut avec le résultat précédent, qui dit que $\alpha^k \wedge \beta^k = 1$. \square

Proposition 5.20. *Si les a_i sont 2 à 2 premiers entre eux et divisent $x \in \mathbb{Z}$, alors $\prod a_i \mid x$.*

preuve. Supposons $n = 2$: soient $p \neq q$ deux diviseurs de x premiers entre eux. Ainsi existe-il $(\alpha, \beta) \in \mathbb{Z}^2$ tel que $x = \alpha p = \beta q$. De $p \mid \beta q$ et $p \wedge q = 1$, on déduit (théorème de Gauss) $p \mid \beta$; d'où $pq \mid x$. On en déduit le résultat pour n quelconque, par une récurrence élémentaire. \square

Corollaire 5.21. *Si les (a_i) sont 2 à 2 premiers entre eux, alors $\text{ppcm}(a_1, \dots, a_n) = \prod_{i=1}^n a_i$.*

Corollaire 5.22. $\forall (a, b) \in \mathbb{Z}^2, (a \wedge b)(a \vee b) = |ab|$

preuve. Posons $\delta = a \wedge b$, $\mu = a \vee b$, $a = \delta a'$, $b = \delta b'$ de sorte que $a' \wedge b' = 1$, donc $a' \vee b' = |a'b'|$. On a alors $\delta\mu = \delta^2(a' \wedge b')(a' \vee b') = \delta^2|a'b'| = |\delta a'| |\delta b'| = |a||b|$. \square

Définition 5.6. On appelle *représentant irréductible* d'un rationnel $r \neq 0$ tout couple $(\alpha, \beta) \in (\mathbb{Z}^*)^2$ tel que $r = \frac{\alpha}{\beta}$ et $\alpha \wedge \beta = 1$.

Proposition 5.23. *Tout rationnel non nul admet au moins un représentant irréductible. Soit $r \in \mathbb{Q}^*$ et (α, β) un représentant irréductible de r ; tout représentant de r est de la forme $(k\alpha, k\beta)$, $k \in \mathbb{Z}^*$. Tout rationnel non nul admet exactement deux représentants irréductibles, (α, β) et $(-\alpha, -\beta)$.*

preuve. Soit $r \in \mathbb{Q}^* : \exists (p, q) \in \mathbb{Z} \times \mathbb{Z}^*, r = p/q$. Posons $\delta = p \wedge q$, de sorte que $p = \delta p'$, $q = \delta q'$ avec $p' \wedge q' = 1$. (p', q') est donc un représentant irréductible de r .

(α, β) représente r , donc $\forall k \in \mathbb{Z}^*$, $(k\alpha, k\beta)$ représente aussi r : c'est trivial. Réciproquement, si $r = \alpha/\beta = p/q$, alors $\alpha q = \beta p$. Ainsi, $\alpha \mid \beta p$ avec $\alpha \wedge \beta = 1$, donc (Gauss) $\alpha \mid p$ et $\exists k \in \mathbb{Z}$, $p = k\alpha$. De même $\exists l \in \mathbb{Z}$, $q = l\beta$. En réinjectant $\frac{\alpha}{\beta} = \frac{k\alpha}{l\beta} = \frac{\alpha k}{\beta l}$, donc (en simplifiant par $\frac{\alpha}{\beta} = r \neq 0$) $1 = \frac{k}{l}$, cad $k = l$. Enfin, un représentant $(k\alpha, k\beta)$ est irréductible ssi $k\alpha \wedge k\beta = |k|(\alpha \wedge \beta) = 1$, cad ssi $|k| = 1$. \square

5.4. Nombres premiers.

Définition 5.7. $p \in \mathbb{N}$ est *premier* si $p \geq 2$ et $\forall a \in \mathbb{N}^*, a \mid p \implies a \in \{1, p\}$.

Proposition 5.24. *Soit p premier et $a \in \mathbb{Z}^*$. On a $p \mid a$ ou $p \wedge a = 1$.*

preuve. En effet, $\delta = p \wedge a$ est un diviseur positif de p , donc $\delta \in \{1, p\}$. \square

Corollaire 5.25. *Si p, q sont deux nombres premiers distincts, alors $p \wedge q = 1$.*

Corollaire 5.26. Soit p premier, $n \geq 1$ et $(x_1, \dots, x_n) \in (\mathbb{Z}^*)^n : p \mid \prod x_i \iff (\exists i \in \llbracket 1, n \rrbracket, p \mid x_i)$.

preuve. Si $\forall i, p \nmid a_i$, cad $p \wedge a_i = 1$, alors $p \wedge \prod a_i = 1$, cad $p \nmid \prod a_i$, réciproque triviale. \square

Théorème 5.27 (décomposition en facteurs premiers). *Tout entier $n \geq 2$ admet une décomposition en produit de nombres premiers, unique à l'ordre près des facteurs.*

preuve. L'existence est triviale, par récurrence forte sur $n \geq 2$.

Unicité. Supposons $n = p_1^{\alpha_1} \dots p_n^{\alpha_n} = q_1^{\beta_1} \dots q_m^{\beta_m}$, où $p_1 < p_2 < \dots < p_n$ sont premiers et $\forall i \in \llbracket 1, n \rrbracket, \alpha_i \geq 1$ (idem pour les (q_j) et (β_j)). $\forall i \in \llbracket 1, n \rrbracket$, alors $p_i \mid n = q_1^{\beta_1} \dots q_m^{\beta_m}$, donc (corollaire 5.26) $\exists j \in \llbracket 1, m \rrbracket, p_i \mid q_j$, cad $p_i = q_j$ (corollaire 5.25). De même $\forall j \in \llbracket 1, m \rrbracket, \exists i \in \llbracket 1, n \rrbracket, q_j = p_i$. Ainsi $n = m$ et $(p_1, \dots, p_n) = (q_1, \dots, q_n)$. Il reste à démontrer que $(\alpha_1, \dots, \alpha_n) = (\beta_1, \dots, \beta_n)$.

Supposons par l'absurde que $(\alpha_1, \dots, \alpha_n) \neq (\beta_1, \dots, \beta_n)$, cad qu' $\exists i \in \llbracket 1, n \rrbracket, \alpha_i \neq \beta_i$. On a donc $p_i^{\alpha_i} \prod_{j \neq i} p_j^{\alpha_j} = p_i^{\beta_i} \prod_{j \neq i} p_j^{\beta_j}$. Si $\beta_i < \alpha_i$, alors $p_i^{\alpha_i - \beta_i} \prod_{j \neq i} p_j^{\alpha_j} = \prod_{j \neq i} p_j^{\beta_j}$, donc (corollaire 5.26) $\exists j \neq i, p_i \mid p_j$ cad cad $p_i = p_j$: contradiction avec (p_1, \dots, p_n) 2 à 2 distincts. Idem quand $\beta_i > \alpha_i \dots$ \square

Théorème 5.28. *L'ensemble \mathcal{P} des nombres premiers est infini.*

preuve. A supposer \mathcal{P} fini, soit N son plus grand élément, $M = N! + 1$ et p un diviseur premier de M . Comme $p \leq N, p \mid N!$, donc $p \mid (M - N!) = 1$: absurde. \square

Proposition 5.29. Soient $a, b \geq 2, a = \prod p_i^{\alpha_i}, b = \prod p_i^{\beta_i}$, où les p_i sont premiers distincts, les α_i et les β_i sont des entiers naturels. Alors $a \wedge b = \prod p_i^{\min(\alpha_i, \beta_i)}$ et $a \vee b = \prod p_i^{\max(\alpha_i, \beta_i)}$.

preuve. pgcd. On suppose sans restriction que $(p_i)_{1 \leq i \leq n}$ est strictement croissant et que les $(\alpha_i)_{1 \leq i \leq n}$ et les $(\beta_i)_{1 \leq i \leq n}$ ne sont pas tous nuls. Par le théorème de décomposition, $\delta = a \wedge b = q_1^{\gamma_1} \dots q_m^{\gamma_m}$ où $(q_j)_{1 \leq j \leq m}$ est strictement croissant et les γ_j sont ≥ 1 . D'abord, $\forall j \in \llbracket 1, m \rrbracket, q_j \mid \delta$ (puisque $\gamma_j \geq 1$), donc $q_j \mid a$ et $q_j \mid b$. Ainsi – les $(\alpha_i)_{1 \leq i \leq n}$ et $(\beta_i)_{1 \leq i \leq n}$ n'étant pas tous nuls – comme q_j est premier, $\exists i \in \llbracket 1, n \rrbracket, q_j \mid p_i$ (corollaire 5.26) cad $q_j = p_i$. On peut donc écrire $\delta = p_1^{\delta_1} \dots p_n^{\delta_n}$ avec $(\delta_i)_{1 \leq i \leq n} \in \mathbb{N}^n$. Soit $i \in \llbracket 1, n \rrbracket$. Partant de $\delta = p_i^{\delta_i} \prod_{j \neq i} p_j^{\delta_j} \mid a = p_i^{\alpha_i} \prod_{j \neq i} p_j^{\alpha_j}$, on a $p_i^{\delta_i} \mid p_i^{\alpha_i} \prod_{j \neq i} p_j^{\alpha_j}$. Or $p_i^{\delta_i} \wedge \prod_{j \neq i} p_j^{\alpha_j} = 1$, donc (théorème de Gauss) $p_i^{\delta_i} \mid p_i^{\alpha_i}$, d'où $\delta_i \leq \alpha_i$. De même $\delta_i \leq \beta_i$. Enfin, si $\delta_i < \min(\alpha_i, \beta_i)$, alors $\delta p_i > \delta$ divise toujours a et b : impossible par maximalité de δ ; donc $\delta_i = \min(\alpha_i, \beta_i)$.

ppcm. Soit $\mu = a \vee b$ et $(\mu_i) = \max(\alpha_i, \beta_i)$. a et b divisent μ , donc $\forall i \in \llbracket 1, n \rrbracket, p_i^{\alpha_i}$ et $p_i^{\beta_i}$ divisent δ , cad $p_i^{\mu_i} \mid \mu$. Les $(p_i^{\mu_i})$ étant 2 à 2 premiers entre eux, $\prod p_i^{\mu_i} \mid \mu$, cad qu' $\exists \lambda \geq 1, \mu = \lambda \prod p_i^{\mu_i}$. Or $\forall k \geq 1, k \prod p_i^{\mu_i} \in a\mathbb{Z} \cap b\mathbb{Z}$, donc par minimalité de $\mu, \lambda = 1$. \square

Corollaire 5.30. *Les lois \wedge et \vee sont distributives l'une sur l'autre dans \mathbb{Z}^* .*

6. LIMITES ET CONTINUITÉ

6.1. Limites.

6.1.1. Éléments de topologie.

Définition 6.1. On appelle *droite numérique achevée* l'ensemble $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$. On y prolonge la relation d'ordre \leq par $\forall x \in \overline{\mathbb{R}}, -\infty \leq x \leq +\infty$. On prolonge aussi les opérations, sauf dans les fameux cas de «formes indéterminées».

Remarque. Ce prolongement des opérations ne se substitue pas aux démonstrations des résultats de type «limites et opérations» vu en première. Il permet juste de les énoncer de façon concise.

Définition 6.2. On appelle *voisinage* de $a \in \overline{\mathbb{R}}$ toute partie de \mathbb{R} contenant un intervalle du type :

- $[a - \varepsilon; a + \varepsilon]$ si $a \in \mathbb{R}$ (pour un certain $\varepsilon > 0$),
- $] - \infty; A[$ (resp. $]A; +\infty[$) si $a = -\infty$ (resp. $+\infty$) (pour un certain $A \in \mathbb{R}$).

L'ensemble des voisinages de a se note $\mathcal{V}(a)$. On dira, par exemple, que « $f \geq g$ au voisinage de $+\infty$ » s'il existe un voisinage $V \in \mathcal{V}(+\infty)$ tel que $\forall x \in V, f(x) \geq g(x)$. Autrement dit, « $f \geq g$ au voisinage de $+\infty$ » s'il existe $A \in \mathbb{R}$ tel que $\forall x \geq A, f(x) \geq g(x)$. De même, $f \geq g$ au voisinage d'un $x_0 \in \mathbb{R}$ s'il existe $\varepsilon > 0$ tel que $\forall x \in [x_0 - \varepsilon, x_0 + \varepsilon], f(x) \geq g(x)$, etc. . .

