Module I.1 : Fondements

I.1.1 Il est bien évident que, si $a = a'$ et $b = b'$, alors $\{\{a\},\{a,b\}\} = \{\{a'\},\{a',b'\}\}$. Pour démontrer la réciproque, supposons que $\{\{a\},\{a,b\}\} = \{\{a'\},\{a',b'\}\}$ (méthode de l'hypothèse auxiliaire). Nous procéderons par disjonction de cas, selon que le membre de gauche de cette égalité est un singleton ou une paire.

Dans le premier cas, $\{a\} = \{a,b\}$, et $a = b$. Le membre droit de l'égalité est également un singleton, et $\{a'\} = \{a',b'\}$, d'où $a' = b'$. L'égalité se réécrit alors $\{\{a\}\} = \{\{a'\}\}$, qui entraîne $\{a\} = \{a'\}$, puis $a = a'$. On a donc $a = a' = b = b'$, et, en particulier, $a = a'$ et $b = b'$ comme désiré.

Dans le second cas, $\{a\} \neq \{a,b\}$, autrement dit, $a \neq b$. L'ensemble $\{\{a\},\{a,b\}\}$ a donc pour éléments un singleton et une paire. Il en est donc de même de l'ensemble $\{\{a'\},\{a',b'\}\}$. Dans ce dernier, la paire ne peut être $\{a'\}$, c'est donc $\{a',b'\}$. Ainsi, $\{a'\}$ (seul singleton) est égal à $\{a\}$ et $\{a',b'\}$ (seule paire) est égal à $\{a,b\}$. De la première égalité, on tire $a' = a$, donc, avec la seconde, $\{a,b\} = \{a,b'\}$. Comme $b \neq a$ et $b' \neq a' = a$ (on a des paires), on en déduit $b = b'$, comme désiré.

I.1.2 Pour la première question, procédons par équivalences :

$$X \in \mathcal{P}(A \cap B) \iff X \subset A \cap B \iff X \subset A \quad \text{et} \quad X \subset B$$
$$\iff X \in \mathcal{P}(A) \quad \text{et} \quad X \in \mathcal{P}(B) \iff X \in \mathcal{P}(A) \cap \mathcal{P}(B),$$

d'où la conclusion : $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

Supposons maintenant A et B disjoints : $A \cap B = \varnothing$. Pour toute partie X de $A \cup B$, on peut écrire $X = Y \cup Z$, où $Y := (X \cap A) \in \mathcal{P}(A)$ et $Z := (X \cap B) \in \mathcal{P}(B)$. Introduisons deux applications :

$$\begin{array}{rcl} \mathcal{P}(A \cup B) & \stackrel{\varphi}{\to} & \mathcal{P}(A) \times \mathcal{P}(B) \\ X & \mapsto & (X \cap A, X \cap B), \end{array}$$

et

$$\begin{array}{rcl} \mathcal{P}(A) \times \mathcal{P}(B) & \stackrel{\psi}{\to} & \mathcal{P}(A \cup B) \\ (Y,Z) & \mapsto & Y \cup Z. \end{array}$$

Le raisonnement précédent montre que $X = \psi\big(\varphi(X)\big)$.

Par ailleurs, pour tout $(Y,Z) \in \mathcal{P}(A) \times \mathcal{P}(B)$:

$$\varphi\big(\psi(Y,Z)\big) = \varphi(Y \cup Z) = \big((Y \cup Z) \cap A, (Y \cup Z) \cap B\big) = (Y,Z),$$

car $(Y \cup Z) \cap A = (Y \cap A) \cup (Z \cap A) = Y \cup \varnothing = Y$, et similairement pour Z. Les applications φ et ψ sont donc réciproques l'une de l'autre. On voit donc que, *lorsque A et B sont supposés disjoints*, $\mathcal{P}(A \cup B)$ est, de manière naturelle, en bijection avec $\mathcal{P}(A) \times \mathcal{P}(B)$.

I.1.3 1) Comme $E_0 = \varnothing$, tous ses éléments en sont des sous-ensembles et la propriété à démontrer est trivialement vraie pour $k = 0$. Supposons (hypothèse de récurrence) que, pour un certain $k \in \mathbb{N}$, tout élément de E_k en est un sous-ensemble. Les éléments de $E_{k+1} = E_k \cup \{E_k\}$ sont d'une part ceux de E_k, d'autre part, E_k lui même. Les premiers sont des sous-ensembles

de E_k (hypothèse de récurrence), donc de E_{k+1} puisque $E_k \subset E_{k+1}$. Le dernier est sous-ensemble de E_{k+1} par construction.
2) Puisque $E_0 = \varnothing$ et que E_1 est un singleton, donc non vide, l'inclusion $E_0 \subset E_1$ est stricte. Supposons (hypothèse de récurrence) que, pour un certain $k \in \mathbb{N}$, $E_{k+1} \neq E_k$, autrement dit, que l'inclusion $E_k \subset E_{k+1}$ est stricte.
Démontrons par l'absurde que $E_{k+2} \neq E_{k+1}$.
Si l'on avait $E_{k+2} = E_{k+1}$, de l'égalité $E_{k+2} = E_{k+1} \cup \{E_{k+1}\}$, on déduirait que $E_{k+1} \in E_{k+1} = E_k \cup \{E_k\}$. Comme, par hypothèse de récurrence, $E_{k+1} \neq E_k$, on aurait donc $E_{k+1} \in E_k$ donc, d'après la question 1, $E_{k+1} \subset E_k$, donc $E_{k+1} = E_k$, contradiction. On a bien prouvé (par l'absurde) que $E_{k+2} \neq E_{k+1}$ pour cet entier k, donc (par récurrence) que $E_{k+1} \neq E_k$ pour tout k. Comme $E_k \subset E_{k+1}$, on a bien une suite strictement croissante pour l'inclusion. Chacun de ces ensembles a exactement un élément de plus que le précédent ; comme E_0 a 0 éléments, chaque E_k a k éléments. Cela sera précisé dans la solution de l'exercice I.1.29 de la page 59.

I.1.4 1) Supposons l'axiome de fondation vrai. Soit $(x_n)_{n\in\mathbb{N}}$ une suite d'ensembles telle que $\forall i \in \mathbb{N}\ ,\ x_{i+1} \in x_i$. Soit $x = \{x_i \mid i \in \mathbb{N}\}$ l'image de cette suite : cet ensemble n'est évidemment pas vide. D'après l'axiome de fondation, il existe donc $y \in x$ tel que $y \cap x = \varnothing$. Cet élément y de x est l'un des x_i (par définition de x), et l'on a alors $x_{i+1} \in x_i$ et $x_{i+1} \in x$, ce qui contredit la condition $y \cap x = \varnothing$; ainsi, une telle suite n'existe pas. Nous démontrerons la réciproque par contraposée, autrement dit, nous prouverons que la négation de l'axiome de fondation implique l'existence d'une suite $(x_n)_{n\in\mathbb{N}}$ telle que $\forall i \in \mathbb{N}\ ,\ x_{i+1} \in x_i$. La négation de l'axiome de fondation dit qu'il existe un ensemble $x \neq \varnothing$ tel que, pour tout $y \in x$, $y \cap x \neq \varnothing$. Nous prenons alors pour x_0 un élément quelconque de x (c'est possible puisque x est non vide). Appliquant la négation de l'axiome de fondation à $y = x_0$, nous trouvons $x_1 \in x \cap x_0$. Par récurrence, appliquant la négation de l'axiome de fondation à $y = x_k$, nous trouvons $x_{k+1} \in x \cap x_k$. La suite $(x_n)_{n\in\mathbb{N}}$ ainsi construite vérifie bien $\forall i \in \mathbb{N}\ ,\ x_{i+1} \in x_i$.
2) Si l'on avait $x \in x$, la suite constante $x_n = x$ vérifierait $\forall i \in \mathbb{N}\ ,\ x_{i+1} \in x_i$ et contredirait donc l'axiome de fondation (question 1). S'il existait un ensemble x de tous les ensembles, il serait évidemment élément de lui-même !
3) Puisque $x \subset s(x)$, on a une suite croissante pour la relation d'inclusion (qui est une relation d'ordre). Il suffit de démontrer que la suite est strictement croissante, c'est-à-dire que $x \neq s(x)$. Comme $s(x) = x \cup \{x\}$, cela équivaut à $x \notin x$, qui découle de l'axiome de fondation (question 2).
4) Les deux relations indiquées portent sur x seul (la lettre y étant en réalité muette) ; notons les $A(x)$ et $B(x)$. Comme par hypothèse $\forall y\ ,\ y \notin y$, le prédicat $A(x)$ dit que x est vide. Il est collectivisant, et l'on trouve :

$$\{x \mid (\forall y \in x\ ,\ y \in y)\} = \{\varnothing\}.$$

Pour la même raison, le prédicat $B(x)$ est vrai pour tout ensemble x. S'il était collectivisant, il existerait donc un ensemble de tous les ensembles.

I.1.5 Si c, d, e sont deux à deux distincts, il n'existe aucune surjection de E sur F. Dans le cas contraire, il y a des surjections. Si $c = d = e$, il n'existe aucune injection de E dans F. Dans le cas contraire, il y a au moins deux éléments distincts dans F et il existe des injections de E dans F. Il y a des bijections de E dans F si, et seulement si, F a deux éléments distincts, c'est-à-dire si, et seulement si, l'on est dans l'un des cas suivants : $c = d \neq e$, $c = e \neq d$, $e = d \neq c$.

I.1.6 Si $B = f\big(f^{-1}(B)\big)$, comme $f^{-1}(B) \subset E \Rightarrow f\big(f^{-1}(B)\big) \subset f(E)$, on a $B \subset f(E) = \operatorname{Im} f$.

Supposons réciproquement que $B \subset \operatorname{Im} f$. On a $f\big(f^{-1}(B)\big) \subset B$ (indépendamment de l'hypothèse) par définition de $f^{-1}(B)$. Prouvons l'inclusion réciproque. Soit $y \in B$; comme $B \subset \operatorname{Im} f$, il existe $x \in E$ tel que $f(x) = y$. Par définition de $f^{-1}(B)$, $x \in f^{-1}(B)$; donc $y = f(x) \in f\big(f^{-1}(B)\big)$. Cela étant vérifié par tout $y \in B$, on a bien l'inclusion $B \subset f\big(f^{-1}(B)\big)$.

Notons que l'on a en fait, *sans aucune hypothèse*, $f\big(f^{-1}(B)\big) = B \cap \operatorname{Im} f$.

I.1.7 Vérifions (bien que l'énoncé ne le demande pas expressément) l'équivalence :

$$A = f^{-1}\big(f(A)\big) \Leftrightarrow \big(\forall x \in A\ ,\ \forall x' \in E\ :\ f(x) = f(x') \Rightarrow x' \in A\big).$$

Supposons d'abord $A = f^{-1}\big(f(A)\big)$, et soient $x \in A$ et $x' \in E$ tels que $f(x) = f(x')$. Alors $f(x') \in f(A)$, d'où $x' \in f^{-1}\big(f(A)\big) = A$. Supposons réciproquement que l'on a l'implication $\forall x \in A\ ,\ \forall x' \in E\ :\ f(x) = f(x') \Rightarrow x' \in A$ et prouvons l'égalité $A = f^{-1}\big(f(A)\big)$ par double inclusion. L'inclusion $A \subset f^{-1}\big(f(A)\big)$ est vraie sans aucune hypothèse, par définition de l'image réciproque $f^{-1}\big(f(A)\big)$. Soit donc $x' \in f^{-1}\big(f(A)\big)$, de sorte que $f(x') \in f(A)$: on a donc $f(x') = f(x)$ pour un $x \in A$, et l'hypothèse faite entraîne que $x' \in A$. On a donc démontré l'inclusion $f^{-1}\big(f(A)\big) \subset A$, donc l'égalité voulue.

Soit maintenant A une partie saturée. Alors, par définition, $A = f^{-1}(B)$ avec $B = f(A)$. Soit réciproquement $A = f^{-1}(B)$, avec $B \subset F$, et montrons que A est saturée en utilisant l'équivalence. Il faut prendre $x \in A$ et $x' \in E$ tels que $f(x) = f(x')$ et en déduire que $x' \in A$. Mais $f(x) \in B$, d'où $f(x') \in B$, d'où $x' \in f^{-1}(B) = A$.

I.1.8 Tout d'abord, il doit y avoir un ensemble F tel que f est une application de E dans F et g une application de F dans E.

Si l'on applique les deux dernières des « nombreuses règles » de la page 17 (celles qui y sont démontrées), on voit que g est surjective (car $g \circ f$ l'est) et que f est injective (car $g \circ f$ l'est). On ne peut pas dire mieux, comme le montre l'exemple suivant. On prend $E := \{a\}$, $F := \{b, c\}$ (avec $b \neq c$) ; puis pour f l'application $a \mapsto b$ et pour g l'unique application possible. Alors $g \circ f = \mathrm{Id}_E$ et f n'est pas surjective et g pas injective.

I.1.9 (i) Si $f = f' \circ u$, alors $\operatorname{Im} f = f(E) = f'(u(E)) \subset f'(F) = \operatorname{Im} f'$. Supposons réciproquement que $\operatorname{Im} f \subset \operatorname{Im} f'$. On définit une application $u : E \to E'$ de la manière suivante : pour tout $x \in E$, $f(x) \in \operatorname{Im} f \subset \operatorname{Im} f'$, et il existe donc au moins un antécédent $x' \in E'$ tel que $f(x) = f'(x')$. On pose alors $u(x) = x'$ pour l'un quelconque de ces antécédents x'. Il est immédiat que l'on a $f(x) = (f' \circ u)(x)$. Cela étant vrai pour tout $x \in E$, on a bien $f = f' \circ u$.

(ii) Si $f' = v \circ f$, on a les implications :

$$f(x_1) = f(x_2) \Longrightarrow v\big(f(x_1)\big) = v\big(f(x_2)\big) \Longrightarrow f'(x_1) = f'(x_2).$$

Supposons réciproquement que l'implication $f(x_1) = f(x_2) \Rightarrow f'(x_1) = f'(x_2)$ est vérifiée. On définit une application $v : F \to F'$ de la manière suivante : soit $y \in F$; si $y \notin \operatorname{Im} f$, on

prend pour $v(y)$ un élément arbitraire de F'. Si $y \in \operatorname{Im} f$, quels que soient les antécédents $x_1, x_2 \in E$ de y par f, on a $f(x_1) = f(x_2) = y$, d'où, par hypothèse, $f'(x_1) = f'(x_2) = y'$. On choisit alors pour $v(y)$ cet élément $y' \in F'$, qui est bien défini indépendamment du choix de l'antécédent de y. Il est immédiat que l'on a bien $f' = v \circ f$.
Remarquons toutefois que *cette démonstration n'est valable que si l'on suppose* $F' \neq \varnothing$: il a en effet fallu choisir un élément arbitraire de F'. Dans le cas où $F' = \varnothing$, on a nécessairement $E = \varnothing$ (sinon, il n'y aurait pas d'application f'), mais la conclusion n'est pas correcte.

I.1.10 Notons, pour simplifier ce qui suit, ψ l'application étudiée. Nous allons commencer par traiter trois cas particuliers.
Supposons d'abord que E est vide. Alors $\mathcal{F}(E, F)$ et les $\mathcal{F}(E_i, F)$ sont tous des singletons, et ψ est toujours bijective. Dorénavant, nous supposerons donc que E n'est pas vide.
Supposons ensuite que F est vide (et E non vide). On sait que, dans ce cas, $\mathcal{F}(E, F)$ est vide. Puisque sa source est vide, ψ est injective. Elle est surjective (et donc bijective) si, et seulement si, son but est vide, c'est-à-dire si, et seulement si, l'un des $\mathcal{F}(E_i, F)$ est vide, c'est-à-dire si, et seulement si, l'un des E_i est non vide.
Supposons enfin que F est un singleton. Alors $\mathcal{F}(E, F)$ et les $\mathcal{F}(E_i, F)$ sont tous des singletons, et ψ est toujours bijective.
Nous supposerons dorénavant que E est non vide et que F a au moins deux éléments distincts.
Nous démontrerons que ψ est injective (resp. surjective) si, et seulement si, $(E_i)_{i\in I}$ est un recouvrement de E (resp. les E_i sont deux à deux disjoints).
Supposons que $(E_i)_{i\in I}$ soit un recouvrement de E, c'est-à-dire que $\bigcup_{i\in I} E_i = E$. Alors toute application f de E dans F est totalement déterminée par ses restrictions $f_i := f_{|E_i}$, de sorte que l'application étudiée est injective. Si les E_i ne recouvrent pas E, soit $x \in E$ qui n'appartient à aucun E_i, et soit f une application quelconque de E dans F. on peut définir une application g qui prend les mêmes valeurs que f, sauf que $f(x) \neq g(x)$ (c'est possible précisément parce que F a au moins deux éléments). Alors f et g ont même image par ψ, qui n'est donc pas injective. La première équivalence est démontrée.
Supposons que les E_i soient deux à deux disjoints. Si l'on se donne une famille $(f_i)_{i\in I}$ de $\prod_{i\in I} \mathcal{F}(E_i, F)$, on peut définir $f : E \to F$ qui prend sur chaque E_i les mêmes valeurs que f_i et qui prend des valeurs arbitraires hors de $\bigcup_{i\in I} E_i$. Cela montre que ψ est surjective. S'il existe $i \neq j$ et $x \in E_i \cap E_j$, en choisissant f_i et f_j telles que $f_i(x) \neq f_j(x)$, on voit qu'elles ne peuvent être restrictions d'une même application f. L'application ψ n'est donc pas surjective. La deuxième équivalence est démontrée.
Les arguments qui précèdent montrent que, pour que $(f_i)_{i\in I} \in \prod_{i\in I} \mathcal{F}(E_i, F)$ soit dans $\operatorname{Im}\psi$, autrement dit, pour que les $f_i : E_i \to F$ soient les restrictions d'une même application $f : E \to F$, il faut, et il suffit, que :

$$\forall i, j \in I \ , \ f_{i|E_i\cap E_j} = f_{j|E_i\cap E_j}.$$

I.1.11 Remarquons tout d'abord que, si une loi admet un élément neutre e, il est idempotent et simplifiable ; et que c'est le seul élément à la fois idempotent et simplifiable.
Dans $(\mathcal{P}(E), \cup)$, le neutre est $\varnothing$, et c'est l'unique élément simplifiable, donc l'unique élément inversible. L'unique élément absorbant est E et tous les éléments sont idempotents.

Dans $(\mathcal{P}(E), \cap)$, le neutre est E, et c'est l'unique élément simplifiable, donc l'unique élément inversible. L'unique élément absorbant est $\varnothing$ et tous les éléments sont idempotents.

I.1.12 Soit $f : (A, \star) \to (B, \top)$ un morphisme.
Si $a \star a = a$, alors $f(a) \top f(a) = f(a \star a) = f(a)$: l'image d'un idempotent par f est bien un idempotent.
Si $E \subset E'$, l'inclusion canonique $\mathcal{P}(E) \subset \mathcal{P}(E')$ définit un morphisme de $(\mathcal{P}(E), \cup)$ dans $(\mathcal{P}(E'), \cup)$ et un morphisme de $(\mathcal{P}(E), \cap)$ dans $(\mathcal{P}(E'), \cap)$. De l'exercice précédent découlent alors les conclusions voulues.

I.1.13 Pour composer r éléments égaux à x avec une opération binaire $\star$, on doit écrire $a \star b$, où a est obtenu en composant p éléments égaux à x et b est obtenu en composant q éléments égaux à x avec $p + q = r$. Pour chaque couple $(p, q) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que $p + q = n$, on obtient ainsi $c_{p-1}c_{q-1}$ couples (a, b). On en déduit l'égalité $c_{r-1} = \sum_{p+q=r} c_{p-1}c_{q-1}$. Les changements d'indices $n = r - 1$, $i = p - 1$, $j = q - 1$ donnent la relation voulue. Comme $c_0 = c_1 = 1$ et $c_2 = 2$, on trouve successivement : $c_3 = c_0c_2 + c_1^2 + c_2c_0 = 5$, puis $c_4 = c_0c_3 + c_1c_2 + c_2c_1 + c_3c_0 = 14$. Par exemple, les cinq compositions mettant en jeu quatre éléments égaux à x sont : $x\star\big(x\star(x\star x)\big)$, $x\star\big((x\star x)\star x\big)$, $(x\star x)\star(x\star x)$, $\big((x\star x)\star x\big)\star x$ et $\big(x\star(x\star x)\big)\star x$.

I.1.14 Notons $\star$ la loi et $m : E \times E \to E$ l'application $(x, y) \mapsto x \star y$. L'associativité se traduit par des formules du type $m\big(m(x, y), z\big) = m\big(x, m(y, z)\big)$ et la commutativité par des formules du type $m(x, y) = m(y, x)$.
Pour traduire l'associativité en diagramme, on remarque que :

$$\big(m(x, y), z\big) = (m \times \mathrm{Id}_E)\big((x, y), z\big).$$

De même, $m\big(x, m(y, z)\big) = (Id_E \times m)\big(x, (y, z)\big)$. On obtient finalement le diagramme commutatif de gauche ci-dessous. Comme expliqué dans le cours, on a froidement identifié à $E \times E \times E$ les ensembles $(E \times E) \times E$ et $E \times (E \times E)$.
Pour traduire la commutativité en diagramme, on remarque que $(y, x) = <p_2, p_1>(x, y)$. On obtient finalement le diagramme commutatif de droite ci-dessous.

$$\begin{array}{ccc} E \times E \times E & \xrightarrow{m \times \mathrm{Id}_E} & E \times E \\ \downarrow{\scriptstyle \mathrm{Id}_E \times m} & & \downarrow{\scriptstyle m} \\ E \times E & \xrightarrow{\quad m \quad} & E \end{array} \qquad \begin{array}{ccc} E \times E & \xrightarrow{<p_2, p_1>} & E \times E \\ & \searrow^{m} & \downarrow{\scriptstyle m} \\ & & E \end{array}$$

I.1.15 Il est immédiat que $\complement_E A \subset B \Leftrightarrow A \cup B = E$ et que $B \subset \complement_E A \Leftrightarrow A \cap B = \varnothing$. Sous cette forme, les relations sont visiblement symétriques.

I.1.16 Notons $\mathcal{R}$ l'intersection des $\mathcal{R}_i$. Alors la relation $x \mathcal{R} y$ équivaut à : $x - y$ est multiple de $n_1, \ldots, n_k$, autrement dit, à : $x - y$ est multiple de $\mathrm{ppcm}(n_1, \ldots, n_k)$. Ainsi, l'intersection des $\mathcal{R}_i$ est la relation de congruence modulo $\mathrm{ppcm}(n_1, \ldots, n_k)$.

I.1.17 On a vu dans le cours que $\mathcal{R}$ est bien une relation d'équivalence. Soit W' un supplémentaire de W. L'égalité $V = W \oplus W'$ entraîne :

$$\forall v \in V \ , \ \exists! w' \in W' \ : \ v - w' \in W.$$

En effet, dans cette écriture, w' est le projeté de v sur W' parallèlement à W. La relation ci-dessus se réécrit :

$$\forall v \in V \ , \ \exists! w' \in W' \ : \ v \ \mathcal{R} \ w'.$$

Sous cette forme, elle dit exactement que W' est un ensemble de représentants pour $\mathcal{R}$.

I.1.18 Considérons trois suites $\underline{u} = (u_n)_{n\in\mathbb{N}}$, $\underline{v} = (v_n)_{n\in\mathbb{N}}$ et $\underline{w} = (w_n)_{n\in\mathbb{N}}$. Pour démontrer la réflexivité : $\underline{u} \sim \underline{u}$, il suffit de prendre $p = 0$ dans la relation qui définit $\sim$. Pour démontrer la symétrie, on observe que, si $\underline{u} \sim \underline{v}$, l'entier p tel que $\forall n \geqslant p \ , \ u_n = v_n$ est aussi tel que $\forall n \geqslant p \ , \ v_n = u_n$, d'où $\underline{v} \sim \underline{u}$. Pour démontrer la transitivité, supposons que $\underline{u} \sim \underline{v}$ et $\underline{v} \sim \underline{w}$. Il existe donc $p \in \mathbb{N}$ tel que $\forall n \geqslant p \ , \ u_n = v_n$ et $q \in \mathbb{N}$ tel que $\forall n \geqslant p \ , \ v_n = w_n$. Soit $r = \max(p, q)$ le plus grand de ces deux entiers. Alors, pour tout $n \geqslant r$, on a $u_n = v_n$ (car $n \geqslant p$) et $v_n = w_n$ (car $n \geqslant q$), donc $u_n = w_n$. Ainsi : $\forall n \geqslant r \ , \ u_n = w_n$, et l'on a bien $\underline{u} \sim \underline{w}$.

I.1.19 1) Le plus simple est ici de considérer l'ordre strict associé. Il est défini par : $(u_n)_{n\in\mathbb{N}} < (v_n)_{n\in\mathbb{N}}$ si, et seulement s'il existe $p \in \mathbb{N}$ tel que $u_p < v_p$ et $\forall n < p \ , \ u_n = v_n$. Il s'agit alors de démontrer que cette relation est antiréflexive (on n'a jamais $\underline{u} < \underline{u}$) et transitive. Le premier point est évident (il ne peut exister de $p \in \mathbb{N}$ tel que $u_p < u_p$). Supposons donc $\underline{u} < \underline{v}$ et $\underline{v} < \underline{w}$. Soient p un entier tel que $u_p < v_p$ et $\forall n < p \ , \ u_n = v_n$, et q un entier tel que $v_q < w_q$ et $\forall n < q \ , \ v_n = w_n$. Nous distinguerons trois cas :

1. Si $p < q$, on a $\forall n < p \ , \ u_n = v_n = w_n \Rightarrow u_n = w_n$, et $u_p < v_p = w_p \Rightarrow u_p < w_p$;
2. si $p = q$, on a $\forall n < p \ , \ u_n = v_n = w_n \Rightarrow u_n = w_n$, et $u_p < v_p < w_p \Rightarrow u_p < w_p$;
3. si $q < p$, on a $\forall n < q \ , \ u_n = v_n = w_n \Rightarrow u_n = w_n$, et $u_q = v_q < w_q \Rightarrow u_q < w_q$.

Dans tous les cas, on en déduit que $\underline{u} < \underline{w}$ et la relation est bien transitive.
Pour démontrer que l'ordre est total, on considère deux suites $\underline{u} \neq \underline{v}$. Soit p le plus petit entier tel que $u_p \neq v_p$ (il en existe par hypothèse). On a donc $\forall n < p \ , \ u_n = v_n$. Si $u_p < v_p$, alors $\underline{u} < \underline{v}$ et si $v_p < u_p$, alors $\underline{v} < \underline{u}$.
2) Soient $A, B \subset \mathbb{N}$ et soient $\underline{u}, \underline{v} \in \{0,1\}^{\mathbb{N}}$ les suites associées. Alors $\underline{u} \neq \underline{v}$ signifie que la différence symétrique $A \oplus B := (A \setminus B) \cup (B \setminus A)$ est non vide (car $A \oplus B = \varnothing \Leftrightarrow A = B$), et la relation stricte $\underline{u} < \underline{v}$ signifie que le plus petit élément de $A \oplus B$ appartient à $B \setminus A$.
3) Tout entier $n \in \mathbb{N}$ s'écrit de manière unique sous la forme $n = \sum_{k\geqslant 0} \beta_k 2^k$, où les chiffres binaires (ou bits) $\beta_k \in \{0,1\}$ sont nuls à partir d'un certain rang. Se donner une telle écriture revient à se donner l'ensemble fini $A := \{k \in \mathbb{N} \mid \beta_k = 1\} \subset \mathbb{N}$, et l'on a alors $n = \sum_{a\in A} 2^a$.
L'application de l'énoncé est donc bien une bijection de $\mathcal{P}_f(\mathbb{N})$ sur $\mathbb{N}$.
4) Si $A \mapsto n$ et $B \mapsto p$, il s'agit décrire une condition nécessaire et suffisante portant sur A et B pour que $n < p$. On sait que cela équivaut à la condition : le bit de plus fort poids qui diffère entre les écritures de n et p vaut 0 pour n et 1 pour p, autrement dit, le plus grand élément de $A \oplus B$ appartient à $B \setminus A$.

I.1.20 De manière générale, notons $\overline{\mathcal{R}}$ la clôture réflexive transitive d'une relation $\mathcal{R}$ sur l'ensemble E. On a l'équivalence :

$$a\ \mathcal{R}\ b \Longleftrightarrow \exists a_0, \ldots, a_n \in E\ :\ a = a_0\ ,\ b = a_n \quad \text{et} \quad \forall i \in [\![0, n-1]\!], a_i\ \mathcal{R}\ a_{i+1}.$$

En effet, la relation $\mathcal{S}$ définie par le membre droit de l'équivalence logique est réflexive transitive et contient $\mathcal{R}$ (c'est évident) ; et, pour toute relation réflexive transitive $\mathcal{T}$ qui contient $\mathcal{R}$, on a les implications :

$$(\forall i \in [\![0, n-1]\!], a_i\ \mathcal{R}\ a_{i+1}) \Longrightarrow (\forall i \in [\![0, n-1]\!], a_i \mathcal{T} a_{i+1}) \Longrightarrow a_0 \mathcal{S} a_n,$$

autrement dit, $\mathcal{T}$ contient $\mathcal{S}$. La relation $\mathcal{S}$ est donc bien la plus petite relation réflexive transitive qui contient $\mathcal{R}$, c'est-à-dire, par définition, $\overline{\mathcal{R}}$.
Supposons maintenant $\mathcal{R}$ symétrique. Il est alors immédiat que la relation $\mathcal{S}$ définie ci-dessus est symétrique, car on a les implications :

$$(\forall i \in [\![0, n-1]\!], a_i\ \mathcal{R}\ a_{i+1}) \Longrightarrow (\forall i \in [\![0, n-1]\!], a_{i+1}\ \mathcal{R}\ a_i) \Longrightarrow a_n \mathcal{S} a_0.$$

Autrement dit, $\overline{\mathcal{R}}$ est symétrique. Comme elle est réflexive transitive, c'est bien une relation d'équivalence.

I.1.21 Dire qu'il existe un cycle pour $\mathcal{R}$ équivaut à dire qu'il existe $x \neq y$ tels que (avec les notations de l'exercice précédent) $x\overline{\mathcal{R}}y$ et $y\overline{\mathcal{R}}x$, *i.e.* que $\overline{\mathcal{R}}$ n'est pas antisymétrique. Prouvons maintenant l'équivalence annoncée.
Si $\mathcal{R}$ engendre une relation d'ordre $\mathcal{S}$, celle-ci est réflexive transitive et elle contient donc la clôture réflexive transitive $\overline{\mathcal{R}}$. Comme $\mathcal{S}$ est antisymétrique, $\overline{\mathcal{R}}$ l'est également, ce qui a deux conséquences : $\mathcal{R}$ n'admet pas de cycles (selon l'argument ci-dessus) ; $\overline{\mathcal{R}}$ est une relation d'ordre, donc la relation d'ordre engendrée par $\mathcal{R}$.
Si $\mathcal{R}$ n'admet pas de cycle, on a vu que $\overline{\mathcal{R}}$ est antisymétrique. C'est donc une relation d'ordre, et $\mathcal{R}$ engendre bien une relation d'ordre.

I.1.22 Montrons d'abord par récurrence que $E_k = \{E_0, \ldots, E_{k-1}\}$. C'est vrai pour $k = 0$ par convention (ensemble vide) et pour $k = 1$ puisque $E_0 = \varnothing$ et $E_1 = \{\varnothing\}$.
Supposons que $E_k = \{E_0, \ldots, E_{k-1}\}$. Alors :

$$E_{k+1} = E_k \cup \{E_k\} = \{E_0, \ldots, E_{k-1}\} \cup \{E_k\} = \{E_0, \ldots, E_k\},$$

ce qui achève la preuve.
La relation $x \in y$ sur E_k est donc équivalente à la relation d'inclusion stricte, qui est bien une relation d'ordre stricte. C'est donc encore une relation d'ordre stricte sur $\bigcup\limits_{k \in \mathbb{N}} E_k$.

I.1.23 La preuve que l'on a bien une relation d'ordre est exactement la même qu'à la question 1 de l'exercice V ; de même pour la preuve que cet ordre est total si ceux des E_i le sont.
Supposons maintenant I fini et les E_i bien ordonnés. Puisque I est bien ordonné, on peut aussi bien prendre $I = [\![1, n]\!]$ (car tout ensemble totalement ordonné à n éléments est isomorphe à $[\![1, n]\!]$ muni de l'ordre naturel). On sait déjà que $E = \prod\limits_{i \in I} E_i$ est totalement ordonné.
Il suffit donc de vérifier qu'il est artinien, autrement dit, que toute suite décroissante de E est

stationnaire. Notons $\underline{x}_p = (x_1^{(p)}, \dots, x_n^{(p)})$ le terme général (d'indice $p \in \mathbb{N}$) d'une telle suite décroissante. Par définition de l'ordre lexicographique, la suite $(x_1^{(p)})_{p\in\mathbb{N}}$ de E_1 est décroissante. Comme E_1 est bien ordonné, cette suite est stationnaire, donc constante à partir d'un certain rang $p_1 \in \mathbb{N}$. La suite décroissante $(\underline{x}_p)_{p\geqslant p_1}$ de E est formée de termes ayant tous la même première composante, puisque $(x_1^{(p)})_{p\geqslant p_1}$ est constante. Par définition de l'ordre lexicographique, cela entraîne que la suite $(x_2^{(p)})_{p\geqslant p_1}$ de E_2 est décroissante. Comme E_2 est bien ordonné, cette suite est stationnaire, donc constante à partir d'un certain rang $p_2 \geqslant p_1$. Réitérant cet argument, on construit successivement des entiers $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_n$ tels que, pour tout $k \in [\![1, n]\!]$, les suites $(x_i^{(p)})_{p\geqslant p_k}$ $(1 \leqslant i \leqslant k)$ sont constantes. En particulier, la suite $(\underline{x}_p)_{p\geqslant p_n}$ de E est constante.

I.1.24 Soit $(E_n)_{n\in\mathbb{N}}$ une suite décroissante de parties finies de E. Alors $(\operatorname{card} E_n)_{n\in\mathbb{N}}$ est une suite décroissante d'entiers naturels, donc elle stationne à partir d'un certain rang n_0. Pour tout entier $n \geqslant n_0$, on a donc $E_{n+1} \subset E_n$ et $\operatorname{card} E_{n+1} = \operatorname{card} E_n$, donc $E_{n+1} = E_n$. La suite $(E_n)_{n\in\mathbb{N}}$ stationne donc au rang n_0.

I.1.25 Soit $(x_n)_{n\in\mathbb{N}}$ une suite strictement décroissante de E. Alors $\big(f(x_n)\big)_{n\in\mathbb{N}}$ est une suite strictement décroissante de $\mathbb{N}$, ce qui est impossible. Cela montre que E est artinien. Prenons pour E l'ensemble des parties finies d'un ensemble X ayant au moins deux éléments $x \neq y$ (E est ordonné par l'inclusion) et pour f l'application card. Celle-ci est strictement croissante, car si A est strictement inclus dans B (et qu'ils sont finis), alors $\operatorname{card} A < \operatorname{card} B$. On obtient ainsi un exemple où E n'est pas totalement ordonné (car $\{x\}$ et $\{y\}$ ne sont pas comparables).

I.1.26 Soit $\aleph$ le cardinal de l'ensemble E de tous les ensembles. Comme toute partie de E est un ensemble, c'est un élément de E, et l'on a $\mathcal{P}(E) \subset E$, donc $2^{\aleph} \leqslant \aleph$, ce qui est impossible.

I.1.27 On montre ces formules par des bijections explicites. Soient E_1, E_2 et E_3 des ensembles de cardinaux respectifs $\aleph_1$, $\aleph_2$ et $\aleph_3$. On peut de plus (et on le fera) supposer que E_2 et E_3 sont disjoints.

Notons p_1 et p_2 les projections de $E_1 \times E_2$ sur E_1 et sur E_2. L'application $f \mapsto (p_1 \circ f, p_2 \circ f)$ est une bijection de $\mathcal{F}(E_3, E_1 \times E_2)$ sur $\mathcal{F}(E_3, E_1) \times \mathcal{F}(E_3, E_2)$, dont la bijection réciproque est $(u, v) \mapsto <u, v>$. On en déduit la première formule.

L'exercice I.1.10 donne une bijection de $\mathcal{F}(E_2 \cup E_3, E_1)$ sur $\mathcal{F}(E_2, E_1) \times \mathcal{F}(E_3, E_1)$. On en déduit la deuxième formule.

