

DM n° 5 : Relations, réels

Correction du problème 1 – Treillis et algèbres de Boole

Partie I – Treillis

1. Soit (E, \leq) un ensemble totalement ordonné. Soit $(x, y) \in E^2$. Comme E est totalement ordonné, on a $x \leq y$ et $y \leq x$. Ainsi, dans les deux cas, le sous-ensemble $\{x, y\}$ admet un minimum et un maximum, donc une borne supérieure et une borne inférieure. Ainsi, (E, \leq) est un treillis.

2. (i) Soit $(x, y) \in \mathbb{N}^*$. Alors un entier z de \mathbb{N}^* minore x et y si et seulement si $z \mid x$ et $z \mid y$; le plus grand des minorants existe, et est par définition le pgcd de x et y (le « plus grand » est ici à prendre au sens de la divisibilité et non de la relation usuelle sur \mathbb{N}^* , mais cela revient au même ici, tous les diviseurs communs de x et y divisent le pgcd). Ainsi, $\{x, y\}$ admet une borne inférieure, et $x \wedge y = \text{pgcd}(x, y)$.

Un raisonnement similaire amène l'existence de la borne supérieure, et $x \vee y = \text{ppcm}(x, y)$.

Ainsi, $\boxed{\mathbb{N}^* \text{ muni de la relation de divisibilité est un treillis}}$.

(ii) Soit $(Y, Z) \in \mathcal{P}(X)$. Alors les minorants U de Y et Z sont les ensembles tels que $U \subset Y$ et $U \subset Z$. Ils vérifient tous $U \subset Y \cap Z$, et $Y \cap Z$ vérifie bien $Y \cap Z \subset Y$ et $Y \cap Z \subset Z$. Ainsi, $Y \cap Z$ est le plus grand des minorants de Y et Z . On en déduit que la borne supérieure de Y et Z existe, et $\boxed{Y \wedge Z = Y \cap Z}$.

On montre par le même raisonnement que Y et Z admettent une borne supérieure, et $\boxed{Y \vee Z = Y \cup Z}$.

Ainsi, $\boxed{(\mathcal{P}(X), \subset)}$ est un treillis.

3. • Puisque $\emptyset \in \mathcal{P}(X)$, et pour tout $Y \in \mathcal{P}(X)$, $\emptyset \subset Y$, \emptyset est le minimum de $\mathcal{P}(X)$.

Puisque $E \in \mathcal{P}(X)$ et pour tout $Y \in \mathcal{P}(X)$, $Y \subset E$, E est le maximum de $\mathcal{P}(X)$.

Ainsi, $\boxed{\mathcal{P}(X) \text{ est borné}}$, et en utilisant les notations introduites, $0 = \emptyset$, et $1 = E$.

• Soit $Y \in \mathcal{P}(E)$, et définissons $Y^c = \complement_X Y$. On a alors

$$Y \wedge Y^c = Y \cap Y^c = \emptyset = 0 \quad \text{et} \quad Y \vee Y^c = Y \cup Y^c = E = 1.$$

Ainsi, $\boxed{\mathcal{P}(X) \text{ est complémenté}}$.

• D'après le cours, l'intersection est distributive sur l'union et vice-versa, donc $\boxed{\mathcal{P}(X) \text{ est distributif}}$.

4. Soit (E, \leq) un treillis borné, complémenté et distributif.

(a) • Soit $x \in E$. Comme 0 est le minimum de E , le seul minorant de 0 est 0 , et c'est aussi un minorant de x . Ainsi, l'ensemble des minorants de 0 est $\{0\}$, qui admet un plus grand élément, à savoir 0 . Ainsi, $\boxed{x \wedge 0 = 0}$

• De même, les majorants de x et 0 sont tous supérieurs à x et x lui-même est un majorant de x et 0 . Ainsi, il s'agit du plus petit. Donc $\boxed{x \vee 0 = 0}$.

• De même, les minorants de x et 1 sont tous inférieurs à x et x lui-même est un minorant de x et 1 (puisque 1 est le maximum). Ainsi, il s'agit du plus grand. Donc $\boxed{x \wedge 1 = x}$.

• Enfin, le seul majorant de 1 est 1 lui-même, qui est aussi majorant de x , donc $\boxed{x \vee 1 = 1}$.