Définition 6.3. Soit $X \subset \mathbb{R}$ et $a \in \overline{\mathbb{R}}$. On dit que a est *adhérent* à X si tout voisinage de a rencontre X . On note appelle *adhérence* de X l'ensemble \overline{X} des points adhérents à X .

Remarque. Intuitivement, \overline{X} est l'ensemble des points vers lesquels on peut *tendre* en restant dans X . En pratique, on retiendra que l'adhérence d'un intervalle de \mathbb{R} est obtenue en fermant ses bornes (y compris d'éventuelles bornes infinies).

Lemme 6.1 (de séparation). *Deux éléments distincts de $\overline{\mathbb{R}}$ ont des voisinages disjoints, cad*

$$\forall a, b \in \overline{\mathbb{R}}, \quad a \neq b \implies \exists (U, V) \in \mathcal{V}(a) \times \mathcal{V}(b), \quad U \cap V = \emptyset$$

6.1.2. *Définition.*

Définition 6.4. Soit $A \subset \mathbb{R}$, $b \in \overline{\mathbb{R}}$ et $a \in \overline{\mathcal{D}_f \cap A}$. Par définition,

$$\lim_{\substack{x \rightarrow a \\ x \in A}} f(x) = b \iff \forall V \in \mathcal{V}(b), \exists U \in \mathcal{V}(a), f(U \cap A) \subset V$$

Remarque. – Par défaut, $A = \mathcal{D}_f$ ou \mathbb{R} – ce qui revient au même. Si $a \in \mathbb{R}$ et $A =]a; +\infty[$ (resp. $] - \infty; a[$), on parle de *limite à droite* (resp. *gauche*) que l'on note $\lim_{a+} f$ (resp. $\lim_{a-} f$).

– Si $\mathcal{D}_f = \mathbb{N}$ on définit ainsi la *limite d'une suite*. Remarquons déjà que $\overline{\mathbb{N}} = \mathbb{N} \cup \{+\infty\}$ et que $\forall n \in \mathbb{N}, \lim_{x \rightarrow n} f(x) = f(n)$ (sans intérêt) : on ne s'intéresse donc qu'à $\lim_{+\infty} f$.

Proposition 6.2. *Une limite, si elle existe, est unique.*

preuve. Supposons $\lim_{a,A} f = l$, $\lim_{a,A} f = l'$ et $l \neq l'$; soient $U \in \mathcal{V}(l)$, $V \in \mathcal{V}(l')$ disjoints. Alors $\exists X, Y \in \mathcal{V}(a)$, $f(X \cap A) \subset U$ et $f(Y \cap A) \subset V$. Donc $f((X \cap Y) \cap A) \subset U \cap V = \emptyset$. Cela dit, $X \cap Y \in \mathcal{V}(a)$ et $a \in \overline{\mathcal{D}_f \cap A}$ donc $(X \cap Y) \cap (\mathcal{D}_f \cap A) \neq \emptyset$: contradiction. \square

Remarque. Les opérations sur les limites sont supposés connus, mais le lecteur est invité à démontrer quelque uns de ces résultats, pour apprendre concrètement à manipuler les epsilons et les voisinages.

6.1.3. *Résultats usuels sur les limites.*

Théorème 6.3 (limite d'une composée). *Soient $(a, b) \in \overline{\mathcal{D}_f} \times \overline{\mathcal{D}_g}$ et $c \in \overline{\mathbb{R}}$. Si $\lim_a f = b$ et $\lim_b g = c$, alors $\lim_a (g \circ f) = c$.*

preuve. Soit $W \in \mathcal{V}(c)$. $\lim_b g = c$, donc il existe $V \in \mathcal{V}(b)$ tel que $g(V) \subset W$. De même $\lim_a f = b$ nous donne $U \in \mathcal{V}(a)$ tel que $f(U) \subset V$. On a bien trouvé $U \in \mathcal{V}(a)$ tel que $g \circ f(U) \subset W$. \square

Corollaire 6.4. *Soient $a \in \overline{\mathcal{D}_f}$ et $b \in \overline{\mathbb{R}}$. Si $\lim u_n = a$ et $\lim_a f = b$ alors $\lim f(u_n) = b$.*

Proposition 6.5. *Soit $a \in \overline{\mathcal{D}_f \cap \mathcal{D}_g}$. Si $f \leq g$ au voisinage de a et que $\lim_a f$ et $\lim_a g$ existent, alors $\lim_a f \leq \lim_a g$.*

preuve. Par l'absurde, en remarquant que si $a, b \in \overline{\mathbb{R}}$ vérifient $a < b$, alors il existe un voisinage U de a et un voisinage V de b tels que $\forall (x, y) \in U \times V, x < y$. \square

Théorème 6.6 (convergence monotone). *Soit f croissante au voisinage de $+\infty$:*

- (1) *si f est majorée, f a une limite finie en $+\infty$,*
- (2) *sinon f tend vers $+\infty$ en $+\infty$.*

preuve. (1) Soit $V \in \mathcal{V}(+\infty)$ tel que f est croissante majorée sur V et $s = \sup f(V)$, de sorte que $\forall \varepsilon > 0, \exists x_0 \in V, f(x_0) \in [s - \varepsilon, s]$. f est croissante sur $V \cap [x_0, +\infty[$, donc $f(V \cap [x_0, +\infty[) \subset [s - \varepsilon, s]$. Ceci étant pour tout $\varepsilon > 0$, $\lim_{+\infty} f = s$.

(2) $\forall A \in \mathbb{R}$, f n'est pas majorée par A , donc $\exists x_0, f(x_0) \geq A$. Par croissance, on a $\forall x \geq x_0, f(x) \geq f(x_0) \geq A$. Ainsi $\forall A \in \mathbb{R}, \exists x_0, \forall x \geq x_0, f(x) \geq A$, soit $\lim_{+\infty} f = +\infty$. \square

Remarque. De même une fonction décroissante minorée au voisinage de $+\infty$ a une limite finie. On laisse au lecteur le soin d'énoncer (et de démontrer, ou plutôt déduire) les résultats correspondants en $-\infty$ et même en a^+, a^- pour $a \in \mathbb{R}$. Idem pour les suites (en $+\infty$).

Théorème 6.7 (d'encadrement). *Si $u \leq f \leq v$ au voisinage de ∞ et que u et v ont une même limite finie ℓ en $+\infty$, alors $\lim_{+\infty} f = \ell$.*

preuve. Soit $\varepsilon > 0$ et $(A, B) \in \mathbb{R}^2$ tels que $\forall x \geq A, |u(x) - \ell| \leq \varepsilon$ et $\forall x \geq B, |v(x) - \ell| \leq \varepsilon$. On pose alors $M = \max(A, B)$ de sorte que $\forall x \geq M, |u(x) - \ell| \leq \varepsilon$ et $|v(x) - \ell| \leq \varepsilon$. Par l'inégalité triangulaire (vraie sur \mathbb{C} donc sur \mathbb{R}), $|f(x) - \ell| \leq |f(x) - u(x)| + |u(x) - \ell| \leq |v(x) - u(x)| + \varepsilon$. Toujours par l'inégalité triangulaire, $|v(x) - u(x)| \leq |v(x) - \ell| + |\ell - u(x)| \leq 2\varepsilon$, d'où $|f(x) - \ell| \leq 3\varepsilon$. \square

Remarque. Ce résultat s'applique évidemment à des suites, il s'applique aussi en $-\infty$ et même en a^+ ou en a^- pour $a \in \mathbb{R}$ (laissé au lecteur).

6.2. Continuité.

6.2.1. Définition.

Définition 6.5. Dire que f est continue en $a \in \mathcal{D}_f$ signifie que f a une limite en a ; cette limite est alors nécessairement $f(a)$. On dit que f est continue sur un intervalle I lorsque la restriction de f à I est continue en tout point.

preuve. Supposons que $\lim_a f = l \neq f(a)$. Soit $U \in \mathcal{V}(f(a))$ et $V \in \mathcal{V}(l)$ disjoints. Alors il existe $A, B \in \mathcal{V}(a)$ tels que $f(A) \subset U$ et $f(B) \subset V$. Alors $f(a) \in U \cap V = \emptyset$: contradiction avec $a \in \mathcal{D}_f$. \square

Définition 6.6. Lorsque f a une limite finie l en un réel a , on dit qu'on la prolonge par continuité en posant $f(a) = l$. En effet, la prolongée est continue.

Remarque. Une fonction est continue sur un intervalle lorsque sa courbe est d'un seul tenant.

6.2.2. Premières propriétés.

Corollaire 6.8. Si f est continue en a et $\lim_{n \rightarrow \infty} u_n = a$, alors $\lim_{n \rightarrow \infty} f(u_n) = f(a)$.

Corollaire 6.9. Si $X \subset \mathbb{R}$ est stable par une fonction continue f et (u_n) est définie par $u_0 \in X$ et $u_{n+1} = f(u_n)$, alors sa limite éventuelle est un point fixe de f (ie. une solution de $f(x) = x$).

preuve. Remarquez que (par une récurrence élémentaire), (u_n) est bien définie. Par ailleurs, si $\lim u_n = l$, alors par composition on a $\lim u_{n+1} = l$ puis $\lim f(u_n) = f(l)$, d'où $l = f(l)$. \square

Proposition 6.10. Si $X \subset \mathbb{R}$ et $f : X \rightarrow \mathbb{R}$ est une application strictement monotone, alors f est injective. D'ailleurs, f induit une bijection de X sur $f(X)$.

preuve. En effet, si $x, y \in X$ sont distincts, il se rangent dans un ordre strict et leurs images aussi, donc $f(x) \neq f(y)$. Par ailleurs, l'application $g : X \rightarrow f(X) \ x \mapsto f(x)$ est surjective par construction (et injective puisque f l'est). \square

Proposition 6.11. Soit I un intervalle et $f : I \rightarrow \mathbb{R}$ continue et strictement monotone. Alors $f(I)$ est un intervalle (corollaire 6.16) et $\tilde{f} : I \rightarrow f(I) \ x \mapsto f(x)$ est bijective. Sa bijection réciproque, notée abusivement $f^{-1} : f(I) \rightarrow I$, est continue et strictement monotone de même sens que f .

preuve. \tilde{f} est notoirement bijective : surjective par définition et injective car strictement monotone. Supposons f strictement croissante : $\forall (a, b) \in f(I)^2, f^{-1}(a) \geq f^{-1}(b) \implies f(f^{-1}(a)) \geq f(f^{-1}(b))$, cad $a \geq b$. Par contraposée $\forall (a, b) \in f(I)^2, a < b \implies f^{-1}(a) < f^{-1}(b)$: f^{-1} est strictement croissante. Pour la continuité soit $b \in f(I)$ et $a = f^{-1}(b)$. En raisonnant par contraposée, on remarque que $\forall y \in f(I), f(a - \varepsilon) < y < f(a + \varepsilon) \implies a - \varepsilon < f^{-1}(y) < a + \varepsilon$. En posant $\eta = \min\{b - f(a - \varepsilon), f(a + \varepsilon) - b\} > 0$, on a bien $f^{-1}(]b - \eta, b + \eta]) \subset]a - \varepsilon, a + \varepsilon[$: f^{-1} est continue en b . Si f est strictement décroissante : même raisonnement en inversant les inégalités. \square

6.2.3. Le théorème de Bolzano-Weierstrass.

Lemme 6.12 (suites adjacentes). Soient (a_n) et (b_n) deux suites réelles, telles que

$$\begin{cases} \forall n \in \mathbb{N}, & a_n \leq a_{n+1} \leq b_{n+1} \leq b_n \\ \lim (a_n - b_n) = 0 \end{cases}$$

Alors (a_n) et (b_n) convergent vers la même limite.

preuve. (a_n) est croissante et majorée par b_0 donc converge de limite α . De même, (b_n) converge de limite β . Puis $\lim(a_n - b_n) = \alpha - \beta = 0$ donne $\alpha = \beta$. \square