Nous allons maintenant définir deux applications :

$$\varphi : \mathcal{F}\big(E_3, \mathcal{F}(E_2, E_1)\big) \to \mathcal{F}(E_3 \times E_2, E_1)$$
$$\psi : \mathcal{F}(E_3 \times E_2, E_1) \to \mathcal{F}\big(E_3, \mathcal{F}(E_2, E_1)\big).$$

La première application est ainsi définie. Si $f \in \mathcal{F}\big(E_3, \mathcal{F}(E_2, E_1)\big)$, autrement dit, $f : E_3 \to \mathcal{F}(E_2, E_1)$, on définit $g := \varphi(f)$ comme l'application $g : E_3 \times E_2 \to E_1$ $(x_3, x_2) \mapsto \big(f(x_3)\big)(x_2)$. Comme, pour $x_3 \in E_3$, on a $f(x_3) : E_2 \to E_1$, l'élément

$\big(f(x_3)\big)(x_2)$ de E_1 est bien défini, g est bien une application de $E_3 \times E_2$ dans E_1 et φ est bien une application de $\mathcal{F}\big(E_3, \mathcal{F}(E_2, E_1)\big)$ dans $\mathcal{F}(E_3 \times E_2, E_1)$.
La seconde application est ainsi définie. Soit $g \in \mathcal{F}(E_3 \times E_2, E_1)$. On définit $f := \psi(g)$ comme l'application $f : E_3 \to \mathcal{F}(E_2, E_1)$ qui, à $x_3 \in E_3$, associe l'application $x_2 \mapsto g(x_3, x_2) \in E_1$. Il est immédiat, comme ci-dessus, que l'on a bien $f \in \mathcal{F}\big(E_3, \mathcal{F}(E_2, E_1)\big)$.
Nous laisserons au lecteur le soin de vérifier que les applications φ et ψ sont bien réciproques l'une de l'autre : c'est très facile. Ce sont donc des bijections, et l'on en déduit la troisième formule.

I.1.28 Si $E \cap F = \varnothing$ et si $F' \subset F$, alors $E \cap F' = \varnothing$ et $E \cup F' \subset E \cup F$, d'où $\operatorname{card} E + \operatorname{card} F' \leqslant \operatorname{card} E + \operatorname{card} F$. En vertu de la commutativité, cela règle le cas de la somme.
De même, si $F' \subset F$, alors $E \times F' \subset E \times F$, d'où $\operatorname{card} E \times \operatorname{card} F' \leqslant \operatorname{card} E \times \operatorname{card} F$. En vertu de la commutativité, cela règle le cas du produit.
De même, si $F' \subset F$, alors $\mathcal{F}(E, F') \subset \mathcal{F}(E, F)$, d'où :

$$(\operatorname{card} F')^{\operatorname{card} E} \leqslant (\operatorname{card} F)^{\operatorname{card} E}.$$

Supposons maintenant que $E' \subset E$ et considérons l'application de restriction $f \mapsto f_{|E'}$ de $\mathcal{F}(E, F)$ dans $\mathcal{F}(E', F)$. *Supposons que F est non vide*. Alors cette application est surjective (une application $f' : E' \to F$ s'étend en une application $f : E \to F$ en attribuant une image arbitraire aux éléments de $E \setminus E'$. On a alors l'inégalité $(\operatorname{card} F)^{\operatorname{card} E'} \leqslant (\operatorname{card} F)^{\operatorname{card} E}$.
Cependant, si $F = \varnothing$, cette démonstration tombe en défaut, car il n'y a pas d'image arbitraire à attribuer aux éléments de $E \setminus E'$. De fait, l'inégalité $0^{\operatorname{card} E'} \leqslant 0^{\operatorname{card} E}$ est fausse si $\operatorname{card} E' = 0$ et $\operatorname{card} E \neq 0$. Rappelons en effet que $0^{\aleph}$ vaut 1 si $\aleph = 0$ et 0 si $\aleph > 0$.

I.1.29 Comme cet exercice semble établir des propriétés de $\mathbb{N}$ en utilisant les propriétés de $\mathbb{N}$, nous allons un peu modifier les notations afin de mieux différencier les "entiers intuitifs" des "entiers de von Neumann". Pour tout ensemble x, nous noterons $s(x) := x \cup \{x\}$ ("successeur" de x). Les entiers de von Neumann sont donc $\varnothing$ et ses successeurs.
(i) Montrons d'abord que, si x est fini, alors $y := s(x)$ est fini. Si $y = x$, c'est évident (il découle d'ailleurs de l'exercice V que ce cas ne peut se produire pour les entiers de von Neumann). Nous devons donc montrer que, si $a \notin E$, alors E fini $\Rightarrow F := E \cup \{a\}$ fini . Par contraposée, nous supposons que $g : F \to F$ est une application injective non bijective et nous voulons en déduire une application injective non bijective $f : E \to E$. Si $g(a) = a$, ou si a n'admet pas d'antécédent par g, alors la restriction f de g à E convient. Supposons donc qu'il existe $b \in E$ tel que $g(b) = a$. Puisque g est injective, $c := g(a) \neq a$, donc $c \in E$. Nous posons alors, pour $x \in E$, $f(x) = g(x)$ si $x \neq b$ et $f(b) = c$. Il est clair que $f : E \to E$ est encore injective non bijective.
Comme $\varnothing$ est fini, ses successeurs sont finis. Ici intervient un "principe intuitif de récurrence" qui permet de conclure que les entiers de von Neumann sont tous finis. Cependant, dans l'ensemble de tous les entiers de von Neumann, l'application $x \mapsto s(x)$ est injective (cela découle de la question 2 de l'exercice V), et pas surjective car $\varnothing$ n'admet pas d'antécédent ($x \cup \{x\}$ contient l'élément x donc n'est pas vide). L'ensemble des entiers de von Neumann est donc infini.
(ii) Soit E un ensemble infini. On construit itérativement des applications injectives de chacun

des entiers de von Neumann dans E selon le procédé suivant. Pour $\varnothing$, on prend l'application vide. Si $f : x \to E$ est une application injective donnée, elle n'est pas bijective, sinon (d'après la première question) E serait fini. Il existe donc $y \in E$ sans antécédent. En posant $g_{|x} := f$ et $g(x) := y$, on définit $g : s(x) \to E$ injective. Si l'on admet l'existence d'un ensemble $\mathbb{N}$ des entiers de von Neumann, on déduit de la solution de l'exercice V que $\mathbb{N}$ est également la réunion des entiers de von Neumann, et que les applications injectives $f : x \to E$ construites ci-dessus se recollent en une application injective $\mathbb{N} \to E$. Il n'est cependant pas clair que nous puissions déduire l'existence de $\mathbb{N}$ des axiomes assez imprécis qui ont été donnés dans le cours.

I.1.30 D'après le module II.1, l'application $(q, r) \mapsto qk + r$ de $\mathbb{N} \times \{0, \dots, k-1\}$ dans $\mathbb{N}$ est bijective et l'application de l'énoncé est sa réciproque. Comme $\operatorname{card}\big(\mathbb{N} \times \{0, \dots, k-1\}\big) = \big(\operatorname{card} \mathbb{N}\big) \times \big(\operatorname{card}\{0, \dots, k-1\}\big)$, on a bien $k\aleph_0 = \aleph_0$.

I.1.31 Notons, pour $n, p \in \mathbb{N}$:

$$E_{n,p} = \{\underline{u} = (u_k)_{k\in\mathbb{N}} \in \mathbb{N}^{(\mathbb{N})} \mid \forall k\ ,\ u_k < p \quad \text{et} \quad \forall k \geqslant n\ ,\ u_k = 0\}.$$

Alors $E_{n,p}$ est fini, de cardinal p^n. De plus, $\mathbb{N}^{(\mathbb{N})} = \bigcup\limits_{n,p\in\mathbb{N}} E_{n,p}$ est une union dénombrable d'ensembles finis, donc un ensemble dénombrable.

I.1.32 Puisque $1 \leqslant 2 \leqslant \aleph_0$, on a $\aleph \leqslant 2\aleph = \aleph + \aleph \leqslant \aleph\aleph_0$ (exercice I.1.28) et il suffit donc de montrer que $\aleph = \aleph\aleph_0$. Soit donc E un ensemble infini de cardinal $\aleph$, et notons $\mathcal{F}$ l'ensemble des parties X de $\mathcal{P}(E)$ telles que : $\forall x \in X\ ,\ \operatorname{card} x = \aleph_0$ et $\forall x \neq y \in X\ ,\ x \cap y = \varnothing$. On ordonne $\mathcal{F}$ par l'inclusion. On vérifie alors facilement que l'union de toute chaîne de $\mathcal{F}$ est un élément de $\mathcal{F}$, qui est donc inductif. D'après le lemme de Zorn, $\mathcal{F}$ admet donc un élément maximal $X \in \mathcal{F}$: c'est un ensemble de parties dénombrables et deux à deux disjointes de E. Soit $E' = \bigcup\limits_{x\in X} x$. Cette union étant disjointe, on a $\operatorname{card} E' = (\operatorname{card} X)\aleph_0$. Par ailleurs, $E \backslash E'$ est fini (s'il était infini, il contiendrait un sous-ensemble dénombrable x' et $X \cup \{x'\}$ serait un majorant strict de X dans $\mathcal{F}$, contredisant la maximalité de X dans $\mathcal{F}$). Soient $\aleph' = \operatorname{card} X$ et $p = \operatorname{card} E' \in \mathbb{N}$. On a donc $\aleph = \aleph'\aleph_0 + p$. On peut maintenant calculer :

$$\aleph\aleph_0 = \aleph'\aleph_0\aleph_0 + p\aleph_0 = \aleph'\aleph_0 + p\aleph_0 == (\aleph' + p)\aleph_0.$$

Si $\aleph'$ est un cardinal fini, on trouve que $\aleph = \aleph_0 = \aleph\aleph_0$. Si $\aleph'$ est un cardinal infini, on trouve que $\aleph' + p = \aleph'$, d'où $\aleph\aleph_0 = \aleph'\aleph_0 \leqslant \aleph$, d'où $\aleph\aleph_0 = \aleph$.
Puisque $\aleph + \aleph = \aleph + 0 \not\Rightarrow \aleph = 0$ et que $\aleph\aleph_0 = \aleph.1 \not\Rightarrow \aleph_0 = 1$, on voit qu'aucun cardinal infini $\aleph$ n'est simplifiable pour l'addition ou pour la multiplication.
En revanche, tout cardinal fini $n \in \mathbb{N}$ est simplifiable pour l'addition. Supposons en effet que $n + \aleph = n + \aleph'$. Si $\aleph$ est fini, $\aleph'$ l'est aussi et l'on est ramené au calcul dans $\mathbb{N}$; sinon, $n + \aleph = \aleph$ (par exemple parce que $\aleph \leqslant \aleph + n \leqslant \aleph + \aleph_0 = \aleph$) et $n + \aleph' = \aleph'$, d'où $\aleph = \aleph'$. Le lecteur vérifiera de même que tout cardinal fini non nul est simplifiable pour la multiplication.

I.1.33 On veut montrer que $\aleph_0^{\aleph_0}$ et $(2^{\aleph_0})^{\aleph_0}$ sont égaux à $2^{\aleph_0}$. Comme $2 \leqslant \aleph_0 \leqslant 2^{\aleph_0}$ entraîne $2^{\aleph_0} \leqslant \aleph_0^{\aleph_0} \leqslant (2^{\aleph_0})^{\aleph_0}$ (exercice I.1.28), il suffit de voir que $2^{\aleph_0} = (2^{\aleph_0})^{\aleph_0}$. Or, ce dernier vaut $2^{\aleph_0^2}$ (exercice I.1.27), donc $2^{\aleph_0}$.

I.1.34 Table de vérité du connecteur de Sheffer :

P	Q	$P \mid Q$
V	V	F
V	F	V
F	V	V
F	F	V

On vérifie alors les égalités suivantes : $P \mid P = \neg P$; puis : $P \wedge Q = (P \mid Q) \mid (P \mid Q)$, $P \vee Q = (P \mid P) \mid (Q \mid Q)$ et $P \Rightarrow Q = P \mid (Q \mid Q)$ (ces égalités sont en fait l'écriture abrégée d'équivalences logiques).
Le seul autre connecteur binaire dont on puisse dériver tous les connecteurs logiques est le connecteur NOR (comme "Not Or") défini par la formule $\neg(P \vee Q)$. Le lecteur vérifiera, par exemple, que $\neg P = P$ NOR P, que $P \vee Q = (P \text{ NOR } Q)$ NOR $(P \text{ NOR } Q)$, et que $P \wedge Q = (P \text{ NOR } P)$ NOR $(Q \text{ NOR } Q)$.

I.1.35 On dresse des tables de vérité :

P	Q	$P \Rightarrow Q$	$P \wedge (P \Rightarrow Q)$	$\big(P \wedge (P \Rightarrow Q)\big) \Rightarrow Q$
V	V	V	V	V
V	F	F	F	V
F	V	V	F	V
F	F	V	F	V

P	$\neg P$	$P \Leftrightarrow (\neg P)$	$P \Rightarrow (\neg P)$
V	F	F	F
F	V	F	V

De cette table, on déduit aussi que $P \Rightarrow (\neg P)$ équivaut à $\neg P$: ce n'est ni une tautologie, ni une contradiction. Pratiquement, si l'on démontre qu'une assertion implique son contraire, c'est que cette assertion est fausse.

I.1.36 Soient $P_1, \ldots, P_k$ les symboles de propositions qui apparaissent dans F ou dans G. Supposons d'abord que F et G sont logiquement équivalentes. Alors, pour toutes valeurs $x_1, \ldots, x_k \in \{\text{V}, \text{F}\}$ attribuées à $P_1, \ldots, P_k$, les formules F et G prennent toutes deux la valeur V ou toutes deux la valeur F. Dans les deux cas, la formule $F \Leftrightarrow G$ prend la valeur V (car F $\Leftrightarrow$ F et V $\Leftrightarrow$ V ont pour valeur V). C'est donc une tautologie.
Supposons réciproquement que la formule $F \Leftrightarrow G$ est une tautologie. Alors, pour toutes valeurs $x_1, \ldots, x_k \in \{\text{V}, \text{F}\}$ attribuées à $P_1, \ldots, P_k$, la formule $F \Leftrightarrow G$ prend la valeur V, donc les formules F et G prennent toutes deux la valeur V ou toutes deux la valeur F. Dans tous les cas, elles prennent la même valeur. elles sont donc logiquement équivalentes.

I.1.37 Il ne s'agit, bien sûr, pas d'un exercice d'analyse, mais de bien appliquer les méthodes de démonstration ! Puisque l'on veut démontrer une implication :

$$\big(\lim_{n\to+\infty} u_n = 1\big) \Longrightarrow \big(\exists n \in \mathbb{N} \ : \ \forall p \geqslant n \ , \ u_p > 0\big), \tag{30}$$

on peut appliquer la méthode de l'hypothèse auxiliaire. On suppose donc l'hypothèse vérifiée : $(u_n)_{n\in\mathbb{N}}$ est une suite de réels telle que $\lim\limits_{n\to+\infty} u_n = 1$. On veut alors démontrer que $\big(\exists n \in \mathbb{N} \ : \ \forall p \geqslant n \ , \ u_p > 0\big)$. On va le démontrer par l'absurde : autrement dit, on suppose que c'est la négation de cette assertion qui est vraie. D'après les règles logiques sur les quantificateurs, cette négation s'écrit :

$$\forall n \in \mathbb{N} \ , \ \exists p \geqslant n \ : \ u_p \leqslant 0. \tag{31}$$

On va d'abord en déduire qu'il existe une sous-suite de la suite $(u_n)_{n\in\mathbb{N}}$ dont tous les termes sont négatifs ou nuls. D'après (31), appliqué à $n := 0$, il existe un entier $p \geqslant 0$ tel que $u_p \leqslant 0$. Notons le p_0. De même, en appliquant (31) à $n := p_0 + 1$, on trouve un entier $p \geqslant p_0 + 1$ (c'est-à-dire $p > p_0$) tel que $u_p \leqslant 0$. Notons le p_1. Supposons ainsi trouvés des entiers $p_0 < \cdots < p_k$ tels que $u_{p_0}, \ldots, u_{p_k} \leqslant 0$. En appliquant (31) à $n := p_k + 1$, on trouve un entier $p \geqslant p_k + 1$ (c'est-à-dire $p > p_k$) tel que $u_p \leqslant 0$. Notons le p_{k+1}. La sous-suite $(u_{p_k})_{k\in\mathbb{N}}$ de la suite $(u_n)_{n\in\mathbb{N}}$ n'a donc que des termes négatifs ou nuls. Or, il résulte du cours d'analyse (module IV.1) que toute sous-suite de $(u_n)_{n\in\mathbb{N}}$ a pour limite 1, et aussi qu'une suite convergente de réels négatifs ou nuls a pour limite un réel négatif ou nul. Nous en déduisons $1 \leqslant 0$, ce qui est impossible, d'où une contradiction. Notre hypothèse (31) est donc fausse ; c'est donc sa négation qui est vraie. Mais celle-ci est la conclusion de l'implication (30). Cette conclusion ayant été prouvée en supposant la prémisse (*i.e.* le membre gauche du signe $\Rightarrow$) vraie (hypothèse auxiliaire), l'implication 30 est démontrée.
Dans la pratique, on n'annonce pas aussi lourdement l'emploi de l'hypothèse auxiliaire. On dit simplement : "supposons l'hypothèse $\lim\limits_{n\to+\infty} u_n = 1$ vérifiée et prouvons la conclusion ..." En revanche, il est préférable d'annoncer nettement une démonstration par l'absurde.

I.1.38 Notons ici, pour $n, p \in \mathbb{N}$, $C_n^p := \dfrac{n!}{p!(n-p)!}$ si $0 \leqslant p \leqslant n$ et 0 autrement. On a donc $C_n^0 = 1$, $C_n^n = 1$ et $C_0^p = \delta_{p,0}$, c'est-à-dire, selon la notation de Kronecker, 1 si $p = 0$ et 0 autrement.
Par ailleurs, la relation de Pascal dit que $C_{n+1}^{p+1} = C_n^p + C_n^{p+1}$. On la démontre comme suit. Si $p > n$, les deux membres de l'égalité sont nuls. Si $p = n$, les deux membres de l'égalité valent 1. Si $0 \leqslant p \leqslant n-1$, c'est un calcul :

$$\begin{aligned}
\frac{n!}{p!(n-p)!} + \frac{n!}{(p+1)!(n-p-1)!} &= (p+1)\frac{n!}{(p+1)!(n-p)!} + (n-p)\frac{n!}{(p+1)!(n-p)!} \\
&= (n+1)\frac{n!}{(p+1)!(n-p)!} \\
&= \frac{(n+1)!}{(p+1)!(n-p)!} \\
&= C_{n+1}^{p+1}.
\end{aligned}$$

Formulons maintenant l'hypothèse de récurrence $H(r)$:

$$\forall n, p \in \mathbb{N}\ ,\ n+p=r \Longrightarrow C_n^p \in \mathbb{N}.$$

Pour $r=0$, le seul couple possible est $(n,p)=(0,0)$ et, comme $C_0^0=1$, $H(0)$ est vraie. Supposons l'hypothèse vraie jusqu'à $r-1$ (récurrence forte), autrement dit, soit r un entier non nul, et supposons $H(0)$,..., $H(r-1)$ vraies. Soient $n, p \in \mathbb{N}$ tels que $n+p=r$. Si $n=0$ ou $p=0$, on sait que C_n^p vaut 0 ou 1, donc est entier. Si $n, p \geqslant 1$ (ce qui implique que $r \geqslant 2$), la relation de Pascal dit que $C_n^p = C_{n-1}^{p-1} + C_{n-1}^p$. Par $H(r-2)$, $C_{n-1}^{p-1} \in \mathbb{N}$ et, par $H(r-1)$, $C_{n-1}^p \in \mathbb{N}$; donc $C_n^p \in \mathbb{N}$ et la démonstration est achevée.

Module II.1 : Arithmétique

II.1.1 Puisque l'ensemble ordonné $\mathcal{N}$ vérifie les conditions (N1), (N2), (N3), il possède un plus petit élément, notons-le ω. Par ailleurs, tout $x \in \mathcal{N}$ possède un successeur, notons-le $s(x)$, ce qui définit une application s de $\mathcal{N}$ dans lui-même. Appliquons le théorème 2 de la page 64. Il existe une unique application f de $\mathbb{N}$ dans $\mathcal{N}$ telle que d'une part $f(0) = \omega$ et d'autre part $f(n+1) = s\big(f(n)\big)$ pour tout $n \in \mathbb{N}$.

Pour tout $n \in \mathbb{N}$, $f(n+1) = s\big(f(n)\big) > f(n)$, ce qui montre que f est strictement croissante, en particulier f est injective. De plus, soient $m, n \in \mathbb{N}$. Si $m < n$, on a $f(m) < f(n)$, si $n < m$, on a $f(n) < f(m)$, et bien sûr $f(m) = f(n)$ lorsque $m = n$. Ainsi $m \leqslant n$ équivaut à $f(m) \leqslant f(n)$. Au total, f est une bijection de $\mathbb{N}$ sur $f(\mathbb{N})$, respectant l'ordre.

Notons que, pour démontrer le théorème 1 de la page 64 et le théorème 2 de la page 64, seules les propriétés (N1), (N2) et (N3) de $\mathbb{N}$ ont été utilisées. Puisque $\mathcal{N}$ vérifie ces propriétés, on peut échanger les rôles de $\mathbb{N}$ et $\mathcal{N}$ dans ce qui précède. Il existe donc une unique application g de $\mathcal{N}$ dans $\mathbb{N}$ telle que d'une part $g(\omega) = 0$ et d'autre part $g\big(s(x)\big) = g(x) + 1$ pour tout $x \in \mathcal{N}$. Considérons l'application $h = f \circ g$ de $\mathcal{N}$ dans lui-même. Elle vérifie $h(\omega) = \omega$ et, pour tout $x \in \mathcal{N}$,

$$h\big(s(x)\big) \;= f\left(g\big(s(x)\big)\right) \;=\; f\big(g(x)+1\big) \;=\; s\left(f\big(g(x)\big)\right) \;=\; s\big(h(x)\big)\,.$$

D'après l'assertion d'unicité du théorème 2 de la page 64, h est l'application identité de $\mathcal{N}$. On en déduit en particulier que f est surjective. En conclusion, f est une bijection de $\mathbb{N}$ sur $\mathcal{N}$ respectant l'ordre.

Il reste à montrer que, si f' est une bijection de $\mathbb{N}$ sur $\mathcal{N}$ respectant l'ordre, on a $f' = f$. Le fait que f' respecte l'ordre entraîne que, pour tout $n \in \mathbb{N}$, $f'(n+1) = s\big(f'(n)\big)$. Soient en effet $y \in \mathcal{N}$ et p son unique antécédent par f' : $y = f'(p)$. Alors $\big(y > f'(n)\big)$ équivaut à $(p > n)$, ou encore à $(p \geqslant n+1)$, c'est-à-dire à $\big(y \geqslant f'(n+1)\big)$. D'où notre assertion, en vertu de la définition du successeur de $f'(n)$. Dans ces conditions, l'égalité $f' = f$ résulte de l'assertion d'unicité du théorème 2 de la page 64.

II.1.2 Démontrons l'inégalité $f(n) \geqslant n$ par récurrence sur l'entier n. Puisque $f(0) \in \mathbb{N}$, on a bien $f(0) \geqslant 0$. Supposons que l'on ait $f(n) \geqslant n$ pour un certain entier n. Puisque f est strictement croissante, $f(n+1) > f(n)$. Comme $f(n)$ et $f(n+1)$ sont des entiers, on a $f(n+1) \geqslant f(n) + 1$, par définition du successeur. Mais $f(n) \geqslant n$, donc $f(n+1) \geqslant f(n) + 1 \geqslant n + 1$, d'où l'inégalité cherchée pour l'entier $n+1$. L'inégalité $f(n) \geqslant n$ est donc vraie pour tout entier n.

Supposons maintenant que f soit surjective, et montrons qu'alors f est l'application identique de $\mathbb{N}$, ce qui signifie que $f(n) = n$ pour tout $n \in \mathbb{N}$. Raisonnons par l'absurde, et soit $m \in \mathbb{N}$ le plus petit entier tel que $f(m) \neq m$, soit $f(m) > m$, vu l'alinéa précédent. Soit maintenant $k \in \mathbb{N}$. Si $k < m$, on a $f(k) = k < m$, en vertu du caractère minimal de m. Si $k = m$, on a $f(k) = f(m) > m$. Si $k > m$, on a $f(k) > f(m) > m$, donc $f(k) > m$. Dans tous les cas, $f(k) \neq m$. Il en résulte que m n'appartient pas à $f(\mathbb{N})$, ce qui contredit la surjectivité de f.

II.1.3 La réflexivité est évidente : si $(x, y) \in \mathbb{N}^2$, on a $x = x$ et $y \leqslant y$, donc $(x, y) \leqslant (x, y)$. Soient $(x, y),\ (x', y') \in \mathbb{N}^2$ tels que $(x, y) \leqslant (x', y')$ et $(x', y') \leqslant (x, y)$. Si $x = x'$,

par définition $y \leqslant y'$ et $y' \leqslant y$, donc $y = y'$ et ainsi $(x, y) = (x', y')$. Sinon, on a par exemple $x < x'$, mais cela contredit $(x', y') \leqslant (x, y)$. D'où l'antisymétrie. Soient enfin $(x, y), (x', y'), (x'', y'') \in \mathbb{N}^2$ tels que $(x, y) \leqslant (x', y')$ et $(x', y') \leqslant (x'', y'')$. D'abord $x \leqslant x'$ et $x' \leqslant x''$, donc $x \leqslant x''$. Si $x < x''$, on a par définition $(x, y) \leqslant (x'', y'')$. Sinon, $x = x''$, d'où $x = x' = x''$. Dans ce cas, $y \leqslant y'$ et $y' \leqslant y''$, d'où $y \leqslant y''$ et par suite $(x, y) \leqslant (x'', y'')$. D'où la transitivité. La relation $\leqslant$ est donc une relation d'ordre sur $\mathbb{N}^2$.

La condition (N3) est vérifiée par l'ensemble ordonné $\mathbb{N}^2$: pour tout $(x, y) \in \mathbb{N}^2$, on a $(x, y) < (x + 1, y)$. La condition (N1) est vérifiée également. Soit en effet E une partie non vide de $\mathbb{N}^2$. Considérons la première projection $p : (x, y) \mapsto x$ de $\mathbb{N}^2$ sur $\mathbb{N}$. Alors $p(E)$ est une partie non vide de $\mathbb{N}$, soit a son plus petit élément. Par construction, $Z := \{y \in \mathbb{N} \mid (a, y) \in E\}$ est une partie non vide de $\mathbb{N}$, soit b son plus petit élément. D'abord $(a, b) \in E$. Soit ensuite $(x, y) \in E$. En premier lieu, $x \in p(E)$, donc $x \geqslant a$. Si $x > a$, on a $(a, b) < (x, y)$. Si $x = a$, $y \in Z$, donc $y \geqslant b$, et par suite $(a, b) \leqslant (a, y) = (x, y)$. Ainsi (a, b) est le plus petit élément de E.

L'ensemble ordonné $\mathbb{N}^2$ ne vérifie pas la condition (N2). En effet la partie $\{0\} \times \mathbb{N}$ de $\mathbb{N}^2$ est majorée par $(1, 0)$, mais elle n'a pas de plus grand élément, car $(0, n) < (0, n + 1)$ pour tout $n \in \mathbb{N}$.

Il est clair que, pour tout $(x, y) \in \mathbb{N}^2$, $(x, y + 1)$ est le successeur de (x, y). Par contre, l'élément $(1, 0)$ est distinct du plus petit élément de $\mathbb{N}^2$, à savoir $(0, 0)$, mais cet élément ne possède pas de prédécesseur. En effet les éléments de $\mathbb{N}^2$ strictement inférieurs à $(1, 0)$ sont les $(0, n)$, $n \in \mathbb{N}$, et nous avons vu que $\{0\} \times \mathbb{N}$ n'a pas de plus grand élément.

II.1.4 Il suffit de montrer que, si a, b sont deux entiers fixés, on a $(a + b) + c = a + (b + c)$ pour tout $c \in \mathbb{N}$. Raisonnons par récurrence sur c. C'est vrai si $c := 0$, car $x + 0 = x$ pour tout $x \in \mathbb{N}$ (théorème et définition 5 de la page 66, propriété 1). Si $(a+b)+c = a+(b+c)$ pour un certain entier c, la propriété 2 du théorème et définition 5 de la page 66 donne, vu l'hypothèse :

$$\begin{aligned}(a + b) + (c + 1) &= \big[(a + b) + c\big] + 1 = \big[a + (b + c)\big] + 1 \\ &= a + \big[(b + c) + 1\big] = a + \big[b + (c + 1)\big],\end{aligned}$$

d'où l'égalité au rang $c + 1$.

II.1.5 1) Démontrons par récurrence sur l'entier $n \in \mathbb{N}$, la propriété $\mathcal{P}(n)$ suivante : pour *tout* $k \in [\![0, n]\!]$, $\binom{n}{k}$ est un entier. La propriété $\mathcal{P}(0)$ est vraie, car $\binom{0}{0} = 1$. Soit n un entier tel que $\mathcal{P}(n)$ soit vraie, montrons que $\mathcal{P}(n + 1)$ est vraie. Soit $k \in [\![0, n + 1]\!]$. Si $k := 0$, $\binom{n+1}{k} = \binom{n+1}{0} = 1$ est entier. Si $k \geqslant 1$, la formule (4) de la page 79 donne :

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

Puisque $\mathcal{P}(n)$ est vraie, les deux termes du membre de droite sont entiers, donc le premier membre est entier, ce qui prouve que $\mathcal{P}(n + 1)$ est vraie.

2) Fixons l'entier p.

Pour tout entier $q \geqslant p$, posons $S(q) := \sum_{n=p}^{q} \binom{n}{p}$. Prouvons l'égalité $S(q) = \binom{q+1}{p+1}$ par récurrence sur q. Le cas $q = p$ est clair, car $S(p) = \binom{p}{p} = 1 = \binom{p+1}{p+1}$. Supposons que, pour un certain entier $q \geqslant p$, on ait $S(q) = \binom{q+1}{p+1}$. Alors :

$$S(q+1) \;=\; S(q) + \binom{q+1}{p} \;=\; \binom{q+1}{p+1} + \binom{q+1}{p} \;=\; \binom{q+2}{p+1},$$

la dernière égalité venant de la formule (4) citée. La formule de l'énoncé est donc vraie pour tout entier $q \geqslant p$.

II.1.6 De manière intuitive, on peut par exemple appliquer $0, 1, 2, 3, 4, \ldots$ sur $0, -1, 1, -2, 2, \ldots$. Précisons : définissons une application f de $\mathbb{N}$ dans $\mathbb{Z}$ en posant $f(n) := n/2$ si n est pair et $f(n) := -(n+1)/2$ si n est impair. En sens inverse, définissons une application g de $\mathbb{Z}$ dans $\mathbb{N}$ en posant $g(k) := 2k$ si $k \geqslant 0$ et $g(k) := -2k - 1$ si $k < 0$. Montrons que f et g sont deux bijections réciproques l'une de l'autre.

Soit $n \in \mathbb{N}$. Si n est pair, écrivons $n := 2p$. Alors $f(n) = p \geqslant 0$, donc $g\big(f(n)\big) = g(p) = 2p = n$. Si n est impair, écrivons $n := 2p - 1$, où $p \in \mathbb{N}^*$. Alors $f(n) = -p < 0$, donc $g\big(f(n)\big) = g(-p) = 2p - 1 = n$. Ainsi $g \circ f$ est l'identité de $\mathbb{N}$.

Soit ensuite $k \in \mathbb{Z}$. Si $k \geqslant 0$, $g(k) = 2k$ est pair, donc $f\big(g(k)\big) = k$. Si $k < 0$, $g(k) = -2k - 1$ est impair, donc $f\big(g(k)\big) = -\big((-2k-1)+1\big)/2 = k$. Ainsi $f \circ g$ est l'identité de $\mathbb{Z}$.

II.1.7 Supposons donc $n > 1$ écrit comme en (10). Soit $d \in \mathbb{N}^*$. D'après le théorème 38 de la page 87, d divise n si, et seulement si, $\nu_p(d) \leqslant \nu_p(n)$ pour tout $p \in \mathbb{P}$. Cela revient à dire que $\nu_p(d) = 0$ si $p \notin \{q_1, \ldots, q_s\}$ et $\nu_{q_i}(d) \leqslant e_i$ pour $i = 1, \ldots, s$. Soit $I = [\![0, e_1]\!] \times [\![0, e_2]\!] \times \cdots \times [\![0, e_s]\!]$. D'après le théorème 37 de la page 86, l'application $(\alpha_1, \ldots, \alpha_s) \longmapsto q_1^{\alpha_1} \cdots q_s^{\alpha_s}$ est une bijection de I sur l'ensemble des diviseurs strictement positifs de n. Le nombre de ces diviseurs est donc le cardinal de I, c'est-à-dire, en vertu du théorème 18 de la page 73, le produit $(e_1 + 1)(e_2 + 1) \cdots (e_s + 1)$.

II.1.8 Tout d'abord $1 + 1 = 2 = 10_2$. Tous les calculs ci-après sont en base 2, nous omettrons donc l'indice 2. Voici la table d'addition (à gauche) et la table de multiplication (à droite) en base 2 :

	0	1
0	0	1
1	1	10

et

	0	1
0	0	0
1	0	1

Effectuons l'addition $1011 + 101$, en notant les retenues :

$$\begin{array}{rr} & \overset{1\,1\,1}{1011} \\ + & 101 \\ \hline = & 10000 \end{array}$$

En système décimal, cela correspond à l'égalité $11 + 5 = 16$. Effectuons de même la multiplication 1011×11 :

$$\begin{array}{rr} & 1011 \\ \times & 11 \\ \hline \end{array}$$

$$\begin{array}{rr} & \overset{1\,1\,1}{01011} \\ + & 1011 \\ \hline = & 100001 \end{array}$$

En système décimal, cela correspond à l'égalité $11 \times 3 = 33$.

II.1.9 Soit $n \in \mathbb{N}^*$, écrit en base 10 : $n = (a_r a_{r-1} \cdots a_1 a_0)_{10}$, autrement dit $n = \sum_{k=0}^{r} a_k 10^k$.

On peut écrire $n = 100m + t$, en posant $t := (a_1 a_0)_{10} = 10a_1 + a_0$ et $m := \sum_{k=2}^{r} a_k 10^{k-2}$.

Puisque 4 divise 100, n est multiple de 4 si, et seulement si, t l'est. Ainsi la divisibilité de n par 4 se teste sur les deux derniers chiffres (à droite) de n. Ainsi 1984 est multiple de 4 car 84 l'est, mais 2026 n'est pas multiple de 4, car 4 ne divise pas 26.

Passons à la divisibilité par 9. L'idée est que $9 = 10 - 1$. À l'aide de la formule (8) de la page 82, on en déduit que, pour tout $k \in \mathbb{N}$, 9 divise $10^k - 1$. Soit alors S la somme des chiffres de n. On a $n - S = \sum_{k=0}^{r} a_k(10^k - 1)$, donc 9 divise $n - S$. Il en résulte que n est divisible par 9 si, et seulement si, S l'est. Par exemple 846 est multiple de 9 car $8+4+6 = 18$ l'est, et 1925 n'est pas multiple de 9 car $1 + 9 + 2 + 5 = 17$ n'est pas multiple de 9. Voici un autre exemple : $n = 384\,165$ est multiple de 9. En effet, la somme des chiffres de n est 27, et la somme des chiffres de 27 est 9.

II.1.10 Appliquons le théorème 31 de la page 81 avec $b = 10$. L'application $f : (a_0, \ldots, a_{n-1}) \mapsto \sum_{k=0}^{n-1} a_k 10^k$ est une bijection de $[\![0, 9]\!]^n$ sur $[\![0, 10^n[\![$. L'ensemble des entiers de $[\![0, 10^n[\![$ dont l'écriture décimale ne comporte pas le chiffre 7 est l'image par f de $([\![0, 9]\!] \setminus \{7\})^n$, son cardinal est donc 9^n. Ainsi l'ensemble des entiers de $[\![1, 10^n[\![$ dont l'écriture décimale ne comporte pas le chiffre 7 est de cardinal $9^n - 1$.