(b) Soit $(x, y, z) \in E^3$ et $m = \inf(\inf(x, y), z)$, $m' = \inf(x, \inf(y, z))$.

• On a $m \leq \inf(x, y)$ et $m \leq z$, et comme $\inf(x, y) \leq x$ et $\inf(x, y) \leq y$, on a $m \leq x$, $m \leq y$ et $m \leq z$. Des deux dernières inégalités, on tire que m est un minorant de $\{y, z\}$, donc, par définition, $m \leq \inf(y, z)$. Cette inégalité, associée à $m \leq x$ montre que m est un minorant de $\{x, \inf(y, z)\}$, donc, par définition, $m \leq m'$.

- Le même raisonnement montre que $m' \leq m$.

Ainsi, $\inf(\inf(x, y), z) = \inf(x, \inf(y, z))$, soit $(x \wedge y) \wedge z = x \wedge (y \wedge z)$.

- (c) Soit x' et x'' deux complémentaires de x , et soit $y = (x \wedge x') \vee x''$.

- Par définition d'un complémentaire, on a $y = 0 \vee x'' = x''$.
- Par ailleurs, par distributivité,

$$y = (x \wedge x') \vee (x' \wedge x'') = 1 \wedge (x' \wedge x'') = x' \wedge x''.$$

- Ainsi, $x'' = x' \wedge x''$, donc x'' est un majorant de x' et x'' . En particulier, $x'' \geq x'$.
- En intervertissant les rôles de x' et x'' , il vient $x' \geq x''$.
- L'antisymétrie de la relation d'ordre amène alors $x' = x''$

On en déduit que $(x \wedge x')$ est unique.

- (d) • Pour la première identité, il suffit de montrer que $x^c \vee y^c$ est LE complémentaire de $x \wedge y$. Pour cela on a deux vérifications à faire, en utilisant l'associativité des bornes supérieures (de même type), la commutativité, et la distributivité :

$$\begin{aligned} * \quad & (x \wedge y) \wedge (x^c \vee y^c) = (x \wedge y \wedge x^c) \vee (x \wedge y \wedge y^c) = (0 \wedge y) \vee (x \wedge 0) = 0 \vee 0 = 0. \\ * \quad & (x \wedge y) \vee (x^c \vee y^c) = (x \wedge x^c \vee y^c) \wedge (y \wedge x^c \vee y^c) = (1 \wedge y^c) \wedge (1 \wedge x^c) = 1 \wedge 1 = 1. \end{aligned}$$

on en déduit que $(x \wedge y)^c = x^c \vee y^c$

- Par unicité du complémentaire, on voit immédiatement que x est le complémentaire de x^c , donc $(x^c)^c = 0$. Cela nous dispense de refaire tout l'argument pour obtenir la deuxième loi de De Morgan ; on peut la retrouver à partir de la première :

$$(x \wedge y)^c = ((x^c)^c \vee (y^c)^c)^c = ((x^c \wedge y^c)^c)^c = (x^c \wedge y^c).$$

On a bien obtenu : $(x \wedge y)^c = x^c \wedge y^c$

5. (a) Soit $x \in E$.

- $x + 0 = (x \wedge 0^c) \vee (x^c \wedge 0) = (x \wedge 1) \vee 0 = x$, donc $x + 0 = x$.
- $x \times 1 = x \wedge 1 = x$ donc $x \times 1 = x$
- $x^2 = x \wedge x = x$, donc $x^2 = x$
- $x + x = (x \wedge x^c) \vee (x^c \wedge x) = 0 \vee 0 = 0$, soit : $x + x = 0$.

- (b) • Les opérations \wedge et \vee (correspondant aux bornes inférieures et supérieures) sont commutatives. On en déduit facilement la commutativité de $+$.

- Soit $(x, y, z) \in E$. On a

$$\begin{aligned} (x + y) + z &= ((x \wedge y^c) \vee (x^c \wedge y)) + z \\ &= (((x \wedge y^c) \vee (x^c \wedge y)) \wedge z^c) \vee (((x \wedge y^c) \vee (x^c \wedge y))^c \wedge z) \\ &= (x \wedge y^c \wedge z^c) \vee (x^c \wedge y \wedge z^c) \vee ((x^c \wedge y) \wedge (x \wedge y^c)) \wedge z \\ &= (x \wedge y^c \wedge z^c) \vee (x^c \wedge y \wedge z^c) \vee (x^c \wedge y^c \wedge z) \vee (x \wedge y \wedge z). \end{aligned}$$

Cette expression étant symétrique en x , y et z , on obtient la même chose en intervertissant l'ordre initial des variables, donc, en utilisant la commutativité déjà justifiée,

$$(x + y) + z = (y + z) + x = x + (y + z).$$

Ainsi, $+$ est associative.