Théorème 6.13 (Bolzano-Weierstrass). *Toute suite réelle bornée admet une sous-suite⁴ convergente.*

preuve. Soient $a < b$ deux réels et (x_n) une suite d'éléments de $[a, b]$. On va construire par récurrence des suites adjacentes (a_n) et (b_n) et une extractrice $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ strictement croissante telle que $\forall n \in \mathbb{N}, x_{\varphi(n)} \in [a_n, b_n]$. Au rang 0, on pose $(a_0, b_0) = (a, b)$ et $\varphi(0) = 0$. Soit $n \in \mathbb{N}$ tel que l'on ai pu construire les 3 suites jusqu'au rang n avec :

$$(6.1) \quad \begin{cases} \forall k \in \llbracket 0, n \rrbracket, & a_k \leq a_{k+1} \leq b_{k+1} \leq b_k \text{ et } |a_{k+1} - b_{k+1}| = \frac{1}{2}|a_k - b_k| \\ \forall k \in \llbracket 0, n \rrbracket, & x^{-1}([a_k, b_k]) = \{n \in \mathbb{N}, x_n \in [a_k, b_k]\} \text{ est infini, et } x_{\varphi(k)} \in [a_k, b_k] \end{cases}$$

On pose $c_n = \frac{1}{2}(a_n + b_n) : x^{-1}([a_n, b_n]) = x^{-1}([a_n, c_n] \cup [c_n, b_n]) = x^{-1}([a_n, c_n]) \cup x^{-1}([c_n, b_n])$ est infini, donc au moins un des deux ensembles $x^{-1}([a_n, c_n])$ et $x^{-1}([c_n, b_n])$ est infini. Si $x^{-1}([a_n, c_n])$ est infini, on pose $(a_{n+1}, b_{n+1}) = (a_n, c_n)$; sinon $(a_{n+1}, b_{n+1}) = (c_n, b_n)$. L'ensemble (a_{n+1}, b_{n+1}) étant infini dans \mathbb{N} , il n'est donc pas majoré et on peut y choisir $\varphi(n+1) > \varphi(n)$. Ainsi (6.1) est vraie jusqu'au rang $n+1$, ce qui achève la récurrence.

Par construction, (a_n) et (b_n) sont adjacentes : $\forall n \in \mathbb{N}, a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$ et $|a_n - b_n| = 2^{-n}|a - b| \xrightarrow[n \rightarrow \infty]{} 0$, donc (a_n) et (b_n) convergent vers une même limite \bar{x} . Par construction toujours, φ est strictement croissante et $\forall n \in \mathbb{N}, x_{\varphi(n)} \in [a_n, b_n]$. De l'encadrement $a \leq a_n \leq x_{\varphi(n)} \leq b_n \leq b$, on déduit $\lim x_{\varphi(n)} = \bar{x}$ (théorème 6.7) et $\bar{x} \in [a, b]$ (proposition 6.5). \square

6.2.4. Images d'intervalles.

Corollaire 6.14. *Une application continue sur un segment est bornée et atteint ses bornes.*

preuve. Soit $f : [a, b] \rightarrow \mathbb{R}$ continue. Si f n'est pas majorée : $\forall n \in \mathbb{N}, \exists x_n \in [a, b], f(x_n) \geq n$. Donc il existe une suite (x_n) d'éléments de $[a, b]$ telle que $\lim f(x_n) = +\infty$ (convergence monotone). D'après le théorème de Bolzano-Weierstrass, il existe une extractrice φ telle que $\lim x_{\varphi(n)} = \bar{x} \in [a, b]$. D'une part, $\lim f(x_{\varphi(n)}) = +\infty$ et d'autre part, $\lim f(x_{\varphi(n)}) = f(\bar{x})$ par continuité de f en \bar{x} : contradiction. Ainsi f est-elle majorée. De même $-f$ est majorée, donc f est minorée.

Par définition de $s = \sup\{f(x), x \in [a, b]\}$, il existe une suite (x_n) d'éléments de $[a, b]$ telle que $\lim f(x_n) = s$. Par Bolzano-Weierstrass, il existe une extractrice φ telle que $\lim x_{\varphi(n)} = \bar{x} \in [a, b]$. On a $\lim f(x_{\varphi(n)}) = s$ et $\lim f(x_{\varphi(n)}) = f(\bar{x})$, par continuité de f en \bar{x} . Donc $f(\bar{x}) = s$: le sup est atteint. De même, $-f$ atteint son supremum, donc f atteint son infimum. \square

Théorème 6.15 (valeurs intermédiaires). *Soit I un intervalle et $f : I \rightarrow \mathbb{R}$ une fonction continue. Entre deux valeurs prises, toute valeur intermédiaire est prise : $\forall (a, b) \in I^2, [f(a), f(b)] \subset f([a, b])$.*

preuve. On suppose sans restriction $a \neq b$ et $f(a) \neq f(b)$. On raisonne alors par l'absurde en supposant qu'il existe un $z \in]f(a), f(b)[\neq \emptyset$ tel que $z \notin f([a, b])$. Considérons les ensembles

$$X = \{x \in [a, b]; f(x) < z\} \quad \text{et} \quad Y = \{y \in [a, b]; f(y) > z\}$$

X et Y sont bornés (car $X, Y \subset f^{-1}([a, b])$ qui est borné, corollaire 6.14) et l'un des deux est non vide (car $z \notin f([a, b])$), par exemple $X \neq \emptyset$. On pose alors $x_0 = \sup X$ (donc $f(x_0) \leq z$, par passage à la limite) et si $f(x_0) < z$, la continuité de f en x_0 contredit la maximalité de $x_0 : f(x_0) = z$. De même, si $X = \emptyset$ et $Y \neq \emptyset$, on pose $x_0 = \inf Y$ et $f(x_0) = z$. \square

Corollaire 6.16. *L'image d'un intervalle par une application continue est un intervalle.*

preuve. Le lecteur vérifiera (c'est facile) que $X \subset \mathbb{R}$ est un intervalle ss'il est convexe, ie :

$$\forall (x, y) \in X^2, [x, y] = \{\lambda x + (1 - \lambda)y, 0 \leq \lambda \leq 1\} \subset X$$

Si I est un intervalle et $f : I \rightarrow \mathbb{R}$ est continue, le théorème des valeurs intermédiaires nous donne $\forall (y_1, y_2) \in f(I)^2, [y_1, y_2] \subset f(I)$: ainsi $f(I)$ est convexe et c'est un intervalle. \square

Corollaire 6.17. *Il résulte du corollaire 6.14 et du corollaire 6.16 que l'image d'un segment par une application continue est un segment.*

⁴On appelle sous-suite de (u_n) une suite du type $(u_{\varphi(n)})$ où $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ est strictement croissante. On a alors $\forall n \in \mathbb{N}, \varphi(n) \geq n$, donc si (u_n) a une limite $l \in \overline{\mathbb{R}}$ il en est de même de toutes ses suites extraites.

Corollaire 6.18. *Le tableau ci-contre permet de calculer l'image $f(I)$ d'un intervalle I par une application f continue et monotone. L'existence des limites écrites résultant à chaque fois de la monotonie de f (théorème 6.6).*

I	$f \nearrow$	$f \searrow$
$[a, b]$	$[f(a), f(b)]$	$[f(b), f(a)]$
$]a, b[$	$]f(a), \lim_b f[$	$] \lim_b f, f(a)[$
$]a, b]$	$] \lim_a f, f(b)]$	$[f(b), \lim_a f[$
$]a, b[$	$] \lim_a f, \lim_b f[$	$] \lim_b f, \lim_a f[$

6.2.5. *Puissance réelle d'exposant rationnel.*

Définition 6.7. – Pour $a \in \mathbb{R}^*$ et $n \in \mathbb{Z}$; a^n est le produit de n termes égaux à a si $n > 0$, l'inverse de a^{-n} si $n < 0$ et 1 si $n = 0$.

– Soit $n \in \mathbb{N}^*$. L'application $f : \mathbb{R}_+ \rightarrow \mathbb{R}_+, x \mapsto x^n$ est bijective ; sa bijection réciproque étant la racine n -ième, notée $\sqrt[n]{\cdot}$.

preuve. Ce raisonnement est classique, il faut impérativement le comprendre et savoir le refaire :

- f est strictement monotone donc injective (proposition 6.10).
- f est continue et croissante, donc (corollaire 6.18) $f(\mathbb{R}_+) = [f(0), \lim_{+\infty} f[= \mathbb{R}_+ : f$ est surjective. \square

Définition 6.8. Soit $a \in \mathbb{R}_+^*$, $r \in \mathbb{Q}$ et (p, q) son unique représentant irréductible tel que $q > 0$. On définit $a^r = (\sqrt[q]{a})^p$. Pour tout représentant $(p', q') \in \mathbb{Z} \times \mathbb{N}^*$ de r , on a aussi $(\sqrt[q']{a})^{p'} = a^r$.

preuve. Cette dernière égalité est laissée en exercice (utiliser la proposition 1.6). On verra plus loin comment généraliser cette définition à des exposants irrationnels. \square

7. DÉRIVATION, PRIMITIVES

7.1. Dérivation.

Notation. I, J seront des intervalles de \mathbb{R} non triviaux (ie. non vides et non réduits à un point). On notera $\overset{\circ}{I}$ l'intervalle obtenu en ouvrant les bornes de I : on l'appelle *intérieur* de I .

7.1.1. Nombre dérivé.

Définition 7.1. On dit que $f : I \rightarrow \mathbb{R}$ est dérivable en $a \in I$ lorsque $\lim_{h \rightarrow 0} \frac{f(a+h) - f(a)}{h}$ existe et est finie ; cette limite est alors notée $f'(a)$ et appelée *nombre dérivé* de f en a . On définit aussi les *nombre dérivés à gauche et à droite* (quand les limites existent et sont finies) comme

$$f'_g(a) = \lim_{h \rightarrow 0^-} \frac{f(a+h) - f(a)}{h} \quad f'_d(a) = \lim_{h \rightarrow 0^+} \frac{f(a+h) - f(a)}{h}$$

Proposition 7.1. (1) f est dérivable en $a \in \overset{\circ}{I}$ ssi f est dérivable à gauche et à droite en a et $f'_g(a) = f'_d(a)$: dans ce cas, $f'(a) = f'_g(a) = f'_d(a)$.

(2) Approximation affine locale. f est dérivable en $a \in I$ ssi $\exists \varphi : I \rightarrow \mathbb{R}$ telle que

$$\lim_a \varphi = 0 \quad \text{et} \quad \forall x \in I, f(x) - f(a) = (x - a) [f'(a) + \varphi(x)]$$

(3) Si f est dérivable en $a \in I$, alors f est continue en a .