II.1.11 L'égalité $2^{2^n} = F_n - 1$ implique $2^{2^{n+1}} = F_n^2 - 2F_n + 1$. Il en résulte que le reste de la division de $2^{2^{n+1}}$ par F_n est 1. Si a, b sont deux entiers et si le reste de la division de a (resp. b) par F_n est 1, il est clair que le reste de la division de ab par F_n est aussi 1. Par récurrence, on en déduit que, pour tout entier $k \geqslant n + 1$, le reste de la division de 2^{2^k} par F_n est 1. En particulier le reste de la division de 2^{2^m} par F_n est 1, donc le reste de la division de $F_m = 2^{2^m} + 1$ par F_n est 2, ce qui montre que F_n divise $F_m - 2$.

Pour tout $n \in \mathbb{N}$, F_n est un entier impair et $F_n \geqslant 3$, donc F_n possède un facteur premier p_n (théorème 33 de la page 83). Montrons que, si $n, m \in \mathbb{N}$ sont distincts, $p_n \neq p_m$. On peut par exemple supposer $n < m$. Nous avons vu que F_n divise $F_m - 2$, donc p_n divise $F_m - 2$. Par contre, p_m divise F_m mais $p_m \neq 2$, donc p_m ne divise pas $F_m - 2$, et par suite $p_m \neq p_n$.
Lorsque n décrit $\mathbb{N}$, les p_n sont donc des nombres premiers deux à deux distincts, ce qui montre que l'ensemble des nombres premiers est infini : on retrouve le théorème 35 de la page 85.

II.1.12 1) Pour tout entier $n \in \mathbb{N}^*$, notons $D(n)$ l'ensemble des diviseurs strictement positifs de n. Si $x \in D(a)$ et $y \in D(b)$, xy divise ab, d'où une application $f : (x, y) \mapsto xy$ de $D(a) \times D(b)$ dans $D(ab)$. Inversement, soit $d \in D(ab)$. Alors $d \wedge a \in D(a)$ et $d \wedge b \in D(b)$, d'où une application $g : d \mapsto (d \wedge a, d \wedge b)$ de $D(ab)$ dans $D(a) \times D(b)$. Montrons que f et g sont deux bijections réciproques l'une de l'autre.

Soit $(x, y) \in D(a) \times D(b)$. Puisque a est premier avec b, il est premier avec y. Le théorème de Gauß montre donc que $xy \wedge a = x \wedge a = x$. De même $xy \wedge b = y \wedge b = y$, d'où $g\big(f(x, y)\big) = (xy \wedge a, xy \wedge b) = (x, y)$.

Soient inversement $d \in D(ab)$ et $x := d \wedge a,\ y := d \wedge b$. Montrons que $xy = d$. Notons les égalités suivantes, valables pour trois entiers α, β, γ quelconques (pour les démontrer, on peut utiliser les formules (13) et (14) du texte) :

$$\alpha \wedge (\beta \vee \gamma) \ = \ (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)\,, \ \ \alpha \vee (\beta \wedge \gamma) \ = \ (\alpha \vee \beta) \wedge (\alpha \vee \gamma)\,.$$

Puisque a et b sont premiers entre eux, $x \wedge y = 1$, donc $xy = x \vee y$. Ainsi :

$$xy \ = \ x \vee y \ = \ (d \wedge a) \vee (d \wedge b) \ = \ d \wedge (a \vee b) \ = \ d \wedge ab \ = \ d\,.$$

D'où notre assertion : $f\big(g(d)\big) = d$.

Nous pouvons maintenant calculer $s(ab) = \sum_{d \in D(ab)} d$ en effectuant le changement d'indice bijectif défini par f :

$$s(ab) = \sum_{d \in D(ab)} d = \sum_{(x,y) \in D(a) \times D(b)} xy = \left(\sum_{x \in D(a)} x \right) \left(\sum_{y \in D(b)} y \right) = s(a)s(b)\,.$$

2) Puisque M_p est premier, ses seuls diviseurs strictement positifs sont 1 et M_p, donc $s(M_p) = 1 + M_p = 2^p$. Par ailleurs, les diviseurs de 2^{p-1} sont les 2^h, $h = 0, \ldots, p-1$, d'où, en vertu de la formule (8) :

$$s(2^{p-1}) \ = \ 1 + 2 + 2^2 + \cdots + 2^{p-1} \ = \ 2^p - 1 \ = \ M_p\,.$$

L'entier M_p est impair, donc premier avec 2^{p-1}. D'après la question 1, il vient :

$$s(N) \ = \ s(2^{p-1}M_p) \ = \ s(2^{p-1})s(M_p) \ = \ M_p \times 2^p \ = \ 2N\,.$$

3) Là encore m est premier avec 2^r, donc la question 1 donne :

$$2^{r+1}m \ = \ 2N \ = \ s(N) \ = \ s(2^r)s(m) \ = \ (2^{r+1} - 1)s(m)\,.$$

Les entiers $2^{r+1} - 1$ et 2^{r+1} sont premiers entre eux, et $2^{r+1} - 1$ divise $2^{r+1}m$, il divise donc m, en vertu du théorème de Gauß : il existe $t \in \mathbb{N}^*$ tel que $m = (2^{r+1} - 1)t$. L'égalité $2^{r+1}m = (2^{r+1} - 1)s(m)$ donne donc $s(m) = 2^{r+1}t$.

Observons que t et m divisent m, et $t \neq m$ parce que $r \geqslant 1$. Par ailleurs $t + m = 2^{r+1}t = s(m)$. Il en résulte que $D(m) = \{t, m\}$. Mais $1 \in D(m)$, d'où nécessairement $t = 1$. En outre $m > 1$, et m n'a que deux diviseurs strictement positifs (1 et m), *i.e.* m est premier. Or $m = 2^{r+1} - 1$, donc $p := r + 1$ est nécessairement premier (*cf.* l'exercice 8 de la page 84). Alors $m = 2^{r+1} - 1 = 2^p - 1 = M_p$.

Voici le résultat obtenu (il est dû à Euler). Soit N un entier *pair* strictement positif. Pour que N soit parfait, il faut et il suffit qu'il existe un nombre premier p, tel que d'une part le nombre de Mersenne $M_p = 2^p - 1$ soit aussi premier, et d'autre part $N = 2^{p-1}M_p$. Les premiers p répondant à la question sont $2, 3, 5, 7$, car $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ et $M_7 = 127$ sont premiers, d'où les nombres parfaits pairs suivants :

$$2^1 \times 3 = 6\,,\ \ 2^2 \times 7 = 28\,,\ \ 2^4 \times 31 = 496\,,\ \ 2^6 \times 127 = 8128\,.$$

Signalons qu'à ce jour, on ne connaît aucun entier *impair* parfait, mais on ne sait pas démontrer que de tels entiers n'existent pas.

II.1.13 Écrivons donc $ab = n^2$, où $n \in \mathbb{N}^*$. Soit p un nombre premier. Si p divise a, il ne divise pas b (car a et b sont premiers entre eux). Ainsi $\nu_p(b) = 0$, d'où $\nu_p(a) = \nu_p(n^2) = 2\nu_p(n)$, en vertu de la formule (12). Ainsi $\nu_p(a)$ est pair, et c'est aussi vrai si p ne divise pas a (alors $\nu_p(a) = 0$). Appliquons maintenant la formule (11). On en déduit que

$$a \;=\; \prod_{p\,\in\,\mathbb{P}} p^{\nu_p(a)} \;=\; a'^2\,, \quad \text{où} \quad a' \;:=\; \prod_{p\,\in\,\mathbb{P}} p^{\nu_p(a)/2}\,.$$

La formule définissant l'entier a' est licite : d'une part il s'agit en fait d'un produit fini, d'autre part, chaque $\nu_p(a)/2$ est entier. Ainsi a est un carré, de même b est un carré.

Soient maintenant x, y deux entiers impairs : $x := 2t + 1$ et $y := 2u + 1$, où t, u sont entiers. Alors :

$$x^2 + y^2 = (2t+1)^2 + (2u+1)^2 = (4t^2 + 4t + 1) + (4u^2 + 4u + 1) = 4(t^2 + t + u^2 + u) + 2\,.$$

Il en résulte que le reste de la division de $x^2 + y^2$ par 4 est 2, donc $x^2 + y^2$ est multiple de 2 mais pas de 4.

II.1.14 Un triplet $(u, v, w) \in (\mathbb{N}^*)^3$ est pythagoricien si, et seulement s'il existe un triangle rectangle dont l'hypoténuse a pour longueur w et les deux autres côtés ont pour longueurs u et v (théorème de Pythagore et sa réciproque). C'est ce qui explique l'adjectif pythagoricien. On se propose donc de trouver les triangles rectangles dont les longueurs des trois côtés sont des entiers.

Supposons d'abord que d, a, b soient trois entiers comme dans l'énoncé et définissons u, v, w par les formules $(*)$. Alors :

$$\begin{aligned} u^2 + v^2 &= d^2\big[(a^2 - b^2)^2 + 4a^2b^2\big] = d^2\big[(a^4 - 2a^2b^2 + b^4) + 4a^2b^2\big] \\ &= d^2\big[a^4 + 2a^2b^2 + b^4\big] = d^2(a^2 + b^2)^2 \;=\; w^2\,. \end{aligned}$$

De plus, $u > 0$ parce que $a > b > 0$ et $d > 0$, de même $v > 0$, et évidemment $w > 0$, ce qui prouve que (u, v, w) est un triplet pythagoricien.

Soit inversement (u, v, w) un triplet pythagoricien. Supposons d'abord que u, v, w soient premiers entre eux. À cause de l'égalité $u^2 + v^2 = w^2$, on voit en fait que u, v, w sont premiers

entre eux *deux à deux*. Parmi les entiers u, v, w, il y en a au plus un qui est pair (si deux d'entre eux étaient pairs, ils ne seraient pas premiers entre eux). De plus, u et v ne peuvent être tous les deux impairs, car sinon l'exercice précédent montrerait que w^2 est multiple de 2 mais pas de 4, ce qui est absurde. Quitte à échanger u et v nous supposerons donc v pair et u, w impairs.

Partons des égalités $u^2 = w^2 - v^2 = (w+v)(w-v)$. Les entiers $w+v$ et $w-v$ sont premiers entre eux. En effet, dans le cas contraire, il existerait un nombre premier p divisant $w+v$ et $w-v$, $p \neq 2$ puisque $w+v$ est impair. Alors p diviserait $2w = (w+v)+(w-v)$ et $2v = (w+v)-(w-v)$, donc p diviserait aussi w et v (d'après le lemme d'Euclide), contredisant le fait que v, w soient premiers entre eux.

Appliquons l'exercice précédent. Les entiers $w+v$ et $w-v$ sont premiers entre eux et leur produit u^2 est un carré, donc chacun d'eux est un carré. Il existe donc $r, s \in \mathbb{N}^*$ tels que $w+v = r^2$ et $w-v = s^2$. Comme $w+v$ et $w-v$ ont même parité et $w+v > w-v$, r, s ont même parité et $r > s$, donc $a := (r+s)/2$ et $b := (r-s)/2$ appartiennent à $\mathbb{N}^*$ et $a > b$. Maintenant $a+b = r$ donc $w+v = (a+b)^2$, et $a-b = s$ donc $w-v = (a-b)^2$. On en déduit :

$$w = \frac{1}{2}\Big[(a+b)^2 + (a-b)^2\Big] = a^2+b^2 \quad \text{et} \quad v = \frac{1}{2}\Big[(a+b)^2 - (a-b)^2\Big] = 2ab\,.$$

Ensuite $u^2 = (w+v)(w-v) = r^2s^2$, donc $u = rs = \big[(r+s)/2\big]^2 - \big[(r-s)/2\big]^2$, c'est-à-dire $u = a^2 - b^2$. D'où les égalités voulues :

$$u \;=\; a^2-b^2\,,\;\; v \;=\; 2ab\,,\;\; w \;=\; a^2+b^2\,.$$

Enfin $a \wedge b = 1$, parce que $a \wedge b$ divise évidemment u, v et w.

Soit maintenant (u, v, w) un triplet pythagoricien quelconque, posons $d := u \wedge v$. Alors d divise u et v, donc d^2 divise u^2 et v^2 ; par suite d^2 divise $u^2+v^2 = w^2$, ce qui entraîne que d divise w. Écrivons $u := du'$, $v := dv'$, $w := dw'$. Le triplet (u', v', w') est toujours pythagoricien, mais cette fois $u' \wedge v' = 1$. *A fortiori* u', v', w' sont premiers entre eux. D'après le cas traité ci-dessus, il existe deux entiers a, b premiers entre eux, vérifiant $a > b \geqslant 1$ et tels que u', v', w' soient donnés par les formules :

$$u' \;:=\; a^2-b^2\,,\;\; v' \;:=\; 2ab\,,\;\; w' \;:=\; a^2+b^2\,.$$

On en déduit comme désiré les égalités suivantes :

$$u \;=\; d(a^2-b^2)\,,\;\; v \;=\; 2dab\,,\;\; w \;=\; d(a^2+b^2)\,.$$

Détaillons la solution « géométrique » suggérée dans l'énoncé.

Considérons le point $A := (-1, 0) \in C$. À tout point $M := (x, y) \in C \setminus \{A\}$, associons la pente t de la droite AM, c'est-à-dire $t := y/(x+1)$. Alors $y = t(x+1)$, d'où $t^2(x+1)^2 = y^2 = 1-x^2$, soit $t^2(1+x) = 1-x$ puisque $x \neq -1$.

Ainsi $x = (1-t^2)/(1+t^2)$, d'où l'on déduit $1+x = 2/(1+t^2)$ puis $y = 2t/(1+t^2)$.

Inversement, si $t \in \mathbb{R}$ et si l'on pose :

$$x(t) \;:=\; \frac{1-t^2}{1+t^2} \quad \text{et} \quad y(t) \;:=\; \frac{2t}{1+t^2}\,, \qquad (**)$$

le point $\big(x(t), y(t)\big)$ appartient à C, puisque

$$x(t)^2 + y(t)^2 \;=\; \frac{(1-t^2)^2+4t^2}{(1+t^2)^2} \;=\; \frac{(1+t^2)^2}{(1+t^2)^2} \;=\; 1\,.$$

De plus $x(t) \neq -1$, *i.e.* $\big(x(t), y(t)\big) \neq A$. Il en résulte que $t \mapsto \big(x(t), y(t)\big)$ est une bijection de $\mathbb{R}$ sur $C \setminus \{A\}$, *i.e.* les formules $(**)$ définissent une paramétrisation de $C \setminus \{A\}$.
On peut retrouver cette paramétrisation à l'aide de la trigonométrie.
Soit $M = (x, y) \in C \setminus \{A\}$, *i.e.* $x \neq -1$. On sait qu'il existe un unique $\theta \in]-\pi, \pi[$ tel que $x = \cos\theta$ et $y = \sin\theta$. Posons $t := \tan(\theta/2)$. Les lignes trigonométriques de l'angle double $\theta = 2(\theta/2)$ sont données par les formules classiques :

$$\cos\theta = \frac{1-t^2}{1+t^2}\,,\ \ \sin\theta = \frac{2t}{1+t^2}\,,\ \ \tan\theta = \frac{2t}{1-t^2}\,,$$

la dernière formule étant valable si $t \neq \pm 1$, soit $\theta \neq \pm\pi/2$. On retrouve les formules $(**)$: $x = x(t)$ et $y = y(t)$.
Soit maintenant (u, v, w) un triplet pythagoricien. Supposons comme précédemment u, v, w premiers entre eux et v pair (u, w sont donc impairs). Posons $x := u/w$ et $y := v/w$. L'égalité $u^2 + v^2 = w^2$ implique $x^2 + y^2 = 1$. Notons que x, y sont des nombres rationnels strictement positifs. Ainsi $t = y/(x+1)$ est un rationnel strictement positif. En outre, vu ce qui précède, $x = x(t)$ et $y = y(t)$. Écrivons t sous forme irréductible : $t = b/a$, où $a, b \in \mathbb{N}^*$ sont premiers entre eux. Alors :

$$x \,=\, x(t) \,=\, \frac{1-t^2}{1+t^2} \,=\, \frac{a^2-b^2}{a^2+b^2}\,,\ \ y \,=\, y(t) \,=\, \frac{2t}{1+t^2} \,=\, \frac{2ab}{a^2+b^2}\,.$$

La fraction u/w est irréductible. Comme $u/w = x = (a^2-b^2)/(a^2+b^2)$, il existe $k \in \mathbb{N}^*$ tel que $a^2 - b^2 = ku$ et $a^2 + b^2 = kw$. De même la fraction v/w est irréductible, donc $2ab = kv$. L'entier k divise $a^2 + b^2$ et $a^2 - b^2$, donc k divise $2a^2$ et $2b^2$. Il en résulte que k divise $(2a^2) \wedge (2b^2) = 2$, donc k vaut 1 ou 2. Supposons que $k = 2$. Alors $ab = v$ est pair, donc l'un des entiers a, b est pair et l'autre impair. C'est absurde, car $a^2 - b^2 = 2u$ est pair. Finalement $k = 1$, d'où :

$$u \,=\, a^2 - b^2\,,\ \ v \,=\, 2ab\,,\ \ w \,=\, a^2 + b^2\,.$$

Nous avons retrouvé les formules obtenues précédemment.

II.1.15 Si $(a, b) \in [\![1, m]\!] \times [\![1, n]\!]$, on a effectivement :

$$a + (b-1)m \leqslant m + (n-1)m = mn\,.$$

Ainsi $(a, b) \mapsto a + (b-1)m$ est une application f de $[\![1, m]\!] \times [\![1, n]\!]$ dans $[\![1, mn]\!]$. Montrons que f est surjective. Soit $x \in [\![1, mn]\!]$, effectuons la division euclidienne de x par m : $x = qm + r$, où $q, r \in \mathbb{N}$ et $r < m$. Si $r = 0$, on a $1 \leqslant q \leqslant n$ et $x = qm = m + (q-1)m = f(m, q)$. Supposons $r > 0$. Alors $q < n$, et $x = f(r, q+1)$.
Montrons que f est injective. Soient $(a, b), (a', b') \in [\![1, m]\!] \times [\![1, n]\!]$ tels que $f(a, b) = f(a', b')$, soit $a + (b-1)m = a' + (b'-1)m$. Cette égalité s'écrit aussi : $a - a' = m(b' - b)$. Comme $a, a' \in [\![1, m]\!]$, on a $|a - a'| \leqslant m - 1 < m$, d'où $m|b' - b| < m$, soit $|b' - b| < 1$. Mais $|b' - b| \in \mathbb{N}$, donc $|b' - b| = 0$, *i.e.* $b = b'$, d'où l'on déduit $a = a'$.
En conclusion, f est une bijection de $[\![1, m]\!] \times [\![1, n]\!]$ sur $[\![1, mn]\!]$, ce qui montre que le cardinal de $[\![1, m]\!] \times [\![1, n]\!]$ est mn : on retrouve le théorème 18 de la page 73.

II.1.16 1) Soit g l'application $(x, y) \mapsto (y, x + y)$ de $\mathbb{N}^2$ dans $\mathbb{N}^2$. D'après le théorème 2 de la page 64, il existe une unique application f de $\mathbb{N}$ dans $\mathbb{N}^2$ telle que $f(0) = (0, 1)$ et

$f(n+1) = g\big(f(n)\big)$ pour tout $n \in \mathbb{N}$. Si $n \in \mathbb{N}$, $f(n)$ est un couple d'entiers, notons F_n et v_n ses composantes : autrement dit $f(n) = (F_n, v_n)$. Vu la définition de g, on a pour tout entier n :

$$(F_{n+1}, v_{n+1}) = f(n+1) = g\big((F_n, v_n)\big) = (v_n, F_n + v_n)\,,$$

ce qui montre que $v_n = F_{n+1}$, et par suite $v_{n+1} = F_{n+2}$. Il en résulte que $F_{n+2} = v_n + F_n = F_{n+1} + F_n$, donc les F_n vérifient la relation de récurrence indiquée. Enfin $(0,1) = f(0) = (F_0, v_0) = (F_0, F_1)$, donc $F_0 = 0$ et $F_1 = 1$. Ainsi la suite $(F_n)_{n\geqslant 0}$ a les propriétés requises.

2) Notons les premières valeurs de F_n :

$$F_0 = 0,\ F_1 = F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 5\,.$$

Vu la relation de récurrence définissant la suite $(F_n)_{n\geqslant 0}$, il est clair que $F_k > 0$ dès que $k \geqslant 1$ et $F_k > F_{k-1}$ dès que $k \geqslant 3$ (car alors $F_{k-2} > 0$). Il en résulte que, si $k \geqslant 4$, la division euclidienne de F_k par F_{k-1} s'écrit : $F_k = 1 \times F_{k-1} + F_{k-2}$: le quotient est 1 et le reste est F_{k-2}.

On en déduit immédiatement, par récurrence sur m, que l'algorithme d'Euclide (théorème 41 de la page 89), appliqué avec $a := F_m$ et $b := F_{m-1}$, conduit aux suites $(q_1, \dots, q_{m-2})$ et $(r_1, \dots, r_m)$ définies ainsi : $r_k := F_{m-k+1}$ pour tout $k \in [\![1, m-1]\!]$, $r_m := 0$, $q_k := 1$ pour tout $k \in [\![1, m-3]\!]$ et $q_{m-2} := 2$. Cela correspond aux divisions euclidiennes successives suivantes :

$$\begin{cases} F_m = 1 \times F_{m-1} + F_{m-2} \\ F_{m-1} = 1 \times F_{m-2} + F_{m-3} \\ \dots \\ F_5 = 1 \times F_4 + F_3 \\ F_4 = 1 \times F_3 + F_2 \\ F_3 = 2 \times F_2 + 0\,. \end{cases}$$

Le dernier reste non nul est $F_2 = 1$, donc le pgcd de F_m et F_{m-1} vaut 1. Noter que le nombre de divisions euclidiennes effectuées est $m-2$. Tout ce qui précède est valable lorsque $m \geqslant 3$. Si $m = 2$, l'algorithme d'Euclide se réduit à l'égalité $F_2 = 1 \times F_1 + 0$.

3) Démontrons l'inégalité $r_{n+2-k} \geqslant F_{k+1}$ par récurrence sur $k \in [\![1, n]\!]$. Pour $k = 1$, on a $r_{n+1} \geqslant 1 = F_2$. Pour $k = 2$, on a $r_n \geqslant r_{n+1} + 1 \geqslant 2 = F_3$. Soit $k \in [\![1, n-2]\!]$, supposons que l'inégalité voulue soit vraie pour k et $k+1$. Autrement dit $r_{n+2-k} \geqslant F_{k+1}$ et $r_{n+1-k} \geqslant F_{k+2}$.

L'égalité $r_{n-k} = q_{n-k} r_{n-k+1} + r_{n-k+2}$ implique alors $r_{n-k} \geqslant q_{n-k} F_{k+2} + F_{k+1}$. Mais $r_{n-k} > r_{n-k+2}$, donc $q_{n-k} \geqslant 1$, d'où $r_{n-k} \geqslant F_{k+2} + F_{k+1} = F_{k+3}$, ce qui prouve l'inégalité voulue pour $k+2$. En conclusion, cette inégalité est vraie pour tout $k \in [\![1, n]\!]$. Pour $k = n$, on obtient $b = r_2 \geqslant F_{n+1}$.

4) Observons que t et u sont les deux racines de l'équation $x^2 - x - 1 = 0$. Ainsi $t^2 = t + 1$, d'où $t^{k+2} = t^{k+1} + t^k$ et de même $u^{k+2} = u^{k+1} + u^k$, ceci pour tout $k \in \mathbb{N}$.

Démontrons l'égalité de l'énoncé par récurrence sur k. Elle est vraie si $k := 0$, car $F_0 = 0$ et $t^0 = 1 = u^0$. Elle est vraie pour $k := 1$, car $t - u = \sqrt{5}$ et $F_1 = 1$. Considérons un entier $k \geqslant 2$, et supposons que l'égalité visée soit vraie pour tous les entiers $h \in [\![0, k-1]\!]$. Alors

$$F_{k-2} = \frac{t^{k-2} - u^{k-2}}{\sqrt{5}}\,,\ F_{k-1} = \frac{t^{k-1} - u^{k-1}}{\sqrt{5}}\,,$$

d'où l'on déduit :

$$F_k \;=\; F_{k-1}+F_{k-2} \;=\; \frac{1}{\sqrt{5}}\left[(t^{k-1}+t^{k-2})-(u^{k-1}+u^{k-2})\right]\,, \quad \text{soit}$$

$$F_k \;=\; \frac{t^k-u^k}{\sqrt{5}}\cdot$$

Cette égalité est donc vraie pour tout $k\in\mathbb{N}$.

5) Reprenons les notations de la question 3. L'inégalité $F_{n+1}\leqslant b$ et l'égalité de la question précédente donnent : $t^{n+1}-u^{n+1}\leqslant b\sqrt{5}$. Par ailleurs $|u|<1$ (une valeur approchée de u à $0{,}001$ près est $-0{,}618$), donc $t^{n+1}\leqslant 1+b\sqrt{5}$. On en déduit l'inégalité de l'énoncé :

$$n+1 \;\leqslant\; \frac{\ln\bigl(1+b\sqrt{5}\bigr)}{\ln t}\,, \quad \text{soit} \quad n+1 \;\leqslant\; E\left(\frac{\ln\bigl(1+b\sqrt{5}\bigr)}{\ln t}\right).$$

Soit maintenant m le nombre de chiffres décimaux de b, *i.e.* le seul entier tel que $10^{m-1}\leqslant b<10^m$. Ainsi $b\leqslant 10^m-1$. On en déduit les inégalités :

$$n \;\leqslant\; \psi(m) \;:=\; E\left(\frac{\ln\bigl(1+\sqrt{5}(10^m-1)\bigr)}{\ln t}\right)-1 \;\leqslant\; \frac{\ln\bigl(10^m\sqrt{5}\bigr)}{\ln t}-1\,.$$

Lorsque m vaut $1,2$ ou 3, on constate que $\psi(m)=5m$, d'où $n\leqslant 5m$. Supposons $m\geqslant 4$. Il nous suffit de prouver l'inégalité :

$$\frac{\ln\bigl(10^m\sqrt{5}\bigr)}{\ln t} \;\leqslant\; 5m+1\,, \quad \text{soit} \quad m(5\ln t-\ln 10) \;\geqslant\; \frac{1}{2}\ln 5-\ln t\,.$$

On vérifie que $5\ln t-\ln 10>0,1$ et $(\ln 5)/2-\ln t<0,4$, d'où la conclusion.

II.1.17 1) Soit $(x,y)\in\mathbb{N}^{*2}$ et posons $(x',y'):=f\bigl((x,y)\bigr)$, $(x'',y'):=f\bigl((x',y')\bigr)$. La définition de f montre qu'on a toujours $x'+y'\leqslant x+y$, et par suite $x''+y''\leqslant x'+y'$. En outre, si $x>y$, on est dans l'un des cas b), c), e), et cette définition montre que $x'+y'<x+y$. Si l'on se trouve dans le cas d), $(x',y')=(y,x)$, donc $x'>y'$, d'où $x''+y''<x'+y'$ vu ce qui précède. Tout cela donne l'inégalité $x''+y''<x+y$ dès que $x\neq y$.
Cela étant, supposons par l'absurde $a_n\neq b_n$ pour tout n. D'après l'alinéa précédent, $a_{n+2}+b_{n+2}<a_n+b_n$ pour tout $n\in\mathbb{N}$. La suite $(a_{2k}+b_{2k})_{k\geqslant 0}$ est donc une suite strictement décroissante d'entiers naturels, ce qui contredit le théorème 4 de la page 66.

2) Soient $(x,y)\in\mathbb{N}^{*2}$ et $(x',y'):=f\bigl((x,y)\bigr)$. Posons $d:=x\wedge y$, $d':=x'\wedge y'$. Calculons d' en fonction de d, en distinguant les différents cas. Dans les cas a) et d), il est clair que $d'=d$. Dans le cas c), x est impair, donc $x\wedge y=x\wedge(2y')=x\wedge y'$ en vertu du théorème de Gauß, d'où $d=d'$ dans ce cas. Dans le cas e), x et y sont impairs, et le même argument montre que $d=d'$.
Supposons enfin que l'on soit dans le cas b). Si y est impair, $d=d'$ comme ci-dessus. Par contre, si y est pair, $y=2y'$, la distributivité de la multiplication par rapport au pgcd donne $d=(2x')\wedge(2y')=2d'$. En résumé, $d=d'$ sauf si x,y sont distincts et tous deux pairs, auquel cas $d=2d'$.
Venons-en à la question posée. Pour tout $k\in\mathbb{N}$, posons $d_k:=a_k\wedge b_k$, de sorte que $d=a\wedge b$ est égal à d_0 et $d_n=a_n$ (car $a_n=b_n$). Si $k\in\mathbb{N}$, ce qui précède montre que $d_k=d_{k+1}$ sauf

si a_k et b_k sont distincts et tous deux pairs, auquel cas $d_k = 2d_{k+1}$. On en déduit que l'entier h cherché est le nombres d'entiers $k \in [\![0, n-1]\!]$ tels que a_k et b_k soient tous les deux pairs.

3) Appliquons la définition de f mécaniquement :

$$(a_0, b_0) = (9000, 1575)\,,\ (a_1, b_1) = (4500, 1575)\,,\ (a_2, b_2) = (2250, 1575)\,,$$
$$(a_3, b_3) = (1125, 1575)\,,\ (a_4, b_4) = (1575, 1125)\,,\ (a_5, b_5) = (1125, 225)\,,$$
$$(a_6, b_6) = (225, 450)\,,\ (a_7, b_7) = (225, 225)\,.$$

Ainsi $n = 7$, $a_7 = 225$ et $h = 0$, donc $9000 \wedge 1575 = 225$.

4) Voici un programme renvoyant le pgcd d de a et b :

```
PGCD(a,b)
x:= a; y:= b; d:=1;
tant que x <> y faire
   (si x mod 2 = 0
      alors
         (x:= x/2;
         si y mod 2 = 0
            alors
               d:= 2*d
            sinon
               rien
         )
      sinon
         (si y mod 2 = 0
            alors
               y = y/2
            sinon
               (si x < y
                  alors
                     (z:= x; x:= y; y:= z)
                  sinon
                     (z:= x; x:= y; y:= (z-x)/2)
               )
         )
   )
d:= d*x;
rendre(d)
```

5) La conclusion est évidente si $a = b$, c'est-à-dire $n = 0$, ou si $1 \leqslant n \leqslant 4$, car alors $\log_2\big(\max(a,b)\big) \geqslant 1$. Supposons $n \geqslant 5$, et posons $M := \max(a,b)$. Soient $(x,y) \in \mathbb{N}^{*2}$ et $(x',y') = f\big((x,y)\big)$. Si l'on n'est pas dans l'un des cas a) ou d), la définition de f montre que l'on a $x'y' \leqslant xy/2$. Lorsqu'on applique f successivement pour construire la suite $\big((a_k,b_k)\big)_{k\geqslant 0}$, on ne peut se trouver deux fois de suite dans l'un des cas a) ou d), sauf à partir du moment où cette suite stationne. Il en résulte que, pour tout $k \in [\![0, n-2]\!]$, on a $a_{k+2}b_{k+2} \leqslant a_k b_k/2$.

Supposons n pair, écrivons $n := 2p$. Alors $a_n b_n \leqslant ab/2^p \leqslant M^2/2^p$. Mais $a_n b_n \geqslant 1$, donc $2^p \leqslant M^2$, puis $2^n \leqslant M^4$. Supposons n impair, écrivons $n := 2p+1$. Alors $a_{n-1}b_{n-1} \leqslant ab/2^p$. Lorsqu'on passe de (a_{n-1}, b_{n-1}) à (a_n, b_n) en appliquant f, on n'est pas

dans l'un des cas a) ou d), donc $a_n b_n \leqslant a_{n-1}b_{n-1}/2$. Dans ces conditions, $a_n b_n \leqslant ab/2^{p+1}$, d'où comme ci-dessus $2^{p+1} \leqslant M^2$, puis $2^{n+1} = 2^{2(p+1)} \leqslant M^4$. *A fortiori* $2^n \leqslant M^4$.
Ainsi $2^n \leqslant M^4$ dans tous les cas. En prenant les logarithmes en base 2, on en déduit l'inégalité voulue : $n \leqslant 4\log_2(M)$.

II.1.18 1) Rappelons d'abord que r est le seul entier tel que $p^r \leqslant n < p^{r+1}$ (*cf.* l'exercice 7 de la page 82). L'inégalité $n < p^{r+1}$ montre en outre que $\nu_p(n) \leqslant r$.
Cela étant, soit donc F l'ensemble des couples $(k,t) \in [\![1,r]\!] \times [\![1,n]\!]$ tels que p^k divise t. La formule de Fubini donne :

$$\operatorname{card}(F) \;=\; \sum_{t=1}^{n} \operatorname{card}\left(\left\{k \in [\![1,r]\!] \;\middle|\; p^k \mid t\right\}\right) \;=\; \sum_{k=1}^{r} \operatorname{card}\left(\left\{t \in [\![1,n]\!] \;\middle|\; p^k \mid t\right\}\right).$$

Soit d'abord $t \in [\![1,n]\!]$. Par définition de $\nu_p(t)$, un entier $k \in \mathbb{N}^*$ est tel que p^k divise t si et seulement si $k \leqslant \nu_p(t)$. Puisque $t \leqslant n < p^{r+1}$, on a $\nu_p(t) \leqslant r$, vu l'alinéa précédent, appliqué à t au lieu de n. Il en résulte que tout $k \in \mathbb{N}^*$ tel que p^k divise t vérifie $k \leqslant r$. Comme $\nu_p(t)$ est le nombre d'entiers $k \geqslant 1$ tels que $k \leqslant \nu_p(t)$ (!), on en déduit ceci :

$$\operatorname{card}\left(\left\{k \in [\![1,r]\!] \;\middle|\; p^k \mid t\right\}\right) \;=\; \nu_p(t).$$

Sommons ces égalités pour $t = 1, \ldots, n$. Par définition, $n!$ est le produit de tous les entiers $t \in [\![1,n]\!]$. D'après la formule (12) du texte, m est la somme des $\nu_p(t)$, t décrivant $[\![1,n]\!]$. D'où $\operatorname{card}(F) = m$.
Soit maintenant $k \in [\![1,r]\!]$. D'abord $u \mapsto up^k$ est une bijection de $\mathbb{N}^*$ sur l'ensemble des multiples (strictement positifs) de p^k. Ensuite, si $u \in \mathbb{N}^*$ et $t := up^k$, l'inégalité $t \leqslant n$ équivaut à $u \leqslant n/p^k$, ou encore, par définition de la partie entière, à $u \leqslant E(n/p^k)$. Ainsi

$$\operatorname{card}\left(\left\{t \in [\![1,n]\!] \;\middle|\; p^k \mid t\right\}\right) \;=\; \operatorname{card}\left(\left\{u \in \mathbb{N}^* \;\middle|\; u \leqslant E(n/p^k)\right\}\right) \;=\; E(n/p^k).$$

La formule de Fubini donne maintenant le résultat attendu :

$$m \;=\; \operatorname{card}(F) \;=\; \sum_{k=1}^{r} E\left(\frac{n}{p^k}\right).$$

2) Écrivons $n = n' + n''$, en posant :

$$n' \;:=\; a_r p^r + \cdots + a_k p^k \quad \text{et} \quad n'' \;:=\; a_{k-1}p^{k-1} + \cdots + a_1 p + a_0.$$

L'exercice 7 de la page 82 donne $n'' < p^k$, de sorte que

$$\frac{n}{p^k} \;=\; a_r p^{r-k} + \cdots + a_{k+1}p + a_k + \frac{n''}{p^k} \;=\; t + \frac{n''}{p^k},$$

où t est un entier. Comme $n''/p^k \in [0,1[$, t est la partie entière de n/p^k :

$$E\left(\frac{n}{p^k}\right) \;=\; a_r p^{r-k} + \cdots + a_{k+1}p + a_k \;=\; \sum_{j=k}^{r} a_j p^{j-k}.$$

3) Les deux questions précédentes donnent les égalités :

$$m \;=\; \sum_{k=1}^{r}\left(\sum_{j=k}^{r} a_j p^{j-k}\right) \;=\; \sum_{j=1}^{r} a_j \left(\sum_{k=1}^{j} p^{j-k}\right) \;=\; \sum_{j=1}^{r} a_j \left(\sum_{h=0}^{j-1} p^h\right).$$

La dernière égalité vient du changement d'indice $h := j-k$, où $j \in [\![1, r]\!]$ est fixé. Multiplions par $p-1$, et utilisons la formule (8) du texte :

$$m(p-1) \;=\; \sum_{j=1}^{r} a_j(p-1)\left(\sum_{h=0}^{j-1} p^h\right) \;=\; \sum_{j=1}^{r} a_j(p^j-1)\,.$$

Puisque $p^0 = 1$, on en déduit ceci :

$$m(p-1) \;=\; \sum_{j=0}^{r} a_j(p^j-1) \;=\; \sum_{j=0}^{r} a_j p^j - \sum_{j=0}^{r} a_j \;=\; n - S\,.$$

La formule de Legendre en résulte.