- L'associativité de \times n'est rien d'autre que l'associativité des bornes inférieures qu'on a déjà utilisé dans l'argument précédent.
- Soit $(x, y, z) \in E^3$. On a alors :

$$x \times (y + z) = x \wedge ((y \wedge z^c) \vee (y^c \wedge z)) = (x \wedge y \wedge z^c) \vee (x \wedge y^c \wedge z)$$

D'autre part :

$$\begin{aligned}
x \times y + x \times z &= ((x \sim y) \sim (x \sim z)^c) \cup ((x \sim y)^c \sim (x \sim z)) \\
&= (x \sim y \sim x^c) \cup (x \sim y \sim z^c) \cup (x^c \sim x \sim z) \cup (y^c \sim x \sim z) \\
&= 0 \cup (x \sim y \sim z^c) \cup 0 \cup (x \sim y^c \sim z) \\
&= (x \sim y \sim z^c) \cup (x \sim y^c \sim z)
\end{aligned}$$

Ainsi, on a bien la distributivité $x \times (y + z) = x \times y + x \times z$.

Partie II – Algèbres de Boole

1. Cela provient de la partie précédente, $\mathcal{P}(X)$ étant un treillis borné complémenté et distributif. Le complément correspondant à la complémentation usuelle dans $\mathcal{P}(X)$, on se rend compte que l'addition correspond à la différence symétrique. La dernière question de la partie I permet alors d'affirmer que

$\mathcal{P}(X)$ muni de Δ et \cap est une algèbre de Boole.

On a déjà dit que $0 = \emptyset$ et $1 = E$.

2. (a) On a :

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y,$$

d'où $0 = xy + yx$.

- (b) i. En particulier, pour $y = 1$, on obtient $x + x = 0$, donc $x = -x$

ii. En combinant les deux derniers résultats, pour tout $(x, y) \in A^2$, $xy = -yx = yx$, donc \times est commutative.

3. On définit sur A une relation par :

$$\forall (x, y) \in A, \quad x \leqslant y \iff xy = x.$$

- (a) • Soit $x \in A$, on a $x^2 = x$, donc $x \leqslant x$. Ainsi, \leqslant est réflexive.
• Soit $(x, y) \in A^2$ tels que $x \leqslant y$ et $y \leqslant x$. Alors $xy = x$ et $yx = y$. Comme $xy = yx$, on en déduit que $x = y$. Ainsi, \leqslant est antisymétrique.
• Soit $(x, y, z) \in A^3$ tels que $x \leqslant y$ et $y \leqslant z$. On a alors $xy = x$ et $yz = y$, d'où $xz = (xy)z = x(yz) = xy = x$. Ainsi, $x \leqslant z$. Donc \leqslant est transitive.

Il s'agit donc d'une relation réflexive, antisymétrique et transitive, donc d'une relation d'ordre sur A .

- (b) Pour tout $x \in A$:

- $0 \times x = (0 + 0) \times x = (0 \times x) + (0 \times x) = 0$, d'après 2(b)(i). Donc $0 \leqslant x$.
 On en déduit que 0 est le minimum de A .
- $x \times 1 = x$ par définition, donc $x \leqslant 1$. Ainsi, 1 est le maximum de A .

- (c) • On a $(xy)x = yx^2 = yx = (xy)$, donc $xy \leqslant x$;
• De même $xy \leqslant y$. Ainsi, xy est un minorant de x et de y .
• Soit $z \leqslant x$ et $z \leqslant y$. Alors $zx = z$ et $zy = z$, d'où $zxy = zy = z$, donc $z \leqslant xy$.
• On en déduit que xy est le plus grand des minorants de x et y , donc la borne inférieure (ce qui montre son existence) : $xy = x \cap y$.