Proposition 7.2. Soient $a \in I, \lambda \in \mathbb{R}, f, g : I \rightarrow \mathbb{R}$ dérivables en a . Alors $f + g, \lambda f, fg$ et (si $g(a) \neq 0$) f/g sont dérivables en a et :

$$\begin{aligned} (f + g)'(a) &= f'(a) + g'(a), & (\lambda f)'(a) &= \lambda f'(a) \\ (fg)'(a) &= f'(a)g(a) + f(a)g'(a), & \left(\frac{f}{g}\right)'(a) &= \frac{f'(a)g(a) - g'(a)f(a)}{g(a)^2} \end{aligned}$$

preuve. $\forall h \neq 0$ tel que $a + h \in I$, on écrit que

$$\begin{aligned} (f + g)(a + h) - (f + g)(a) &= [f(a + h) - f(a)] + [g(a + h) - g(a)] \\ (\lambda f)(a + h) - (\lambda f)(a) &= \lambda[f(a + h) - f(a)] \\ (fg)(a + h) - (fg)(a) &= g(a + h)[f(a + h) - f(a)] + f(a)[g(a + h) - g(a)] \end{aligned}$$

On divise par h et on fait tendre h vers 0, ce qui prouve les 3 premiers résultats. Pour le quotient,

$$\frac{1}{h} \left[\frac{1}{g(a+h)} - \frac{1}{g(a)} \right] = -\frac{g(a+h) - g(a)}{hg(a)g(a+h)} = -\frac{g(a+h) - g(a)}{h} \frac{1}{g(a)g(a+h)} \xrightarrow{h \rightarrow 0} -\frac{g'(a)}{g(a)^2}$$

Ainsi, $1/g$ est dérivable en a et $\left(\frac{1}{g}\right)'(a) = -\frac{g'(a)}{g(a)^2}$. Enfin, $\frac{f}{g} = f \times \frac{1}{g} \dots$ □

Théorème 7.3. Soient $f : I \rightarrow \mathbb{R}$ et $g : J \rightarrow \mathbb{R}$ tel que $f(I) \subset J$. Si f est dérivable en a et g est dérivable en $f(a)$, alors $g \circ f$ est dérivable en a , et $(g \circ f)'(a) = f'(a)(g' \circ f)(a)$.

preuve. g est dérivable en $b = f(a)$, donc $\exists \psi : J \rightarrow \mathbb{R}$ de limite 0 en b telle que :

$$\forall y \in J, \quad g(y) - g(b) = (y - b) [g'(b) + \psi(y)]$$

$f(I) \subset J$, donc $\forall x \in I, \quad g(f(x)) - g(b) = (f(x) - b) [g'(b) + \psi(f(x))]$. En divisant par $x - a$:

$$\forall x \in I \setminus \{a\}, \quad \frac{(g \circ f)(x) - (g \circ f)(a)}{x - a} = \frac{f(x) - b}{x - a} [(g' \circ f)(a) + \psi(f(x))]$$

$\lim_a f = f(a) = b$ (f est continue en a) et $\lim_b \psi = 0$, donc $\psi(f(x)) \xrightarrow{x \rightarrow a} 0$. Par ailleurs, $\frac{f(x) - b}{x - a} \xrightarrow{x \rightarrow a} f'(a)$ (f est dérivable en a) d'où le résultat. □

Théorème 7.4. Soit $a \in I$ et $f : I \rightarrow \mathbb{R}$ strictement monotone, continue sur I , dérivable en a avec $f'(a) \neq 0$. La réciproque $f^{-1} : f(I) \rightarrow I$ est dérivable en $b = f(a)$ et $(f^{-1})'(b) = \frac{1}{f'(a)}$.

Remarque. Rappelons que $f(I)$ est un intervalle, puisque f est continue (corollaire 6.16). De plus, l'application $\tilde{f} : I \rightarrow f(I), x \mapsto f(x)$ est surjective par construction et injective car strictement monotone : on note abusivement $f^{-1} : f(I) \rightarrow I$ sa bijection réciproque.

preuve. $\forall y \in f(I) \setminus \{b\}, \quad \frac{f^{-1}(y) - f^{-1}(b)}{y - b} = \frac{f^{-1}(y) - a}{f(f^{-1}(y)) - f(a)} = \left(\frac{f(f^{-1}(y)) - f(a)}{f^{-1}(y) - a} \right)^{-1}$. Remarquons que $f^{-1}(y) \neq a$, parce que sinon (en composant par f) on aurait $y = b$, ce qui justifie cette «inversion de fraction». On reconnaît le taux de variation de f entre a et $f^{-1}(y)$. f^{-1} est continue (proposition 6.11) en b , d'où le résultat (par composition de limites). □

7.1.2. Fonction dérivée.

Définition 7.2. Si $f : I \rightarrow \mathbb{R}$ est dérivable en tout point de I , on note $f' : I \rightarrow \mathbb{R}$ l'application qui à $x \in I$ associe le nombre dérivé $f'(x)$.

Proposition 7.5. Soient $\lambda \in \mathbb{R}, f, g : I \rightarrow \mathbb{R}$ dérivables sur I . Alors $f + g, \lambda f, fg$ et (si g ne s'annule pas sur I) f/g sont dérivables sur I et :

$$(f + g)' = f' + g' \quad (\lambda f)' = \lambda f' \quad (fg)' = f'g + fg' \quad \left(\frac{f}{g}\right)' = \frac{f'g - g'f}{g^2}$$

Théorème 7.6. Soient $f : I \rightarrow \mathbb{R}$ et $g : J \rightarrow \mathbb{R}$ tel que $f(I) \subset J$. Si f est dérivable sur I et g est dérivable sur $f(I)$, alors $g \circ f$ est dérivable sur I et $(g \circ f)' = (g' \circ f)f'$.

Théorème 7.7. Soit $f : I \rightarrow \mathbb{R}$ strictement monotone, dérivable sur I , telle que f' ne s'annule pas sur I . La réciproque $f^{-1} : f(I) \rightarrow I$ est dérivable sur l'intervalle $f(I)$ et $(f^{-1})' = \frac{1}{f' \circ f^{-1}}$.

Remarque. Les trois résultats qui précèdent ne sont que des réécritures des résultats locaux correspondants, vu en (7.1.1) : il n'y a rien à démontrer !

Définition 7.3. – On définit par récurrence la notion de dérivée n -ième : $f^{(0)} = f$ et si $f^{(n)}$ est dérivable, alors on note $f^{(n+1)}$ sa dérivée.

– On dit que f est de classe \mathcal{C}^n (resp. \mathcal{C}^∞) sur I si f est n fois (resp. indéfiniment) dérivable sur I et que $f^{(n)}$ est continue sur I . On note $\mathcal{C}^n(I)$ et $\mathcal{C}^\infty(I)$ les ensemble de fonctions correspondants.

Proposition 7.8. Soient $\lambda \in \mathbb{R}, f, g : I \rightarrow \mathbb{R}$ n fois dérivables sur I . Alors $f + g, \lambda f, fg$ et (si g ne s'annule pas sur I) f/g sont n fois dérivables sur I . De plus $(f + g)^{(n)} = f^{(n)} + g^{(n)}$ et $(\lambda f)^{(n)} = \lambda f^{(n)}$.

preuve. On sait déjà que l'énoncé est vrai pour $n = 1$ (proposition 7.5). Soit $n \in \mathbb{N}^*$ tel que l'énoncé est vrai au rang n . Soient $\lambda \in \mathbb{R}$, $f, g : I \rightarrow \mathbb{R}$ $n + 1$ fois dérivables sur I .

Par l'énoncé au rang n appliqué à (f', g') , $(f + g)' = f' + g'$ est n fois dérivable et $[(f + g)']^{(n)} = (f')^{(n)} + (g')^{(n)}$, cad $(f + g)^{(n+1)} = f^{(n+1)} + g^{(n+1)}$. Par l'énoncé au rang n appliqué à f' , $(\lambda f)' = \lambda f'$ est n fois dérivable et $[(\lambda f)']^{(n)} = \lambda (f')^{(n)}$, cad $(\lambda f)^{(n+1)} = \lambda f^{(n+1)}$.

$(fg)' = f'g + fg'$ est n fois dérivable : on applique 3 fois l'énoncé au rang n à (f', g) , (f, g') , $(f'g, f'g')$. $(f/g)' = (f'g - g'f)/g^2$ est n fois dérivable : on applique 4 fois l'énoncé au rang n à (f', g) , (g', f) , $(f'g, g'f)$ et $(f'g - g'f, g^2)$. \square

Proposition 7.9. Soient $f : I \rightarrow \mathbb{R}$ et $g : J \rightarrow \mathbb{R}$, n fois dérivables, telles que $f(I) \subset J$. Alors $g \circ f$ est n fois dérivable sur I .

preuve. On sait déjà que l'énoncé est vrai pour $n = 1$ (théorème 7.6). Soit $n \in \mathbb{N}^*$ tel que le théorème est vrai au rang n . Soient $f : I \rightarrow \mathbb{R}$ et $g : J \rightarrow \mathbb{R}$ $n + 1$ fois dérivables, telles que $f(I) \subset J$. Il suffit d'écrire $(g \circ f)' = (g' \circ f)f' : g' \circ f$ est n fois dérivable le théorème au rang n (appliqué à f et g'), f' est n fois dérivable, donc le produit $(g' \circ f)f'$ l'est aussi (proposition 7.8) : $(g \circ f)'$ est n fois dérivable, cad que $g \circ f$ est $n + 1$ fois dérivable. \square

Proposition 7.10. Soit $f : I \rightarrow \mathbb{R}$ strictement monotone, n fois dérivable sur I , telle que f' ne s'annule pas sur I . La réciproque $f^{-1} : f(I) \rightarrow I$ est alors n fois dérivable sur l'intervalle $f(I)$.

preuve. On sait déjà que l'énoncé est vrai pour $n = 1$ (proposition 7.9). Soit $n \in \mathbb{N}^*$ tel que l'énoncé est vrai au rang n . Soit $f : I \rightarrow \mathbb{R}$ strictement monotone, $n + 1$ fois dérivable sur I , telle que f' ne s'annule pas sur I . Alors (proposition 7.9) $(f^{-1})' = 1/(f' \circ f^{-1})$ est n fois dérivable sur I , par les résultats précédents : f^{-1} est donc $n + 1$ fois dérivable sur I , ce qui achève la récurrence. \square

Remarque. Dans les énoncés précédents, on peut remplacer « n fois dérivable» par «de classe \mathcal{C}^n » : il n'y a qu'à faire de même dans les démonstrations ! Ceci étant pour tout n , on peut donc remplacer « n fois dérivable» par «infiniment dérivable».

7.1.3. Variations des fonctions.

Lemme 7.11. Si $f : I \rightarrow \mathbb{R}$ dérivable a un extrémum local en $a \in \overset{\circ}{I}$, alors $f'(a) = 0$.

preuve. $\overset{\circ}{I}$ est ouvert, donc $\exists \varepsilon > 0$, $[a - \varepsilon, a + \varepsilon] \subset I$. On suppose sans restriction (quitte à raisonner sur $-f$) qu'il s'agit d'un maximum local : $\forall |h| \leq \varepsilon$, $f(a + h) - f(a) \leq 0$. Par conséquent

$$\forall h \in [-\varepsilon, 0[, \frac{f(a + h) - f(a)}{h} \geq 0 \quad \text{et} \quad \forall h \in]0, \varepsilon], \frac{f(a + h) - f(a)}{h} \leq 0$$

Par passage à la limite quand $h \rightarrow 0^-$ et $h \rightarrow 0^+$, on en déduit $f'_g(a) \geq 0$ et $f'_d(a) \leq 0$. Or f est dérivable en a , donc $f'_g(a) = f'_d(a) = f'(a)$: nécessairement $f'(a) = 0$. \square

Théorème 7.12 (Rolle). Soit $f : [a, b] \rightarrow \mathbb{R}$ dérivable sur $]a, b[$ et continue sur $[a, b]$ telle que $f(a) = f(b) = 0$. Alors il existe $c \in]a, b[$ tel que $f'(c) = 0$.

preuve. Si $f = 0$, c'est trivial. Sinon, quitte à considérer $-f$, on peut supposer sans restriction qu'il existe $x \in]a, b[$ tel que $f(x) > 0$. Ainsi, $s = \sup\{f(x), x \in [a, b]\} \geq f(x) > 0$. f étant continue sur le segment $[a, b]$, s est atteint (corollaire 6.14) en au moins un point $c \in]a, b[$ ($c \notin \{a, b\}$ puisque $f(a) = f(b) = 0$). Ainsi, $f(c)$ est un maximum local de f et on a $f'(c) = 0$ d'après le lemme précédent. \square

Corollaire 7.13 (théorème des accroissements finis). Si $f : [a, b] \rightarrow \mathbb{R}$ est dérivable sur $]a, b[$ et continue sur $[a, b]$ alors $\exists c \in]a, b[$ tel que $f(b) - f(a) = f'(c)(b - a)$. Autrement dit, la courbe de f sur $[a, b]$ admet une tangente parallèle à la corde.

preuve. Soit $g : [a, b] \rightarrow \mathbb{R}$ l'unique fonction affine qui coïncide avec f sur $\{a, b\}$, cad :

$$\forall x \in [a, b], \quad g(x) - f(a) = \frac{f(b) - f(a)}{b - a}(x - a)$$

En appliquant Rolle à $f - g$, il existe $c \in]a, b[$ tel que $(f - g)'(c) = f'(c) - \frac{f(b) - f(a)}{b - a} = 0$. \square

Corollaire 7.14 (inégalité des accroissements finis). Soit $f : [a, b] \rightarrow \mathbb{R}$ dérivable sur $]a, b[$ et continue sur $[a, b]$ telle que $m \leq f' \leq M$ sur $]a, b[$. Alors $m(b - a) \leq f(b) - f(a) \leq M(b - a)$.