Prenons $p := 2$ et $n := 1000$. On a :

$$1000 \;=\; 512+256+128+64+32+8 \;=\; 2^9+2^8+2^7+2^6+2^5+2^3\,.$$

Autrement dit, l'écriture de n en base 2 est $n = 1111101000_2$. En tous cas la somme S vaut 6 (dans l'écriture binaire de n, il y a six chiffres égaux à 1). La formule de Legendre donne ici $(p-1=1)$: $\nu_2(1000!) = 1000 - S = 994$.

II.1.19 D'après la proposition 57 de la page 98 (ici $d = 1$), il existe $(u_0, v_0) \in \mathbb{Z}^2$ tel que $au_0 + bv_0 = t$. De plus, les solutions $(u, v) \in \mathbb{Z}^2$ de l'équation $au + bv = t$ sont exactement les couples $(u_0 + kb, v_0 - ka)$, où k décrit $\mathbb{Z}$. Il reste à prouver l'existence d'un $k \in \mathbb{Z}$ tel que les entiers $u := u_0 + kb$ et $v := v_0 - ka$ soient positifs, ce qui se traduit par les inégalités suivantes (parce que $a > 0$ et $b > 0$) :

$$\frac{-u_0}{b} \;\leqslant\; k \;\leqslant\; \frac{v_0}{a}\cdot \qquad (*)$$

La différence entre les rationnels v_0/a et $-u_0/b$ est :

$$\frac{v_0}{a} + \frac{u_0}{b} \;=\; \frac{au_0+bv_0}{ab} \;=\; \frac{t}{ab}\cdot$$

Par hypothèse $t/ab > 1$, donc l'exercice 14 de la page 103 donne l'existence d'un $k \in \mathbb{Z}$ vérifiant les inégalités $(*)$.

II.1.20 Écrivons $S := T + 1/2^m$, où T est la somme des $1/k$ pour tous les entiers $k \in [\![1, n]\!]$ distincts de 2^m. On peut écrire $T := A'/B'$, où $A' \in \mathbb{N}^*$ et B' est le ppcm de tous les entiers $k \in [\![1, n]\!]$ distincts de 2^m. Considérons un tel entier k. L'idée est que k n'est pas multiple de 2^m, car sinon k s'écrirait $k = 2^m t$, $t \in \mathbb{N}^*$ étant un entier distinct de 1. Cela impliquerait $k \geqslant 2^{m+1} > n$, ce qui est absurde. Ainsi $\nu_2(k) \leqslant m-1$. D'après le théorème et définition 42 de la page 90, on en déduit l'inégalité $\nu_2(B') \leqslant m-1$. Soit alors A/B la forme irréductible de S. Il vient :

$$\frac{A}{B} \;=\; \frac{A'}{B'} + \frac{1}{2^m} \;=\; \frac{2^m A' + B'}{2^m B'}\,.$$

Puisque 2^m ne divise pas B', il ne divise pas $2^m A' + B'$, et il en résulte que $\nu_2(2^m A' + B') = \nu_2(B')$. Comme $B(2^m A' + B') = 2^m AB'$, la formule (12) du texte montre que $\nu_2(B) = \nu_2(2^m A) = m + \nu_2(A)$. En particulier $\nu_2(B) \geqslant m \geqslant 1$. Mais $A \wedge B = 1$, donc $\nu_2(A) = 0$, d'où $\nu_2(B) = m$. En tous cas $B \geqslant 2$, donc $S = A/B$ n'est pas un entier (la forme irréductible d'un entier z est $z/1$).

II.1.21 On peut supposer x non nul. Écrivons le rationnel x sous forme irréductible : $x = a/b$, où $b \in \mathbb{N}^*$, $a \in \mathbb{Z}$, $a \neq 0$ et $a \wedge b = 1$. Alors $x^n = a^n/b^n$. Mais a^n et b^n sont premiers entre eux. Dans le cas contraire, il existerait un nombre premier p divisant a^n et b^n. D'après le lemme d'Euclide, p diviserait a et b, contredisant l'hypothèse $a \wedge b = 1$. Ainsi a^n/b^n est une forme irréductible de x^n. Or x^n est entier, donc $b^n = 1$, d'où évidemment $b = 1$.
Finalement $x = a$ est entier.

II.1.22 Puisque $a \wedge b = 1$, l'équation $ub - av = 1$ a au moins une solution $(u_0, v_0) \in \mathbb{Z}^2$. Les autres solutions (u, v) de cette équation sont de plus données par $u := u_0 + ka$ et $v := v_0 + kb$, où $k \in \mathbb{Z}$ est arbitraire. L'intervalle $[\![n - v_0 + 1, n + b - v_0]\!]$ est formé de b entiers consécutifs, il contient donc un unique multiple de b. Il existe ainsi un unique $k \in \mathbb{Z}$ tel que $n - v_0 + 1 \leqslant (k + 1)b \leqslant n + b - v_0$, soit $n - v_0 < (k + 1)b \leqslant n + b - v_0$, ou encore $n - b < v_0 + kb \leqslant n$. Il suffit donc de poser $v := v_0 + kb$ et $u := u_0 + kb$ pour obtenir l'existence et l'unicité d'un couple $(u, v) \in \mathbb{Z}^2$ vérifiant les conditions $ub - av = 1$ et $n - b < v \leqslant n$.
Posons donc $t := u/v$. D'abord $v \in [\![1, n]\!]$, car $n - b < v \leqslant n$ et $b \leqslant n$. Ensuite $u \wedge v = 1$, parce que $ub - av = 1$. Par ailleurs $u \leqslant v$, car $b > a$ ($x < y \leqslant 1$) donc $1 = ub - va > (u - v)b \geqslant u - v$. Il en résulte que $t = u/v \in \mathcal{F}_n$. De plus $ub - va > 0$, *i.e.* $t = u/v > a/b = x$. Puisque x, y sont consécutifs dans $\mathcal{F}_n$, il vient $t \geqslant y$.
Si $t = y$, on a $c = u$ et $d = v$, d'où $bc - ad = ub - av = 1$, comme désiré. Supposons $t > y$, et montrons que cela mène à une contradiction. Partons des égalités :

$$t - x = \frac{u}{v} - \frac{a}{b} = \frac{ub - av}{bv} = \frac{1}{bv}\,, \quad y - x = \frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd} \quad \text{et}$$

$$t - y = \frac{u}{v} - \frac{c}{d} = \frac{ud - vc}{vd}\,.$$

On en déduit les minorations $y - x \geqslant 1/bd$ et $t - y \geqslant 1/vd$, d'où :

$$\frac{1}{bv} = t - x = (t - y) + (y - x) \geqslant \frac{1}{bd} + \frac{1}{vd} = \frac{v + b}{bvd} > \frac{n}{bvd}\,.$$

Ainsi $bvd > bvn$, donc $d > n$, ce qui est absurde car $y = c/d \in \mathcal{F}_n$. En conclusion, on a bien $bc - ad = 1$.
Supposons que $x = a/b$, $y = c/d$ et $z = e/f$ soient trois termes consécutifs de $\mathcal{F}_n$ ($x < y < z$). D'après ce qui précède, $bc - ad = 1$, et de même $de - cf = 1$. Autrement dit, $y - x = 1/bd$ et $z - y = 1/df$. Il en résulte que $b(y - x) = f(z - y)$, d'où $(b + f)y = fz + bx = e + a$. Cela donne l'égalité voulue : $y = (a + e)/(b + f)$.

II.1.23 Soit donc E un ensemble dénombrable, muni d'une relation d'ordre total vérifiant les hypothèses a) et b) de l'énoncé. Nous allons montrer qu'il existe une bijection g de D sur E respectant l'ordre. Remplaçant E par $\mathbb{Q}$, qui vérifie les mêmes conditions que E, on en déduira qu'il existe une bijection h de D sur $\mathbb{Q}$ respectant l'ordre. Alors $f = g \circ h^{-1}$ sera une bijection de $\mathbb{Q}$ sur E respectant l'ordre. Il nous suffit ainsi de construire une bijection g de D sur E respectant l'ordre.
Commençons par introduire quelques notations. Pour tout $n \in \mathbb{N}$, notons D_n l'ensemble des rationnels de la forme $a/2^n$, où $a \in \mathbb{Z}$. Comme $a/2^n = (2a)/2^{n+1}$, on a $D_n \subset D_{n+1}$ pour

tout n, et D est par définition la réunion des D_n, $n \in \mathbb{N}$. En outre $D_0 = \mathbb{Z}$. Posons ensuite $\Delta_0 := \mathbb{Z}$ et $\Delta_n := D_n \setminus D_{n-1}$ pour tout entier $n \geqslant 1$. Les Δ_n, $n \in \mathbb{N}$, forment une *partition* de D, *i.e.* ils sont deux à deux disjoints et leur réunion est D.

Numérotons les éléments de E, *i.e.* considérons une bijection $k \mapsto a_k$ de $\mathbb{N}$ sur E (une telle bijection existe, puisque E est dénombrable). Puisque E ne possède pas d'élément maximum, il existe une suite $(u_p)_{p\geqslant 0}$ d'éléments de E, strictement croissante et telle que $u_0 = a_0$. On peut construire cette suite par récurrence comme suit, partant de $u_0 := a_0$. Si l'on a déjà défini $u_0, \dots, u_p$ pour un certain $p \in \mathbb{N}$ de sorte que $u_0 < u_1 < \cdots < u_p$, on pose $u_{p+1} := a_k$, où $k \in \mathbb{N}$ est le plus petit entier tel que $u_p < a_k$ (un tel k existe puisque u_p n'est pas élément maximum de E et puisque l'ordre sur E est total). Pour tout $p \in \mathbb{N}$, il existe un unique $k_p \in \mathbb{N}$ tel que $u_p = a_{k_p}$, et les k_p, $p \in \mathbb{N}$, sont deux à deux distincts.

Montrons que, si $x \in E$, il existe $p \in \mathbb{N}$ tel que $x \leqslant u_p$. En effet, raisonnons par l'absurde, en supposant $x > u_p$ pour tout $p \in \mathbb{N}$. Soit $h \in \mathbb{N}$ l'entier tel que $x = a_h$. Pour tout $p \in \mathbb{N}$, on a donc $a_h > u_p$. La définition de u_{p+1} donne alors $k_{p+1} \leqslant h$. Ainsi $h \geqslant k_{p+1}$ pour tout $p \in \mathbb{N}$, ce qui est absurde puisque les k_r, $r \in \mathbb{N}$ sont des éléments de $\mathbb{N}$ deux à deux distincts.

Puisque E ne possède pas d'élément minimum, on peut de manière analogue construire une suite $(v_p)_{p\geqslant 0}$ d'éléments de E, strictement décroissante et telle que $v_0 = a_0$. Comme ci-dessus, pour tout $x \in E$, il existe $p \in \mathbb{N}$ tel que $x \geqslant v_p$. Définissons maintenant une application g_0 de $\mathbb{Z}$ dans E comme suit. Soit $m \in \mathbb{Z}$. Alors :

$$g_0(m) = \begin{cases} u_m & \text{si } m \geqslant 0 \\ v_{-m} & \text{si } m < 0\,. \end{cases}$$

Cette définition montre que $g_0 : \mathbb{Z} \to E$ est strictement croissante, c'est donc une bijection, respectant l'ordre, de $\mathbb{Z}$ sur $g_0(\mathbb{Z})$. En outre, pour tout $x \in E$, il existe un unique entier $m \in \mathbb{Z}$ tel que $g_0(m) \leqslant x < g_0(m+1)$.

Nous allons *prolonger* g_0 en une application g_1 de D_1 dans E comme suit. D'abord $g_1(t) := g_0(t)$ pour tout $t \in \mathbb{Z}$. Il nous faut ensuite définir $g_1(t)$ pour tout rationnel $t \in \Delta_1$. Un tel t s'écrit : $t = a/2$, où $a \in \mathbb{Z}$ est impair (sinon $t \in \mathbb{Z}$), *i.e.* $t = (2b+1)/2$, où $b \in \mathbb{Z}$. Ainsi $b < t < b+1$, et $g_0(b) < g_0(b+1)$. Utilisons maintenant la condition b) de l'énoncé, disant que E n'a pas de trous. Il existe des $x \in E$ tels que $g_0(b) < x < g_0(b+1)$, *i.e.* il existe $h \in \mathbb{N}$ tel que $g_0(b) < a_h < g_0(b+1)$. Notant k le plus petit de ces entiers, nous posons alors : $g_1(t) := a_k$. Ainsi $g_1(b) < g_1(t) < g_1(b+1)$. Soit $m \in \mathbb{Z}$. Puisque g_0 est strictement croissante, on a $g_1(m) < g_1(t)$ si $m \leqslant b$ et $g_1(m) > g_1(t)$ si $m > b$, *i.e.* $m \geqslant b+1$.

Montrons que g_1 est strictement croissante. Vu ce qui précède, il suffit de montrer que, si $t \in \Delta_1$ est comme ci-dessus et si $t' \in \Delta_1$, $t < t'$ implique $g_1(t) < g_1(t')$. On écrit encore $t' = (2b'+1)/2$, où $b' \in \mathbb{Z}$ et $b < b'$ puisque $t < t'$. Alors $b' \geqslant b+1$, d'où

$$g_1(b) < g_1(t) < g_1(b+1) \leqslant g_1(b') < g_1(t') < g_1(b'+1)\,,$$

ce qui établit l'inégalité $g_1(t) < g_1(t')$.

Soit $x \in E$. Il existe un unique $b \in \mathbb{Z}$ tel que $g_0(b) \leqslant x < g_0(b+1)$.

Comme $g_0(b) = g_1(b) < g_1\big((2b+1)/2\big) < g_1(b+1) = g_0(b+1)$, on a soit $g_1(b) \leqslant x < g_1\big((2b+1)/2\big)$, soit $g_1\big((2b+1)/2\big) \leqslant x < g_1(b+1)$ (exclusivement). Il existe donc un unique $m \in \mathbb{Z}$ tel que $g_1(m/2) \leqslant x < g_1\big((m+1)/2\big)$ (m vaut $2b$ ou $2b+1$).

La construction de g_1 à partir de g_0 se généralise. Plus précisément, considérons un entier $n \geqslant 1$. Supposons construite une application strictement croissante g_n de D_n dans E vérifiant la condition suivante : pour tout $x \in E$, il existe un unique $m \in \mathbb{Z}$ tel que

$g_n(m/2^n) \leqslant x < g_n\big((m+1)/2^n\big)$. C'est bien le cas si $n = 1$. Nous allons *prolonger* g_n en une application g_{n+1} de D_{n+1} dans E comme suit. D'abord $g_{n+1}(t) := g_n(t)$ pour tout $t \in D_n$. Il nous faut ensuite définir $g_{n+1}(t)$ pour tout rationnel $t \in \Delta_{n+1}$. Un tel t s'écrit : $t = a/2^{n+1}$, où $a \in \mathbb{Z}$ est impair (sinon $t \in D_n$), *i.e.* $t = (2b+1)/2^{n+1}$, où $b \in \mathbb{Z}$. Ainsi $b/2^n < t < (b+1)/2^n$, et par conséquent $g_n(b/2^n) < g_n\big((b+1)/2^n\big)$. Puisque E n'a pas de trous, il existe des $x \in E$ tels que $g_n(b/2^n) < x < g_n\big((b+1)/2^n\big)$, *i.e.* il existe $h \in \mathbb{N}$ tel que $g_n(b/2^n) < a_h < g_n\big((b+1)/2^n\big)$. Notant k le plus petit de ces entiers, nous posons alors : $g_{n+1}(t) := a_k$. Ainsi $g_{n+1}(b/2^n) < g_{n+1}(t) < g_{n+1}\big((b+1)/2^n\big)$. Comme dans le cas $n = 0$, on montre d'une part que $g_{n+1} : D_{n+1} \to E$ est strictement croissante, et d'autre part que, pour tout $x \in E$, il existe un unique $m \in \mathbb{Z}$ tel que $g_{n+1}(m/2^{n+1}) \leqslant x < g_{n+1}\big((m+1)/2^{n+1}\big)$. En conclusion, nous avons construit, pour tout $n \in \mathbb{N}$, une application g_n de D_n dans E ayant les propriétés requises.

Définissons enfin une application $g : D \to E$ comme suit. Soit $t \in D$. Il existe un unique $n \in \mathbb{N}$ tel que $t \in \Delta_n$, et nous posons $g(t) := g_n(t)$. Cette définition montre que, pour tout $n \in \mathbb{N}$, la restriction de g à D_n n'est autre que g_n. Il est alors clair que g est strictement croissante, c'est donc une bijection, respectant l'ordre, de D sur $g(E)$. Pour conclure, il nous suffit de montrer que g est *surjective*.

Raisonnons par l'absurde, en supposant $g(D) \neq E$. Il existe alors un plus petit entier $k \in \mathbb{N}$ tel que $a_k \notin g(D)$. Soit $n \in \mathbb{N}$. Nous savons qu'il existe un unique entier $m_n \in \mathbb{Z}$ tel que $g_n(m_n/2^n) < a_k < g_n\big((m_n+1)/2^n\big)$. Posons $t = (2m_n+1)/2^{n+1}$. Par définition de g_{n+1}, $g(t) = g_{n+1}(t) = a_{h_n}$, où $h_n \in \mathbb{N}$ est le plus petit entier tel que $g_n(m_n/2^n) < a_{h_n} < g_n\big((m_n+1)/2^n\big)$. On en déduit l'inégalité $h_n \leqslant k$. Lorsque n décrit $\mathbb{N}$, les entiers h_n sont deux à deux distincts. En effet, si $n, n' \in \mathbb{N}$ sont distincts, on a :

$$a_{h_{n'}} \;=\; g\left(\frac{2m_{n'}+1}{2^{n'+1}}\right) \;\neq\; g\left(\frac{2m_n+1}{2^{n+1}}\right) \;=\; a_{h_n}\,.$$

Dans ces conditions, on ne peut avoir $k \geqslant h_n$ pour tout $n \in \mathbb{N}$. Cette contradiction achève de montrer que g est surjective, et ainsi g est une bijection, respectant l'ordre, de D sur E.

Module II.2 : Groupes, anneaux, corps

II.2.1 Soit donc un ensemble à n éléments. Par définition, une loi de composition sur E est une application de $E \times E$ dans E, *i.e.* un élément de $\mathcal{F}(E \times E, E)$. Puisque $E \times E$ est de cardinal n^2 (théorème 18 de la page 73), $\mathcal{F}(E \times E, E)$ est de cardinal n^{n^2}, en vertu du théorème 24 de la page 76. Il y a donc n^{n^2} lois de composition sur E.

Numérotons les éléments de E : $x_1, \dots, x_n$. Soit T l'ensemble des couples (x_i, x_j), où $i, j \in [\![1, n]\!]$ et $i \leqslant j$. Le cardinal de T est $n(n+1)/2$. En effet, $(i, j) \mapsto (x_i, x_j)$ est une bijection de $S := \big\{(i, j) \in [\![1, n]\!]^2 \;\big|\; i \leqslant j\big\}$ sur T. Pour tout $j \in [\![1, n]\!]$, il y a j indices $i \in [\![1, n]\!]$ tels que $(i, j) \in S$, soit $i \leqslant j$. D'après la formule de Fubini (*cf.* l'exemple de la page 72), il vient :

$$\operatorname{card}(T) \;=\; \operatorname{card}(S) \;=\; 1 + 2 + \cdots + n \;=\; \frac{n(n+1)}{2}\,.$$

L'idée est maintenant la suivante : une loi *commutative* sur E est entièrement déterminée par sa restriction à T. Formellement, à toute loi $\mu : E \times E \to E$ sur E, associons sa restriction à T. Nous obtenons une application f de $\mathcal{F}(E \times E, E)$ dans $\mathcal{F}(T, E)$. Soit $\nu \in \mathcal{F}(T, E)$. Il existe une unique loi commutative $\mu \in \mathcal{F}(E \times E, E)$ telle que $f(\mu) = \nu$, elle est définie ainsi : pour tout $(i, j) \in [\![1, n]\!]^2$,

$$\mu(x_i, x_j) \;=\; \begin{cases} \nu(x_i, x_j) & \text{si } i \leqslant j \\ \nu(x_j, x_i) & \text{si } i > j\,. \end{cases}$$

Ainsi la restriction de f à l'ensemble des lois commutatives sur E est une bijection de cet ensemble sur $\mathcal{F}(T, E)$. Le nombre de lois commutatives sur E est donc le cardinal de $\mathcal{F}(T, E)$, c'est-à-dire $n^{n(n+1)/2}$ (théorème 24 de la page 76).

II.2.2 Soient $f, g \in \mathcal{F}(\mathbb{R}, \mathbb{R})$. Supposons f et g paires. Pour tout $x \in \mathbb{R}$, la définition de $f + g$ et fg (définition 12 de la page 117) donne :

$$(f+g)(-x) \;=\; f(-x) + g(-x) \;=\; f(x) + g(x) \;=\; (f+g)(x)\,,$$

et de même

$$(fg)(-x) \;=\; f(-x)g(-x) \;=\; f(x)g(x) \;=\; (fg)(x)\,.$$

Ainsi $f + g$ et g sont paires, ce qui montre que S est à la fois additivement stable et multiplicativement stable. Si maintenant f, g sont impaires on a, pour tout $x \in \mathbb{R}$:

$$(f+g)(-x) \;=\; f(-x) + g(-x) \;=\; \big(-f(x)\big) + \big(-g(x)\big) \;=\; -(f+g)(x)\,,$$

et de même

$$(fg)(-x) \;=\; f(-x)g(-x) \;=\; \big(-f(x)\big)\big(-g(x)\big) \;=\; (fg)(x)\,.$$

Ainsi $f+g$ est impaire, ce qui montre que I est additivement stable ; par contre fg est paire. En fait I n'est pas multiplicativement stable : par exemple la fonction sinus est impaire, mais son carré est une fonction paire non nulle, elle n'est donc pas impaire. L'élément neutre multiplicatif de $\mathcal{F}(\mathbb{R}, \mathbb{R})$, à savoir la fonction constante 1, est paire, donc S est un sous-anneau de $\mathcal{F}(\mathbb{R}, \mathbb{R})$. En effet, il est clair que l'opposée d'une fonction paire est paire.

II.2.3 Il s'agit de montrer que, pour tout $a \in H$, l'inverse a^{-1} de a dans G appartient à H (*cf.* la définition 4 de la page 120). D'après le théorème et définition 21 de la page 125, l'ordre de a est

fini, c'est un entier $n \geqslant 1$, tel que $a^n = 1$. Comme H est multiplicativement stable, $a^n \in H$, *i.e.* $1 \in H$. Mais alors, dans G, on a $a^{-1}a = 1 = a^n = a^{n-1}a$, d'où $a^{-1}a = a^{n-1}a$. Puisque a est un élément régulier de G, cette égalité montre que $a^{n-1} = a^{-1}$. Si $n = 1$, $1 = a^n = a$, donc $a^{-1} = 1 \in H$. Si $n \geqslant 2$, $a^{n-1} \in H$ parce que H est multiplicativement stable, donc $a^{-1} \in H$.

Procédons autrement. Considérons la translation à gauche $t_a : x \mapsto ax$; c'est une *permutation* de G (proposition 10 de la page 119). Soit f la restriction de t_a à H. Pour tout $x \in H$, $f(x) = ax \in H$ puisque H est multiplicativement stable. Nous pouvons ainsi considérer f comme application de H dans lui-même, et f est injective car t_a l'est. D'après le théorème 15 de la page 71, f est aussi surjective. En particulier $a \in f(H)$, *i.e.* il existe $x \in H$ tel que $a = ax$; nécessairement $x = 1$ (a est régulier dans G), donc $1 \in H$. Maintenant $1 \in H = f(H)$, *i.e.* il existe $y \in H$ tel que $1 = ay$. Cette fois $y = a^{-1}$, d'où $a^{-1} \in H$.

II.2.4 Notons le groupe multiplicativement. D'abord $1 \in C_G(a)$, car $1a = a = a1$. Soient $x, y \in C_G(a)$: $ax = xa$ et $ay = ya$. Par associativité, il vient :

$$a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a,$$

donc xy commute avec a. Multiplions ensuite par x^{-1}, à gauche et à droite, les deux membres de l'égalité $ax = xa$: $x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1}$. Dans cette égalité, le premier membre vaut $(x^{-1}a)(xx^{-1}) = x^{-1}a$, et le deuxième vaut : $(x^{-1}x)(ax^{-1}) = ax^{-1}$. D'où $x^{-1}a = ax^{-1}$, ce qui montre que $x^{-1} \in C_G(a)$. Ainsi $C_G(a)$ est un sous-groupe de G (définition 4 de la page 120).

L'intersection des $C_G(a)$ pour *tous* les $a \in G$ est formée des $x \in G$ commutant avec *tout* élément de G. C'est donc le *centre* de G (exercice 2 de la page 121).

II.2.5 Pour tout $x \in G$, multiplions à gauche par x^{-1} les deux membres de l'égalité $x^2 = 1$. Il vient $x = x^{-1}$: tout élément de G est son propre inverse. Soient alors $a, b \in G$, montrons que $ab = ba$. Par hypothèse, $1 = (ab)^2 = (ab)(ab)$, soit $ab = (ab)^{-1}$. Mais $(ab)^{-1} = b^{-1}a^{-1}$ (propriété 4 de la proposition 9 de la page 119). D'où :

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba\,,$$

compte tenu du début de cette preuve. Ainsi a et b commutent, ceci pour tous $a, b \in G$, *i.e.* G est commutatif.

Voici une autre solution, sans utiliser les inverses. Soient $a, b \in G$. Par hypothèse, $(ab)^2 = a^2 = b^2 = 1$. Partons de $1 = (ab)^2 = abab$. Multiplions à gauche par a : $a = a^2bab = bab$. Multiplions l'égalité $a = bab$ par b à droite : $ab = bab^2 = ba$.

II.2.6 Notons f l'application $x \mapsto ax$ de $\mathbb{Z}$ dans lui-même. Pour tous $x, y \in \mathbb{Z}$, on a $f(x + y) = a(x + y) = ax + ay = f(x) + f(y)$ (distributivité de la multiplication par rapport à l'addition), donc f est un morphisme de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}, +)$. Si $a = 0$, f est la fonction nulle (constante égale à 0), elle n'est pas injective. Supposons $a \neq 0$. Le noyau de f, formé des $x \in \mathbb{Z}$ tels que $ax = 0$, est trivial (parce que l'anneau $\mathbb{Z}$ est intègre). Ce morphisme est donc injectif (théorème 20 de la page 124).

Supposons f surjectif. En particulier $1 \in f(\mathbb{Z})$, *i.e.* il existe un $x \in \mathbb{Z}$ tel que $ax = 1$. Autrement dit a est un élément inversible de l'anneau $\mathbb{Z}$, c'est-à-dire $a = \pm 1$. La réciproque est évidente, car les applications $x \mapsto x$ et $x \mapsto -x$ sont des bijections de $\mathbb{Z}$ sur lui-même.

II.2.7 Notons les deux groupes multiplicativement. Posons donc :

$$H := \big\{x \in G \;\big|\; f(x) = g(x)\big\},$$

et montrons que H est un sous-groupe de G.

En premier lieu, $1_G \in H$, car $f(1_G) = 1_{G'} = g(1_G)$. Soient $x, y \in H$: $f(x) = g(x)$ et $f(y) = g(y)$. Comme f et g sont des morphismes, il vient :

$$f(xy) \;=\; f(x)f(y) \;=\; g(x)g(y) \;=\; g(xy)\,, \quad \text{donc} \quad xy \in H\,.$$

De même, en vertu de l'assertion 2 de la proposition 18 de la page 123,

$$f(x^{-1}) \;=\; f(x)^{-1} \;=\; g(x)^{-1} \;=\; g(x^{-1})\,,$$

donc $x^{-1} \in H$. Il en résulte que H est un sous-groupe de G.

Supposons maintenant que S soit une partie génératrice de G et que $f(x) = g(x)$ pour tout $x \in S$. Alors H est un sous-groupe de G contenant S, donc $H = G$ (proposition 15 de la page 122). Autrement dit, $f(x) = g(x)$ pour tout $x \in G$, *i.e.* $f = g$.

II.2.8 1) Démontrons que la loi $\top$ est associative. Soient $a, b, c \in \mathbb{Z}$ et par ailleurs $\varepsilon, \eta, \zeta \in \{-1, 1\}$. Par définition de la loi $\top$, il vient d'un côté :

$$\big[(a,\varepsilon)\top(b,\eta)\big]\top(c,\zeta) = (a+\varepsilon b, \varepsilon\eta)(c,\zeta) = \big((a+\varepsilon b)+(\varepsilon\eta)c, (\varepsilon\eta)\zeta\big)\,,$$

et d'un autre côté :

$$(a,\varepsilon)\big[(b,\eta)(c,\zeta)\big] = (a,\varepsilon)(b+\eta c, \eta\zeta) = \big(a+\varepsilon(b+\eta c), \varepsilon(\eta\zeta)\big)\,.$$

Les égalités (dans $\mathbb{Z}$) $(a+\varepsilon b)+(\varepsilon\eta)c = a+\varepsilon(b+\eta c)$ et $(\varepsilon\eta)\zeta = \varepsilon(\eta\zeta)$ prouvent l'associativité de $\top$.

Vérifions que $(0,1)$ est élément neutre pour la loi $\top$. Soit $(a,\varepsilon) \in G$. Alors :

$$(0,1)\top(a,\varepsilon) = (0+1a, 1\varepsilon) = (a,\varepsilon)\,,\ (a,\varepsilon)\top(0,1) = (a+\varepsilon 0, \varepsilon 1) = (a,\varepsilon)\,.$$

Soit enfin $(a,\varepsilon) \in G$. Cherchons un symétrique (b,η) de (a,ε) pour la loi $\top$. Nous voulons en particulier que l'égalité $(b,\eta)\top(a,\varepsilon) = (0,1)$ soit vérifiée. Cette égalité équivaut aux deux égalités $b+\eta a = 0$ et $\eta\varepsilon = 1$. Il y a une solution unique évidente : $\eta = \varepsilon$ et $b = -\varepsilon a$. Encore faut-il vérifier que $(a,\varepsilon)\top(b,\eta) = (0,1)$. Compte tenu des valeurs de b et η, il vient :

$$(a,\varepsilon)\top(b,\eta) = (a+\varepsilon b, \varepsilon\eta) = \big(a+\varepsilon(-\varepsilon a), \varepsilon^2\big) = (0,1)\,,$$

puisque $\varepsilon^2 = 1$. Cela achève de montrer que G, muni de la loi $\top$, est un groupe.

Ce groupe n'est pas commutatif : par exemple, si $a, b \in \mathbb{Z}$, $(a,-1)\top(b,-1) = (a-b,1)$, de même $(b,-1)\top(a,-1) = (b-a,-1)$.

Ainsi $(-1,1) = (0,-1)\top(1,-1) \neq (1,-1)\top(0,-1) = (1,1)$.

2) En général, si $t \in \mathbb{Z}$, $(t,-1)\top(t,-1) = (0,1)$, donc $(t,-1) \in G$ est d'ordre 2. Soit maintenant H le sous-groupe de G engendré par $\{a,b\}$. Il contient déjà $c := b\top a = (1,-1)\top(0,-1) = (1,1)$. Observons ensuite que, pour tous $x, y \in \mathbb{Z}$, $(x,1)\top(y,1) = (x+y,1)$. Cela montre que $x \mapsto (x,1)$ est un morphisme de $(\mathbb{Z},+)$ dans $(G,\top)$. Il en résulte que, si $n \in \mathbb{N}^*$, on a :

$$(n,1) \;=\; \overbrace{c\top c\top\cdots\top c}^{n \text{ termes}} \in H\,.$$

Le symétrique de $(n,1)$ pour $\top$, à savoir $(-n,1)$ appartient alors aussi à H, *i.e.* $(n,1) \in H$ pour tout $n \in \mathbb{Z}$. Enfin, si $x \in \mathbb{Z}$, il vient :

$$(x,-1) \;=\; (x,1)\top(0,-1) \;=\; (x,1)\top a \in H\,, \quad \text{d'où} \quad H = G\,.$$

En conclusion, $\{a,b\}$ est une partie génératrice de G.

II.2.9 1) Observons d'abord que c, d, e s'expriment en fonction de a et b :

$$c = ab\,,\ \ d = bc = b(ab) = bab\,,\ \ e = cd = (ab)(bab) = ab^2ab\,. \tag{1}$$

Soit H le sous-groupe de G engendré par a et b. Il contient a et b, donc aussi c, d, e, à cause des formules (1). Comme (a, b, c, d, e) est une famille génératrice de G, H est égal à G, *i.e.* la famille (a, b) engendre G.

L'égalité $de = a$ s'écrit $(bab)(ab^2ab) = a$, d'où la première formule $(**)$. De même l'égalité $ea = b$ s'écrit $(ab^2ab)a = b$, d'où la deuxième formule $(**)$. Ensuite,

$$a = babab^2ab\,,\ \text{d'où}\ \ a^2 = (babab^2ab)a = (bab)(ab^2aba) = (bab)b = bab^2\,,$$

ce qui donne la troisième formule $(**)$. Enfin, en utilisant la première et la troisième formule $(**)$, on obtient :

$$a \ = \ babab^2ab \ = \ (ba)(bab^2)(ab) \ = \ (ba)a^2(ab) \ = \ ba^4b\,,$$

d'où la dernière formule $(**)$.

2) L'idée est d'observer que les cinq égalités $(*)$ sont invariantes par permutation circulaire de a, b, c, d, e. Plus précisément, posons :

$$a' := b\,,\ b' := c\,,\ c' := d\,,\ d' := e\,,\ e' := a\,.$$

Alors $a'b' = bc = d = c'$, de même $b'c' = cd = e = d'$, etc jusqu'à $e'a' = ab = c = b'$. Le raisonnement fait en 1 sur a, b, c, d, e s'applique donc aussi à a', b', c', d', e'. En particulier, $b'a'^4b' = a'$, c'est-à-dire $cb^4c = b$. Mais $c = ab$, donc $(ab)b^4(ab) = b$ soit, en simplifiant à droite par b : $ab^5a = 1$. En multipliant à gauche et à droite par a^{-1}, on en déduit l'égalité $b^5 = a^{-2}$.

Comme ci-dessus, par permutation circulaire, on peut déduire de l'égalité $b^5 = a^{-2}$ l'égalité $c^5 = b^{-2}$. Alors :

$$c^{5^2} \ = \ (c^5)^5 \ = \ (b^{-2})^5 \ = \ (b^5)^{-2} \ = \ (a^{-2})^{-2} \ = \ a^4\,.$$

Appliquons à nouveau notre permutation circulaire : $d^5 = c^{-2}$, d'où :

$$d^{5^3} \ = \ (d^5)^{5^2} \ = \ (c^{-2})^{5^2} \ = \ (c^{5^2})^{-2} \ = \ (a^4)^{-2} \ = \ a^{-8}\,.$$

Encore une fois : $e^5 = d^{-2}$, d'où :

$$e^{5^4} \ = \ (e^5)^{5^3} \ = \ (d^{-2})^{5^3} \ = \ (d^{5^3})^{-2} \ = \ (a^{-8})^{-2} \ = \ a^{16}\,.$$

Une dernière fois : $a^5 = e^{-2}$, d'où :

$$a^{5^5} \ = \ (a^5)^{5^4} \ = \ (e^{-2})^{5^4} \ = \ (e^{5^4})^{-2} \ = \ (a^{16})^{-2} \ = \ a^{-32}\,.$$

Finalement, $a^{5^5} = a^{-32}$.

3) Posons $N := 5^5 + 32$ (en fait $N = 3157$). Nous venons de voir que $a^N = 1$, de sorte que a est d'ordre fini m divisant N (*cf.* le théorème et définition 21 de la page 125). En particulier, m est premier avec 10, c'est-à-dire premier avec 2 et premier avec 5. D'après l'exercice 5 de la page 131, a^{-2} est un générateur de $\langle a\rangle$. Par permutation circulaire, on a aussi $b^N = 1$, d'où cette fois $\langle b^5\rangle = \langle b\rangle$. L'égalité $b^5 = a^{-2}$ implique donc la suivante : $\langle b\rangle = \langle a\rangle$. Puisque $b \in \langle b\rangle$, il en résulte que $b \in \langle a\rangle$.