- (d) On raisonne de même :

- $x(x + y + xy) = x^2 + xy + x^2y = x + xy + xy = x$, donc $x \leqslant x + y + xy$.
 • De même $y \leqslant x + y + xy$, donc $x + y + xy$ est un majorant de x et y .
 • Soit z tel que $x \leqslant z$ et $y \leqslant z$. Alors $xz = x$ et $yz = y$. On a alors :

$$(x + y + xy)z = xz + yz + xyz = x + y + xy.$$

On a donc $x + y + xy \leqslant z$.

- Ainsi, $x + y + xy$ est le plus petit des majorants, donc la borne supérieure (qui existe donc) : $x \cup y = x + y + xy$.

- (e) • La commutativité et l'associativité de \sim découlent immédiatement de l'associativité et de la commutativité du produit de A (hypothèse et question 2(b)).
- L'expression de la loi \sim et la commutativité de \times et $+$ amène de façon immédiate la commutativité de \sim .
- Soit $(x, y, z) \in A^3$. On a :

$$x \sim (y \sim z) = x \sim (y + z + yz) = x + (y + z + yz) + x(y + z + yz) = x + y + z + yz + xz + xy + xyz.$$

En développant de même $(x \sim y) \sim z$, on obtient la même expression d'où l'associativité.

- Soit $(x, y, z) \in A^3$. On a
 - * $x \sim (y \sim z) = x + yz + xyz,$
 - * $(x \sim y) \sim (x \sim z) = (x + y + xy)(x + z + xz) = x^2 + xz + x^2z + yx + yz + xyz + x^2y + xyz + x^2yz = x + yz + xyz,$
- d'après les relations $x^2 = x$ et $x + x = 0$. Ainsi, on obtient la même chose, donc \sim est distributive sur \sim .
- Soit $(x, y, z) \in A^3$. On a
 - * $x \sim (y \sim z) = x(y + z + yz) = xy + xz + xyz,$
 - * $(x \sim y) \sim (x \sim z) = xy + xz + xyxz = xy + xz + xyz.$

On en déduit que \sim est distributif sur \sim .

- (f) Soit $x \in A$. On recherche y tel que $xy = 0$ et $x + y + xy = 1$, donc $xy = 0$ et $x + y = 1$, ce qui incite à définir $y = 1 - x = 1 + x$. Montrons que ce choix convient :
- $x \sim (1 + x) = x(1 + x) = x + x^2 = x + x = 0;$
 - $x \sim (1 + x) = x + (1 + x) + x(1 + x) = 1 + x + x = 1.$
- Ainsi, $1 + x$ est bien le complémentaire de x : $x^c = 1 + x$.

Ainsi, toute algèbre de Boole peut être munie d'une relation d'ordre qui en fait un treillis borné complémenté distributif. La réciproque avait été établie dans la partie I.

Partie III – Description des algèbres de Boole finies

Soit A une algèbre de Boole finie.

1. Soit $x \in A$ non nul. Si x est un atome, x est minoré par lui-même.

Supposons que x n'est pas un atome et soit $m(x)$ l'ensemble des minorants stricts de x . L'ensemble $m(x) \setminus \{0\}$ est non vide puisque a n'est pas un atome. Il admet un élément minimal, car sinon, partant d'un élément $b_1 \in m(x) \setminus \{0\}$, n'étant pas minimal, on pourrait trouver $b_2 \in m(x) \setminus \{0\}$ tel que $b_2 < b_1$, puis de la même manière $b_3 < b_2$, et ainsi, construire une suite infinie $b_1 > b_2 > b_3 > \dots > b_n > \dots$ d'éléments deux à deux distincts, ce qui contredit le fait que A est fini.

Ainsi, $m(x) \setminus \{0\}$ admet au moins un élément minimal a . Son seul minorant strict dans $m(x)$ est donc 0 (qui est minorant de tout élément). Ainsi, a est un atome. Comme il est dans $m(x)$, il minore a .

Tout élément x non nul de A est donc minoré par un atome.

2. (a) Soit $(x, y) \in A^2$, et a un atome de A . Supposons que $a \leqslant x \sim y$ et $a \not\leqslant x$. De la dernière propriété, on tire $a \neq a \sim x$. Mais comme $a \sim x \leqslant a$, et que les seuls minorants de a sont a et 0, on en déduit que $a \sim x = 0$. Ainsi, de la première inégalité et de la distributivité, on tire :

$$a = a \sim (x \sim y) = (a \sim x) \sim (a \sim y) = 0 \sim (a \sim y) = a \sim y.$$

Cette égalité implique que $a \leqslant y$.