Corollaire 7.15 (principe de Lagrange). Soit $f : I \rightarrow \mathbb{R}$ continue sur I et dérivable sur $\overset{\circ}{I}$.

- si $f' \geq 0$ (resp. > 0) sur $\overset{\circ}{I}$, alors f est (resp. strictement) croissante sur I .
- si $f' \leq 0$ (resp. < 0) sur $\overset{\circ}{I}$, alors f est (resp. strictement) décroissante sur I .
- si $f' = 0$ sur $\overset{\circ}{I}$, alors f est constante sur I .

preuve. En vertu du corollaire 7.13 : $\forall a < b \in I, \exists c \in]a, b[$ tel que $f(b) - f(a) = f'(c)(b - a)$. Ainsi $f(b) - f(a)$ est du signe (au sens strict) de $f'(c)$, d'où les résultats annoncés. \square

Remarque. Plus généralement, si $f' \geq 0$ sur $\overset{\circ}{I}$, alors f est strictement croissante ssi $\{x \in \overset{\circ}{I}, f'(x) = 0\}$ ne contient aucun intervalle non trivial.

7.2. Primitives.

Définition 7.4. F est une primitive de f sur l'intervalle I lorsque F est dérivable sur I et $F' = f$.

Théorème 7.16. Toute fonction continue sur un intervalle possède des primitives.

preuve. Ce résultat découle de la construction de l'intégrale de Riemann d'une fonction continue (voir le corollaire 9.9 du cours d'intégration). \square

Proposition 7.17. Les primitives d'une même fonction f sur un intervalle I (s'il y en a) sont les $F + \lambda$, où F est une primitive de f et λ décrit \mathbb{R} .

preuve. Si F est une primitive de f sur I , les fonctions $F + \lambda$ sont aussi des primitives de f . Réciproquement, si G est une primitive de f , on a $(G - F)' = 0$, donc $G - F$ est constante (corollaire 7.15). \square

Corollaire 7.18. Si f est définie sur un intervalle I , $x_0 \in I$ et $y_0 \in \mathbb{R}$, alors il existe au plus une primitive F_0 de f telle que $F_0(x_0) = y_0$.

8. LOGARITHMES, EXPONENTIELLES

8.1. Le logarithme népérien.

8.1.1. Définition.

Définition 8.1. Le logarithme népérien – noté \ln – est la primitive nulle en 1 de l'inverse sur \mathbb{R}_+^* .

Corollaire 8.1. On en déduit immédiatement les résultats suivants :

- \ln est infiniment dérivable sur \mathbb{R}_+^* ,
- \ln est strictement croissante sur \mathbb{R}_+^* . Or $\ln 1 = 0$, d'où :

$$\ln x < 0 \iff 0 < x < 1 \quad \text{et} \quad \ln x > 0 \iff x > 1$$

$$- \lim_{h \rightarrow 0} \frac{\ln(1+h)}{h} = \ln'(1) = 1$$

- \ln' décroît strictement, donc (d'après le lemme qui suit) la courbe de \ln est en-dessous de toutes ses tangentes. En particulier, $\forall x > 0, \ln x \leq x - 1$ (avec égalité ssi $x = 1$).

Lemme 8.2. Soit I un intervalle de \mathbb{R} et $f : I \rightarrow \mathbb{R}$ dérivable, telle que f' est croissante (resp. décroissante). Alors la courbe de f sur I est au-dessus (resp. en-dessous) de ses tangentes.

preuve. Supposons f' croissante et fixons $x_0 \in I$. $\forall x \in I, \varphi(x) := f(x) - [f(x_0) + f'(x_0)(x - x_0)]$. φ est dérivable (puisque f l'est) et $\forall x \in I, \varphi'(x) = f'(x) - f'(x_0)$ est du signe de $x - x_0$. Ainsi φ est décroissante sur $I \cap]-\infty, x_0]$, croissante sur $I \cap [x_0, +\infty[$ et $\varphi(x_0) = 0$. Donc $\varphi \geq 0$, cad que la courbe de f est au-dessus de sa tangente en x_0 . Ceci étant vrai $\forall x_0 \in I$, on a bien prouvé le résultat annoncé.

Si f' est décroissante, on applique le résultat qui vient d'être démontré à $-f$. \square

8.1.2. *Logarithme d'un produit, conséquences.*

Théorème 8.3. $\forall a, b > 0, \ln(ab) = \ln a + \ln b.$

preuve. Soit $f : \mathbb{R}_+^* \rightarrow \mathbb{R}$ définie par $f(x) = \ln(ax)$. f est dérivable et $f'(x) = a \frac{1}{ax} = \frac{1}{x}$, donc $\exists C \in \mathbb{R}, f = \ln + C$. Puis $f(1) = \ln a = C$ donne le résultat : $f(x) = \ln a + \ln x$. \square

Corollaire 8.4. (1) $\forall a, b > 0, \ln \frac{a}{b} = \ln a - \ln b.$

(2) $\forall (a, r) \in \mathbb{R}_+^* \times \mathbb{Q}, \ln(a^r) = r \ln a.$

preuve. (1) $\ln a = \ln \left(b \frac{a}{b} \right) = \ln b + \ln \frac{a}{b}$, d'où $\ln \frac{a}{b} = \ln a - \ln b$. En particulier, $\ln \frac{1}{a} = -\ln a$.

(2) Soit $a \in \mathbb{R}_+^*$. $\forall n \in \mathbb{N}, \ln a^n = n \ln a$ (récurrence immédiate). $\forall n \in \mathbb{Z}_-, -n \in \mathbb{N}$ donc $\ln(a^n) = \ln \frac{1}{a^{-n}} = -\ln(a^{-n}) = n \ln a$. Ainsi, $\forall n \in \mathbb{Z}, \ln(a^n) = n \ln a$. Soit $r \in \mathbb{Q}$ et $(p, q) \in \mathbb{Z} \times \mathbb{N}^*, r = \frac{p}{q}$:

$$\begin{cases} \ln(a^{p/q}) = \ln \left[(a^{1/q})^p \right] = p \ln(a^{1/q}) \\ \ln a = \ln \left[(a^{1/q})^q \right] = q \ln(a^{1/q}) \end{cases} \implies \ln(a^{p/q}) = \frac{p}{q} \ln a$$

Ceci étant pour tout $r \in \mathbb{Q}$, on a bien le résultat voulu. \square

8.1.3. *Limites à connaître.*

Proposition 8.5. (1) $\lim_{+\infty} \ln = +\infty$, et $\lim_{0^+} \ln = -\infty$.

(2) $\forall \alpha \in \mathbb{Q}_+^*, \lim_{+\infty} \frac{\ln x}{x^\alpha} = 0$, et $\lim_{0^+} x^\alpha \ln x = 0$.

preuve. (1) $\{\ln 2^n, n \in \mathbb{Z}\}$ n'est ni majoré ni minoré, puisque $\ln 2^n = n \ln 2$ et $\ln 2 > 0$. \ln est croissante, d'où le résultat (avec le théorème 6.6).

(2) Soit $\varphi : \mathbb{R}_+^* \rightarrow \mathbb{R}$ définie par $\varphi(x) = \ln x - \sqrt{x}$ est dérivable sur \mathbb{R}_+^* et $\forall x > 0$,

$$\varphi'(x) = \frac{1}{x} - \frac{1}{2\sqrt{x}} = \frac{1}{\sqrt{x}} \left(\frac{1}{\sqrt{x}} - \frac{1}{2} \right) \quad \text{donc } \varphi \nearrow \text{ sur }]0, 4] \text{ et } \searrow \text{ sur } [4, +\infty[$$

donc $\forall x > 0, \varphi(x) \leq \varphi(4) = 2(\ln 2 - \sqrt{2}) \leq 0$, puisque $\ln 2 \leq 2 - 1 \leq \sqrt{2}$. Ainsi $\forall x \geq 1, 0 \leq \ln x \leq \sqrt{x}$ donc $0 \leq \frac{\ln x}{x} \leq \frac{1}{\sqrt{x}}$: d'où $\lim_{+\infty} \frac{\ln x}{x} = 0$ (théorème d'encadrement). L'égalité $\frac{\ln x}{x^\alpha} = \frac{1}{\alpha} \frac{\ln(x^\alpha)}{x^\alpha}$ permet de conclure par composition.

En écrivant $x^\alpha \ln x = -\frac{\ln(1/x)}{(1/x)^\alpha}$, on est ramené au cas précédent. \square

Corollaire 8.6. $\ln : \mathbb{R}_+^* \rightarrow \mathbb{R}$ est une bijection. En particulier, $\exists ! e \in \mathbb{R}_+^*, \ln e = 1$. Disons juste en passant (sans le démontrer) que $e \approx 2.718\ 281\ 828 \notin \mathbb{Q}$.

preuve. \ln est continue et croissante, donc $\ln(\mathbb{R}_+^*) =]\lim_{0^+} \ln, \lim_{+\infty} \ln[= \mathbb{R}$ (corollaire 6.16) : \ln est surjective. Par ailleurs, \ln est injective car strictement monotone. \square

8.1.4. *Autres fonctions logarithmes.*

Définition 8.2. Soit $a > 0, a \neq 1$. On appelle logarithme en base a , l'application

$$\log_a : \mathbb{R}_+^* \rightarrow \mathbb{R} \quad x \mapsto \log_a x = \frac{\ln x}{\ln a}$$

En particulier, $\ln = \log_e$.

8.2. **L'exponentielle népérienne.**

8.2.1. *Définition, conséquences.* Rappelons que \ln établit une bijection de \mathbb{R}_+^* dans \mathbb{R} , ce qui motive la définition suivante :

Définition 8.3. On appelle *exponentielle (népérienne)* la réciproque de \ln , cad l'unique bijection $\exp : \mathbb{R} \longrightarrow \mathbb{R}_+^*$ vérifiant $\forall x \in \mathbb{R}_+^*, \forall y \in \mathbb{R}, (\ln x = y \iff x = \exp y)$.

Remarque. Graphiquement, leur courbes sont symétriques par rapport à la première bissectrice. Cela permet de prévoir beaucoup de ses propriétés.

Corollaire 8.7. *Conséquences de la définition, l'exponentielle :*

- (1) transforme les sommes en produits, donc les différences en quotients et les opposés en inverses.
- (2) est dérivable et égale à sa dérivée : appliquer le théorème 7.7.
- (3) croît strictement sur \mathbb{R} .

preuve. (1) Pour montrer que $\exp(a+b) = \exp(a)\exp(b)$, il suffit de vérifier l'égalité des logarithmes⁵ : c'est immédiat. Il s'en suit que $\exp(a-b) = \frac{\exp(a)}{\exp(b)}$. En particulier, $\exp(-x) = \frac{\exp(0)}{\exp x} = \frac{1}{\exp x}$.

(3) Conséquence immédiate de (2) : $\exp' = \exp > 0$ sur \mathbb{R} . □

Remarque. \exp' croît strictement sur \mathbb{R} , donc (même remarque que pour \ln) sa courbe est au dessus de ses tangentes. On retiendra que $\forall x \in \mathbb{R}, \exp x \geq x + 1$ (avec égalité ssi $x = 0$).

8.2.2. *Limites à connaître.*

Proposition 8.8. (1) $\lim_{x \rightarrow +\infty} \exp x = +\infty$, et $\lim_{x \rightarrow -\infty} \exp x = 0$.

(2) $\forall \alpha \in \mathbb{Q}_+^*, \lim_{x \rightarrow +\infty} \frac{\exp x}{x^\alpha} = +\infty$.

preuve. (1) $\forall x \in \mathbb{R}, \exp x \geq x + 1 \xrightarrow{x \rightarrow +\infty} +\infty$ et $\exp x = \frac{1}{\exp(-x)} \xrightarrow{x \rightarrow -\infty} 0$.