Le sous-groupe $\langle a\rangle$ de G contient ainsi a et b, il est donc égal à G, puisque la famille (a, b) engendre G. Dans ces conditions, G est cyclique, en particulier il est abélien. Revenons alors aux égalités $(**)$. Puisque G est commutatif, les égalités $bab^2 = a^2$ et $ba^4b = a$ s'écrivent

respectivement $ab^3 = a^2$ et $a^4b^2 = a$ soit, après simplification, $b^3 = a$ et $b^2 = a^{-3}$. Ainsi $b = b^3(b^2)^{-1} = a(a^{-3})^{-1} = a^4$, d'où l'on déduit :

$$a = b^3 = (a^4)^3 = a^{12}, \quad \text{soit} \quad a^{11} = 1.$$

Résumons : G est un groupe cyclique, engendré par a, dont l'ordre m (égal à l'ordre de G) divise 11. Puisque 11 est premier, m vaut 1 ou 11. Dans le premier cas, G est trivial, et dans le second G est cyclique d'ordre 11, *i.e.* isomorphe à $(\mathbb{Z}/11\mathbb{Z}, +)$.

4) La question précédente suggère de poser $b := a^4$. Ensuite, nous n'avons guère le choix. Nous devons poser $c := ab = a^5$, $d := bc = a^4a^5 = a^9$, et enfin $e := cd = a^5a^9 = a^{14} = a^3$ (car $a^{11} = 1$). Il reste à vérifier les égalités $de = a$ et $ea = b$:

$$de = a^9a^3 = a^{12} = a \quad \text{et} \quad ea = a^3a = a^4 = b.$$

II.2.10 Puisque G est commutatif, on a $(ab)^k = a^kb^k$ pour tout $k \in \mathbb{Z}$ (formule (18)). Ainsi $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = 1$. Cela montre que ab est d'ordre fini divisant mn. Pour prouver que l'ordre de ab est mn il suffit de voir que tout entier $k \in \mathbb{Z}$ tel que $(ab)^k = 1$ est multiple de mn (*cf.* l'assertion 3 du théorème et définition 21 de la page 125). Considérons un tel entier k. Partons des égalités :

$$1 = \left[(ab)^k\right]^m = (ab)^{mk} = a^{mk}b^{mk} = (a^m)^kb^{mk} = b^{mk}.$$

Puisque b est d'ordre n, n divise mk. Mais $m \wedge n = 1$, donc n divise k, d'après le théorème de Gauß (théorème 54 de la page 97). De manière symétrique, m divise k. Ainsi k est un multiple commun de m et n, *i.e.* un multiple de leur ppcm. Or ce ppcm est mn (théorème 44 de la page 90), donc k est multiple de mn.

II.2.11 1) Tout d'abord, chaque H_i est un sous-groupe de G. Le produit A est alors le groupe produit de $H_1, \ldots, H_n$ (exemple 2 de la page 118). Soient alors $y := (y_1, \ldots, y_n)$ et $z := (z_1, \ldots, z_n)$ deux éléments de A : pour $i = 1, \ldots, n$, y_i et z_i sont des éléments de H_i. Par définition de la loi produit, $y + z = (y_1 + z_1, \ldots, y_n + z_n)$. Par définition de f, $f(y + z)$ vaut :

$$(y_1 + z_1) + \cdots + (y_n + z_n) = (y_1 + \cdots + y_n) + (z_1 + \cdots + z_n) = f(y) + f(z),$$

la première égalité venant de la commutativité de G. Ainsi $f : A \to G$ est un morphisme.

Soit $i \in [\![1, n]\!]$. Il est clair que x_i est l'image par f de l'élément $y = (y_1, \ldots, y_n)$ de A défini par $y_i := x_i$ et $y_j := 0$ pour tout $j \in [\![1, n]\!]$ distinct de i. Ainsi $f(A)$ contient tous les x_i, d'où $f(A) = G$: f est surjectif.

2) Appliquons d'abord le théorème 20 de la page 124 (formule (20)) au morphisme f. Puisque f est surjectif, ladite formule montre que l'ordre n de G divise l'ordre de A. En particulier, p divisant n par hypothèse, il divise l'ordre de A.

Pour tout $i \in [\![1, n]\!]$, notons k_i l'ordre de x_i, c'est-à-dire l'ordre du groupe H_i. L'ordre de A est le produit des k_i, et ainsi p divise le produit des k_i. D'après le lemme d'Euclide (théorème 36 de la page 85), il existe un $i \in [\![1, n]\!]$ tel que p divise k_i. Écrivons $k_i := pt$, où $t \in \mathbb{N}^*$. D'après l'exercice 5 de la page 131, x_i^t est d'ordre p (plus simplement $(x_i^t)^p = x_i^{k_i} = 1$ mais $x_i^t \neq 1$, par définition de l'ordre d'un élément). Nous avons ainsi trouvé un élément de G ayant pour ordre p.

II.2.12 Si $s \in \mathfrak{S}(E)$, $f \circ s \circ f^{-1}$ est une bijection de F sur F, *i.e.* une permutation de F, comme composée de trois bijections. Notons $\theta : s \mapsto f \circ s \circ f^{-1}$ l'application de $\mathfrak{S}(E)$ dans $\mathfrak{S}(F)$ obtenue. On vérifie immédiatement que θ est bijective, la bijection réciproque étant l'application $t \mapsto f^{-1} \circ t \circ f$ de $\mathfrak{S}(F)$ dans $\mathfrak{S}(E)$. Il suffit donc de montrer que θ est un morphisme (de groupes). Pour tous $s, s' \in \mathfrak{S}(E)$, il vient :

$$\theta(s) \circ \theta(s') = (f \circ s \circ \underbrace{f^{-1}}_{\mathrm{id}}) \circ (\underbrace{f}_{\mathrm{id}} \circ s' \circ f^{-1}) = f \circ (s \circ s') \circ f^{-1} = \theta(s \circ s')\,.$$

II.2.13 L'application s est involutive ($s \circ s = 1$), c'est donc une permutation de $\mathbb{Z}$, *i.e.* un élément de $\mathfrak{S}(\mathbb{Z})$, d'ordre 2. Il est clair que t est une bijection de $\mathbb{Z}$ sur lui-même (translation de vecteur 1), la bijection réciproque étant l'application $x \mapsto x - 1$ (translation de vecteur -1). Ainsi $t \in \mathfrak{S}(\mathbb{Z})$. Soit $x \in \mathbb{Z}$. On a :

$$s\big(t(x)\big) = s(x+1) = -(x+1) = -x - 1, \quad \text{et} \quad t\big(s(x)\big) = t(-x) = -x + 1\,.$$

Ainsi $s \circ t \neq t \circ s$, et même $(s \circ t)(x) \neq (t \circ s)(x)$ pour tout $x \in \mathbb{Z}$. Cela montre que le groupe $\mathfrak{S}(\mathbb{Z})$ n'est pas commutatif, ce que nous savions déjà (exemple de la page 127), et même que le sous-groupe Γ de $\mathfrak{S}(\mathbb{Z})$ engendré par s et t n'est pas commutatif.

Posons $u := t \circ s \in \Gamma$. Comme nous l'avons vu, $u(x) = 1 - x$ pour tout $x \in \mathbb{Z}$, donc u est involutive $\big(1 - (1 - x) = x\big)$. Considérons maintenant le groupe $(G, \top)$ étudié dans l'exercice II.2.8. L'idée est de chercher un isomorphisme f de G sur Γ appliquant les éléments $a = (0, -1)$ et $b = (1, -1)$ de G sur u et s respectivement. Définissons $f : G \to \Gamma$ comme suit. Pour tout $n \in \mathbb{Z}$ et tout $\varepsilon \in \{-1, 1\}$, nous posons :

$$f\big((n, \varepsilon)\big) := \begin{cases} t^{-n} & \text{si } \varepsilon = 1 \\ u \circ t^{n} & \text{si } \varepsilon = -1\,. \end{cases}$$

Ainsi $f(a) = f\big((0, -1)\big) = u$ et $f(b) = f\big((1, -1)\big) = u \circ t$. Or $u \circ t = s$: pour tout $x \in \mathbb{Z}$, $(u \circ t)(x) = u(x + 1) = 1 - (x + 1) = -x = s(x)$. Il en résulte que $f(b) = s$.

Montrons que f est un morphisme. Soient $m, n \in \mathbb{Z}$ et $\varepsilon, \eta \in \{-1, 1\}$. D'abord

$$f\big((m, \varepsilon) \top (n, \eta)\big) = f\big((m + \varepsilon n, \varepsilon\eta)\big)\,.$$

Notons w le second membre de cette égalité. Distinguons quatre cas, suivant les valeurs de ε et η.

1. Cas $\varepsilon = \eta = 1$. Alors $w = f\big((m + n, 1)\big) = t^{-(m+n)}$.

   D'un autre côté, $f\big((m, 1)\big) = t^{-m}$ et $f\big((n, 1)\big) = t^{-n}$, d'où l'égalité voulue, à savoir :

   $$f\big((m, \varepsilon) \top (n, \eta)\big) = f\big((m, \varepsilon)\big) \circ f\big((n, \eta)\big)\,. \qquad (**)$$

2. Cas $\varepsilon = -1,\ \eta = 1$. Alors $w = f\big((m - n, -1)\big) = u \circ t^{m-n}$.

   D'un autre côté, $f\big((m, -1)\big) = u \circ t^{m}$ et $f\big((n, 1)\big) = t^{-n}$. L'égalité $(**)$ est encore vraie.

3. Cas $\varepsilon = 1,\ \eta = -1$. Alors $w = f\big((m + n, -1)\big) = u \circ t^{m+n}$.

   D'un autre côté, $f\big((m, 1)\big) = t^{-m}$ et $f\big((n, -1)\big) = u \circ t^{n}$. L'égalité $(**)$ sera vraie si, et seulement si, $u \circ t^{m+n} = t^{-m} \circ u \circ t^{n}$, soit $u \circ t^{m} = t^{-m} \circ u$. Cette égalité sera prouvée plus loin.

4. Cas $\varepsilon = \eta = -1$. Alors $w = f\big((m-n,1)\big) = t^{n-m}$.

   D'un autre côté, $f\big((m,-1)\big) = u \circ t^m$ et $f\big((n,-1)\big) = u \circ t^n$. L'égalité $(**)$ sera vraie si, et seulement si, $t^{n-m} = u \circ t^m \circ u \circ t^n$, soit $t^{-m} = u \circ t^m \circ u$. Puisque $u^2 = 1$, la dernière égalité est équivalente à celle que nous avons admise.

Pour achever de prouver que f est un morphisme, il suffit ainsi d'établir, pour tout $m \in \mathbb{Z}$, l'égalité suivante (en notant que $u = u^{-1}$) :

$$u \circ t^m \circ u^{-1} \;=\; t^{-m}\,. \qquad (***)$$

Considérons l'application $g : \sigma \mapsto u \circ \sigma \circ u^{-1}$ de $\mathfrak{S}(\mathbb{Z})$ dans lui-même. D'après l'exemple de la page 124, g est un automorphisme de $\mathfrak{S}(\mathbb{Z})$, *i.e.* un morphisme bijectif de $\mathfrak{S}(\mathbb{Z})$ sur lui-même. Il en résulte que, pour tout $n \in \mathbb{Z}$, $g(t^n) = g(t)^n$ (assertion 1 de la proposition 18 de la page 123). Pour prouver l'égalité $(***)$, il suffit donc de voir que $g(t) = t^{-1}$. Puisque $u \circ t = s$, il vient :

$$g(t) = u \circ t \circ u^{-1} = s \circ u^{-1} = s \circ (t \circ s)^{-1} = s \circ s^{-1} \circ t^{-1} = t^{-1}\,.$$

Finalement, f est bien un morphisme de $(G, \top)$ dans Γ.

Nous avons vu que $f(a) = u = t \circ s$ et $f(b) = s$, d'où $f(a \top b) = t \circ s^2 = t$. Ainsi l'image de f contient s et t, qui engendrent Γ, donc $f(G) = \Gamma$: f est surjectif.

Montrons enfin que f est injectif, *i.e.* que $\mathrm{Ker}(f)$ est trivial. Notons d'abord que t est d'ordre infini : pour tout $n \in \mathbb{Z}$, $f\big((n,1)\big) = t^{-n}$ est la translation $x \mapsto x - n$, qui n'est triviale que si $n = 0$. D'autre part, si $n \in \mathbb{Z}$, $f\big((n,-1)\big) = u \circ t^n$ est définie par $x \mapsto u(x+n) = 1-(x+n) = (1-n)-x$, donc $f\big((n,-1)\big) \neq 1$ (choisir un entier $x \in \mathbb{Z}$ tel que $2x \neq 1-n$). En conclusion, f est un morphisme bijectif de G sur Γ, *i.e.* un isomorphisme de G sur Γ.

II.2.14 1) Posons $a := (1\ 2)(3\ 4)$, $b := (1\ 3)(2\ 4)$ et $c := (1\ 4)(2\ 3)$. Rappelons une formule de conjugaison importante (*cf.* la formule (22) de la page 126). Soient $n \in \mathbb{N}$ et $i, j \in [\![1, n]\!]$ deux indices distincts. Pour toute permutation $s \in \mathfrak{S}_n$, on a :

$$s \circ (i\ j) \circ s^{-1} \;=\; \big(s(i)\ s(j)\big)\,. \qquad (1)$$

Si donc s laisse fixes i et j, $s \circ (i\ j) \circ s^{-1} = (i\ j)$, soit $s \circ (i\ j) = (i\ j) \circ s$, autrement dit s commute avec $(i\ j)$. Par exemple, si $i, j, k, l \in [\![1, n]\!]$ sont distincts, $(i\ j)$ et $(k\ l)$ commutent, puisque $(k\ l)$ laisse fixes i et j.

Ainsi $(1\ 2)$ et $(3\ 4)$ commutent, donc $a^2 = (1\ 2)^2(3\ 4)^2 = 1$: a est d'ordre 2. De même b et c sont d'ordre 2. Calculons ensuite $ab = a \circ b$. Rappelons qu'une permutation s peut être écrite en indiquant, au-dessous de tout indice i, l'image de i par s. Ainsi :

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}\,,\quad b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}\,.$$

Composons (on effectue d'abord b, puis a) :

$$ab \;=\; a \circ b \;=\; \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\,,\quad \text{soit}\quad ab \;=\; (1\ 4)(2\ 3) \;=\; c\,.$$

Puisque a et b commutent, on a aussi $ba = c$. Ensuite $bc = b(ba) = b^2a = a$, et $cb = (ab)b = ab^2 = a$. De même $ac = a(ab) = a^2b = b$ et $ca = (ba)a = ba^2 = b$. D'où le tableau suivant :

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Ce tableau montre que $V_4 = \{1, a, b, c\}$ est une partie stable de $\mathfrak{S}_4$. Comme chaque élément de V_4 est son propre inverse, V_4 est un sous-groupe de $\mathfrak{S}_4$. Enfin a, b, c sont des permutations *paires* (*cf.* le théorème et définition 26 de la page 129), donc V_4 est un sous-groupe du groupe alterné $\mathfrak{A}_4$. Le fait que V_4 soit isomorphe au groupe (additif) $(\mathbb{Z}/2\mathbb{Z})^2$ va résulter de la question suivante.

2) Soit donc $(G, \times)$ un groupe d'ordre 4 dont tout élément est de carré 1. Notons x, y, z les éléments de G distincts de l'élément neutre 1. Déterminons le produit xy. D'abord $xy \neq 1$: sinon $xy = xx$, d'où $y = x$ en simplifiant à gauche par x. Ensuite $xy \neq x$, car sinon $y = 1$, de même $xy \neq y$, car sinon $x = 1$. Il n'y a pas le choix : $xy = z$. Le même argument montre que le produit de deux éléments distincts parmi x, y, z est égal au troisième élément de $\{x, y, z\}$. Comme x^2, y^2 et z^2 sont égaux à 1, on obtient la table de multiplication suivante :

	1	x	y	z
1	1	x	y	z
x	x	1	z	y
y	y	z	1	x
z	z	y	x	1

Cette table est la même que la précédente, à condition de remplacer a, b, c par x, y, z respectivement. Soit donc f la bijection de V_4 sur G appliquant $1, a, b, c$ sur $1, x, y, z$ respectivement. En fait f est un morphisme, donc un isomorphisme. Il s'agit de vérifier que, si $u, v \in V_4$, on a $f(uv) = f(u)f(v)$. Comme $f(1) = 1$, c'est clair si $u = 1$ ou $v = 1$. C'est aussi vrai si $u = v$, car alors $u^2 = 1$ et aussi $f(u)^2 = 1$. Il reste le cas où $u, v \in \{a, b, c\}$ sont distincts. Dans ce cas, uv est l'élément de $\{a, b, c\}$ distinct de u, v. De plus $f(u), f(v) \in \{x, y, z\}$ sont distincts, donc $f(u)f(v)$ est l'élément de $\{x, y, z\}$ distinct de $f(u), f(v)$. D'où $f(uv) = f(u)f(v)$, à cause de la bijectivité de f. En conclusion, f est un isomorphisme de V_4 sur G.

Voici le résultat obtenu : tout groupe d'ordre 4 dans lequel chaque élément non trivial est d'ordre 2 est isomorphe à V_4. Puisque tout élément non trivial du groupe additif $(\mathbb{Z}/2\mathbb{Z})^2$ est d'ordre 2, le groupe $\big((\mathbb{Z}/2\mathbb{Z})^2, +\big)$ est isomorphe à V_4.

Soit enfin $(G', \times)$ un groupe d'ordre 4. Si $x \in G'$ et $x \neq 1$, l'ordre de x est un entier strictement plus grand que 1 divisant 4 (théorème de Lagrange), cet ordre vaut donc 2 ou 4. Distinguons alors deux cas. Supposons d'abord que G' possède un élément w d'ordre 4. Alors w engendre G', donc G' est cyclique d'ordre 4. Il en résulte que G' est isomorphe à $(\mathbb{Z}/4\mathbb{Z}, +)$, en vertu du théorème 30 de la page 131.

Supposons que G' n'ait aucun élément d'ordre 4. D'après le début de l'alinéa précédent, tout élément de G' distinct de 1 est alors d'ordre 2. Le début de cette question montre dans ce cas que G' est isomorphe à V_4. En conclusion, à isomorphisme près, il y a exactement deux

groupes d'ordre 4, à savoir les groupes additifs $(\mathbb{Z}/2\mathbb{Z})^2$ et $\mathbb{Z}/4\mathbb{Z}$ (ils ne sont pas isomorphes, car le premier de ces groupes n'est pas cyclique, alors que le deuxième l'est).

II.2.15 Par définition, il existe des éléments $a_1, \dots, a_n$ de E deux à deux distincts tels que $c := (a_1\ a_2\ \cdots\ a_n)$ (*cf.* la définition 9 de la page 126). Posons $S := \{a_1, \dots, a_n\}$. Rappelons que tout $x \in E \setminus S$ est un point fixe de c, *i.e.* $c(x) = x$. Il en résulte que, pour tout $j \in \mathbb{Z}$, x est aussi un point fixe de c^j.

Par définition de c, $c(a_1) = a_2$. Si $n \geqslant 3$, $c(a_2) = a_3$, et par suite $c^2(a_1) = c(a_2) = a_3$. Par une récurrence immédiate sur k, on montre que, pour tout $k \in [\![1, n-1]\!]$, on a $c^k(a_1) = a_{k+1}$, et en particulier $c^k \neq 1$, puisque $a_{k+1} \neq a_1$. Ensuite $c^n(a_1) = c\big(c^{n-1}(a_1)\big) = c(a_n) = a_1$, donc $c^n(a_1) = a_1$. De plus, pour tout $j \in [\![2, n]\!]$, $a_j = c^{j-1}(a_1)$, d'où :

$$c^n(a_j) = c^n\big(c^{j-1}(a_1)\big) = c^{n+j-1}(a_1) = c^{j-1}\big(c^n(a_1)\big) = c^{j-1}(a_1) = a_j\,.$$

Ainsi $c^n = 1$. Comme $c^k \neq 1$ pour $k = 1, \dots, n-1$, c est bien d'ordre fini égal à n.

II.2.16 Soit $\mathcal{C}$ l'ensemble des n-cycles de E. Il s'agit de calculer le cardinal de $\mathcal{C}$. Notons $\mathcal{A}$ l'ensemble des arrangements des éléments de E pris n à n. D'après le théorème 27 de la page 77, le cardinal de $\mathcal{A}$ vaut :

$$\operatorname{card}(\mathcal{A}) \;=\; N(N-1)\cdots(N-n+1) \;=\; \frac{N!}{(N-n)!}\,.$$

Soit $\alpha := (a_1, \dots, a_n) \in \mathcal{A}$: $a_1, \dots, a_n$ sont des éléments de E deux à deux distincts. Associons à α le n-cycle $(a_1\ a_2\ \cdots\ a_n) \in \mathfrak{S}(E)$. Nous obtenons ainsi une application f de $\mathcal{A}$ dans $\mathcal{C}$. Par définition même d'un n-cycle, f est surjective. Pour calculer $\operatorname{card}(\mathcal{C})$, nous appliquons la formule (1) de la page 72, qui donne ici :

$$\operatorname{card}(\mathcal{A}) \;=\; \sum_{c\,\in\,\mathcal{C}} \operatorname{card}\,\big(f^{-1}(c)\big)\,. \qquad (*)$$

Soit $c \in \mathcal{C}$. Il existe des éléments $a_1, \dots, a_n$ de E deux à deux distincts tels que $c = (a_1\ a_2\ \cdots\ a_n)$. La fibre $f^{-1}(c)$ est formée des arrangements $\beta = (b_1, \dots, b_n) \in \mathcal{A}$ tels que $(b_1\ b_2\ \cdots\ b_n) = c$. La définition de c montre que $c = (a_2\ a_3\ \cdots\ a_n\ a_1)$ et, plus généralement, pour tout $k \in [\![1, n]\!]$, on a :

$$c \;=\; (a_k\ a_{k+1}\ \cdots\ a_n\ a_1\ a_2\ \cdots\ a_{k-1})\,.$$

On obtient ainsi déjà n éléments de $f^{-1}(c)$ distincts, à savoir :

$$(a_1, \dots, a_n)\,,\ (a_2, \dots, a_n, a_1)\,, \dots, (a_n, a_1, \dots, a_{n-1})\,.$$

Inversement, soit $\beta = (b_1, \dots, b_n) \in f^{-1}(c)$. L'égalité $f(\beta) = c$ signifie que les deux n-cycles $(a_1\ a_2\ \cdots\ a_n)$ et $(b_1\ b_2\ \cdots\ b_n)$ sont égaux. Puisque $c(b_1) = b_2$, b_1 n'est pas un point fixe de $(a_1\ a_2\ \cdots\ a_n)$. Il existe donc un $k \in [\![1, n]\!]$ tel que $b_1 = a_k$. Sur la définition d'un n-cycle, on voit alors aussitôt que $(b_1, \dots, b_n) = (a_k, a_{k+1}, \dots, a_n, a_1, \dots, a_{k-1})$. Ainsi la fibre $f^{-1}(c)$ est formée des n arrangements obtenus ci-dessus, de sorte que $f^{-1}(c)$ est de cardinal n. La formule $(*)$ donne maintenant :

$$\operatorname{card}(\mathcal{A}) \;=\; \sum_{c\,\in\,\mathcal{C}} n \;=\; n\operatorname{card}(\mathcal{C})\,.$$

D'où le cardinal de $\mathcal{C}$:

$$\operatorname{card}(\mathcal{C}) \;=\; \frac{\operatorname{card}(\mathcal{A})}{n} \;=\; \frac{N(N-1)\cdots(N-n+1)}{n}\,.$$

Par exemple, pour $n = 2$, le nombre de transpositions de E est $N(N-1)/2$.

II.2.17 Notons W le second membre de la formule à démontrer. C'est *a priori* un rationnel non nul. Nous allons montrer d'une part que le signe de W est $\varepsilon(s)$, et d'autre part que $|W| = 1$. Cela établira l'égalité $W = \varepsilon(s)$. Notons E l'ensemble des couples $(i,j) \in [\![1,n]\!]^2$ tels que $i < j$.

Soit $(i,j) \in E$. Rappelons que (i,j) est une *inversion* de s si $s(i) > s(j)$; dans ce cas, $s(i) - s(j) < 0$. Si $(i,j) \in E$ n'est pas une inversion de s, $s(i) - s(j) > 0$. Il en résulte que le signe de W est $(-1)^{N(s)}$, où $N(s)$ est le nombre d'inversions de s. D'après la proposition 27 de la page 129, le signe de W est donc $\varepsilon(s)$.

Calculons ensuite $|W|$. Notons P l'ensemble des paires d'éléments de $[\![1,n]\!]$, *i.e.* des parties à deux éléments de $[\![1,n]\!]$. L'idée est que, si $i,j \in [\![1,n]\!]$ sont distincts, $|i-j|$ ne dépend que de la paire $\alpha = \{i,j\} \in P$. Nous pouvons donc sans ambiguïté poser $d(\alpha) := |i-j|$. De plus, $(i,j) \mapsto \{i,j\}$ est une bijection de E sur P, la bijection réciproque étant $\alpha \mapsto \big(\min(\alpha), \max(\alpha)\big)$. La formule de changement d'indice (8) donne ainsi :

$$\prod_{(i,j)\in E} |i-j| \;=\; \prod_{\alpha\in P} d(\alpha)\,.$$

De même, si $(i,j) \in E$ et $\alpha := \{i,j\}$, $\big|s(i) - s(j)\big|$ ne dépend que de la paire $\big\{s(i), s(j)\big\}$, *i.e.* de $s(\alpha)$, image par s de la partie α de $[\![1,n]\!]$; en fait $\big|s(i) - s(j)\big| = d\big(s(\alpha)\big)$. D'où :

$$\prod_{(i,j)\in E} \big|s(i) - s(j)\big| \;=\; \prod_{\alpha\in P} d\big(s(\alpha)\big)\,.$$

Maintenant $\alpha \mapsto s(\alpha)$ est une application bijective de P sur lui-même, la bijection réciproque est $\alpha \mapsto s^{-1}(\alpha)$. La formule de changement d'indice donne ainsi : $\displaystyle\prod_{\alpha\in P} d(\alpha) = \prod_{\beta\in P} d\big(s(\beta)\big)$.

On en déduit les égalités suivantes :

$$\prod_{(i,j)\in E} |i-j| \;=\; \prod_{\alpha\in P} d(\alpha) \;=\; \prod_{\alpha\in P} d\big(s(\alpha)\big) \;=\; \prod_{(i,j)\in E} \big|s(i) - s(j)\big|\,.$$

Revenons à $|W|$:

$$|W| = \prod_{(i,j)\in E} \frac{\big|s(i) - s(j)\big|}{|i-j|} = \left(\prod_{(i,j)\in E} \big|s(i) - s(j)\big|\right) \Big/ \left(\prod_{(i,j)\in E} |i-j|\right) = 1\,.$$

Finalement, $|W| = 1$ et le signe de W est $\varepsilon(s)$, donc $W = \varepsilon(s)$.

II.2.18 Soit plus généralement X un ensemble fini à n éléments ($n \geqslant 1$). Notons $\mathcal{T}$ l'ensemble des transpositions appartenant à $\mathfrak{S}(X)$. Soit donc V une partie génératrice de $\mathfrak{S}(X)$ formée de transpositions, *i.e.* $V \subset \mathcal{T}$. Il s'agit de prouver l'inégalité $\operatorname{card}(V) \geqslant n-1$. Notons d'abord qu'il peut y avoir égalité : dans l'assertion 1 du théorème 24 de la page 127, chacune des parties S et T est une partie génératrice de $\mathfrak{S}_n$, formée de $n-1$ transpositions.

Nous allons démontrer l'inégalité $\operatorname{card}(V) \geqslant n-1$ par récurrence sur n. Le cas $n = 1$ est évident, le cas $n = 2$ aussi, car V ne peut pas être vide (de cardinal 0) puisque $\mathfrak{S}(X)$ n'est pas trivial. Si $n = 3$ et $\operatorname{card}(V) < 2$, nécessairement V est formé d'une seule transposition, qui engendre donc $\mathfrak{S}(X)$, ce qui est absurde, car $\mathfrak{S}(X)$ serait alors cyclique d'ordre 2 (il est en fait d'ordre 6). Supposons maintenant $n \geqslant 4$, le résultat annoncé étant vrai à l'ordre $n-1$. Par ailleurs nous supposons aussi que l'on a $\operatorname{card}(V) \leqslant n-1$; c'est loisible, car, dans le cas

contraire $\mathrm{card}\,(V) > n-1$. Enfin nous noterons A l'ensemble des parties à deux éléments (« paires ») de X de la forme $\{x,y\}$ (ainsi $x \neq y$) telles que $(x\ y) \in V$. Il y a une bijection évidente entre V et A, en particulier $\mathrm{card}\,(A) = \mathrm{card}\,(V)$.

a) Montrons que toute permutation $\sigma \in \mathfrak{S}(X)$ peut s'écrire comme produit d'éléments de V : $\sigma = s_r s_{r-1} \cdots s_2 s_1$, où $r \in \mathbb{N}$ et $s_1, \ldots, s_r \in V$ ($\sigma = 1$ lorsque $r = 0$; nous avons supprimé les symboles $\circ$, pour simplifier). Pour cela, notons Γ l'ensemble des éléments $\sigma \in \mathfrak{S}(X)$ de la forme précédente. Il est clair que Γ est multiplicativement stable et contient 1. Si $\sigma \in \Gamma$, on a aussi $\sigma^{-1} \in \Gamma$. En effet, toute transposition est sa propre inverse, d'où :

$$(s_r s_{r-1} \cdots s_2 s_1)^{-1} \;=\; s_1 s_2 \cdots s_r\,.$$

Ainsi Γ est un sous-groupe de $\mathfrak{S}(X)$, contenant évidemment tout élément de V. Comme V est par hypothèse une partie génératrice de $\mathfrak{S}(X)$, $\Gamma = \mathfrak{S}(X)$.

b) Définissons sur X une relation $\sim$ comme suit. Soient $x, y \in X$. Alors $x \sim y$ si, et seulement s'il existe un entier $m \geqslant 0$ et une suite $(x_0, \ldots, x_m)$ d'éléments de X telle que $x_0 = x$, $x_m = y$ et que, pour tout $k \in [\![0, m-1]\!]$, $x_k \neq x_{k+1}$ et $(x_k\ x_{k+1}) \in V$. On vérifie sans peine que $\sim$ est une relation d'équivalence sur X.

Montrons qu'il n'y a qu'une seule classe modulo $\sim$ (à savoir X). Cela revient à dire que, si $x, y \in X$ sont donnés, on a $x \sim y$. C'est vrai si $y = x$, supposons $y \neq x$. D'après l'alinéa a), il existe un entier $r \geqslant 1$ et $s_1, \ldots, s_r \in V$ tels que $(x\ y) = s_r s_{r-1} \cdots s_2 s_1$. Définissons des éléments $z_0, \ldots, z_r \in X$ par $z_0 := x$ et la relation de récurrence $z_j := s_j(z_{j-1})$ pour $j = 1, \ldots, r$. Évidemment $z_r = y$. Montrons que $z_j \sim x$ pour tout $j \in [\![0, r]\!]$. C'est vrai pour $j = 0$: $z_0 = x \sim x$. Soit $j \in [\![1, r]\!]$, supposons que $z_{j-1} \sim x$. Si z_{j-1} est laissé fixe par s_j, $z_j = z_{j-1}$, donc $z_j \sim x$. Dans le cas contraire, $z_j \neq z_{j-1}$ et s_j s'écrit $s_j = (z_j\ z_{j-1})$. Comme $s_j \in V$, on a par définition $z_j \sim z_{j-1}$, d'où $z_j \sim x$ par transitivité de la relation $\sim$. Finalement $y = z_r \sim x$, comme désiré.

c) Soit E l'ensemble des couples (x, α) formés d'un $x \in X$ et d'une paire $\alpha \in A$ tels que $x \in \alpha$. Calculons $\mathrm{card}\,(E)$ de deux façons, en appliquant la formule de Fubini (*cf.* l'exemple de la page 72). Soit $\alpha \in A$. Cherchons les $x \in X$ tels que $(x, \alpha) \in E$. Ce sont ceux qui appartiennent à α, il y en a donc exactement deux, à savoir les deux éléments de α ! D'où :

$$2\,\mathrm{card}\,(V) = 2\,\mathrm{card}\,(A) = \sum_{\alpha \in A} 2 = \sum_{x \in X} \nu(x)\,.$$

Dans cette formule, si $x \in X$, nous avons noté $\nu(x)$ le nombre de paires $\alpha \in A$ telles que $(x, \alpha) \in E$, c'est-à-dire $x \in \alpha$.

Observons maintenant que, lorsque x décrit X, les entiers $\nu(x)$ ne peuvent pas être tous supérieurs ou égaux à 2, car sinon on aurait, puisque $\mathrm{card}\,(V) \leqslant n-1$:

$$2n \;=\; \sum_{x \in X} 2 \;\leqslant\; \sum_{x \in X} \nu(x) \;=\; 2\,\mathrm{card}\,(V) \;\leqslant\; 2(n-1)\,,$$

ce qui est absurde. Considérons donc un $a \in X$ tel que $\nu(a) \leqslant 1$. En fait $\nu(a) = 1$. Dans le cas contraire $\big(\nu(a) = 0\big)$, pour toute transposition $s = (x\ y)$ appartenant à V, on aurait $a \notin \{x, y\}$, *i.e.* s laisserait fixe a. D'après l'alinéa a), toute permutation $\sigma \in \mathfrak{S}(X)$ est produit d'éléments de V, donc fixerait aussi a. C'est absurde : prendre par exemple $x \in X$, $x \neq a$ et $\sigma = (a\ x)$. Ainsi $\nu(a) = 1$, *i.e.* a appartient à une unique paire $\alpha \in A$, nécessairement de la forme $\alpha = \{a, b\}$, où $b \in X' := X \setminus \{a\}$. Posons $s := (a\ b)$, et aussi $A' := A \setminus \{\alpha\}$.

Si $\beta = \{x, y\} \in A'$, x et y sont par définition distincts de a, donc β est une paire d'éléments de X'. Soit ensuite $t \in V \setminus \{s\}$: $t = (x\ y)$, où $x, y \in X'$ sont distincts. Rappelons que

$t \in \mathfrak{S}(X)$ et que $t(a) = a$. Notons par contre t' la transposition de X' échangeant x et y ($t' = (x\ y)$ dans $\mathfrak{S}(X')$, mais cette notation serait ambiguë) : t' est la restriction de t à X'. Notons $V' \subset \mathfrak{S}(X')$ l'ensemble des t', où t décrit $V \setminus \{s\}$. Il est clair que $t \mapsto t'$ est une bijection de $V \setminus \{s\}$ sur V', de sorte que $\operatorname{card}(V') = \operatorname{card}(V) - 1$.

d) Pour conclure, il suffit de montrer que V', qui est formée de transpositions appartenant à $\mathfrak{S}(X')$, est une partie génératrice de $\mathfrak{S}(X')$. En effet, l'hypothèse de récurrence donnera alors $\operatorname{card}(V') \geqslant \operatorname{card}(X') - 1$, d'où :

$$\operatorname{card}(V) \;=\; 1 + \operatorname{card}(V') \;\geqslant\; 1 + \big[\operatorname{card}(X') - 1\big] \;=\; \operatorname{card}(X') \;=\; n - 1\,,$$

comme désiré.

D'après le théorème 24 de la page 127, l'ensemble des transpositions (échangeant deux éléments de X') est une partie génératrice de $\mathfrak{S}(X')$. Il nous suffit donc de prouver que, si $x, y \in X'$ sont distincts, la transposition $u' := (x\ y) \in \mathfrak{S}(X')$ est produit d'éléments de V'. D'après l'alinéa b), $x \sim y$. Il existe donc un entier $m \geqslant 0$ et une suite $(x_0, \ldots, x_m)$ d'éléments de X telle que $x_0 = x$, $x_m = y$ et que, pour tout $k \in [\![0, m-1]\!]$, $x_k \neq x_{k+1}$ et $(x_k\ x_{k+1}) \in V$. Choisissons une telle suite $(x_0, \ldots, x_m)$ de telle manière que l'entier m soit *minimum*. Bien sûr $m \geqslant 1$, puisque $x \neq y$.