Comment pourraient-on appeler ce résultat ? Lemme d'Euclide par exemple ?

- (b) Récurrence immédiate ! Le cas $n = 1$ est trivial, le cas $n = 2$ (utilisé explicitement dans la preuve de l'hérédité) découle de la question précédente, et l'hérédité est immédiate.

3. Soit E l'ensemble des atomes de A , et $h : A \longrightarrow \mathcal{P}(E)$ définie par :

$$\forall x \in A, \quad h(x) = \{a \in E \mid a \leqslant x\}.$$

- (a) Nous rappelons que \cap est l'intersection dans $\mathcal{P}(E)$, et X^c représente $\complement_E X$. Nous avons donc à vérifier que pour tout $(x, y) \in A^2$, $h(x \cap y) = h(x) \cap h(y)$, et $h(x^c) = \complement_E h(x)$.

- On a :

$$h(x \cap y) = \{a \in E \mid a \leq x \cap y\} = \{a \in E \mid a \leq x \text{ et } a \leq y\} = \{a \in E \mid a \leq x\} \cap \{a \in E \mid a \leq y\} = h(x) \cap h(y).$$

- * Par ailleurs étant donné $a \in h(x^c)$, on a $a \leq x^c$. Si on avait aussi $x \leq a$, on aurait $a \leq x \cap x^c = 0$, donc $a \leq 0$, puis $a = 0$ (0 étant l'élément minimum). Cela contredit le fait qu'un atome est non nul. Ainsi, $a \not\leq x$, donc $a \notin h(x)$, donc $a \in \complement_E h(x)$. On en déduit une première inclusion $h(x^c) \subset \complement_E h(x)$.
- * Réciproquement, soit $a \in \complement_E h(x)$. Alors $a \not\leq x$. Mais comme $a \leq x \cup x^c = 1$, on déduit de la question précédente que $a \leq x^c$, d'où $a \in h(x^c)$. On a donc la seconde inclusion $\complement_E h(x) \subset h(x^c)$.
- * Des deux inclusions, il vient l'égalité $h(x^c) = \complement_E h(x)$

Ainsi, h est un homomorphisme d'algèbres de Boole

- (b) Soit $X = \{a_1, \dots, a_k\} \in \mathcal{P}(E)$, et $x = a_1 \cup \dots \cup a_k \in A$.

- Soit $a \in h(x)$. On a donc $a \leq a_1 \cup \dots \cup a_k$, et comme a est un atome, on déduit de la question 2(b) qu'il existe $i \in [1, k]$ tel que $a \leq a_i$. Comme a_i est un atome, $a = a_i$ ou $a = 0$, ce dernier étant impossible puisque a est un atome. Ainsi, $a = a_i$, donc $a \in X$. On a donc $h(x) \subset X$.
- Réciproquement, tout élément a_i de X vérifie $a_i \leq x$, car a_i est un des termes de la série de bornes supérieures définissant x . Ainsi, comme les a_i sont des atomes, $a_i \in h(x)$. On en déduit que $X \subset h(x)$.
- Des deux inclusions, il vient l'égalité : h(x) = X
- Tout sous-ensemble (non vide, et nécessairement fini puisque A l'est) X de $\mathcal{P}(E)$ admet un antécédent x par h ; c'est le cas aussi de $X = \emptyset$, dont un antécédent est 0 (seul élément de A n'étant pas minoré par un atome). Ainsi, h est surjective.

- (c) C'est un peu plus délicat. Soit $(x, y) \in A^2$ tels que $x \neq y$. Alors $x \cap y \neq x$ ou $x \cap y \neq y$ (sinon, on aurait à la fois $x \leq y$ et $y \leq x$, donc $x = y$). On peut supposer sans perte de généralité que $x \cap y \neq x$. Considérons alors :

$$x = x \cap 1 = x \cap (y \cup y^c) = (x \cap y) \cup (x \cap y^c).$$

Puisque $x \cap y \neq x$, on ne peut pas avoir $x \cap y^c = 0$. Ainsi, d'après la question 1, il existe un atome a minorant $x \cap y^c$. On a alors $a \in h(x)$ et $a \in h(y^c) = \complement_E h(y)$, donc $a \notin h(y)$. On a donc démontré que $h(x) \neq h(y)$.