(2) $\ln\left(\frac{\exp x}{x^\alpha}\right) = x - \alpha \ln x = x \left(1 - \alpha \frac{\ln x}{x}\right) \xrightarrow{x \rightarrow +\infty} +\infty$, d'où le résultat (en composant extérieurement par \exp). □

8.3. Puissance réelle d'exposant réel.

Définition 8.4. Pour tout $a \in \mathbb{R}_+^*$ et $b \in \mathbb{R}$, on définit $a^b = \exp(b \ln a)$. Ainsi, $\forall x \in \mathbb{R}, \exp(x) = e^x$: notation plus pratique. On définit donc – entre autres – des fonctions

- *puissances* : $\mathbb{R}_+^* \longrightarrow \mathbb{R}_+^*, x \longmapsto x^a = \exp(a \ln x)$ (*puissance d'exposant $a \in \mathbb{R}$*)
- *exponentielles* : $\mathbb{R} \longrightarrow \mathbb{R}_+^*, x \longmapsto a^x = \exp(x \ln a)$ (*exponentielle de puissance $a \in \mathbb{R}_+^*$*)

L'étude de ces fonctions résulte de façon élémentaire de celle de la fonction \exp .

8.4. Caractérisation algébriques.

Théorème 8.9. *Si $f : \mathbb{R} \longrightarrow \mathbb{R}$ est continue en au moins un point x_0 et transforme les sommes en sommes (ie. $\forall x, y \in \mathbb{R}, f(x+y) = f(x) + f(y)$), alors f est linéaire.*

preuve. $f(0) = f(0) + f(0)$, donc $f(0) = 0$. $\forall x \in \mathbb{R}, f(x) + f(-x) = f(0) = 0$, donc f est impaire. Enfin, $\forall (x, \varepsilon) \in \mathbb{R}^2, f(x+\varepsilon) - f(x) = f(\varepsilon) = f(x_0 + \varepsilon) - f(x_0) \xrightarrow{\varepsilon \rightarrow 0} 0$ donc f est continue sur \mathbb{R} .

Par une récurrence élémentaire sur n , on a $\forall n \in \mathbb{N}, \forall a \in \mathbb{R}^n, f\left(\sum_{i=1}^n a_i\right) = \sum_{i=1}^n f(a_i)$. Maintenant, $\forall r \in \mathbb{Q}_+, \exists (p, q) \in \mathbb{N} \times \mathbb{N}^*, r = p/q$ et

$$\begin{cases} f\left(\frac{p}{q}\right) = f\left(\sum_{i=1}^p \frac{1}{q}\right) = \sum_{i=1}^p f\left(\frac{1}{q}\right) = pf\left(\frac{1}{q}\right) \\ f(1) = f\left(\sum_{i=1}^q \frac{1}{q}\right) = \sum_{i=1}^q f\left(\frac{1}{q}\right) = qf\left(\frac{1}{q}\right) \end{cases} \implies f\left(\frac{p}{q}\right) = \frac{p}{q}f(1), \text{ soit } f(r) = rf(1).$$

puis $\forall r \in \mathbb{Q}_-, f(r) = -f(-r) = -(-r)f(1) = rf(1)$. Ainsi $\forall r \in \mathbb{Q}, f(r) = rf(1)$.

Soit $x \in \mathbb{R}$ et (r_n) une suite de rationnels qui tend vers x (par ex. le développement décimal à 10^{-n} près par défaut). D'une part $f(r_n) = r_n f(1) \xrightarrow{n \rightarrow \infty} x f(1)$ et d'autre part $f(r_n) \xrightarrow{n \rightarrow \infty} f(x)$ (f est continue en x). Par unicité de $\lim f(r_n)$, il vient $f(x) = x f(1)$. □

⁵On rappelle que \ln est injective, cad que $\forall (x, y) \in (\mathbb{R}_+^*)^2, \ln x = \ln y \implies x = y$.

Corollaire 8.10. Si $f : \mathbb{R}_+^* \rightarrow \mathbb{R}$ est continue en au moins un point x_0 et transforme les produits en sommes, alors f est une fonction logarithme (ou $f = 0$).

preuve. $f \circ \exp$ est continue en $\ln x_0$ et transforme les sommes en sommes, donc $f \circ \exp = f(e)\text{Id}_{\mathbb{R}}$. En composant intérieurement par \ln , on obtient (par associativité) $f = f(e)\ln$. \square

Corollaire 8.11. Si $f : \mathbb{R} \rightarrow \mathbb{R}_+^*$ est continue en au moins un point x_0 et transforme les sommes en produits, alors f est une fonction exponentielle.

preuve. $\ln \circ f$ est continue en x_0 et transforme les sommes en sommes, donc $\ln \circ f = \ln f(1)\text{Id}_{\mathbb{R}}$. En composant extérieurement par \exp , on obtient (par associativité) $f = \exp_{f(1)}$. \square

Corollaire 8.12. Si $f : \mathbb{R}_+^* \rightarrow \mathbb{R}_+^*$ est continue en au moins un point x_0 et transforme les produits en produits, alors f est une fonction puissance.

preuve. $\ln \circ f$ est continue en x_0 et transforme les produits en sommes, donc $\exists \alpha \in \mathbb{R}$, $\ln \circ f = \alpha \ln$. En composant extérieurement par \exp , on obtient $\forall x \in \mathbb{R}_+^*$, $f(x) = \exp(\alpha \ln x) = x^\alpha$. \square

Exemple 8.1. Hélas, toutes les fonctions ne sont pas «continues en au moins un point», cad qu'il existe des fonctions discontinues partout, comme la fonction indicatrice de \mathbb{Q} . En effet,

$$\mathbf{1}_{\mathbb{Q}} : \mathbb{R} \rightarrow \mathbb{R} \quad x \mapsto \begin{cases} 1 & \text{si } x \in \mathbb{Q} \\ 0 & \text{sinon} \end{cases}$$

est discontinue sur \mathbb{R} puisque tout rationnel (resp. irrationnel) est limite d'une suite d'irrationnels (resp. de rationnels).

9. INTÉGRATION

9.1. Définition de l'intégrale de Riemann. Soient $a \leq b$ deux réels.

9.1.1. Cas des fonctions en escalier.

Définition 9.1. $\sigma = (x_0, \dots, x_n) \in \mathbb{R}^{n+1}$ est une *subdivision* de $[a, b]$ si

$$x_0 = a < x_1 < \dots < x_{n-1} < x_n = b$$

Le *pas* d'une telle subdivision est le réel $|\sigma| = \max_{0 \leq k \leq n-1} (x_{k+1} - x_k)$.

Définition 9.2. Une application $\varphi : [a, b] \rightarrow \mathbb{R}$ est en *escalier* s'il existe une subdivision $\sigma = (x_0, \dots, x_n)$ telle que φ est constante sur $]x_k, x_{k+1}[$, pour tout $0 \leq k \leq n-1$. Une telle subdivision est dite *adaptée* à φ . On notera \mathcal{E} l'ensemble des fonctions en escalier sur $[a, b]$.

Définition 9.3. En notant λ_k la valeur de φ sur $]x_k, x_{k+1}[$, le réel $I(\varphi) = \sum_{k=0}^{n-1} \lambda_k (x_{k+1} - x_k)$ ne dépend pas du choix de la subdivision σ adaptée à φ et s'appelle *intégrale* de φ sur $[a, b]$.

Proposition 9.1. \mathcal{E} est stable par combinaison linéaire et produit et I est une forme linéaire :

$$\forall (\varphi, \psi) \in \mathcal{E}^2, \forall (\lambda, \mu) \in \mathbb{R}^2, \quad \lambda\varphi + \mu\psi \in \mathcal{E}, \quad \varphi\psi \in \mathcal{E} \quad \text{et} \quad I(\lambda\varphi + \mu\psi) = \lambda I(\varphi) + \mu I(\psi)$$

Proposition 9.2. $\forall \varphi \in \mathcal{E}, \varphi \geq 0 \implies I(\varphi) \geq 0$: I est une forme linéaire positive.

Remarque. On peut avoir $\varphi \geq 0$, $\varphi \neq 0$ et $I(\varphi) = 0$ (prendre les λ_k nuls et au moins une valeur > 0 en un point de la subdivision). En fait, si l'on modifie une fonction en escalier en un nombre fini de points, elle reste en escalier et son intégrale ne varie pas.

Corollaire 9.3. La linéarité permet d'en déduire que si $\varphi \leq \psi$, alors $I(\varphi) \leq I(\psi)$: I est croissante.

preuve. En effet si $\psi - \varphi \geq 0$, alors $I(\psi - \varphi) = I(\psi) - I(\varphi) \geq 0$. \square

9.1.2. *Cas des fonctions Riemann-intégrables.*

Définition 9.4. Soit une application bornée $f : [a, b] \rightarrow \mathbb{R}$. On peut donc définir

$$I^- = \sup\{I(u); u \in \mathcal{E}, u \leq f\} \quad \text{et} \quad I^+ = \inf\{I(v); v \in \mathcal{E}, f \leq v\}$$

On a toujours $I^- \leq I^+$ et lorsque $I^- = I^+$, on dit que f est *Riemann-intégrable* et on définit :

$$\int_a^b f = \int_a^b f(t)dt = I^- = I^+$$

preuve. Soient $X = \{I(u); u \in \mathcal{E}, u \leq f\}$ et $Y = \{I(v); v \in \mathcal{E}, f \leq v\}$. f est bornée : $m \leq f \leq M$, donc $I(m) \in X \neq \emptyset$ et $I(M) \in Y \neq \emptyset$. De plus, Y est minoré par tout élément de X et X est majoré par tout élément de Y . Ainsi X et Y admettent un supremum et un infimum, vérifiant $\sup X \leq \sup Y$. \square

Remarque. f est donc Riemann-intégrable ssi $\forall \varepsilon > 0, \exists (u, v) \in \mathcal{E}^2, u \leq f \leq v$ et $I(v - u) \leq \varepsilon$.

Exemple 9.1. La fonction caractéristique des rationnels ($\mathbf{1}_{\mathbb{Q}}(x) = 1$ si $x \in \mathbb{Q}$, 0 sinon) n'est pas Riemann-intégrable sur $[0, 1]$ (comme sur tout segment). En effet, $I^- = 0$ et $I^+ = 1$.

Proposition 9.4. *L'ensemble \mathcal{R} des fonctions Riemann-intégrables est stable par combinaison linéaire et produit, et l'intégrale est une forme linéaire positive, donc croissante.*

Remarque. Il est clair que cet espace contient \mathcal{E} et que l'intégrale y coïncide avec I .

9.1.3. *Approximation des fonctions continues.*

Théorème 9.5 (Heine). *Soit $f : [a, b] \rightarrow \mathbb{R}$ continue. Alors f est uniformément continue cad que*

$$\forall \varepsilon > 0, \exists \eta > 0, \forall (x, y) \in [a, b]^2, \quad |x - y| < \eta \implies |f(x) - f(y)| < \varepsilon$$

Toute la nuance avec la simple continuité tient dans le fait que η ne dépend que de ε .

preuve. Supposons ce résultat faux, cad (un peu de logique ne fait pas de mal)

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

On prend $\eta = 2^{-n}$ de sorte qu'il existe deux suites (x_n) et (y_n) telles que

$$\forall n \in \mathbb{N}, \quad |x_n - y_n| < 2^{-n} \text{ et } |f(x_n) - f(y_n)| \geq \varepsilon$$

Par Bolzano-Weierstrass, il existe une extractrice φ telle que $\lim_{n \rightarrow \infty} x_{\varphi(n)} = \bar{x} \in [a, b]$. Avec l'encadrement $|x_{\varphi(n)} - y_{\varphi(n)}| < 2^{-\varphi(n)} \leq 2^{-n}$, on a aussi $\lim_{n \rightarrow \infty} y_{\varphi(n)} = \bar{x}$. Ainsi, par continuité de f en \bar{x} , $\lim_{n \rightarrow \infty} f(x_{\varphi(n)}) = \lim_{n \rightarrow \infty} f(y_{\varphi(n)}) = f(\bar{x})$, donc $f(x_{\varphi(n)}) - f(y_{\varphi(n)}) \xrightarrow{n \rightarrow \infty} 0$: contradiction avec $|f(x_{\varphi(n)}) - f(y_{\varphi(n)})| \geq \varepsilon$. \square

Corollaire 9.6. *Les fonctions continues sont Riemann-intégrables.*

preuve. Soit $f : [a, b] \rightarrow \mathbb{R}$ continue, $\varepsilon > 0$ et $\eta > 0$ tel que

$$\forall (x, y) \in [a, b]^2, \quad |x - y| < \eta \implies |f(x) - f(y)| < \frac{\varepsilon}{b - a}$$

Soit une subdivision $\sigma = (x_0, \dots, x_n)$ de pas $|\sigma| \leq \eta$. Soient $\varphi, \psi \in \mathcal{E}$ égales à f aux points de la subdivision, $\varphi = \min\{f(x), x \in [x_k, x_{k+1}]\}$ sur $]x_k, x_{k+1}[$ et $\psi = \max\{f(x), x \in [x_k, x_{k+1}]\}$ sur $]x_k, x_{k+1}[$. Par construction, on a $\varphi \leq f \leq \psi$ et $\psi - \varphi \leq \frac{\varepsilon}{b - a}$, donc $I(\psi - \varphi) \leq \varepsilon$. Ceci étant $\forall \varepsilon > 0$, f est Riemann-intégrable. \square

Corollaire 9.7. *Les fonctions continues par morceaux (somme d'une fonction continue et d'une fonction en escalier) sont donc Riemann-intégrable.*

9.2. **Calcul d'intégrales.**

9.2.1. *Intégrale et primitives.*

Définition 9.5. Si $a \geq b$, on définit $\int_a^b f = -\int_b^a f$.