Montrons que $x_k \neq a$ pour tout $k \in [\![0, m]\!]$. C'est vrai si $k = 0$ ou $k = m$, car $x_0 = x$ et $x_m = y$ appartiennent à $X' = X \setminus \{a\}$. Raisonnons par l'absurde, et supposons qu'il existe un $k \in [\![1, m-1]\!]$ tel que $x_k = a$. Alors $x_{k-1} \neq a$ et $(x_{k-1}\ a) \in V$, donc $x_{k-1} = b$, car la seule transposition appartenant à V ne laissant pas fixe a est $s = (a\ b)$. De même $x_{k+1} \neq a$ et $(a\ x_{k+1}) \in V$, donc $x_{k+1} = b$. Comme $x \neq y$, nécessairement $n \geqslant 3$. Si $k \leqslant m-2$, la suite $(x_0, \ldots, x_{k-1}, x_{k+2}, \ldots, x_m)$ possède la même propriété que $(x_0, \ldots, x_m)$. En effet $b = x_{k-1} = x_{k+1} \neq x_{k+2}$, et $(x_{k-1}\ x_{k+2}) = (x_{k+1}\ x_{k+2}) \in V$. Cela contredit la minimalité de m. Si $k = m-1$ (donc $k \geqslant 2$), le raisonnement est le même, en considérant la suite $(x_0, \ldots, x_{m-2})$.

Ainsi $x_k \neq a$ pour tout $k \in [\![0, m]\!]$. La minimalité de m entraîne aussi que les x_k sont deux à deux distincts. Pour $k = 0, \ldots, m-1$, posons $t_k := (x_k\ x_{k+1})$, de sorte que $t_k \in V$ et $t_k \neq s$. Dans $\mathfrak{S}(X)$, on a alors, en vertu de la formule (21) :

$$t_0 t_1 \cdots t_{m-2} = (x_0\ x_1)(x_1\ x_2) \cdots (x_{m-2}\ x_{m-1}) = (x_0\ x_1\ \cdots\ x_{m-1})\,.$$

Notons γ le m-cycle $(x_0\ x_1\ \cdots\ x_{m-1}) \in \mathfrak{S}(X)$ et γ' sa restriction à X', c'est-à-dire le m-cycle $(x_0\ x_1\ \cdots\ x_{m-1}) \in \mathfrak{S}(X')$. L'égalité ci-dessus implique, en prenant les restrictions à X' : $\gamma' = t'_0 t'_1 \cdots t'_{m-2}$.

Par ailleurs, puisque $\gamma(x_m) = x_m$ et $\gamma(x_{m-1}) = x_0$, la formule de conjugaison (22) donne $\gamma t_{m-1} \gamma^{-1} = (x_0\ x_m) = (x\ y)$. En prenant les restrictions à X', on obtient l'égalité suivante, dans $\mathfrak{S}(X')$:

$$u' = (x\ y) = \gamma' t'_{m-1} \gamma'^{-1} = t'_0 t'_1 \cdots t'_{m-2} t'_{m-1} t'_{m-2} \cdots t'_1 t'_0\,.$$

La transposition $u' \in \mathfrak{S}(X')$ est donc produit d'éléments de V', ce qui achève de montrer que V' est une partie génératrice de $\mathfrak{S}(X')$, terminant ainsi l'exercice.

II.2.19 D'abord $\operatorname{End}(E)$ contient 0, application nulle de E dans lui-même. Soient ensuite $f, g \in \operatorname{End}(E)$. Il s'agit de voir que les éléments $f + g$ et $-f$ du groupe $\mathcal{F}(E, E)$ sont des morphismes de E dans lui-même. Soient donc $x, y \in E$. Puisque f et g sont des morphismes, $f(x + y) = f(x) + f(y)$ et $g(x + y) = g(x) + g(y)$. Par définition de $f + g$

(*cf.* l'exemple 3 de la page 118), $(f+g)(x) = f(x)+g(x)$, $(f+g)(y) = f(y)+g(y)$ et $(f+g)(x+y) = f(x+y)+g(x+y)$. D'où :

$$(f+g)(x+y) \;= f(x+y)+g(x+y) \;= \big[f(x)+\overbrace{f(y)\big]+\big[g(x)}+g(y)\big]$$

$$= \;\big[f(x)+\overbrace{g(x)\big]+\big[f(y)}+g(y)\big] \;=\; (f+g)(x)+(f+g)(y)\,,$$

ce qui montre que $f+g : E \to E$ est un morphisme. Observer la façon dont la commutativité de E est intervenue. Passons à $-f$. Pour tous $x, y \in E$, il vient :

$$(-f)(x+y) = -f(x+y) = -\big(f(x)+f(y)\big) = \big(-f(y)\big)+\big(-f(x)\big)$$

$$= \big(-f(x)\big)+\big(-f(y)\big) = (-f)(x)+(-f)(y)\,,$$

ce qui montre que $-f \in \mathrm{End}(E)$. En conclusion, $\mathrm{End}(E)$ est un sous-groupe de $\big(\mathcal{F}(E,E),+\big)$.

Si $f, g \in \mathrm{End}(E)$, nous savons que $f\circ g \in \mathrm{End}(E)$, de sorte que $\mathrm{End}(E)$ est une partie stable de $\mathcal{F}(E,E)$ pour la loi $\circ$. Dans l'exercice 6 de la page 133, nous avons vu que $\big(\mathcal{F}(E,E),+,\circ\big)$ n'est en général pas un anneau. La seule propriété des anneaux pouvant être en défaut était l'égalité suivante (« demi-distributivité »), où $f, g, h \in \mathcal{F}(E,E)$:

$$f\circ(g+h) \;=\; (f\circ g)+(f\circ h)\,.$$

Cette égalité devient vraie lorsque $f \in \mathrm{End}(E)$ (g et h peuvent être quelconques). Pour tout $x \in E$, on obtient alors :

$$\big(f\circ(g+h)\big)(x) = f\big((g+h)(x)\big) = f\big(g(x)+h(x)\big) = f\big(g(x)\big)+f\big(h(x)\big)$$

$$= (f\circ g)(x)+(f\circ h)(x) = \big[(f\circ g)+(f\circ h)\big](x)\,,$$

d'où l'égalité voulue. On en déduit ainsi que $\big(\mathrm{End}(E),+,\circ\big)$ est un anneau.

Soit enfin $f \in \mathrm{End}(E)$. Pour que f soit un élément inversible de l'anneau $\big(\mathrm{End}(E),+,\circ\big)$, il faut et il suffit qu'il existe un $g \in \mathrm{End}(E)$ tel que $f\circ g = g\circ f = Id_E$. Cela revient évidemment à dire que f est un automorphisme de E, ou encore que $f : E \to E$ est bijectif (*cf.* le théorème 20 de la page 124).

II.2.20 Puisque $\{0\}$ est un sous-groupe additif de B, $A\times\{0\}$ est un sous-groupe additif de $A\times B$. Soient $x \in A\times\{0\}$ et $t \in A\times B$: il existe $a, a' \in A$ et $b \in B$ tels que $x = (a,0)$ et $t = (a',b)$. Alors $tx = (a',b)(a,0) = (a'a,0) \in A\times\{0\}$. Cela montre que $A\times\{0\}$ est un idéal de $A\times B$, et il en est de même pour $\{0\}\times B$.

Avec des notations évidentes, $(1_A,0_B)(0_A,1_B) = (1_A0_A,0_B1_B) = 0$, où $0 := (0_A,0_B)$ est l'élément neutre additif de $A\times B$. Mais $(1_A,0_B)\neq(0_A,0_B)$ car A n'est pas nul, de même $(0_A,1_B)\neq(0_A,0_B)$ car B n'est pas nul. Il en résulte que $A\times B$ n'est pas intègre.

II.2.21 1) Soit $x := (x_1,\dots,x_n) \in A$. Pour que x soit inversible dans A, il faut et il suffit qu'il existe un $y \in A$ tel que $xy = yx = 1_A$. Cherchant un tel y sous la forme $y := (y_1,\dots,y_n)$, cela revient à dire que, pour tout $i \in [\![1,n]\!]$, il existe $y_i \in A_i$ tel que $x_iy_i = y_i = 1_{A_i}$, à cause de la définition de la multiplication sur A. Autrement dit, chaque x_i doit être inversible dans l'anneau A_i. D'où l'égalité :

$$A^\times \;=\; A_1^\times\times A_2^\times\times\cdots\times A_n^\times\,.$$

C'est *a priori* une égalité entre ensembles mais, étant donnés deux éléments $a := (a_1, \dots, a_n)$ et $b := (b_1, \dots, b_n)$ de $A^\times$, $ab = (a_1 b_1, \dots, a_n b_n)$, et donc le produit de a par b est le même, que ce soit dans le groupe multiplicatif des éléments inversibles de l'anneau A ou dans le groupe produit des groupes multiplicatifs $A_i^\times$.

2) Soit $f \in \mathcal{F}(X, A)$. Supposons d'abord que f soit inversible dans l'anneau $\mathcal{F}(X, A)$: il existe $g \in \mathcal{F}(X, A)$ tel que $fg = c = gf$, où $c : X \to A$ est l'application constante égale à 1, *i.e.* l'élément neutre multiplicatif de $\mathcal{F}(X, A)$. Pour tout $x \in X$; il vient alors : $1 = c(x) = (fg)(x) = f(x)g(x)$, et de même $g(x)f(x) = 1$. Ainsi $f(x)$ est inversible dans A, son inverse étant $g(x)$. D'où $f(X) \subset A^\times$.

Soit réciproquement $f \in \mathcal{F}(X, A)$, supposons que $f(X)$ soit contenu dans $A^\times$. Nous pouvons alors définir une application $g : X \to A$ par la formule $g(x) := f(x)^{-1}$, et il est clair que $fg = c = gf$. Ainsi f est inversible dans l'anneau $\mathcal{F}(X, A)$, et son inverse est g.

II.2.22 Démontrons la formule par récurrence sur n. Notons P_n le premier membre et S_n le deuxième membre de cette formule. Si $n = 0$, $P_0 = a^{2^0} + 1 = a + 1$, et $S_0 = a^0 + a^1 = 1 + a$, la formule est vraie. Supposons la formule vraie pour un certain entier n. Évidemment $P_{n+1} = P_n\big(a^{2^{n+1}} + 1\big)$. D'après l'hypothèse de récurrence, on a donc :

$$P_{n+1} = \big(a^{2^{n+1}} + 1\big) \left(\sum_{j=0}^{2^{n+1}-1} a^j \right) .$$

Distribuons le produit (*i.e.* utilisons la distributivité de la multiplication par rapport à l'addition) :

$$P_{n+1} \;=\; \sum_{j=0}^{2^{n+1}-1} a^j \;+\; \sum_{j=0}^{2^{n+1}-1} a^{2^{n+1}+j} .$$

Dans la deuxième somme, lorsque j varie de 0 à $2^{n+1} - 1$, $2^{n+1} + j$ varie de 2^{n+1} à $2^{n+1} + \big(2^{n+1} - 1\big) = 2^{n+2} - 1$. Par changement d'indice, on en déduit :

$$P_{n+1} \;=\; \sum_{j=0}^{2^{n+1}-1} a^j \;+\; \sum_{j=2^{n+1}}^{2^{n+2}-1} a^j \;=\; \sum_{j=0}^{2^{n+2}-1} a^j \;=\; S_{n+1} ,$$

ce qui prouve la formule au rang $n + 1$.

Donnons une solution n'utilisant pas la récurrence : $n \in \mathbb{N}$ est fixé. Pour calculer P_n, appliquons la formule (28). Pour toute partie I de $[\![0, n]\!]$, notons X_I le produit des a^{2^k}, k décrivant I. Alors P_n est la somme des X_I, I parcourant l'ensemble des parties $\mathcal{P}$ de $[\![0, n]\!]$. Si $I \in \mathcal{P}$, on a :

$$X_I \;=\; \prod_{k \,\in\, I} a^{2^k} \;=\; a^{s(I)}, \quad \text{où} \quad s(I) \;:=\; \sum_{k \,\in\, I} 2^k .$$

Utilisons maintenant le système binaire. D'après le théorème 31 de la page 81, tout entier $j \in [\![0, 2^{n+1} - 1]\!]$ s'écrit de manière unique :

$$j = \sum_{k=0}^{n} a_k 2^k , \quad \text{où} \quad a_0, \dots, a_n \in \{0, 1\} .$$

En posant $I := \big\{k \in [\![0,n]\!] \;\big|\; a_k = 1\big\}$, on a donc $j = s(I)$. En outre $I \mapsto s(I)$ est une bijection de $\mathcal{P}$ sur $[\![0, 2^{n+1}-1]\!]$. Changeons d'indice au moyen de cette bijection :

$$P_n \;=\; \sum_{I\in\mathcal{P}} X_I \;=\; \sum_{I\in\mathcal{P}} a^{s(I)} \;=\; \sum_{j=0}^{2^{n+1}-1} a^j \;=\; S_n\,.$$

II.2.23 1) Démontrons par récurrence sur l'entier $r \geqslant 2$ l'assertion suivante : pour tous entiers $i_1, \dots, i_r \in \mathbb{N}$, le nombre rationnel

$$\frac{(i_1 + i_2 + \cdots + i_r)!}{i_1!\, i_2! \cdots i_r!}\,.$$

est un entier. C'est vrai si $r = 2$, car il s'agit alors du coefficient binomial $\binom{i_1+i_2}{i_1}$. Supposons $r \geqslant 3$, notre assertion étant vraie au rang $r-1$. Soient $i_1, \dots, i_r \in \mathbb{N}$. Posant $i := i_1 + i_2 + \cdots + i_{n-1}$, il vient :

$$\frac{(i_1 + i_2 + \cdots + i_r)!}{i_1!\, i_2! \cdots i_r!} \;=\; \left(\frac{(i+i_r)!}{i!\, i_r!}\right)\left(\frac{(i_1 + i_2 + \cdots + i_{r-1})!}{i_1!\, i_2! \cdots i_{r-1}!}\right).$$

Dans le membre de droite, le premier facteur est un entier, car c'est un coefficient binomial. Le second facteur est un entier, d'après l'hypothèse de récurrence. Notre assertion est ainsi vraie pour tout entier $r \geqslant 2$.

2) Raisonnons par récurrence sur l'entier $r \geqslant 2$. L'hypothèse de récurrence est que la formule du multinôme est vraie quel que soient les choix de l'entier n et de $a_1, \dots, a_r$. Le cas $r = 2$ est connu : c'est la formule du binôme. Supposons $r \geqslant 3$, la conclusion étant vraie au rang $r-1$. Soient n et $a_1, \dots, a_r$ comme dans l'énoncé. Pour tout $k \in \mathbb{N}$, notons E_k l'ensemble des $(r-1)$-uplets $(i_1, \dots, i_{r-1})$ de somme k. Soit F l'ensemble des couples $\big((i_1, \dots, i_{r-1}), k\big)$, où $k \in [\![0,n]\!]$ et $(i_1, \dots, i_{r-1}) \in E_k$. L'application $\big((i_1, \dots, i_{r-1}), k\big) \mapsto (i_1, \dots, i_{r-1}, n-k)$ est clairement une bijection φ de F sur E, la bijection réciproque étant définie par $(i_1, \dots, i_r) \mapsto \big((i_1, \dots, i_{r-1}), n - i_r\big)$.

Posons $b := a_1 + \cdots + a_{r-1}$. Vu l'hypothèse faite sur les a_i, b et a_r commutent. La formule du binôme donne donc :

$$(a_1 + \cdots + a_r)^n \;=\; \sum_{k=0}^{n} \binom{n}{k} b^k a_r^{n-k}$$

Pour calculer chaque b_k, appliquons l'hypothèse de récurrence. Le second membre de l'égalité précédente devient :

$$\sum_{k=0}^{n} \binom{n}{k} \left(\sum_{(i_1,\dots,i_{r-1})\,\in\, E_k} \frac{(i_1 + i_2 + \cdots + i_{r-1})!}{i_1!\, i_2! \cdots i_{r-1}!} a_1^{i_1} \cdots a_{r-1}^{i_{r-1}} \right) a_r^{n-k}\,,$$

ce que nous pouvons encore écrire :

$$\sum_{(i_1,\dots,i_{r-1},k)\,\in\, F} \binom{n}{k} \frac{(i_1 + i_2 + \cdots + i_{r-1})!}{i_1!\, i_2! \cdots i_{r-1}!}\; a_1^{i_1} \cdots a_{r-1}^{i_{r-1}} a_r^{n-k}\,.$$

Le changement d'indices défini par la bijection φ transforme la somme précédente en :

$$\sum_{(i_1,\dots,i_k)\,\in\, E} \binom{n}{i_1 + \cdots + i_{r-1}} \frac{(i_1 + i_2 + \cdots + i_{r-1})!}{i_1!\, i_2! \cdots i_{r-1}!}\; a_1^{i_1} \cdots a_{r-1}^{i_{r-1}} a_r^{i_r}\,.$$

On obtient la formule du multinôme au rang r puisque, dans chaque terme de cette somme, $n = i_1 + i_2 + \cdots + i_r$.

II.2.24 Par hypothèse, il existe un $n \in \mathbb{N}^*$ tel que $x^n = 0$. Rappelons la formule suivante :

$$1 - z^n \;=\; (1-z)(1+z+z^2+\cdots+z^{n-1})\,.$$

Cette formule est valable dans n'importe quel anneau A. Il suffit d'appliquer les règles de calcul dans les anneaux :

$(1-z)(1+z+z^2+\cdots+z^{n-1}) \;=\; (1+z+z^2+\cdots+z^{n-1}) - (z+z^2+z^3+\cdots+z^n)$,

ce qui donne $1 - z^n$, après simplifications. Dans le cas présent, $z^n = 0$, donc $1+z+z^2+\cdots+z^{n-1}$ est inverse de $1-z$ (on a le même calcul que ci-dessus en multipliant par $1-z$ à droite). Ainsi $1-z$ est inversible.

La réciproque est évidemment fausse : dans $\mathbb{Z}$, soit $z := 2$. Alors $1 - z = -1$ est inversible, mais z n'est pas nilpotent : le seul élément nilpotent de $\mathbb{Z}$ est 0.

II.2.25 Rappelons que $eAe := \{eae \;\big|\; a \in A\}$. Soient $x, y \in eAe$: $x := eae$ et $y := ebe$, où $a, b \in A$. Alors $x \pm y = e(a \pm b)e \in eAe$. Comme $0 \in eAe$, cela montre que eAe est un sous-groupe de $(A, +)$, en particulier $(eAe, +)$ est un groupe commutatif. Si x, y sont comme ci-dessus, $xy = (eae)(ebe) = e(aeb)e \in eAe$. En général $1 \notin eAe$, de sorte que eAe n'est pas forcément un sous-anneau de A. Par contre, eAe est une partie multiplicativement stable de A. Si l'on considère $(eAe, +, \times)$, tous les axiomes des anneaux sont vérifiés, parce qu'ils le sont dans A (par exemple distributivité de $\times$ par rapport à $+$), sauf peut-être l'existence d'un élément neutre pour $\times$. Mais il est clair que e convient : si $x = eae \in eAe$, on a $ex = e(eae) = e^2(ae) = eae = x$, et de même $xe = (eae)e = (ea)e^2 = eae = x$. Ainsi $(eAe, +, \times)$ est un anneau, d'élément neutre multiplicatif e.

II.2.26 Soit donc $B := \big\{x \in A \;\big|\; f(x) = g(x)\big\}$. D'abord, $1 \in B$, car $f(1) = 1 = g(1)$, par définition d'un morphisme d'anneaux. Soient $x, y \in B$. La même définition montre que $f(x \pm y) = f(x) \pm f(y)$, de même $g(x \pm y) = g(x) \pm g(y)$. Mais $f(x) = g(x)$ et $f(y) = g(y)$, donc $f(x \pm y) = g(x \pm y)$, *i.e.* $x \pm y \in B$. Le même argument montre que $f(xy) = g(xy)$, d'où $xy \in B$. Ainsi B est un sous-anneau de A.

II.2.27 1) D'abord $1 = 1/1 \in A$. Soient $x, x' \in A$: $x := a/b$ et $x' := a'/b'$, où $a, a', b, b' \in \mathbb{Z}$ et b, b' ne sont pas multiples de p. En vertu des formules $x \pm x' = (ab' \pm a'b)/(bb')$ et $xx' = (aa')/(bb')$, $x \pm x'$ et xx' appartiennent à A, car bb' n'est pas multiple de p, en vertu du lemme d'Euclide. Ainsi A est un sous-anneau de $\mathbb{Q}$.

Soit $x \in A$. Montrons que x est inversible dans A si, et seulement s'il est de la forme $x := a/b$, où $a, b \in \mathbb{Z}$ ne sont pas multiples de p. Si x est de cette forme, l'inverse $1/x$ de x dans $\mathbb{Q}$ est b/a, qui appartient à A vu l'hypothèse. Ainsi $1/x$ est inverse de x *dans* A. Supposons réciproquement que x soit inversible dans A. Cela revient à dire que $x \neq 0$, et que $1/x$ (inverse de x dans $\mathbb{Q}$) appartient à A. Il existe donc des entiers $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ tels que β et δ ne soient pas multiples de p, et que $x = \alpha/\beta$, $1/x = \gamma/\delta$. Alors $1 = (\alpha\gamma)/(\beta\delta)$, *i.e.*

$\alpha\gamma = \beta\delta$. D'après le lemme d'Euclide, p ne divise pas $\beta\delta$, donc p ne divise pas α. Finalement $x = \alpha/\beta$, où α, β ne sont pas multiples de p, *i.e.* x a la forme annoncée. Voici la conclusion :

$$A^\times \;=\; \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z} \setminus p\mathbb{Z} \right\} .$$

2) Soient T une partie de $\mathbb{Q}$ et A le sous-anneau de $\mathbb{Q}$ engendré par T. Montrons d'abord que A est égal à l'ensemble A' formé des sommes finies de produits finis d'éléments de T ou d'opposés d'éléments de T. Par définition d'un sous-anneau, il est clair que $A' \subset A$. Pour l'inclusion inverse, il suffit de montrer que A' est un sous-anneau de $\mathbb{Q}$, ce qui est immédiat. Notons aussi que A contient $\mathbb{Z}$: $1 \in A$ par définition d'un sous-anneau, donc A contient le sous-groupe de $(\mathbb{Q}, +)$ engendré par 1, c'est-à-dire $\mathbb{Z}$.

Soient ensuite P une partie de $\mathbb{P}$, T l'ensemble des $1/p$, p parcourant P, et A le sous-anneau de $\mathbb{Q}$ engendré par T. Si $p \in P$ et $r \in \mathbb{N}^*$, $1/p^r = (1/p)^r \in A$, car A est multiplicativement stable. Soit $n \in \mathbb{N}^*$. Écrivons la factorisation de n :

$$n \;=\; p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m} ,$$

où $p_1, \ldots, p_m$ sont des nombres premiers distincts et $e_1, \ldots, e_m \in \mathbb{N}^*$. Supposons que chaque p_i appartienne à P. Alors, pour tout i, $1/p_i^{e_i} \in A$. Comme A est multiplicativement stable, $1/n \in A$. Ainsi A contient l'inverse de tout entier strictement positif dont chaque facteur premier appartient à P. Si donc $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$, et si chaque facteur premier de b appartient à P, $a/b = a(1/b)$ appartient à A, car $a \in A$ et $1/b \in A$. Inversement, soit $q \in A$. D'après l'alinéa précédent, q est somme finie de produits finis du type $\pm 1/p$, où $p \in P$. On en déduit aussitôt que q s'écrit $q = a/b$, où $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$, et tout facteur premier de b appartient à P.

Prenons $P := \mathbb{P}$. Dans ce cas, $A = \mathbb{Q}$, en vertu de ce qui précède. Le sous-anneau de $\mathbb{Q}$ engendré par les $1/p$, $p \in \mathbb{P}$, est donc égal à $\mathbb{Q}$.

Soient enfin S une partie finie de $\mathbb{Q}$ et B le sous-anneau engendré par S. Écrivons $S := \{q_1, \ldots, q_m\}$. Pour chaque i, $q_i := a_i/b_i$, où $a_i \in \mathbb{Z}$ et $b_i \in \mathbb{N}^*$. Notons P l'ensemble (fini) des nombres premiers divisant au moins l'un des b_i. Soient T l'ensemble des $1/p$, p parcourant P, et A le sous-anneau de $\mathbb{Q}$ engendré par T. Comme nous l'avons vu, chaque q_i appartient à A, donc $S \subset A$ et par suite $B \subset A$. D'un autre côté, nous avons vu que tout élément de A s'écrit a/b, où $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$, et tout facteur premier de b appartient à P. Comme l'ensemble des nombres premiers est infini (théorème 35 de la page 85), il existe un nombre premier p n'appartenant pas à P. Mais alors $1/p \notin A$, *a fortiori* $1/p \notin B$. Cela montre que le sous-anneau de $\mathbb{Q}$ engendré par S n'est pas égal à $\mathbb{Q}$.

II.2.28 Notons I l'ensemble des éléments nilpotents de A, il contient déjà 0. Soient $x, y \in I$, montrons que $x + y \in I$. Il existe par définition deux entiers m, n tels que $x^m = 0$ et $y^n = 0$. Puisque A est commutatif, nous pouvons appliquer la formule du binôme :

$$(x+y)^{m+n} \;=\; \sum_{k=0}^{m+n} \binom{m+n}{k} x^k y^{m+n-k} .$$

Soit $k \in [\![0, m+n]\!]$. Si $k \geqslant m$, $x^k = x^m x^{k-m} = 0$, car $x^m = 0$. Si $k < m$, on a $m + n - k > n$, et alors $y^{m+n-k} = y^n y^{m-k} = 0$, car $y^n = 0$. Dans les deux cas, $x^k y^{m+n-k} = 0$. Ainsi tous les termes de la somme ci-dessus sont nuls, et par suite $(x+y)^{m+n} = 0$, donc $x + y \in I$.

Soient maintenant $x \in I$ et $a \in A$. Il existe $m \in \mathbb{N}$ tel que $x^m = 0$. Alors $(ax)^m = a^m x^m = 0$ (encore la commutativité de A), donc $ax \in I$. Cela montre que I

est un idéal de A. À vrai dire, lorsqu'on applique la définition 15 de la page 137, il faudrait vérifier que I est un sous-groupe de $(A,+)$. Le fait que, pour tout $x \in I$, son opposé $-x$ appartienne aussi à I résulte de ce qui précède : $x \in I$ et $-1 \in A$, donc $-x = (-1)x \in I$.

Soient ensuite $n, k, \bar{k}$ comme dans l'énoncé. Supposons que $\bar{k}$ soit nilpotent : il existe un entier $r \geqslant 1$ tel que $\bar{k}^r = 0$, soit $k^r \equiv 0 \mod n$. Soit p un facteur premier de n. Alors $k^r \equiv 0 \mod p$. Autrement dit, notant $x \in \mathbb{Z}/p\mathbb{Z}$ la classe de k modulo p, $x^r = 0$. Ainsi x est un élément nilpotent de $\mathbb{Z}/p\mathbb{Z}$. Mais $\mathbb{Z}/p\mathbb{Z}$ est intègre (c'est un corps), donc $x = 0$ (*cf.* la propriété de la page 137). Il en résulte que p divise k, *i.e.* k est multiple de chaque facteur premier de n.

Supposons inversement que k soit multiple de chaque facteur premier de n. Considérons la factorisation de n :

$$n \;=\; p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}\,,$$

où $p_1, \ldots, p_m$ sont des nombres premiers distincts et $e_1, \ldots, e_m \in \mathbb{N}^*$. Posons $t := p_1 p_2 \cdots p_m$ et $r := \max(e_1, \ldots, e_m)$. Il est clair que n divise t^r (*cf.* le théorème 38 de la page 87). Par hypothèse, k est multiple de chacun des p_i, c'est donc un multiple du ppcm des p_i. Mais le théorème 44 de la page 90 montre que ce ppcm est t. Ainsi k est multiple de t, donc k^r est multiple de t^r, et *a fortiori* multiple de n. Autrement dit $\bar{k}^r = 0$, ce qui montre que $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ est nilpotent.

II.2.29 Remarquons d'abord que, si $n \in X$, $d \mapsto (d, n/d)$ est une bijection de l'ensemble des diviseurs $d \geqslant 1$ de n sur l'ensemble des couples $(a,b) \in X^2$ tels que $ab = n$. La formule définissant la loi $\star$ peut donc être écrite ainsi :

$$(f \star g)(n) \;=\; \sum_{d \,|\, n} f(d)\, g(n/d) \quad \text{pour tout } n \in X\,. \tag{$*$}$$

Par ailleurs, notons que la loi $\star$ est commutative (parce que la multiplication de $\mathbb{Z}$ l'est). Enfin, si $f, g \in \mathcal{F}(X, \mathbb{Z})$, il est clair que $(f \star g)(1) = f(1)g(1)$.

1) Soit $f \in \mathcal{F}(X, \mathbb{Z})$. Pour tout $n \in X$, il vient :

$$(\delta \star f)(n) \;=\; \sum_{d \,|\, n} \delta(d) f(n/d)\,.$$

Dans le membre de droite, le seul d tel que $\delta(d)$ soit non nul est $d = 1$, d'où $(\delta \star f)(n) = \delta(1) f(n) = f(n)$.

2) Soient $f, g, h \in \mathcal{F}(X, \mathbb{Z})$ et $n \in X$. Par définition,

$$\big((f \star g) \star h\big)(n) \;=\; \sum_{(a,b) \in X^2,\; ab = n} (f \star g)(a) h(b)\,.$$

Le second membre de cette égalité s'écrit ainsi :

$$\sum_{(a,b) \in X^2,\; ab = n} \left(\sum_{(u,v) \in X^2,\; uv = a} f(u) g(v) h(b) \right)\,.$$

Soit $I := \big\{(u,v,b) \in X^3 \;\big|\; uvb = n\big\}$. Pour tout $(a,b) \in X^2$ tel que $ab = n$, notons $I_{(a,b)}$ l'ensemble des triplets (u,v,b), où $(u,v) \in X^2$ vérifie $uv = a$. Les $I_{(a,b)}$ forment une partition de I. La formule (6) donne donc :

$$\sum_{(u,v,b) \in I} f(u) g(v) h(b) \;=\; \sum_{(a,b) \in X^2,\; ab = n} \left(\sum_{(u,v) \in X^2,\; uv = a} f(u) g(v) h(b) \right)\,,$$

c'est-à-dire :

$$\big((f\star g)\star h\big)(n) \;=\; \sum_{(u,v,b)\in I} f(u)g(v)h(b)\,.$$

Vu la commutativité de l'anneau $\mathbb{Z}$, cela peut s'écrire :

$$\big((f\star g)\star h\big)(n) \;=\; \sum_{(u,v,b)\in I} g(v)h(b)f(u)\,.$$

L'application $(u,v,b)\mapsto(b,u,v)$ étant une permutation de I, la formule de changement d'indice (8) donne :

$$\big((f\star g)\star h\big)(n) \;=\; \sum_{(u,v,b)\in I} g(u)h(v)f(b)\,.$$

Le second membre de cette égalité n'est autre que $\big((g\star h)\star f\big)(n)$. Ainsi $(f\star g)\star h=(g\star h)\star f=f\star(g\star h)$, à cause de la commutativité de la loi $\star$. La loi $\star$ est donc associative.

Bien sûr, on pouvait aussi calculer directement $\big(f\star(g\star h)\big)(n)$:

$$\begin{aligned}\big(f\star(g\star h)\big)(n) &= \sum_{(a,b)\in X^2,\ ab=n} f(a)(g\star h)(b)\\ &= \sum_{(a,b)\in X^2,\ ab=n}\left(\sum_{(u,v)\in X^2,\ uv=b} f(a)g(u)h(v)\right).\end{aligned}$$

En utilisant les mêmes arguments que dans le calcul précédent, on obtient encore :

$$\big(f\star(g\star h)\big)(n) \;=\; \sum_{(a,u,v)\in I} f(a)g(u)h(v) \;=\; \sum_{(u,v,b)\in I} f(u)g(v)h(b)\,.$$

La seule propriété restant à vérifier est la distributivité de $\star$ par rapport à $+$. C'est beaucoup plus facile que l'associativité de la loi $\star$. Soient $f,g,h\in\mathcal{F}(X,\mathbb{Z})$ et $n\in X$. Alors $\big((f+g)\star h\big)(n)$ vaut, par définition :

$$\begin{aligned}\sum_{(a,b)\in X^2,\ ab=n}(f+g)(a)h(b) &= \sum_{(a,b)\in X^2,\ ab=n}\big(f(a)+g(a)\big)h(b)\\ &= \sum_{(a,b)\in X^2,\ ab=n} f(a)h(b)+\sum_{(a,b)\in X^2,\ ab=n} g(a)h(b)\\ &= (f\star h)(n)+(g\star h)(n) \;=\; \big[(f\star h)+(g\star h)\big](n)\,,\end{aligned}$$

et ainsi $(f+g)\star h=(f\star h)+(g\star h)$.

3) Il s'agit d'établir l'égalité $\mu\star c=\delta$. D'abord $(\mu\star c)(1)=\mu(1)c(1)$ est bien égal à $\delta(1)=1$. Il reste à montrer que, si n est un entier au moins égal à 2, on a :

$$\sum_{d\,|\,n}\mu(d) \;=\; \delta(n), \quad \text{soit} \quad \sum_{d\,|\,n}\mu(d) \;=\; 0\,.$$

Soient $p_1,\dots,p_r$ les différents facteurs premiers de n (ils sont donc distincts). Puisque $\mu(k)=0$ pour tout entier k ayant un facteur premier p multiple ($\nu_p(k)\geqslant 2$), les diviseurs d de n tels que $\mu(d)\neq 0$ sont les produits de certains des p_i. En d'autres termes, pour toute partie I de $[\![1,r]\!]$, notons p_I le produit des p_i, i parcourant I. Alors, en vertu du théorème 37 de la page 86, $I\mapsto p_I$ est une bijection de l'ensemble des parties de $[\![1,r]\!]$ sur l'ensemble des diviseurs d de n tels que $\mu(d)\neq 0$. De plus, pour toute partie I de $[\![1,r]\!]$, la définition de μ

montre que $\mu(p_I) = (-1)^{|I|}$, en notant ici $|I|$ le cardinal de I. Nous obtenons :

$$\sum_{d\,|\,n} \mu(d) \;=\; \sum_{I} (-1)^{|I|}\,.$$

Mais nous savons que, dans un ensemble fini non vide, il y a autant de parties de cardinal pair que de parties de cardinal impair (voir l'exemple de la page 135). Ainsi $\sum\limits_{d\,|\,n} \mu(d) = 0$, comme désiré.

4) Attention, les fonctions f et g sont à valeurs dans E, pas dans $\mathbb{Z}$. En fait, on peut généraliser $\star$ comme suit. Rappelons d'abord que, si $k \in \mathbb{Z}$ et $x \in E$, kx a été défini dans la définition 3 de la page 119, *cf.* la proposition 11 de la page 120 pour les règles de calcul là-dessus. Soient alors $\varphi \in \mathcal{F}(X, \mathbb{Z})$ et $\psi \in \mathcal{F}(X, E)$. On définit $\varphi \star \psi \in \mathcal{F}(X, E)$ par la formule :

$$(\varphi \star \psi)(n) \;:=\; \sum_{(a,b)\in X^2,\; ab\,=\,n} \varphi(a)\,\psi(b) \quad \text{pour tout } n \in X\,.$$

Il est clair par exemple que, pour toute fonction $\psi \in \mathcal{F}(X, E)$, $\delta \star \psi = \psi$. Pour toutes fonctions $\varphi, \varphi' \in \mathcal{F}(X, \mathbb{Z})$ et $\psi \in \mathcal{F}(X, E)$, on montre ensuite que $(\varphi \star \varphi') \star \psi = \varphi \star (\varphi' \star \psi)$ (« associativité mixte »). Il suffit de reprendre mot pour mot la preuve faite en 2, plus exactement la preuve directe, et non celle qui utilisait la commutativité de la loi $\star$ sur $\mathcal{F}(X, \mathbb{Z})$ (cette commutativité n'a plus de sens ici).

Dans ces conditions, revenons à f et g. La propriété suivante :

$$\Big(\forall n \in X,\; g(n) \;=\; \sum_{d|n} f(d)\Big)$$

signifie que $g = c \star f$, alors que la propriété

$$\Big(\forall n \in X,\; f(n) \;=\; \sum_{d|n} \mu(n/d) g(d)\Big)$$

signifie que $f = \mu \star g$. Si $g = c \star f$, l'associativité mixte et 3 donnent :

$$\mu \star g \;=\; \mu \star (c \star f) \;=\; (\mu \star c) \star f \;=\; \delta \star f \;=\; f\,.$$

Même chose si $f = \mu \star g$:

$$c \star f \;=\; c \star (\mu \star g) \;=\; (c \star \mu) \star g \;=\; \delta \star g \;=\; g\,.$$

D'où l'équivalence de l'énoncé.