Puisque pour tout $(x, y) \in A^2$, $x \neq y$ entraîne $f(x) \neq f(y)$, f est injective.

Ainsi, h est un homomorphisme injectif et surjectif, donc h est un isomorphisme d'algèbres de Boole.

Toute algèbre de Boole finie est donc isomorphe à l'algèbre des parties de l'ensemble de ses atomes.

Correction du problème 2 –

1. Convergence de la série définissant c

Soit, pour tout $n \in \mathbb{N}$, $S_n = \sum_{k=0}^n 10^{-k!}$.

- (a) On peut faire la comparaison de deux manières, soit en rajoutant des termes $10^{-\ell}$ manquant entre les termes présents, soit en majorant chacun des termes $10^{-k!}$ par 10^{-k} . On obtient alors (en prenant la deuxième méthode) :

$$\forall n \in \mathbb{N}, \quad \sum_{k=0}^n 10^{-k!} \leq \sum_{k=0}^n 10^{-k} = \frac{1 - 10^{-n+1}}{1 - 10^{-1}} \leq \frac{1}{1 - 10^{-1}} = \frac{10}{9}.$$

Ainsi, la suite (S_n)_{n ∈ N} est bornée.

- (b) Elle est aussi croissante, car pour tout $n \in \mathbb{N}$,

$$S_{n+1} - S_n = 10^{-(n+1)!} \geq 0.$$

Ainsi, étant croissante et majorée, (S_n) est convergente, donc c = $\sum_{k=0}^{+\infty} 10^{-k!}$ est bien défini.

2. Irrationnalité de c

(a) On utilise ici plutôt la première des majorations suggérées dans la première question. Soit $n \in \mathbb{N}$, et $N > n$.

On a alors :

$$\sum_{k=n+1}^N 10^{-k!} \leq \sum_{\ell=(n+1)!}^{(N+1)!} 10^{-\ell} = 10^{-(n+1)!} \frac{1 - 10^{-(N+1)!+(n+1)!-1}}{1 - 10^{-1}} \leq 10^{-(n+1)!} \cdot \frac{10}{9},$$

d'où finalement,

$$\sum_{k=n+1}^{+\infty} 10^{-k!} \leq \frac{1}{9 \cdot 10^{(n+1)!-1}}.$$

(b) Supposons qu'il existe deux entiers p et q tels que $c = \frac{p}{q}$. On a

$$\frac{p}{q} 10^{n!} = c 10^{n!} = S_n 10^{n!} + 10^{n!} \sum_{k=n+1}^N 10^{-k!},$$

donc

$$q S_n 10^{n!} < p 10^{n!} \leq q S_n 10^{n!} + \frac{10^{n!} q}{9 \cdot 10^{(n+1)!-1}} = q S_n 10^{n!} + \frac{q}{9 \cdot 10^{(n+1)!-n!-1}} = q S_n 10^{n!} + \frac{q}{9 \cdot 10^{n \cdot n!-1}}.$$

Comme $\frac{q}{9 \cdot 10^{n \cdot n!-1}} \rightarrow 0$ lorsque $n \rightarrow 0$, on en déduit qu'il existe une valeur de n telle que

$$\frac{q}{9 \cdot 10^{n \cdot n!-1}} < 1,$$

et donc

$$q S_n 10^{n!} < p 10^{n!} < q S_n 10^{n!} + 1.$$

Ainsi, l'entier $p 10^{n!}$ est strictement encadré entre deux entiers consécutifs ($S_n 10^{n!}$ étant entier comme somme des entiers $10^{n!-k!}$, avec $n! - k! \geq 0$). Ceci est impossible.

On en déduit que c est irrationnel.

3. Inégalité des accroissements finis

On peut soit utiliser l'inégalité triangulaire intégrale, soit (si vous ne la connaissez pas) revenir à un encadrement de f' : pour tout $x \in [a, b]$,

$$-M \leq f'(x) \leq M,$$

et par croissance de l'intégrale,

$$-\int_a^b M \, dx \leq \int_a^b f'(x) \, dx \leq \int_a^b M \, dx, \quad \text{soit:} \quad -(b-a)M \leq f(b) - f(a) \leq (b-a)M.$$

On a bien obtenu

$$|f(b) - f(a)| \leq M(b-a) \quad \text{soit:} \quad |f(b) - f(a)| \leq M|b-a|,$$

puisque $b-a > 0$. Si $b < a$, on obtient la même chose (il suffit d'inverser le rôle de a et b , et de remarquer que du fait des valeurs absolues, l'expression est symétrique en a et b), et pour $a=b$, le résultat est trivial.