L'intégrale, ainsi prolongée, reste évidemment une forme linéaire, mais son signe est celui de $b - a$ (donc $f \mapsto \int_a^b f$ est croissante si $a \leq b$ et décroissante si $a \geq b$).

Lemme 9.8. Soit I un intervalle, $x_0 \in I$ et $f : I \rightarrow \mathbb{R}$ localement Riemann-intégrable⁶ et continue en x_0 . Alors $\forall a \in I$, $F : I \rightarrow \mathbb{R}$ $x \mapsto \int_a^x f$ est dérivable en x_0 et $F'(x_0) = f(x_0)$.

preuve. Soit $\varepsilon > 0$ et η tel que $\forall x \in I$, $|x - x_0| \leq \eta \implies |f(x) - f(x_0)| \leq \varepsilon$ (f est continue en x_0). Alors $\forall x \in I \setminus \{x_0\}$ tel que $|x - x_0| \leq \eta$,

$$\frac{F(x) - F(x_0)}{x - x_0} = \frac{1}{x - x_0} \int_{x_0}^x f \in [f(x_0) - \varepsilon, f(x_0) + \varepsilon]$$

ε étant arbitraire, on a $\frac{F(x) - F(x_0)}{x - x_0} \xrightarrow[x \neq x_0]{x \rightarrow x_0} f(x_0)$. □

Corollaire 9.9. Si f est continue sur I , alors ($\forall a \in I$) F est une primitive de f sur I . Ainsi, f possède-t-elle des primitives (ce qui démontre enfin le théorème 7.16). Si G est une primitive quelconque de f sur I , $G - F$ est constante (proposition 7.17) et on a

$$\int_a^b f = [G(t)]_a^b = [G]_a^b = G(b) - G(a)$$

Remarque. En fait, ce résultat «définit» l'intégrale dans le cadre du programme. Cette présentation simpliste élude les véritables difficultés (le théorème 7.16 et la proposition 7.17).

9.2.2. *Propriétés.* Les résultats suivants sont vrais pour des fonctions localement Riemann-intégrables, mais les démonstrations sont pénibles : on travaillera avec des fonctions continues.

Proposition 9.10 (Chasles). Soit I un intervalle et $f \in \mathcal{C}^0(I)$. Alors

$$\forall (a, b, c) \in I^3, \quad \int_a^c f = \int_a^b f + \int_b^c f$$

preuve. Si F est une primitive de f sur I , alors $F(c) - F(a) = F(c) - F(b) + F(b) - F(a)$. □

Proposition 9.11 (parité). Soit $a \in \mathbb{R}$ et $f \in \mathcal{C}^0([-a, a])$.

(1) Si f est paire, alors $\int_{-a}^a f = 2 \int_0^a f$.

(2) Si f est impaire, alors $\int_{-a}^a f = 0$.

preuve. (1) Soit F une primitive de f sur $[a, b]$ et $\forall |x| \leq a$, $\varphi(x) := \int_{-x}^x f - 2 \int_0^x f$. Alors $\forall |x| \leq a$, $\varphi(x) = F(x) - F(-x) - 2(F(x) - F(0))$. Donc φ est dérivable sur $[-a, a]$ et $\forall |x| \leq a$, $\varphi'(x) = f(x) + f(-x) - 2f(x) = 0$. Ainsi, φ est constante égale à $\varphi(0) = 0$, d'où le résultat : $\varphi(a) = 0$.

(2) Idem, avec $\varphi(x) = \int_{-x}^x f = F(x) - F(-x)$. □

Proposition 9.12 (périodicité). Si $f \in \mathcal{C}^0(\mathbb{R})$ est T -périodique, alors $\int_a^{a+T} f$ ne dépend pas du choix de $a \in \mathbb{R}$ et s'appelle intégrale de f sur une période.

preuve. Soit $\varphi : \mathbb{R} \rightarrow \mathbb{R}$ $a \mapsto \int_a^{a+T} f = F(a+T) - F(a)$ pour une primitive (quelconque) F de f sur \mathbb{R} . φ est dérivable (puisque F l'est) et $\forall a \in \mathbb{R}$, $\varphi'(a) = f(a+T) - f(a) = 0$, donc φ est constante. □

Proposition 9.13 (inégalités usuelles). Soit $f : [a, b] \rightarrow \mathbb{R}$ Riemann-intégrable avec $a \leq b$.

⁶cad Riemann-intégrable sur tout segment inclus dans I .

- (1) Inégalité triangulaire. $\forall f \in \mathcal{R}, \quad \left| \int_a^b f \right| \leq \int_a^b |f|$
- (2) Inégalité de Schwarz. $\forall f, g \in \mathcal{R}, \quad \left| \int_a^b fg \right| \leq \sqrt{\int_a^b f^2} \sqrt{\int_a^b g^2}$

preuve. (1) Il suffit d'intégrer l'encadrement $-|f| \leq f \leq |f|$, par croissance de l'intégrale.

(2) Il suffit de considérer $\varphi(f, g) = \int_a^b fg$ et de remarquer que φ est une forme bilinéaire symétrique positive sur l'espace vectoriel réel \mathcal{R} : on pose alors $\Phi(f) = \varphi(f, f)$ et on procède comme à la proposition 4.1 : $\forall \lambda \in \mathbb{R}, \Phi(f + \lambda g) = \Phi(f) + \lambda^2 \Phi(g) + 2\lambda \varphi(f, g) \geq 0$. Le trinôme précédent est de signe constant sur \mathbb{R} , donc $\Delta' = \varphi(f, g)^2 - \Phi(f)\Phi(g) \leq 0$, d'où le résultat. \square

9.2.3. *Techniques de calcul.*

Proposition 9.14 (intégration par parties). $\forall u, v \in \mathcal{C}^1([a, b]), \int_a^b uv' = [uv]_a^b - \int_a^b u'v$.

preuve. $(uv)' = u'v + v'u$, donc $uv' = (uv)' - u'v$, égalité qu'on intègre de a à b \square

Proposition 9.15 (changement de variable). Soit $\varphi \in \mathcal{C}^1([a, b])$ et $f \in \mathcal{C}^0(\varphi([a, b]))$:

$$\int_a^b f(\varphi(u))\varphi'(u)du = \int_{\varphi(a)}^{\varphi(b)} f(t)dt$$

preuve. Il suffit de remarquer que $(f \circ \varphi)\varphi' = (F \circ \varphi)'$, d'où $\int_a^b (f \circ \varphi)\varphi' = [F \circ \varphi]_a^b = [F]_{\varphi(a)}^{\varphi(b)} = \int_{\varphi(a)}^{\varphi(b)} f$, où F est une primitive quelconque de f sur le segment $\varphi([a, b])$. \square

Exemple 9.2. $\int_0^1 \sqrt{1-x^2} dx = \int_0^{\frac{\pi}{2}} \sqrt{1-\sin^2 t} \cos t dt = \int_0^{\frac{\pi}{2}} \sin t \cos t dt = \frac{1}{2} \int_0^{\frac{\pi}{2}} \sin 2t dt = \frac{\pi}{4}$. Il s'agit, en effet, de l'aire du quart de cercle trigonométrique $\{(x, y) \in (\mathbb{R}_+)^2, x^2 + y^2 \leq 1\}$.

9.2.4. *Intégration numérique.* On va donner trois façons d'approcher numériquement une intégrale (méthodes des rectangles, du point médian et des trapèzes) et on estimera leur vitesse de convergence.

Définition 9.6. On dit qu'une suite (u_n) converge en $\mathcal{O}(v_n)$ vers u_∞ s'il existe une constante α telle qu'à partir d'un certain rang, $|u_n - u_\infty| \leq \alpha v_n$. (v_n) est donc une mesure qualitative de la vitesse de convergence de (u_n) .

Proposition 9.16. Soit $f : [a, b] \rightarrow \mathbb{R}$ et $\forall n \in \mathbb{N}^*, x^n$ la subdivision régulière de $[a, b]$ de pas $p = \frac{b-a}{n}$, cad que $\forall k \in \llbracket 0, n \rrbracket, x_k^n = a + kp = q + k \frac{b-a}{n}$.

- (1) Rectangles : $R_n = p \sum_{k=0}^{n-1} f(x_k^n)$, converge en $\mathcal{O}\left(\frac{1}{n}\right)$ vers $\int_a^b f$, pour f de classe \mathcal{C}^1 .
- (2) Point médian : $M_n = p \sum_{k=0}^{n-1} f\left(\frac{x_k^n + x_{k+1}^n}{2}\right)$, converge en $\mathcal{O}\left(\frac{1}{n^2}\right)$ vers $\int_a^b f$, pour $f \in \mathcal{C}^2$.
- (3) Trapèzes : $T_n = p \sum_{k=0}^{n-1} \frac{f(x_k^n) + f(x_{k+1}^n)}{2}$, converge en $\mathcal{O}\left(\frac{1}{n^2}\right)$ vers $\int_a^b f$, pour $f \in \mathcal{C}^2$.

preuve. Afin d'économiser du papier, on ne va prouver que la méthode des rectangles.

$$\begin{aligned} \left| R_n - \int_a^b f \right| &= \left| p \sum_{k=0}^{n-1} f(x_k^n) - \sum_{k=0}^{n-1} \int_{x_k^n}^{x_{k+1}^n} f \right| = \left| \sum_{k=0}^{n-1} \left(pf(x_k^n) - \int_{x_k^n}^{x_{k+1}^n} f \right) \right| \\ &\leq \left| \sum_{k=0}^{n-1} \int_{x_k^n}^{x_{k+1}^n} (f(x_k^n) - f) \right| = \sum_{k=0}^{n-1} \left| \int_{x_k^n}^{x_{k+1}^n} (f(x_k^n) - f) \right| \leq \sum_{k=0}^{n-1} \int_{x_k^n}^{x_{k+1}^n} |f(x_k^n) - f| \end{aligned}$$

Pour conclure, il nous faut donc majorer convenablement les $|f(x_k^n) - f(t)|$ (pour $t \in [x_k^n, x_{k+1}^n]$). Remarquons que f' est continue sur le segment $[a, b]$ donc bornée (corollaire 6.14). On note alors

$$\|f'\|_\infty = \sup_{[a,b]} |f'| = \sup\{|f'(t)|, t \in [a, b]\}$$

et l'inégalité des accroissements finis appliquée à f sur $[x_k^n, t]$ pour $t \in [x_k^n, x_{k+1}^n]$ nous donne

$$|f(x_k^n) - f(t)| \leq \|f'\|_\infty |x_k^n - t| = \|f'\|_\infty (t - x_k^n)$$

On en déduit que $\int_{x_k^n}^{x_{k+1}^n} |f(x_k^n) - f(t)| dt \leq \|f'\|_\infty \int_{x_k^n}^{x_{k+1}^n} (t - x_k^n) dt = \|f'\|_\infty \frac{p^2}{2}$. Finalement,

$$|R_n - f| \leq \|f'\|_\infty \sum_{k=0}^{n-1} \frac{p^2}{2} = \|f'\|_\infty n \frac{p^2}{2} = \|f'\|_\infty \frac{(b-a)^2}{2n}$$

d'où la convergence (théorème d'encadrement) en $\mathcal{O}(n^{-1})$. \square

Remarque. En fait la convergence des suites R_n, M_n et T_n a lieu pour f Riemann-intégrable (hypothèse beaucoup plus faible). Dans ce cas on ne peut rien dire sur la vitesse de convergence.