II.2.30 Soit donc $a \in \mathbb{Z}$ un entier premier avec n, c'est-à-dire non divisible par $3, 11$ ou 17. Appliquons le théorème chinois (théorème 52 de la page 148). Puisque $3, 11, 17$ sont premiers entre eux deux à deux (ce sont des nombres premiers distincts), le système de congruences :

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 1 \mod 11 \\ x \equiv 1 \mod 17 \end{cases}$$

possède dans $\mathbb{Z}$ une solution unique modulo n, cette solution est bien sûr 1. Ainsi la congruence $a^{n-1} \equiv 1 \mod n$ sera vraie si, et seulement si, chacune des congruences $a^{n-1} \equiv 1 \mod 3$, $a^{n-1} \equiv 11 \mod n$, $a^{n-1} \equiv 17 \mod n$ l'est.

Soit donc $p \in \{3, 11, 17\}$. Puisque p ne divise pas a, le petit théorème de Fermat (théorème 51 de la page 146) donne : $a^{p-1} \equiv 1 \mod p$. Remarquons alors que $p-1$ divise $n-1 = 560$:

2, 10 et 16 sont des diviseurs de 560 ($560 = 16 \times 35$). Il existe donc un entier k tel que $n - 1 = k(p - 1)$, d'où la congruence voulue :

$$a^{n-1} \;=\; (a^{p-1})^k \;\equiv 1^k \;=\; 1 \mod p\,.$$

On peut aussi ne pas invoquer le théorème chinois. Ce qui précède montre que $a^{n-1} - 1$ est multiple de chacun des nombres $3, 11, 17$, *i.e.* est multiple de leur ppcm. Ce ppcm est égal à n, en vertu du théorème 44 de la page 90, de sorte que $a^{n-1} - 1$ est multiple de n, *i.e.* $a^{n-1} \equiv 1 \mod n$.

Le raisonnement est le même avec $n = 1729 = 7 \times 13 \times 19$, parce que chacun des nombres $7 - 1 = 6$, $13 - 1 = 12$, $19 - 1 = 18$ divise $n - 1 = 1728$:

$$1728 \;=\; 6 \times 288 \;=\; 12 \times 144 \;=\; 18 \times 96\,.$$

II.2.31 Écartons le cas évident $n := 1$. Notons $V(n)$ l'ensemble des $x \in \mathbb{Z}/n\mathbb{Z}$ tels que $x^2 = 1$ et soit $N(n) := \operatorname{card} V(n)$. Supposons d'abord que n soit un nombre premier $p \geqslant 3$. Dans ce cas, $K := \mathbb{Z}/p\mathbb{Z}$ est un corps, en particulier K est intègre. Si donc $x \in K$, $x^2 - 1 = (x + 1)(x - 1)$ est nul si, et seulement si, $x = 1$ ou $x = -1$. Comme $p \neq 2$, $-1 \neq 1$ dans K, *i.e.* les classes des entiers -1 et 1 modulo p sont distinctes, de sorte que $N(p) = 2$.

Supposons ensuite que $m = 1$, *i.e.* que n soit primaire : $n := p^r$, où $p \in \mathbb{P}$ et $r \geqslant 1$. Soient $k \in \mathbb{Z}$ et $x := \bar{k} \in \mathbb{Z}/p^r\mathbb{Z}$ sa classe modulo p^r. D'abord $x^2 = 1$ si, et seulement si, p^r divise $(k + 1)(k - 1)$. Si c'est le cas, p divise l'un des entiers $k + 1, k - 1$, d'après le lemme d'Euclide. Mais p ne divise pas ces deux entiers, car il ne divise pas leur différence, égale à 2. Si par exemple p divise $k - 1$, p^r est donc premier avec $k + 1$; le théorème de Gauß montre alors que p^r divise $k - 1$, *i.e.* $x = 1$. De même, si p divise $k + 1$, $x = -1$. Là encore $V(p^r) = \{-1, 1\}$, donc $N(p^r) = 2$.

Supposons $m \geqslant 2$, et considérons la factorisation de n :

$$n \;=\; p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}\,,$$

où $p_1, \ldots, p_m$ sont des nombres premiers distincts et $e_1, \ldots, e_m \in \mathbb{N}^*$. Appliquons le théorème 53 de la page 149 et sa preuve. Les nombres $p_1^{e_1}, \ldots, p_m^{e_m}$ sont premiers entre eux deux à deux. Il existe donc un isomorphisme d'anneaux F de $\mathbb{Z}/n\mathbb{Z}$ sur le produit d'anneaux $(\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{e_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_m^{e_m}\mathbb{Z})$. De plus, soit $x \in \mathbb{Z}/n\mathbb{Z}$, et considérons un entier k tel que x soit la classe de k modulo n. Pour $i = 1, \ldots, m$, notons $x_i \in \mathbb{Z}/p_i^{e_i}\mathbb{Z}$ la classe de k modulo $p_i^{e_i}$. Alors $F(x) = (x_1, \ldots, x_m)$. Compte tenu de la définition de la multiplication sur le produit $(\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{e_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_m^{e_m}\mathbb{Z})$, $x^2 = 1$ si, et seulement si, $F(x)^2 = 1$, *i.e.* si, et seulement si, $x_i^2 = 1$ pour tout i. Il en résulte que $(x_1, \ldots, x_m) \mapsto F^{-1}\big((x_1, \ldots, x_m)\big)$ est une bijection du produit d'ensembles $V(p_1^{e_1}) \times \cdots \times V(p_m^{e_m})$ sur $V(n)$ (en fait c'est un isomorphisme de groupes multiplicatifs). Comme chaque $V(p_i^{e_i})$ est de cardinal 2, en vertu de l'alinéa précédent, $V(n)$ est de cardinal 2^m (*cf.* le théorème 18 de la page 73), *i.e.* $N(n) = 2^m$.

II.2.32 Soit $t \in \mathbb{N}^*$ tel que $2^{2^n} + 1 = pt$. L'entier $2^{2^n} + 1$ est impair, donc $p \geqslant 3$. Soit $x := \bar{2}$ la classe de 2 modulo p, c'est un élément de $\mathbb{Z}/p\mathbb{Z}$. Puisque p est premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps (théorème 55 de la page 151), notons-le K. De plus p ne divise pas 2, donc x est un élément non nul de K , *i.e.* un élément du groupe multiplicatif $K^\times = K^* = K \setminus \{0\}$.

D'après le théorème de Lagrange (théorème 22 de la page 125), l'ordre d de x divise l'ordre du groupe K^*, qui vaut $p - 1$. Par ailleurs, l'égalité $2^{2^n} + 1 = pt$ implique la congruence

$2^{2^n} \equiv -1 \mod p$, c'est-à-dire l'égalité (dans K) $x^{2^n} = -\bar{1}$. Évidemment $-\bar{1} \neq \bar{1}$ (parce que $p \neq 2$), mais $(-\bar{1})^2 = \bar{1}$. Ainsi $x^{2^n} \neq \bar{1}$, *i.e.* 2^n n'est pas multiple de d, mais $x^{2^{n+1}} = \big(x^{2^n}\big)^2 = \bar{1}$, *i.e.* 2^{n+1} est multiple de d. Autrement dit, d divise 2^{n+1}, mais ne divise pas 2^n. Les diviseurs positifs de 2^{n+1} sont les 2^k, pour $k = 0, 1, \ldots, n+1$. Le seul de ces diviseurs qui ne divise pas 2^n est 2^{n+1}, et ainsi $d = 2^{n+1}$. Finalement $2^{n+1} = d$ divise $p-1$, *i.e.* $p-1$ est multiple de 2^{n+1}.

II.2.33 Les idées sont les mêmes que pour l'exercice II.2.30. Soit $N := 56\,786\,730$. On vérifie que N est produit de nombres premiers deux à deux distincts :

$$N = 2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 31 \times 61\,.$$

Considérons l'ensemble $P = \{2, 3, 5, 7, 11, 13, 31, 61\}$, formé de nombres premiers. Les $p \in P$ sont premiers entre eux *deux à deux* (ils sont premiers tout court). D'après le théorème 44 de la page 90, leur ppcm est égal à leur produit N.

Cela étant, soient $a, b \in \mathbb{Z}$ et $T := ab(a^{60} - b^{60})$. Il s'agit de montrer que T est multiple de N. Par définition du ppcm (théorème et définition 42 de la page 90), cela revient à montrer que tout $p \in P$ divise T. C'est évident si p divise a ou p divise b. Dans le cas contraire, p étant premier et ne divisant pas a, le petit théorème de Fermat (théorème 51 de la page 146) donne : $a^{p-1} \equiv 1 \mod p$, et de même $b^{p-1} \equiv 1 \mod p$.

C'est là que l'on comprend le choix de P : P est formé de *tous* les nombres premiers q tels que $q-1$ divise 60 : $1, 2, 4, 6, 10, 12, 30, 60$ sont des diviseurs de 60. La congruence $a^{p-1} \equiv 1 \mod p$ implique donc $a^{60} \equiv 1 \mod p$, de même $b^{60} \equiv 1 \mod p$. Mais alors $a^{60} \equiv b^{60} \mod p$, *i.e.* p divise $a^{60} - b^{60}$, donc p divise T.

II.2.34 Rappelons que, pour tout entier $u \in \mathbb{Z}$, $\bar{u}$ désigne la classe de u modulo N. Voici ce que nous voulons démontrer : il existe deux entiers $T \in \mathbb{N}^*$ et $r \in \mathbb{N}$ tels que $\overline{(n+T)}^{n+T} = \bar{n}^n$ pour tout entier $n \geqslant r$, cette égalité se traduisant ainsi en termes de congruence :

$$(n+T)^{n+T} \equiv n^n \mod N\,. \qquad (*)$$

Posons $T := N\varphi(N)$, où φ est la fonction indicatrice d'Euler (définition 21 de la page 145). Par ailleurs, soit r le plus grand des entiers $\nu_p(N)$, p parcourant l'ensemble des diviseurs premiers de N (voir la formule (11) de la page 86 pour la définition des ν_p). Montrons que T et r répondent à la question. Considérons donc un entier $n \geqslant r$. Comme N divise T, $(n+T)^{n+T} \equiv n^{n+T} \mod N$. Il suffit ainsi de prouver la congruence suivante :

$$n^{n+T} \equiv n^n \mod N, \quad \text{soit} \quad n^n(n^T - 1) \equiv 0 \mod N\,. \qquad (**)$$

D'après le théorème 38 de la page 87, $n^n(n^T - 1) \equiv 0 \mod N$ si, et seulement si, pour tout diviseur premier p de N, p^ν divise $n^n(n^T - 1)$, en posant $\nu := \nu_p(N)$. C'est vrai si p divise n, puisqu'alors n^n est multiple de n^r ($n \geqslant r$) et $r \geqslant \nu$. Si p ne divise pas n, le théorème d'Euler (théorème 50 de la page 146) donne : $n^{\varphi(p^\nu)} \equiv 1 \mod p^\nu$. Comme T est multiple de $\varphi(N)$, qui lui-même est multiple de $\varphi(p^\nu)$ (en vertu de l'assertion 2 du théorème 53 de la page 149), on a bien $n^T \equiv 1 \mod p^\nu$. En conclusion, p^ν divise $n^T - 1$ et *a fortiori* $n^n(n^T - 1)$, et ce pour tout diviseur premier p de N, ce qui établit la congruence $(**)$.

II.2.35 Soit L un corps à quatre éléments. Le groupe additif $(L, +)$ est un groupe d'ordre 4. D'après le théorème de Lagrange, $4x = 0$ pour tout $x \in L$. En particulier $4 \cdot 1_L = 0$. Mais $4 \cdot 1_L = (2 \cdot 1_L)^2$, donc $2 \cdot 1_L$ est nul (L est un anneau intègre). Ainsi L est de caractéristique 2.

Soit maintenant $K = \{0, 1, a, b\}$. Nous voulons définir sur K deux lois $+$ et $\times$ faisant de K un corps, avec 0 (resp. 1) comme élément neutre pour $+$ (resp. $\times$). Supposons que cela soit fait. Vu ce qui précède, K est alors de caractéristique 2, donc $2x = 0$ pour tout $x \in K$. D'après l'exercice II.2.14, la table d'addition de K est nécessairement la suivante :

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

Pour la multiplication, on a déjà $0x = x0 = 0$ et $1x = x1 = x$ pour tout $x \in K$. Il reste à déterminer a^2, b^2, ab et ba. Par régularité, ab est non nul, distinct de a (car $b \neq 1$) et de b (car $a \neq 1$), donc $ab = 1$, de même $ba = 1$. Le même argument montre que a^2 est non nul, distinct de $1 = ab$ (car $a \neq b$) et de $a = 1a$ (car $a \neq 1$), donc $a^2 = b$, de même $b^2 = a$. La table de multiplication de K est donc nécessairement la suivante :

$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Cette analyse étant faite, passons à la synthèse. *Définissons* sur K deux lois $+$ et $\times$ par les deux tables ci-dessus. Il s'agit de montrer que $(K, +, \times)$ est un corps. En vertu de l'exercice II.2.14, nous savons déjà que $(K, +)$ est un groupe commutatif, isomorphe à $\big((\mathbb{Z}/2\mathbb{Z})^2, +\big)$. Ensuite $K^* = K \setminus \{0\}$ est multiplicativement stable. Considérons le groupe $(\mathbb{Z}/3\mathbb{Z}, +)$. Soit $f : \mathbb{Z}/3\mathbb{Z} \to K^*$ la bijection appliquant $\bar{0}, \bar{1}, \bar{2}$ sur $1, a, b$ respectivement. On voit immédiatement que $f(u + v) = f(u)f(v)$ pour tous $u, v \in \mathbb{Z}/3\mathbb{Z}$. On en déduit que $(K^*, \times)$ est un groupe (et que f est un isomorphisme de groupes).

Sur la table de multiplication, on voit que $0x = x0 = 0$ et $1x = x1 = x$ pour tout $x \in K$. On voit aussi que la multiplication est commutative (la table est symétrique par rapport à la diagonale principale). Si $x, y, z \in K$, l'égalité $(xy)z = x(yz)$ est évidente lorsque l'un des éléments x, y, z est nul. Dans le cas contraire, elle résulte du fait que $(K^*, \times)$ soit un groupe. Il nous reste à vérifier la distributivité de la multiplication par rapport à l'addition. Soient donc $x, y, z \in K$, il s'agit de vérifier que $x(y+z) = xy + xz$. C'est évident si x vaut 0 ou 1. C'est aussi évident si $y = 0$ ou $z = 0$ ou encore $y = z$. Supposons que $x = a$. Vu la commutativité de l'addition, les égalités suivantes suffisent pour conclure :

$$a(1+a) \;=\; ab \;=\; a+b \;=\; a+a^2\,,\;\; a(1+b) \;=\; a^2 \;=\; b \;=\; a+ab \quad \text{et}$$

$a(a+b) \;=\; a1 \;=\; a \;=\; b+1 \;=\; a^2+ab$. On conclut de même si $x = b$ (les deux tables ne changent pas lorsqu'on échange a et b).

En conclusion, les deux tables font de $(K, +, \times)$ un corps (commutatif) à quatre éléments.

II.2.36 Soit donc A un anneau intègre fini. Il s'agit de montrer que, si a est un élément non nul de A, a est inversible. Soit $f : A \to A$ l'application $x \mapsto ax$. C'est un morphisme du groupe

$(A,+)$ dans lui-même. Son noyau est formé des $x \in A$ tels que $ax = 0$, il est réduit à $\{0\}$, puisque A est intègre. Ainsi f est injectif (théorème 20 de la page 124). Puisque A est un ensemble fini, f est bijectif (théorème 15 de la page 71). En particulier $1 \in f(A)$, *i.e.* il existe un $x \in A$ tel que $ax = 1$. On en déduit que $a1 = a = 1a = (ax)a = a(xa)$, d'où $xa = 1$ parce que a est régulier pour $\times$. L'élément x est donc inverse de a.

Voici une autre solution. L'application $g : n \mapsto a^n$ de $\mathbb{N}$ dans A ne peut pas être injective, car sinon ce serait une bijection de $\mathbb{N}$ sur l'ensemble fini $g(\mathbb{N}) \subset A$. Il existe donc deux entiers m, n tels que $a^m = a^n$ et $m > n$. Alors $0 = a^m - a^n = a^n(a^{m-n} - 1)$. Mais $a^n \neq 0$ puisque $a \neq 0$, d'où $a^{m-n} = 1$ (par intégrité de A). Dans ces conditions, $aa^{m-n-1} = 1 = a^{m-n-1}a$, donc a^{m-n-1} est inverse de a.

Le lecteur pourra comparer avec l'exercice II.2.3, et aussi avec l'exercice 4 de la page 339.

II.2.37 1) Définissons une application $\beta : \mathcal{F}(X,K) \to \mathcal{P}(X)$ ainsi :

$$\beta(f) \;:=\; f^{-1}(\{1\}) \;=\; \big\{x \in X \;\big|\; f(x) = 1\big\}\,.$$

Si $A \in \mathcal{P}(X)$, la définition de χ_A montre que $A = \big\{x \in X \;\big|\; \chi_A(x) = 1\big\}$, *i.e.* $\beta(\chi_A) = A$. Cela montre que $\beta \circ \chi$ est l'identité de $\mathcal{P}(X)$. Soit $f \in \mathcal{F}(X,K)$, et posons $A := \beta(f)$. Considérons un élément x de X. Par définition de β, $x \in A$ si, et seulement si, $f(x) = 1$. Ainsi $\chi_A(x) = 1$ équivaut à $f(x) = 1$, de sorte que $\chi_A = f$, *i.e.* $\chi\big(\beta(f)\big) = f$. Il en résulte que $\chi \circ \beta$ est l'identité de $\mathcal{F}(X,K)$. En conclusion, χ est une bijection, et la bijection réciproque est β.

2) Montrons que $\chi_{A+B} = \chi_A + \chi_B$ et $\chi_{A\cap B} = \chi_A\chi_B$. Soit $x \in X$. Il s'agit de vérifier les égalités suivantes :

$$\chi_{A+B}(x) \;=\; \chi_A(x) + \chi_B(x) \quad \text{et} \quad \chi_{A\cap B}(x) \;=\; \chi_A(x)\chi_B(x)\,.$$

La deuxième égalité est évidente : comme $\chi_A(x)$ et $\chi_B(x)$ valent chacun 0 ou 1, leur produit vaut 1 si, et seulement si, $\chi_A(x) = \chi_B(x) = 1$, *i.e.* si x appartient à la fois à A et à B, c'est-à-dire appartient à $A \cap B$, ou encore si $\chi_{A\cap B}(x) = 1$.

Pour la première égalité, distinguons quatre cas. Si $x \in A \cap B$, on a $\chi_A(x) + \chi_B(x) = 1 + 1 = 0$. D'un autre côté $x \notin A + B = (A \cup B) \setminus (A \cap B)$, donc $\chi_{A+B}(x) = 0$. Si $x \notin A \cup B$, $\chi_A(x) + \chi_B(x) = 0 + 0 = 0$. D'un autre côté, $x \notin A + B$, donc $\chi_{A+B}(x) = 0$. Supposons ensuite que $x \in A$ et $x \notin B$. Alors $\chi_A(x) + \chi_B(x) = 1 + 0 = 1$. D'un autre côté, $x \in A + B$, donc $\chi_{A+B}(x) = 1$. On a la même conclusion si $x \notin A$ et $x \in B$, ce qui prouve l'égalité $\chi_{A+B} = \chi_A + \chi_B$.

Nous savons que $\big(\mathcal{F}(X,K), +, \times\big)$ est un anneau (exemple 3 de la page 133). Puisque χ est une bijection de $\mathcal{P}(X)$ sur $\mathcal{F}(X,K)$ respectant les lois $+$ et $\times$, on en déduit que $\big(\mathcal{P}(X), +, \times\big)$ est un anneau, par « transport de structure ». Vérifions par exemple l'associativité de l'addition dans $\mathcal{P}(X)$. Soient A, B, C trois parties de X. Alors :

$$\chi_{(A+B)+C} = \chi_{A+B} + \chi_C = (\chi_A + \chi_B) + \chi_C = \chi_A + (\chi_B + \chi_C) = \chi_{A+(B+C)}\,,$$

d'où $(A + B) + C = A + (B + C)$ puisque χ est injective. Les autres propriétés d'un anneau se vérifient de la même façon.

II.2.38 Soit $x \in K$, écrivons $x := a/b$, où $a, b \in A$ et $b \neq 0$. Puisque f est injectif, $f(b) \in A'$ n'est pas nul, ce qui nous permet de poser :

$$F(x) \;=\; f(a)/f(b) \in K'\,. \qquad (*)$$

Pour que cette formule définisse une application F de K dans K', il faut vérifier que, si c/d est une autre fraction représentant x ($c, d \in A$ et $d \neq 0$), $f(a)/f(b) = f(c)/f(d)$. Or $ad = bc$, et f est un morphisme d'anneaux, donc $f(a)f(d) = f(b)f(c)$, soit $f(a)/f(b) = f(c)/f(d)$.

Il est clair que F prolonge f : si $a \in A$, $a = a/1$ et donc, vu la définition de F, $F(a) = f(a)/f(1) = f(a)$ $\big(f(1) = 1$ par définition d'un morphisme d'anneaux$\big)$. En particulier $F(1) = f(1) = 1$. Soient $x, y \in K$, écrivons $x := a/b$ et $y := c/d$, avec $a, b, c, d \in A$ et $b \neq 0$, $d \neq 0$. Alors $x + y = (ad + bc)/(bd)$, d'où :

$$\begin{aligned} F(x+y) &= f(ad+bc)/f(bd) = \big(f(a)f(d) + f(b)f(c)\big)/\big(f(b)f(d)\big) \\ &= f(a)/f(b) + f(c)/f(d) = F(x) + F(y)\,. \end{aligned}$$

De la même façon, $xy = (ac)/(bd)$, d'où :

$$\begin{aligned} F(xy) &= f(ac)/f(bd) = \big(f(a)f(c)\big)/\big(f(b)f(d)\big) \\ &= \big[f(a)/f(b)\big]\big[f(c)f(d)\big] = F(x)F(y)\,. \end{aligned}$$

Ainsi $F : K \to K'$ est un morphisme de corps (*i.e.* d'anneaux) prolongeant f.

Soit $G : K \to K'$ un autre morphisme prolongeant f. Il reste à montrer que $G = F$. Soit $L = \big\{x \in K \;\big|\; F(x) = G(x)\big\}$. D'après l'exemple 1 de la page 153, L est un sous-corps de K. En outre L contient A car, pour tout $a \in A$, $F(a) = f(a) = G(a)$. Soit alors $x \in K$, écrivons $x := a/b$, où $a, b \in A$ et $b \neq 0$. Dans K, on peut aussi écrire $x = ab^{-1}$. Puisque F et G sont des morphismes de corps,

$$F(x) \;=\; F(a)F(b)^{-1} \;=\; f(a)f(b)^{-1} \;=\; G(a)G(b)^{-1} \;=\; G(x)\,,$$

ce qui montre que $F = G$.

II.2.39 D'après le théorème et définition 39 de la page 141, il existe un unique morphisme d'anneaux ε de $\mathbb{Z}$ dans K, il est défini par $\varepsilon(j) := j \cdot 1_K$ pour tout $j \in \mathbb{Z}$. La caractéristique de K est par définition l'unique $n \in \mathbb{N}$ tel que $\mathrm{Ker}(\varepsilon) = n\mathbb{Z}$. Notons aussi que k contient $\varepsilon(\mathbb{Z})$, par exemple parce que $\varepsilon^{-1}(k)$ est un sous-anneau de $\mathbb{Z}$, donc est égal à $\mathbb{Z}$.

Supposons que $n = 0$, de sorte que ε est injectif. D'après l'exercice précédent, ε se prolonge de manière unique en un morphisme de corps f de $\mathbb{Q}$ dans K. Explicitement, si $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, on a :

$$f(a/b) \;=\; \varepsilon(a)\varepsilon(b)^{-1} \;=\; (a \cdot 1_K)(b \cdot 1_K)^{-1}\,.$$

Comme $\mathbb{Q}$ et L sont des corps, f est injectif (proposition 54 de la page 151). C'est donc un isomorphisme de $\mathbb{Q}$ sur le sous-corps $f(\mathbb{Q})$ de K. Il reste à vérifier que $f(\mathbb{Q}) = k$. La définition de k et le fait que $f(\mathbb{Q})$ soit un sous-corps de K impliquent l'inclusion $k \subset f(\mathbb{Q})$. En sens inverse, soient $x \in \mathbb{Q}$, écrivons $x := a/b$, où $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Alors $\varepsilon(a)$ et $\varepsilon(b)$ appartiennent à k, donc $f(x) = \varepsilon(a)\varepsilon(b)^{-1}$ appartient à k, puisque k est un sous-corps de K. D'où $f(\mathbb{Q}) \subset k$, et par suite $f(\mathbb{Q}) = k$.

Supposons que la caractéristique de K soit un nombre premier p. Notons $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ le morphisme canonique. Soit $x \in \mathbb{Z}/p\mathbb{Z}$. Il existe $a \in \mathbb{Z}$ tel que $x = \bar{a} = \pi(a)$. Si b est un autre entier tel que $x = \bar{b} = \pi(b)$, a et b sont congrus modulo p, *i.e.* il existe $t \in \mathbb{Z}$ tel que $b = a + pt$. Comme $\varepsilon(p) = 0$, on en déduit que $\varepsilon(a) = \varepsilon(b)$. Cela permet de définir une application f de $\mathbb{Z}/p\mathbb{Z}$ dans K en posant $f(x) := \varepsilon(a)$. Les formules (24) et (32) montrent que $f : \mathbb{Z}/p\mathbb{Z} \to K$ est un morphisme d'anneaux, et $f \circ \pi = \varepsilon$, par définition de f.

D'après la proposition 54 de la page 151, f est injectif, c'est donc un isomorphisme de $\mathbb{Z}/p\mathbb{Z}$ sur $f(\mathbb{Z}/p\mathbb{Z})$. Puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps, $f(\mathbb{Z}/p\mathbb{Z})$ est un sous-corps de K, il contient donc k. Par ailleurs π est surjectif, d'où :

$$f(\mathbb{Z}/p\mathbb{Z}) \;=\; f\big(\pi(\mathbb{Z})\big) \;=\; \varepsilon(\mathbb{Z}) \;\subset\; k,$$

donc $f(\mathbb{Z}/p\mathbb{Z}) = k$. Soit $a \in \mathbb{Z}$. Alors $f(\bar{a}) = f\big(\pi(a)\big) = \varepsilon(a) = a \cdot 1_K$, ce qui prouve l'existence de f. Si $g : \mathbb{Z}/p\mathbb{Z} \to K$ est un autre morphisme d'anneaux tel que $g(\bar{a}) = a \cdot 1_K$ pour tout $a \in \mathbb{Z}$, on a $g \circ \pi = \varepsilon = f \circ \pi$, d'où $g = f$ puisque π est surjectif.

II.2.40 Soit en général $n \in \mathbb{N}^*$. Dans le module II.5, il est démontré que l'équation $x^n = 1$ a exactement n racines dans $\mathbb{C}$, à savoir les nombres $\cos(2k\pi/n) + i\sin(2k\pi/n)$, k décrivant $[\![0, n-1]\!]$. De plus, dans le cas $n := 3$, ces trois racines sont $1, j, j^2$, où $j := (-1 + i\sqrt{3})/2$ et $j^2 = (-1 - i\sqrt{3})/2$. Dans le cas $n := 5$, les cinq racines cinquièmes de l'unité de $\mathbb{C}$ sont déterminées dans le module II.5.

Le cas de $\mathbb{R}$ est simple : si n est impair, 1 est la seule solution réelle de l'équation $x^n = 1$. En effet, $x \mapsto x^n$ est alors une bijection strictement croissante de $\mathbb{R}$ sur $\mathbb{R}$. Ainsi les équations $x^3 = 1$ et $x^5 = 1$ ont chacune une seule solution dans $\mathbb{R}$, à savoir 1. Si n est pair, -1 et 1 sont les seules solutions réelles de l'équation $x^n = 1$ $\big(x \mapsto x^n$ est alors une bijection strictement croissante de $\big[0, +\infty\big[$ sur lui-même$\big)$.

Notons K le corps $\mathbb{Z}/11\mathbb{Z}$. Le groupe multiplicatif K^* est d'ordre 10. D'après le théorème de Lagrange, il ne possède pas d'élément d'ordre 3. Il en résulte que 1 est la seule solution de l'équation $x^3 = 1$ $(= \bar{1})$ dans K. Posons $\mu_5(K) := \big\{x \in K \;\big|\; x^5 = 1\big\}$. Il est clair que $\mu_5(K)$ est un sous-groupe de $(K^*, \times)$. Son ordre divise donc 10. Ce sous-groupe contient $\bar{3}$, car $3^5 = 243 = 2 \times 11^2 + 1$ est congru à 1 modulo 11. Par contre $\bar{2} \notin \mu_5(K)$, car $2^5 = 32 \equiv -1 \mod 11$. On en déduit que $\mu_5(K)$ est le groupe cyclique d'ordre 5 engendré par $\bar{3}$. Comme $\bar{3}^2 = \bar{9}$, $\bar{3}^3 = \overline{27} = \bar{5}$ et $\bar{3}^4 = \overline{15} = \bar{4}$, on obtient :

$$\mu_5(K) \;=\; \big\{\bar{1}, \bar{3}, \bar{4}, \bar{5}, \bar{9}\big\}.$$

Raisonnons de même avec $K = \mathbb{Z}/19\mathbb{Z}$. Ici le groupe $(K^*, \times)$ est d'ordre 18. Comme 5 ne divise pas 18, 1 est la seule solution de l'équation $x^5 = 1$ dans K. Par contre, on a $\bar{7}^3 = 1$, car $7^3 = 343 = 18 \times 19 + 1 \equiv 1 \mod 19$. Comme $\bar{7}^2 = \overline{49} = \overline{11}$, on en déduit ceci :

$$\mu_3(K) \;=\; \big\{\bar{1}, \bar{7}, \overline{11}\big\}.$$

On peut le voir de deux façons. Anticipant sur le module II.6, portant sur les polynômes, le polynôme $X^3 - 1 \in K[X]$ a au plus trois racines dans K, il en a donc exactement trois, à savoir $\bar{1}, \bar{7}$ et $\overline{11}$. Une autre méthode, plus brutale mais simple, est de déterminer tous les entiers $a \in [\![0, 18[\![$ tels que $a^3 \equiv 1 \mod 19$, on ne trouve que $1, 7$ et 11.

II.2.41 1) Raisonnons comme dans la preuve de la proposition 66 de la page 104. Supposons que 10 soit le carré d'un rationnel q ($q > 0$ par exemple), et soit $q := a/b$ la forme irréductible de q. Alors $a^2 = 10b^2$. Montrons que $b = 1$. Supposons le contraire, et soit p un facteur premier de b. Alors p^2 divise $10b^2 = a^2$, donc p divise a, en vertu du lemme d'Euclide. Ainsi p divise a et b, c'est absurde car $a \wedge b = 1$. Maintenant 10 est le carré d'un entier positif a. C'est manifestement impossible car on aurait $a \in \{1, 2, 3\}$, puisque $4^2 > 10$.

Soient $a, b, c, d \in \mathbb{Q}$ tels que $a + b\sqrt{10} = c + d\sqrt{10}$. Montrons que $a = c$. Supposons $a \neq c$. L'égalité $a - c = (d - b)\sqrt{10}$ implique $(a - c)^2 = 10(b - d)^2$, d'où $10 = q^2$, en posant $q := (a - c)/(b - d) \in \mathbb{Q}$. Cela contredit l'irrationalité de $\sqrt{10}$. Ainsi $a = c$, d'où évidemment $b = d$.

2) D'abord A contient 1. Soient ensuite $x, y \in A$. Écrivons $x := a+b\sqrt{10}$ et $y := c+d\sqrt{10}$, où $a, b, c, d \in \mathbb{Z}$. Alors $x \pm y = (a \pm c) + (b \pm d)\sqrt{10}$ appartient à A. De même,

$$xy \;=\; (a + b\sqrt{10})(c + d\sqrt{10}) \;=\; (ac + 10bd) + (ad + bc)\sqrt{10} \in A\,.$$

Ainsi A est un sous-anneau de $\mathbb{R}$. Le même argument montre que K est un sous-anneau de $\mathbb{R}$. Pour voir que K est un sous-corps de $\mathbb{R}$, il suffit de montrer que, si $x \in K$ n'est pas nul, son inverse $1/x$ (dans $\mathbb{R}$) appartient à K. Écrivons $x := a + b\sqrt{10}$, où $a, b \in \mathbb{Q}$. Par hypothèse $(a, b) \neq (0, 0)$, donc $y = a - b\sqrt{10} \neq 0$, en vertu de 1. Ainsi $xy = (a + b\sqrt{10})(a - b\sqrt{10}) = a^2 - 10b^2$ n'est pas nul, et l'on a :

$$\frac{1}{x} \;=\; \frac{y}{xy} \;=\; \frac{a - b\sqrt{10}}{a^2 - 5b^2}\,.$$

Cela montre que $1/x \in K$. Ainsi K est un sous-corps de $\mathbb{R}$.

Montrons que K est isomorphe au corps des fractions de A. D'abord A est un sous-anneau de K. Soit $x \in K$, écrivons $x := u + v\sqrt{10}$, où $u, v \in \mathbb{Q}$. Mettons chacun des rationnels u, v sous forme de fraction irréductible : $u = a/b$ et $v = c/d$. Alors $x = (ad + bc\sqrt{10})/(bd)$, ce qui s'écrit $x = \alpha\beta^{-1}$, où $\alpha = ad + bc\sqrt{10} \in A$ et $\beta = bd \in A^*$. La remarque suivant le théorème 56 de la page 152 montre alors que K est isomorphe au corps des fractions de A.

3) Soient $a, b, c, d \in \mathbb{Q}$ et $x := a + b\sqrt{10}$, $y := c + d\sqrt{10}$. Comme nous l'avons vu, $xy = (ac + 10bd) + (ad + bc)\sqrt{10}$. Montrons que $N(xy) = N(x)N(y)$. Cela revient à vérifier l'égalité suivante :

$$(a^2 - 10b^2)(c^2 - 10d^2) \;=\; (ac + 10bd)^2 - 10(ad + bc)^2\,.$$

En développant chacun des deux membres, on trouve le même résultat, à savoir $a^2c^2 - 10(a^2d^2 + b^2c^2) + 100b^2d^2$. Si x est écrit comme ci-dessus et $x \neq 0$, nous savons aussi que $a - b\sqrt{10} \neq 0$, d'où $a^2 - 10b^2 = N(x) \neq 0$. Il en résulte bien que N est un morphisme de $(K^*, \times)$ dans $(\mathbb{Q}^*, \times)$. Si $a, b \in \mathbb{Z}$, $a^2 - 10b^2$ est entier, d'où $N(A^*) \subset \mathbb{Z}^*$.

4) Soit $x \in A$, écrivons $x := a + b\sqrt{10}$, où $a, b \in \mathbb{Z}$. Supposons que $x \in A^\times$, et soit $y \in A$ l'inverse de x. Puisque N est un morphisme de groupes multiplicatifs, $1 = N(1) = N(xy) = N(x)N(y)$. Or $N(x), N(y)$ sont des entiers, et il en résulte que $N(x) = N(y) = \pm 1$. Supposons inversement que $a^2 - 10b^2 = N(x) = \pm 1$. Nous avons vu ci-dessus que $1/x = (a - b\sqrt{10})/N(x)$, ce qui montre que $1/x \in A$. Ainsi x est inversible dans A. D'où la conclusion :

$$A^\times \;=\; \big\{x \in A \;\big|\; N(x) = \pm 1\big\}\,.$$

Posons $\theta := 3 + \sqrt{10} \in A$. Alors $\theta \in A^\times$, car $3^2 - 10 \times 1^2 = -1$. Il en résulte que $\theta^n \in A^\times$ pour tout $n \in \mathbb{N}^*$. Par ailleurs $\theta > 1$, donc la suite $(\theta^n)_{n \geqslant 1}$ est strictement croissante ; cette suite étant formée d'éléments de $A^\times$, cela montre que $A^\times$ est infini.

5) Si un entier n est un carré, le chiffre des unités de n peut être $0, 1, 4, 5, 6$ ou 9, mais pas $2, 3, 7$ ou 8. En effet, si $n := m^2$ avec $m \in \mathbb{Z}$, on écrit $m := 10q + r$ où $q \in \mathbb{Z}$ et $r \in [\![0, 9[\![$ (division euclidienne par 10). Alors $n = (10q + r)^2 \equiv r^2 \mod 10$, et il

ne reste plus qu'à constater que les restes modulo 10 de $0^2, 1^2, \ldots, 9^2$ ne prennent que les valeurs indiquées (on peut même se restreindre à $0, \ldots, 5$, quitte à remplacer m par $-m$). Ainsi l'égalité $a^2 - 10b^2 = \pm 2$ est impossible, car elle entraînerait la congruence $a^2 \equiv \pm 2 \mod 10$, signifiant que le chiffre des unités de a^2 est 2 ou 8.