4. Théorème de Liouville (approximation diophantienne)

Le but de cette question est de démontrer le théorème de Liouville, s'énonçant ainsi :

Théorème de Liouville. Soit α un nombre algébrique non rationnel. Alors il existe un réel $A > 0$ et un entier $d \geq 2$, tels que pour tout nombre rationnel $\frac{p}{q}$, $((p, q) \in \mathbb{Z} \times \mathbb{N}^*)$, on ait : $\left| \alpha - \frac{p}{q} \right| \geq \frac{A}{q^d}$.

Soit α un nombre algébrique, c'est-à-dire tel qu'il existe un polynôme P non nul à coefficients entiers vérifiant $P(\alpha) = 0$. On suppose de plus que α n'est pas rationnel.

On admettra dans cette question qu'une fonction continue sur un intervalle fermé est bornée.

- (a) Soit $E = \{\deg P \mid P \in \mathbb{Z}[X], P \neq 0, P(\alpha) = 0\}$. C'est un sous-ensemble non vide (car α est algébrique) de \mathbb{N} . D'après la propriété fondamentale de \mathbb{N} , E admet un minimum d . Comme $d \in E$, il existe un polynôme $P \in \mathbb{Z}[X]$ tel que $P \neq 0$ et $P(\alpha) = 0$, de degré minimal, tel que $d = \deg(P)$.
- (b) Le polynôme P ne peut pas être constant non nul, donc $d \neq 0$. Si $d = 1$, il existe a et b des entiers tels que $a\alpha + b = 0$, donc $\alpha = -\frac{b}{a}$, ce qui contredit le fait que α n'est pas rationnel. Ainsi, $d \geq 2$.
- (c) Si P admet une racine rationnelle q , on peut factoriser P :

$$P = (X - q)Q = (X - q)(a_{d-1}X^{d-1} + \cdots + a_1X + a_0),$$

et en notant $P = b_dX^d + \cdots + b_1X + b_0$, les b_i étant entiers, on obtient :

$$a_{d-1} = b_d \quad \forall k \in \llbracket 1, d-1 \rrbracket, \quad a_{k-1} - a_kq = b_k \quad \dots \quad - a_0q = b_0.$$

L'équation $a_{d-1} = b_d$ nous assure que a_{d-1} est rationnel, puis $a_{d-2} = b_{d-1} + qa_{d-1}$ est aussi rationnel, puis également $a_{d-3} = b_{d-2} + qa_{d-2}$ etc. Ainsi, le polynôme Q est à coefficients rationnels. Par ailleurs, puisque $P(\alpha) = 0$ et $(\alpha - q) \neq 0$, il vient $Q(\alpha) = 0$. Ainsi, α est racine d'un polynôme à coefficients rationnels de degré $d - 1$. Quitte à multiplier par le ppcm des dénominateurs des coefficients de Q , on obtient donc un polynôme à coefficients entiers de degré $d - 1$ dont α est racine, ce qui contredit la minimalité du degré de P .

Ainsi, P ne peut pas admettre de racine rationnelle.

- (d) En reprenant les notations de la question précédente, on a

$$q^d P\left(\frac{p}{q}\right) = \sum_{k=0}^d q^d b_k \left(\frac{p}{q}\right)^k = \sum_{k=0}^d b_k p^k q^{d-k}.$$

Tous les exposants étant positifs, les termes de cette somme sont tous entiers, donc $q^d P\left(\frac{p}{q}\right)$ est un entier. Par ailleurs, $q^d P\left(\frac{p}{q}\right) \neq 0$ d'après la question précédente. Par conséquent, $q^d P\left(\frac{p}{q}\right) \in \mathbb{Z}^*$, donc $|q^d P\left(\frac{p}{q}\right)| \geq 1$.