10. EQUATIONS DIFFÉRENTIELLES

10.1. Introduction.

Définition 10.1. On appelle *équation différentielle d'ordre n sur \mathbb{R}* , une relation entre une fonction inconnue y (n fois dérivable sur \mathbb{R}), ses n premières dérivées et la variable, soit

$$(E) : \Phi(x, y, y', \dots, y^{(n)}) = 0$$

Résoudre ou *intégrer* (E) , c'est trouver toutes ces fonctions (n fois dérivables sur \mathbb{R}).

Définition 10.2. On dit que (E) est :

- *linéaire*, si elle peut s'écrire $a_n(x)y^{(n)} + \dots + a_1(x)y' + a_0(x)y = g(x)$.
- à *coefficients constants*, si les fonctions a_i sont constantes.
- *homogène* (ou sans second membre), si g est nulle.

Notation. On suppose désormais que (E) est linéaire et on note $(H) : a_n(x)y^{(n)} + \dots + a_0(x)y = 0$ l'équation homogène associée.

Théorème 10.1. Si e_0 est une solution particulière de l'équation linéaire (E) , on a l'équivalence : f est solution de (E) ssi $f - e_0$ est solution de (H) . Autrement dit, l'ensemble des solutions de (E) est $\{e_0 + h, h \text{ solution de } (H)\}$.

preuve. Il suffit d'écrire

- (1) $a_n(x)h^{(n)} + \dots + a_1(x)h' + a_0(x)h = 0$
- (2) $a_n(x)f^{(n)} + \dots + a_1(x)f' + a_0(x)f = g(x)$
- (3) $a_n(x)e_0^{(n)} + \dots + a_1(x)e_0' + a_0(x)e_0 = g(x)$

et de dire que :

- si f est solution de (E) , alors (2) - (3) $\implies f - e_0$ est solution de (H) .
- si h est solution de (H) , alors (1) + (3) $\implies h + e_0$ est solution de (E) . \square

10.2. **Solution de $y' = a(x)y + s(x)$.** On suppose a et s continues sur \mathbb{R} .

10.2.1. Equation homogène.

Théorème 10.2. Les solutions de $y' = a(x)y$ sont les $x \mapsto \lambda e^{A(x)}$, pour $\lambda \in \mathbb{R}$ et A primitive de a .

preuve. Soit $h : x \mapsto e^{A(x)}$: h est solution, et $\forall \lambda \in \mathbb{R}$, $(\lambda h)' = \lambda h' = a(\lambda h)$, donc λh est solution. Réciproquement, si f est solution, on pose $z = f/h$ (h ne s'annule pas) : z est dérivable et $z'h^2 = f'h - h'f = (af)h - (ah)f = 0$ donc z est constante. \square

10.2.2. *Solution particulière : méthode de variation de la constante.*

Proposition 10.3. Soit $h : x \mapsto e^{A(x)}$ (solution de $y' = a(x)y$) et λ dérivable sur \mathbb{R} . Alors λh est solution de l'équation complète $y' = a(x)y + s(x)$ ssi $\lambda' = s/h$.

preuve. $(\lambda h)' - a(\lambda h) = \lambda' h + \lambda(h' - ah) = \lambda' h = s$, dès lors que $\lambda' = s/h$. \square

10.3. **Solution de $y'' + ay' + by = 0$.**

10.3.1. *Les solutions.*

Remarque. $x \mapsto e^{rx}$ est solution ssi $r^2 + ar + b = 0$: c'est l'équation caractéristique de (E).

Théorème 10.4. Selon que l'équation caractéristique $r^2 + ar + b = 0$ a

- (1) 2 racines réelles r_1, r_2 , l'ensemble des solutions est $\mathcal{S} = \{x \mapsto \alpha e^{r_1 x} + \beta e^{r_2 x}, (\alpha, \beta) \in \mathbb{R}^2\}$
- (2) 1 racine réelle double r , $\mathcal{S} = \{x \mapsto (\alpha x + \beta)e^{rx}, (\alpha, \beta) \in \mathbb{R}^2\}$
- (3) 2 racines $u \pm iv \in \mathbb{C}$ avec $(u, v) \in \mathbb{R}^2$: $\mathcal{S} = \{x \mapsto e^{ux}(\alpha \cos vx + \beta \sin vx), (\alpha, \beta) \in \mathbb{R}^2\}$.

preuve. D'après le corollaire 10.7, il suffit de trouver 2 solutions non proportionnelles, dans les 3 cas :

- (1) D'après la remarque, $e^{r_1 x}$ et $e^{r_2 x}$ sont deux solutions ; non proportionnelles, puisque $r_1 \neq r_2$.
- (2) De même e^{rx} est solution, et on peut vérifier que $x e^{rx}$ aussi : idem, solutions non proportionnelles.
- (3) $e^{rx} = e^{ux}(\cos vx + i \sin vx)$ et $e^{\bar{r}x} = e^{ux}(\cos vx - i \sin vx)$ sont solutions de (E), mais à valeurs complexes. En fait, leur parties réelles et imaginaires vont donner les 2 solutions attendues. Ainsi, on a les deux solutions $e^{ux} \cos vx$ et $e^{ux} \sin vx$, non proportionnelles. \square

Corollaire 10.5 (oscillateur harmonique). $y'' + \omega^2 y = 0$ a la solution générale :

$$x \mapsto A \cos \omega x + B \sin \omega x \quad (A, B) \in \mathbb{R}^2$$

Remarque. $A \cos \omega x + B \sin \omega x = C(\cos \varphi \cos \omega x + \sin \varphi \sin \omega x) = C \cos(\omega x - \varphi)$, en posant

$$C = \sqrt{A^2 + B^2} \quad \cos \varphi = \frac{A}{C} \quad \sin \varphi = \frac{B}{C}$$

En effet, $\left(\frac{A}{C}\right)^2 + \left(\frac{B}{C}\right)^2 = \left(\frac{A^2}{A^2 + B^2}\right) + \left(\frac{B^2}{A^2 + B^2}\right) = 1$.

10.3.2. *Réciproque.*

Théorème 10.6 (Cauchy). Deux solutions vérifiant une même condition initiale sont égales :

$$\{\exists t_0 \in \mathbb{R}, f(t_0) = g(t_0) \text{ et } f'(t_0) = g'(t_0)\} \implies f = g$$

preuve. (1) On définit le Wronskien de 2 solutions (f, g) par $W_{f,g} = f'g - g'f$, puis on le dérive :

$$W'_{f,g} = (f''g + f'g') - (g''f + g'f') = f''g - g''f = -(af' + bf)g + (ag' + bg)f = -aW_{f,g}$$

Donc $W_{f,g}$ vérifie l'équation différentielle $y' + ay = 0$, d'où $\forall x \in \mathbb{R}, W_{f,g}(x) = W_{f,g}(0)e^{-ax}$. Ainsi, $W_{f,g}$ s'annule tout le temps ou jamais.

(2) On prend maintenant une famille (u, v) de Wronskien non nul⁷ (donc jamais nul, d'après (1)) et une solution f telle que $f(0) = f'(0) = 0$. $W_{f,u}$ et $W_{f,v}$ s'annulent en 0, donc en tout point :

$$\forall x \in \mathbb{R}, \quad \begin{cases} f'(x)u(x) - u'(x)f(x) = 0 \\ f'(x)v(x) - v'(x)f(x) = 0 \end{cases}$$

Ce système en $(f'(x), f(x))$ admet une unique solution, soit $f(x) = f'(x) = 0$, car son déterminant est $W_{u,v}(x) \neq 0$. Ainsi une solution f vérifiant $f(0) = f'(0) = 0$ est nulle.

(3) Soient f et g deux solutions ayant même valeur et même dérivé t_0 . On pose $h(x) = f(t_0 + x) - g(t_0 + x)$. h est donc 2 fois dérivable (sur \mathbb{R}) et $h(0) = h'(0) = 0$. De plus h vérifie $h'' + ah' + bh = 0$. Donc d'après (2), $h = 0$, cad $f = g$. \square

Corollaire 10.7. Les solutions forment un \mathbb{R} -espace vectoriel de dimension 2. Autrement dit, si u, v sont 2 solutions non proportionnelles, alors l'ensemble des solutions de (E) est $\{\alpha u + \beta v, (\alpha, \beta) \in \mathbb{R}^2\}$.

⁷L'existence de solutions u et v telles que $W_{u,v} = u'v - v'u \neq 0$ est assurée par l'étude menée au 10.3.1.

preuve. Soit (u, v) deux solutions linéairement indépendantes. Les vecteurs $(u(0), u'(0))$ et $(v(0), v'(0))$ sont donc linéairement indépendants, car s'il existait $(\alpha, \beta) \in \mathbb{R}^2$ tel que

$$\alpha(u(0), u'(0)) + \beta(v(0), v'(0)) = (0, 0)$$

alors $\alpha u + \beta v$ aurait même condition initiale en 0 que la solution nulle, d'où $\alpha u + \beta v = 0$ (théorème de Cauchy), ce qui contredit l'indépendance linéaire de u et v .

Ainsi, $(u(0), u'(0))$ et $(v(0), v'(0))$ forment une base de \mathbb{R}^2 , donc on peut décomposer la condition initiale en 0 d'une solution quelconque f dans cette base :

$$\exists!(\alpha, \beta) \in \mathbb{R}^2, \quad (f(0), f'(0)) = \alpha(u(0), u'(0)) + \beta(v(0), v'(0))$$

Ainsi, f a même condition initiale que $\alpha u + \beta v$ en 0, donc $f = \alpha u + \beta v$ (théorème de Cauchy). \square

10.4. Méthode d'Euler. Considérons l'équation du pendule simple (qu'on ne sait pas résoudre sous forme close) $\ddot{\theta} + \frac{g}{l} \sin \theta = 0$. En physique, on vous a donné une expression de la période qui découle de l'approximation $\sin \theta \approx \theta$, qui n'est «valable» que si θ reste faible.

Soit $\varepsilon > 0$ assez petit (en l'occurrence devant $T \approx 2\pi\sqrt{l/g}$), θ_n la valeur de θ pour $t = n\varepsilon$. Les conditions initiales, soit $(\theta_0, \dot{\theta}_0)$ déterminent le mouvement, et une suite d'approximations affines donne :

$$\begin{cases} \theta_{n+1} \approx \theta_n + \varepsilon \dot{\theta}_n \\ \dot{\theta}_{n+1} \approx \dot{\theta}_n + \varepsilon \ddot{\theta}_n = \dot{\theta}_n - \varepsilon \frac{g}{l} \sin \theta_n \end{cases}$$

En traçant les points $(n\varepsilon, \theta_n)$ on obtient une approximation de la *courbe intégrale*.

Remarque. La méthode de *Runge-Kutta* consiste à remplacer les approximations affines par des approximations plus fine à l'ordre 2 :

$$\begin{cases} \theta_{n+1} \approx \theta_n + \varepsilon \dot{\theta}_n + \frac{\varepsilon^2}{2} \ddot{\theta}_n = \theta_n + \varepsilon \dot{\theta}_n - \frac{\varepsilon^2 g}{2l} \sin \theta_n \\ \dot{\theta}_{n+1} \approx \dot{\theta}_n + \varepsilon \ddot{\theta}_n + \frac{\varepsilon^2}{2} \theta_n^{(3)} = \dot{\theta}_n - \varepsilon \frac{g}{l} \sin \theta_n - \frac{\varepsilon^2 g}{2l} \dot{\theta}_n \cos \theta_n \end{cases}$$

★ ★ ★