- (e) La fonction P' est continue sur $[\alpha - 1, \alpha + 1]$ (en tant que fonction polynomiale), donc elle est bornée sur cet intervalle d'après le résultat admis. Soit M un majorant de $|P'|$ sur $[\alpha - 1, \alpha + 1]$. Soit alors $\frac{p}{q} \in [\alpha - 1, \alpha + 1]$, $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$. Alors M est aussi un majorant de P' entre α et $\frac{p}{q}$, et P est dérivable de dérivée continue entre ces bornes. Ainsi, d'après l'inégalité des accroissements finis :

$$\left| P(\alpha) - P\left(\frac{p}{q}\right) \right| \leq M \left| \alpha - \frac{p}{q} \right|.$$

Puisque $P(\alpha) = 0$, et d'après la question précédente, il vient

$$\frac{1}{q^d} \leq \left| P\left(\frac{p}{q}\right) \right| \leq M \left| \alpha - \frac{p}{q} \right|.$$

Ainsi, pour tout nombre rationnel $\frac{p}{q} \in [\alpha - 1, \alpha + 1]$, on obtient :

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{1}{Mq^d}.$$

Remarquez la nécessité de choisir M avant α (pour qu'il ne dépende pas de α), et donc de devoir travailler dans un premier temps dans un intervalle fermé borné $[\alpha - 1, \alpha + 1]$ de longueur fixe. On récupère le cas de \mathbb{R} tout entier dans la question suivante.

- (f) Posons $A = \min\left(1, \frac{1}{M}\right)$. Soit $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$.
- Si $\frac{p}{q} \in [\alpha - 1, \alpha + 1]$, alors $\left| \alpha - \frac{p}{q} \right| \geq \frac{1}{Mq^d} \geq \frac{1}{Aq^d}$.
 - Sinon, $\left| \alpha - \frac{p}{q} \right| \geq 1 \geq \frac{1}{q^d} \geq \frac{1}{Aq^d}$, puisque $A \leq 1$.

Ainsi, nous venons de démontrer le théorème de Liouville.

5. Transcendance de c

On appelle *nombre de Liouville* un réel irrationnel x tel que :

$$\forall n \in \mathbb{N}^*, \quad \exists (p_n, q_n) \in \mathbb{Z} \times (\mathbb{N} \setminus \{0, 1\}), \quad \left| x - \frac{p_n}{q_n} \right| \leq \frac{1}{(q_n)^n}.$$

(a) Supposons que x est algébrique (et non rationnel d'après l'hypothèse). Il existe alors d'après le théorème de Liouville un entier d et un réel $A > 0$, qu'on se donne, tels que pour tout $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$, $\left| x - \frac{p}{q} \right| \geq \frac{A}{q^d}$.

On se donne également une suite (p_n, q_n) telle que dans la définition d'un nombre de Liouville. On a alors, pour tout $n \geq d$,

$$\frac{A}{(q_n)^d} \leq \left| x - \frac{p_n}{q_n} \right| \leq \frac{1}{(q_n)^n} = \frac{1}{(q_n)^d} \cdot \frac{1}{(q_n)^{n-d}} \leq \frac{1}{(q_n)^d} \cdot \frac{1}{2^{n-d}},$$

et en gardant que les termes extrêmes, il vient :

$$\forall n \geq d, \quad A \leq \frac{1}{2^{n-d}}.$$

En passant à la limite dans cette inégalité, on obtient $A \leq 0$, ce qui contredit l'hypothèse $A > 0$.

Ainsi, un nombre de Liouville est transcendant.

(b) Montrons que c est un nombre de Liouville. On a déjà montré dans la question 2 qu'il est irrationnel.

Par ailleurs, étant donné $n \in \mathbb{N}^*$, l'encadrement obtenu au cours de cette question s'écrivait :

$$S_n \leq c \leq S_n + 10^{-(n+1)!} \frac{10}{9}.$$

Comme $10^{n!} S_n$ est entier, on peut écrire $S_n = \frac{p_n}{q_n}$, où $p_n \in \mathbb{Z}$, et $q_n = 10^{n!} \geq 2$. On a alors

$$0 \leq c - \frac{p_n}{q_n} \leq \frac{1}{9 \cdot 10^{n!(n+1)-1}} = \frac{1}{q_n^n} \cdot \frac{1}{9 \cdot 10^{n!-1}} \leq \frac{1}{q_n^n}.$$

Ainsi, c est un nombre de Liouville, donc c est transcendant.