La question 4 montre que $2 \notin A^\times$ puisque $N(2) = 4$. Supposons 2 non irréductible dans A. La définition 19 de la page 143 montre alors que 2 peut s'écrire $2 = xy$, où x, y sont des éléments *non inversibles* de A. Compte tenu de 4, on a donc $N(x) \neq \pm 1$. Mais $N(x), N(y)$ sont deux entiers, dont le produit vaut $N(xy) = N(2) = 4$ (en vertu de 3). La seule possibilité est que $N(x) = N(y) = \pm 2$. En écrivant x sous la forme $x := a + b\sqrt{10}$, où $a, b \in \mathbb{Z}$, on a donc $a^2 - 10b^2 = \pm 2$, ce qui contredit l'alinéa précédent. Ainsi 2 est un élément irréductible de A.

6) Posons $x := 4 + \sqrt{10}$ et $y := 4 - \sqrt{10}$, de sorte que

$$xy \;=\; N(x) \;=\; 4^2 - 10 \times 1^2 \;=\; 6 \;=\; 2 \times 3\,.$$

Raisonnons par l'absurde, en supposant que l'anneau A est principal. D'après la question 5, l'élément $2 \in A$ est irréductible, et il divise $xy = 6$. En vertu du théorème 45 de la page 144, 2 divise (dans A) l'un des deux éléments x, y. Il existe donc $z \in A$ et $\varepsilon \in \{-1, 1\}$ tels que $4 + \varepsilon\sqrt{10} = 2z$. Mais $z \in A$ s'écrit $z := c + d\sqrt{10}$, où $c, d \in \mathbb{Z}$. Ainsi $4 + \varepsilon\sqrt{10} = 2c + 2d\sqrt{10}$. D'après 1, on en déduit les égalités $4 = 2c$ et $\varepsilon = 2d$. C'est absurde, car $\varepsilon = \pm 1$ et $d \in \mathbb{Z}$. En conclusion, l'anneau A n'est pas principal.

Module II.3 : Espaces vectoriels et applications linéaires

II.3.1 En utilisant la distributivité à gauche de la loi externe (premier axiome énoncé dans 1), la règle concernant 1 (dernier axiome) et l'associativité de l'addition, on trouve :

$$(1+1).(x+y) = 1.(x+y) + 1.(x+y) = x+y+x+y.$$

Un calcul similaire utilisant d'abord la distributivité à droite (deuxième axiome énoncé dans 1) donne :

$$(1+1).(x+y) = (1+1).x + (1+1).y = x+x+y+y.$$

De l'égalité $x+y+x+y = x+x+y+y$, en simplifiant à gauche par x et à droite par y (car V est un groupe), on déduit : $y+x = x+y$, c'est-à-dire la commutativité.

Soient K un corps et V un groupe commutatif quelconque. Pour tout $(\lambda, x) \in K \times V$, nous *posons* $\lambda.x := 0_V$. Il est alors immédiat que tous les axiomes des espaces vectoriels sont vérifiés, à la seule exception de l'axiome $1.x = x$. Celui-ci n'est donc pas conséquence des autres.

II.3.2 Pour clarifier ce qui suit, rappelons d'abord la différence entre deux notations très proches. Dans tout groupe abélien noté additivement, on peut définir, pour $m \in \mathbb{Z}$ et pour tout élément x du groupe, un élément mx du groupe : $0x = 0$, $1x = x$, $2x = x+x$, puis de proche en proche, $(n+1)x = nx + x$ (ici, $n \in \mathbb{N}$) ; si $m = -n$ est négatif, on pose $mx = -(nx)$. Ainsi, dans le $\mathbb{Q}$-espace vectoriel V, la notation $2x$ représente $x+x$ et la notation $(-2)x$ représente $-(x+x)$. Les propriétés de cette opération ont été étudiées dans le module II.2.

Par ailleurs, le $\mathbb{Q}$-espace vectoriel V est muni d'une loi externe $a.x$ définie pour $a \in \mathbb{Q}$ et $x \in V$. En particulier, si $m \in \mathbb{Z}$ et $x \in V$, on a un élément $m.x \in V$ qui n'a *a priori* pas de rapport avec mx. Il s'agit ici de démontrer que c'est le même. Nous noterons 0_V l'élément neutre de V.

On fixe donc $x \in V$, et l'on veut démontrer que, pour tout entier $m \in \mathbb{Z}$, on a l'égalité $mx = m.x$. Prouvons le d'abord pour $m \in \mathbb{N}$ par récurrence sur m. On a vu au début de la section 1 que $0.x = 0_V$. Comme, par définition, $0x = 0_V$, la propriété est vraie pour $m = 0$. Supposons-la vraie pour un entier naturel $m \in \mathbb{N}$: $mx = m.x$. Alors, par définition, $(m+1)x = mx + x$. Par ailleurs, d'après les axiomes des espaces vectoriels, $(m+1).x = m.x + 1.x = m.x + x$. Comme, par hypothèse de récurrence, $m.x = mx$, on a bien $(m+1).x = (m+1)x$. Ceci achève la preuve pour $m \in \mathbb{N}$. Supposons enfin $m \in \mathbb{Z}$ négatif. Alors $m = -n$, où $n \in \mathbb{N}$. On a donc $n.x = nx$. D'après l'une des règles démontrées au début de la section 1, $(-n).x = -(n.x)$. Comme, par définition, $(-n)x = -(nx)$, on a bien $m.x = mx$. Cette démonstration *très facile* a été écrite en grand détail uniquement à cause du risque de confusion des notations : nous revenons maintenant à un style plus naturel !

En particulier, nous noterons ax la loi externe de V et 0 l'élément neutre de V.

Montrons maintenant que le groupe V est sans torsion. Supposons donc $m \in \mathbb{Z} \setminus \{0\}$ et soit $x \in V$ tel que $mx = 0$. Alors :

$$x = 1x = \big(\frac{1}{m}m\big)x = \frac{1}{m}(mx) = \frac{1}{m}0 = 0.$$

Montrons de même que le groupe est divisible. Soient donc $m \in \mathbb{Z} \setminus \{0\}$ et $x \in V$, et posons $y := \dfrac{1}{m}x$. Alors :

$$my = m\big(\frac{1}{m}x\big) = \big(m\frac{1}{m}\big)x = 1x = x.$$

En fait, dire que V est sans torsion (resp. divisible) équivaut à dire que, pour tout $m \in \mathbb{Z}\setminus\{0\}$, l'application $x \mapsto mx$ de V dans V est injective (resp. surjective). Or, dans le cas d'un $\mathbb{Q}$-espace vectoriel , c'est une homothétie de rapport $m \neq 0$, donc une bijection. Cependant, ces deux propriétés ne vont pas toujours ensemble :

1. Le groupe additif $(\mathbb{Z}, +)$ est sans torsion mais il n'est pas divisible.
2. Le groupe multiplicatif $(\mathbb{C}^*, .)$ est divisible, mais il n'est pas sans torsion. En effet, dans ce cas, la notation étant multiplicative, cela signifierait que, pour tout $m \in \mathbb{Z} \setminus \{0\}$, l'égalité $x^m = 1$ entraîne $x = 1$. C'est bien sûr faux !

II.3.3 Soit V un groupe abélien sans torsion et divisible. D'après l'exercice précédent, cela signifie que, quel que soit l'entier relatif non nul m, l'application $x \mapsto mx$ de V dans lui-même est bijective. Notons h_m cette application. De la commutativité de V on déduit de plus que, pour tous $x, y \in V$, on a $m(x + y) = mx + my$, *i.e.* h_m est un automorphisme du groupe G.
Montrons d'abord l'unicité de la loi externe qui ferait de V un $\mathbb{Q}$-espace vectoriel. D'après l'exercice précédent, cette loi externe vérifie nécessairement $m.x = mx = h_m(x)$, donc, pour tout rationnel non nul $r = \dfrac{m}{n}$:

$$h_n(r.x) = n.(r.x) = (nr).x = m.x = h_m(x),$$

de sorte que l'on a $r.x = h_n^{-1}\big(h_m(x)\big)$. Pour $m = 0$ et $r = 0$, c'est encore vrai, et l'on voit que la loi externe est complètement déterminée par les applications h_m ($m \in \mathbb{Z}$), qui, à leur tour, sont complètement déterminées par la loi de groupe. Cela établit l'unicité.
Il s'agit maintenant de démontrer qu'en posant, pour tout rationnel $r = \dfrac{m}{n} \in \mathbb{Q}$ (où $m \in \mathbb{Z}$ et $n \in \mathbb{Z} \setminus \{0\}$) :

$$r.x := h_n^{-1}\big(h_m(x)\big),$$

on définit bien une structure de $\mathbb{Q}$-espace vectoriel sur le groupe V. Tout d'abord, il faut montrer que la loi est bien définie et ne dépend pas de l'écriture particulière choisie. On suppose donc que $r = \dfrac{m}{n} = \dfrac{m'}{n'}$. Alors $mn' = m'n$. Or, pour tous $a, b \in \mathbb{Z}$, et tout $x \in V$, on a établi dans le module II.2 l'égalité $a(bx) = (ab)x$. Cela entraîne $h_a \circ h_b = h_b \circ h_a = h_{ab}$. De $mn' = m'n$ on déduit donc $h_m \circ h_{n'} = h_{m'} \circ h_n$, d'où, pour $x \in V$, $h_n^{-1}\big(h_m(x)\big) = h_{n'}^{-1}\big(h_{m'}(x)\big)$. Le produit externe $r.x$ est donc bien défini.
La vérification des axiomes des espaces vectoriels repose alors sur les propriétés des applications h_m. Du fait que ce sont des endomorphismes du groupe V on déduit que l'application $x \mapsto r.x := h_n^{-1}\big(h_m(x)\big)$ l'est, d'où la distributivité à droite. De l'égalité $(a+b)x = ax + bx$, on déduit d'abord $h_{mn'+m'n} = h_{mn'} + h_{m'n}$, puis, avec les égalités $h_m \circ h_{n'} = h_{mn'}$ et $h_m \circ h_{n'} = h_{m'n}$, que $h_{r+r'} = h_r + h_{r'}$: c'est la distributivité à gauche. La relation $r'.(r.x) = (r'r).x$ vient de l'égalité $h_{r'r} = h_{r'} \circ h_r$ qui découle de l'égalité valable dans tout groupe : $m'(mx) = (m'm)x$ (et de la définition $h_r = h_n^{-1} \circ h_m$). Enfin, l'égalité $1.x = x$ est évidente avec notre définition de la loi externe.

II.3.4 Rappelons que l'addition sur $\mathcal{P}(E)$ est la différence symétrique $\oplus$ et que la loi externe y est définie par $0.A = \varnothing$ et $1.A = A$. Si $A, B \in \mathcal{P}(F)$, alors $A \oplus B$, $0.A$ et $1.A$ sont des sous-ensembles de F. Comme $\mathcal{P}(F)$ contient $\varnothing$, c'est bien un sous–espace vectoriel de $\mathcal{P}(E)$.
Une combinaison linéaire triviale est toujours nulle (ici, elle vaut donc $\varnothing$). Une combinaison

linéaire non triviale s'écrit $\lambda_1 x_1 + \cdots + \lambda_k x_k$, les λ_i étant non nuls : ici, ils valent donc 1 et la combinaison linéaire s'écrit $x_1 + \cdots + x_k$. On peut commencer par éliminer les répétitions (chaque fois que $x_i = x_j$, on a ici $x_i + x_j = 0$ car $A \oplus A = \varnothing$). Supposons donc que les x_i sont des singletons $\{a_i\}$ deux à deux distincts. Alors $x_1 + \cdots + x_k$ est l'ensemble $\{a_1, \ldots, a_k\}$. On conclut que le sous-espace vectoriel de $\mathcal{P}(E)$ engendré par les singletons est l'ensemble $\mathcal{P}_f(E)$ des parties finies de E.

II.3.5 On a $x + x = 1.x + 1.x = (1+1).x = 0.x = 0$, car, dans le groupe $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, on a l'égalité $1 + 1 = 0$.
Soit V un groupe (noté additivement) tel que, pour tout $x \in V$, on ait $x + x = 0$. Alors, pour tous $x, y \in V$:

$$x+y+x+y = 0 \quad \text{et} \quad x+x+y+y = 0+0 = 0 \Rightarrow x+y+x+y = x+x+y+y \Rightarrow y+x = x+y,$$

et le groupe est bien commutatif.
Si l'on pose maintenant $0.x = 0$ et $1.x = 1$ (on n'a pas le choix), on vérifie, exactement comme dans le cas de la structure de $\mathbb{F}_2$-espace vectoriel sur $\mathcal{P}(E)$, que les axiomes des espaces vectoriels sont valides.

II.3.6 On sait *a priori* que tout sous–espace vectoriel non trivial de V est au moins dénombrable, car il contient une droite vectorielle. Si A est fini de cardinal $n \neq 0$, notons le $A = \{a_1, \cdots, a_n\}$. L'application de $\mathbb{Q}^n$ dans V qui, à $(\lambda_1, \ldots, \lambda_n) \in \mathbb{Q}^n$ associe $\sum_{i=1}^{n} \lambda_i a_i \in V$, a par définition pour image $\mathrm{Vect}_{\mathbb{Q}}(A)$, qui est donc dénombrable (puisque $\mathbb{Q}^n$ l'est). Si A est dénombrable, on peut l'énumérer : $A = \{a_1, \cdots, a_n, \cdots\}$. Notons alors $A_n := \{a_1, \cdots, a_n\}$. On vérifie facilement que $\mathrm{Vect}_{\mathbb{Q}}(A) = \bigcup_{n \geqslant 1} \mathrm{Vect}_{\mathbb{Q}}(A_n)$: c'est une union dénombrable d'ensembles dénombrables, donc un ensemble dénombrable.
Si le $\mathbb{Q}$-espace vectoriel $\mathbb{R}$ était engendré par une partie dénombrable, il serait donc dénombrable, d'où la conclusion demandée. On peut en fait démontrer que toute base de $\mathbb{R}$ sur $\mathbb{Q}$ a la puissance du continu.

II.3.7 Il est évident que, pour $\lambda, \mu \in \mathbb{Q}$ et $x, y \in \mathbb{R}$, on a la relation :

$$\sqrt{2}(\lambda x + \mu y) = \lambda(\sqrt{2}x) + \mu(\sqrt{2}y),$$

qui prouve que l'application de l'énoncé est bien linéaire, donc un endomorphisme. Pour qu'elle soit une homothétie, il faudrait que l'on puisse écrire $\sqrt{2}x = \alpha x$ *pour un scalaire rationnel* $\alpha \in \mathbb{Q}$, ce qui n'est pas le cas. Contrairement aux apparences, cette application n'est pas une homothétie du $\mathbb{Q}$-espace vectoriel $\mathbb{R}$. En revanche, c'est bien une homothétie du $\mathbb{R}$-espace vectoriel $\mathbb{R}$.

II.3.8 Pour tout morphisme de groupes, on a $f(mx) = mf(x)$ pour $m \in \mathbb{Z}$. De plus, on a vu dans l'exercice II.3.2 que $m.x = mx$. On peut alors calculer :

$$nf(x) = f(nx) = f\big((m(n/m))\,x\big) = mf\big((n/m)x\big),$$

d'où $f\big((n/m)x\big) = (n/m)f(x)$, et f est bien $\mathbb{Q}$-linéaire.

II.3.9 (i) Notons $D = \mathrm{Vect}(x_0)$, qui est un supplémentaire de H. Les formes linéaires f et g coïncident sur H et sur D, donc sur $H + D = V$. Elles sont donc égales.
(ii) Puisque f et g sont non nulles, $f(x_0)$ et $g(x_0)$ sont des scalaires non nuls. On a donc $\lambda := \dfrac{f(x_0)}{g(x_0)} \in K^*$. Les formes linéaires f et $h : x \mapsto \lambda g(x)$ ont même noyau H et vérifient $f(x_0) = h(x_0)$, donc sont égales. On a donc égalité entre la forme f et la forme $x \mapsto \lambda g(x)$ (qui sera notée λg à la section 2.4). *Si deux formes linéaires ont même noyau, elles sont proportionnelles.* (Cette affirmation reste évidemment vraie si l'une des deux formes est nulle.)

II.3.10 (i) De l'égalité $(\lambda P + \mu Q)(a) = \lambda P(a) + \mu Q(a)$, on déduit que $P \mapsto P(a)$ est bien une forme K-linéaire sur $K[X]$; cette forme est non nulle puisque $1 \mapsto 1$. Son noyau est l'hyperplan H formé des polynômes P tels que $P(a) = 0$ (c'est donc l'idéal $(X - a)K[X]$, voir le module II.6). De l'égalité $(\lambda P + \mu Q) - (\lambda P + \mu Q)(a) = \lambda\big(P - P(a)\big) + \mu\big(Q - Q(a)\big)$, on déduit que l'application $P \mapsto P - P(a)$ est linéaire. Son image est incluse dans H, puisque tout polynôme de la forme $P - P(a)$ s'annule en a. Sa restriction à H est l'identité, puisque $P - P(a) = P$ pour $P \in H$. Selon la section 2.3, c'est bien un projecteur d'image H.
(ii) On sait (module II.6) que la dérivation sur $K[X]$ est K-linéaire ; c'est donc un endomorphisme de $K[X]$. Puisque l'on a supposé que K est de caractéristique nulle, on a les équivalences (on note $P = \sum\limits_{k\geqslant 0} a_k X^k$) :

$$P' = 0 \Longleftrightarrow \sum_{k>0} k a_k X^{k-1} = 0 \Longleftrightarrow \forall k > 0\ ,\ k a_k = 0 \Longleftrightarrow \forall k > 0\ ,\ a_k = 0 \Longleftrightarrow P = a_0.$$

(Naturellement, pour un corps de caractéristique non nulle, l'équivalence utilisée $k a_k = 0 \Leftrightarrow a_k = 0$ serait en défaut.) On voit donc que $\mathrm{Ker}\, D$ est formé des polynômes constants. Toujours parce que a supposé que K est de caractéristique nulle, le polynôme $P = \sum\limits_{k\geqslant 0} a_k X^k$ admet pour antécédent le polynôme $\sum\limits_{k=0}^{n} \dfrac{a_k}{k+1} X^{k+1}$ et D est surjective : $\mathrm{Im}\, D = K[X]$.
(iii) Le lecteur vérifiera sans peine que $I(\lambda P + \mu Q) = \lambda I(P) + \mu I(Q)$; l'application I est donc K-linéaire, et c'est bien un endomorphisme de $K[X]$. On a les implications (avec les mêmes notations) :

$$I(P) = 0 \Longrightarrow \forall k \geqslant 0\ ,\ \frac{a_k}{k+1} = 0 \Longrightarrow \forall k \geqslant 0\ ,\ a_k = 0 \Longleftrightarrow P = 0,$$

de sorte que I est injective : $\mathrm{Ker}\, I = \{0\}$. Comme les images des éléments X^k de la base canonique sont les $\dfrac{1}{k+1} X^{k+1}$, on voit que $\mathrm{Im}\, I$ est le sous–espace vectoriel de $K[X]$ engendré par les X^{k+1} (c'est donc l'idéal $XK[X]$, voir le module II.6) ; en particulier, I n'est pas surjective.
Pour déterminer $I \circ D$ et $D \circ I$, on examine leur effet sur la base canonique :

$$\begin{aligned} (I \circ D)(X^k) &= \begin{cases} 0 \text{ si } k = 0 \\ I\big(k X^{k-1}\big) = X^k \text{ si } k > 0 \end{cases} \\ (D \circ I)(X^k) &= D\Big(\frac{1}{k+1} X^{k+1}\Big) = X^k. \end{aligned}$$

Ainsi, $I \circ D$ est l'application linéaire $P \mapsto P - P(0)$ et $D \circ I = \mathrm{Id}_{K[X]}$.

II.3.11 (i) On a :

$$(\mathrm{Id}_V - p)^2 = \mathrm{Id}_V^2 - 2p\,\mathrm{Id}_V + p^2 = \mathrm{Id}_V - 2p + p = \mathrm{Id}_V - p,$$

car $p^2 = p$. L'endomorphisme q est donc bien un projecteur.

(ii) On a $s = p - q = p - (\mathrm{Id}_V - p) = 2p - \mathrm{Id}_V$. On en tire :

$$s^2 = 4p^2 - 4p\,\mathrm{Id}_V + \mathrm{Id}_V^2 = 4p - 4p + \mathrm{Id}_V = \mathrm{Id}_V\,.$$

L'endomorphisme s est donc involutif.

(iii) Supposons $s^2 = \mathrm{Id}_V$. Puisque le corps K n'est pas de caractéristique 2, l'égalité $s = 2p - \mathrm{Id}_V$ équivaut à $p = \dfrac{1}{2}\,\mathrm{Id}_V + \dfrac{1}{2}s$. On a alors :

$$p^2 = \frac{1}{4}\,\mathrm{Id}_V^2 + \frac{2}{4}\,\mathrm{Id}_V\, s + \frac{1}{4}s^2 = \frac{1}{4}\,\mathrm{Id}_V + \frac{1}{2}s + \frac{1}{4}\,\mathrm{Id}_V = \frac{1}{2}\,\mathrm{Id}_V + \frac{1}{2}s = p,$$

et p est bien un projecteur.

II.3.12 Il est clair que D et I sont linéaires (règles de base du calcul des dérivées et des primitives). De plus, si f est de classe $\mathcal{C}^\infty$, sa dérivée et ses primitives le sont aussi. On a donc bien $D, I \in \mathcal{L}(V)$. La dérivée de la fonction $x \mapsto \displaystyle\int_0^x f(t)\,\mathrm{d}t$ est f, donc $DI = Id_V$. Enfin, notant (très classiquement) $f' = D(f)$, on calcule $I(f')$: c'est la fonction $x \mapsto \displaystyle\int_0^x f'(t)\,\mathrm{d}t = f(x) - f(0)$. On en déduit que ID est l'endomorphisme $f \mapsto f - f(0)$ de V. Ce n'est pas l'identité (par exemple, toute fonction constante est dans son noyau). Si I ou D était inversible, la relation $DI = Id_V$ entraînerait qu'ils sont inverses l'un de l'autre et donc que $ID = Id_V$. On en conclut que $D, I \notin GL(V)$. Les applications étudiées ici ont des propriétés très voisines de celles étudiées dans l'exercice II.3.10.

II.3.13 La bijectivité découle du théorème 2 de la page 24 (module I.1). L'application réciproque de V dans $\mathbb{F}_2^n$ associe à $A \subset E$ le n-uplet $\big(\chi_A(1), \ldots, \chi_A(n)\big)$. Ce sont des isomorphismes de groupes à cause des conséquences des tables de multiplication 3 de la page 28 énumérées à la fin de la section 4 du même module. Reste à vérifier la propriété $\chi(\lambda x) = \lambda\chi(x)$, ce qui est immédiat en distinguant les deux cas possibles : $\lambda = 0$ et $\lambda = 1$.

Si $\lambda \in \mathbb{F}_2^{(E)}$, il est naturel de poser $\chi(\lambda) := \lambda^{-1}(1)$. Avec cette définition plus générale (qui entraîne les mêmes propriétés), on constate que l'image dans $V = \mathcal{P}(E)$ du sous-espace $\mathbb{F}_2^{(E)}$ est l'ensemble $\mathcal{P}_f(E)$ des parties finies de E.

II.3.14 On a les équivalences :

$$\begin{aligned} f' \circ f = 0 &\iff \forall x \in V\ ,\ f'\big(f(x)\big) = 0 \\ &\iff \forall x \in V\ ,\ f(x) \in \mathrm{Ker}\, f' \\ &\iff f(V) \subset \mathrm{Ker}\, f' \\ &\iff \mathrm{Im}\, f \subset \mathrm{Ker}\, f', \end{aligned}$$

d'où la première affirmation. On a les égalités :

$$\mathrm{Im}(f' \circ f) = \{f'\big(f(x)\big) \mid x \in V\} = \{f'(y) \mid y \in \mathrm{Im}\, f\} = f'(\mathrm{Im}\, f),$$

d'où la deuxième affirmation. On a enfin les équivalences :

$$x \in \mathrm{Ker}(f' \circ f) \iff f'\big(f(x)\big) = 0 \iff f(x) \in \mathrm{Ker}\, f' \iff x \in f^{-1}(\mathrm{Ker}\, f'),$$

d'où la troisième et dernière affirmation.

II.3.15 (i) On a les équivalences :

$$\begin{aligned} x \in f^{-1}\left(\bigcap_{i\in I} W_i'\right) &\iff f(x) \in \bigcap_{i\in I} W_i' \\ &\iff \forall i \in I\ ,\ f(x) \in W_i' \\ &\iff \forall i \in I\ ,\ x \in f^{-1}(W_i') \\ &\iff \bigcap_{i\in I} f^{-1}(W_i'), \end{aligned}$$

d'où l'égalité.

(ii) Soit $i \in [\![1,p]\!]$: alors $W_i \subset W_1 + \cdots + W_p$, d'où $f(W_i) \subset f\left(W_1 + \cdots + W_p\right)$. Puisque c'est vrai pour tout i, on a $f(W_1) + \cdots + f(W_p) \subset f\left(W_1 + \cdots + W_p\right)$.

Réciproquement, tout élément y de $f\left(W_1 + \cdots + W_p\right)$ s'écrit :

$$f(x_1 + \cdots + x_p) \quad \text{où} \quad x_1 \in W_1, \ldots, x_p \in W_p.$$

On a donc par linéarité $y = f(x_1) + \cdots + f(x_p) \in f(W_1) + \cdots + f(W_p)$, d'où $f\left(W_1 + \cdots + W_p\right) \subset f(W_1) + \cdots + f(W_p)$.

On conclut bien que $f\left(W_1 + \cdots + W_p\right) = f(W_1) + \cdots + f(W_p)$.

(iii) Soit $i \in [\![1,p]\!]$: alors $W_i' \subset W_1' + \cdots + W_p'$, d'où $f^{-1}(W_i') \subset f^{-1}\left(W_1' + \cdots + W_p'\right)$. Puisque c'est vrai pour tout i, on a $f^{-1}(W_1') + \cdots + f^{-1}(W_p') \subset f^{-1}\left(W_1' + \cdots + W_p'\right)$, et cela, sans invoquer la surjectivité de f. Soit maintenant $x \in f^{-1}\left(W_1' + \cdots + W_p'\right)$. Alors on peut écrire $f(x) = y_1 + \cdots + y_p$, avec $y_1 \in W_1', \ldots, y_p \in W_p'$. Puisque l'on a supposé f surjective, il existe $x_1 \in f^{-1}(W_1'), \ldots, x_p f^{-1}(W_p')$ tels que $y_1 = f(x_1), \ldots, y_p = f(x_p)$. De l'égalité $f(x) = f(x_1) + \cdots + f(x_p)$, on tire $x = x_1 + \cdots + x_p + k$, où $k \in \mathrm{Ker}\, f$. On réécrit cette égalité sous la forme $x = x_1 + \cdots + x_{p-1} + (x_p + k)$. Comme $f(x_i) = y_i \in W_i'$, on a $x_i \in f^{-1}(W_i')$ pour $i \in [\![1, p-1]\!]$. Comme $f(x_p + k) = f(x_p) + f(k) = y_p + 0 \in W_p'$, on a $x_p + k \in f^{-1}(W_p')$. Ainsi, $x = x_1 + \cdots + x_p + k \in f^{-1}(W_1') + \cdots + f^{-1}(W_p')$, d'où $f^{-1}\left(W_1' + \cdots + W_p'\right) \subset f^{-1}(W_1') + \cdots + f^{-1}(W_p')$, d'où finalement :

$$f^{-1}\left(W_1' + \cdots + W_p'\right) = f^{-1}(W_1') + \cdots + f^{-1}(W_p').$$

Les droites D_1' et D_2' étant distinctes, $D_1' + D_2' = \mathbb{R}^2$, d'où :

$$p^{-1}(D_1' + D_2') = p^{-1}(\mathbb{R}^2) = \mathbb{R}^2.$$

Par ailleurs, ces droites n'étant pas horizontales, on ne peut avoir $(x,0) \in D_1'$ ou $(x,0) \in D_2'$ que si $x = 0$. On a donc $p^{-1}(D_1') = p^{-1}(D_2') = \{0\} \times \mathbb{R}$, d'où

$p^{-1}(D_1') + p^{-1}(D_2') = \{0\} \times \mathbb{R}$. La surjectivité était donc une hypothèse justifiée dans la première partie de cette question.

(iv) Fixons $j \in I$. Alors $\bigcap_{i\in I} W_i \subset W_j$, d'où $f\left(\bigcap_{i\in I} W_i\right) \subset f(W_j)$. Comme c'est vrai pour tout j, on a $f\left(\bigcap_{i\in I} W_i\right) \subset \bigcap_{i\in I} f(W_i)$, et cela, sans invoquer l'injectivité de f. Soit maintenant $y \in \bigcap_{i\in I} f(W_i)$. Pour tout i, on a $y \in f(W_i)$, et l'on peut écrire $y = f(x_i)$ avec $x_i \in W_i$. Puisque tous les x_i ont même image et que l'on a supposé f injective, ils sont tous égaux. Soit x cet élément : il appartient à tous les W_i, donc $x \in \bigcap_{i\in I} W_i$, donc $y \in f\left(\bigcap_{i\in I} W_i\right)$. On a donc $\bigcap_{i\in I} f(W_i) \subset f\left(\bigcap_{i\in I} W_i\right)$, et finalement $f\left(\bigcap_{i\in I} W_i\right) = \bigcap_{i\in I} f(W_i)$.
Les droites D_1 et D_2 étant distinctes, $D_1 \cap D_2 = \{0\}$, d'où $p(D_1 \cap D_2) = \{0\}$. Les droites D_1 et D_2 n'étant pas verticales, $p(D_1) = p(D_2) = \mathbb{R}\times\{0\}$, d'où $p(D_1)\cap p(D_2) = \mathbb{R}\times\{0\}$. L'injectivité était donc une hypothèse justifiée dans la première partie de cette question.

II.3.16 Tout $x \in V$ s'écrit d'une manière au moins comme combinaison linéaire $x = \sum_{i\in I} \lambda_i x_i$.

On en déduit :

$$f(x) = f\left(\sum_{i\in I} \lambda_i x_i\right) = \sum_{i\in I} \lambda_i f(x_i) = \sum_{i\in I} \lambda_i g(x_i) = g\left(\sum_{i\in I} \lambda_i x_i\right) = g(x),$$

le troisième signe d'égalité étant justifié par l'hypothèse $\forall i \in I\ ,\ f(x_i) = g(x_i)$. On a donc bien $f = g$.

II.3.17 Nous démontrerons l'indépendance linéaire des f_a par l'absurde. Supposons que les f_a ne sont pas linéairement indépendants. Il existe donc des réels deux à deux distincts $a_1, \dots, a_k$ et des réels non nuls $\lambda_1, \dots, \lambda_k$ tels que :

$$\lambda_1 f_{a_1} + \cdots + \lambda_k f_{a_k} = 0. \tag{32}$$

On peut de plus choisir une telle relation linéaire de longueur minimale, *i.e.* telle que k est le plus petit possible. Nous allons fabriquer une relation plus courte, ce qui donnera une contradiction. Remarquons d'abord que, puisque les fonctions f_a sont non nulles, on a $k \geqslant 2$. On sait que la dérivée de f_a est af_a. En dérivant la relation (32), on trouve donc :

$$\lambda_1 a_1 f_{a_1} + \cdots + \lambda_k a_k f_{a_k} = 0. \tag{33}$$

On multiplie (32) par a_k et l'on en soustrait (33), ce qui donne :

$$\lambda_1(a_1 - a_k) f_{a_1} + \cdots + \lambda_{k-1}(a_{k-1} - a_k) f_{a_k} = 0. \tag{34}$$

Comme par hypothèse les $\lambda_i(a_i - a_k)$ sont non nuls pour $i \in [\![1, k-1]\!]$, la relation linéaire (34) est du même type que (32), mais strictement plus courte, contredisant l'hypothèse.

II.3.18 (i) Supposons les suites $g^{(q)}$ $(q \in \mathbb{R})$ liées. Il existe alors des réels deux à deux distincts $q_1 < \cdots < q_k$ et des réels non nuls $a_1, \dots, a_k$ tels que $a_1 g^{(q_1)} + \cdots + a_k g^{(q_k)} = 0$, c'est-à-dire $\forall n \in \mathbb{N}\ ,\ u_n := a_1 q_1^n + \cdots + a_k q_k^n = 0$. On sait que le comportement pour $n \to +\infty$

d'une suite géométrique $g^{(q)}$ de raison q dépend essentiellement du module $|q|$. La raison q_i de plus grand module est soit q_1, soit q_k, soit les deux. On est donc conduit à distinguer trois cas :
Si $\forall i \neq k\ ,\ |q_i| < |q_k|$, lorsque $n \to +\infty$ on a $u_n \sim a_k q_k^n$ ce qui contredit la nullité de u_n.
Si $\forall i \neq 1\ ,\ |q_i| < |q_1|$, lorsque $n \to +\infty$ on a $u_n \sim a_1 q_1^n$ ce qui contredit la nullité de u_n.
Si $\forall i \neq k \quad$ et $\quad \neq k\ ,\ |q_i| < |q_1| = |q_k|$, on a nécessairement $q_1 = -q_k$ et $q_1 < 0 < q_k$. Puisque a_1 et a_k sont non nuls, on a nécessairement soit $a_1 + a_k \neq 0$ soit $a_1 - a_k \neq 0$. Dans le premier cas, lorsque $n \to +\infty$ on a $u_{2n} \sim (a_1 + a_k) q_k^{2n}$; dans le second cas, lorsque $n \to +\infty$ on a $u_{2n+1} \sim (-a_1 + a_k) q_k^{2n+1}$; dans les deux cas, on a contredit la nullité de u_n.
Le lecteur devinera aisément que ce raisonnement déjà un peu compliqué se complique encore si l'on considère des suites géométriques sur $\mathbb{C}$: il peut alors y avoir beaucoup de q_i ayant même module et il devient difficile d'étudier le "terme dominant" de u_n. C'est pourquoi, dans le cas d'un corps quelconque, on utilisera une méthode analogue à celle de l'exercice précédent.
(ii) On suppose à nouveau les suites $g^{(q)}$ $(q \in K)$ liées. Il existe alors des scalaires (c'est-à-dire des éléments de K) deux à deux distincts $q_1, \dots, q_k$ et des scalaires non nuls $a_1, \dots, a_k$ tels que $a_1 g^{(q_1)} + \cdots + a_k g^{(q_k)} = 0$, c'est-à-dire $\forall n \in \mathbb{N}\ ,\ u_n := a_1 q_1^n + \cdots + a_k q_k^n = 0$. On peut de plus supposer que la relation linéaire ci-dessus est la plus courte possible, *i.e.* que k est minimal. On ne peut avoir $k = 1$ car aucune suite $g^{(q)}$ n'est nulle (même la suite $g^{(0)}$ prend les valeurs $1, 0, 0, \dots$ puisque, par convention, $0^0 = 1$). On a donc $k \geqslant 2$. Puisque la suite des u_n est identiquement nulle, celle des $u_{n+1} - q_k u_n$ l'est également ; mais cela s'écrit :

$$\forall n \in \mathbb{N}\ ,\ a_1(q_1 - q_k)q_1^n + \cdots + a_{k-1}(q_{k-1} - q_k)q_{k-1}^n = 0,$$

soit une relation linéaire non triviale strictement plus courte entre les $g^{(q)}$, contredisant la minimalité de k.
(iii) Si les $g^{(q,k)}$ sont liées, partent d'une relation linéaire non triviale $\sum a_{q,k} g^{(q,k)} = 0$, on regroupe les termes correspondant à une même valeur de q et l'on obtient une relation linéaire :

$$\forall n \in \mathbb{N}\ ,\ u_n := \sum_{i=1}^{k} P_i(n) q_i^n = 0, \tag{35}$$

dans laquelle $P_1, \dots, P_k$ sont des polynômes non nuls (à coefficients dans K), $q_1, \dots, q_k$ sont des scalaires deux à deux distincts et l'on a choisi k minimal. On calcule alors :

$$\forall n \in \mathbb{N}\ ,\ P_k(n)u_{n+1} - q_k P_k(n+1)u_n = \sum_{i=1}^{k} \big(q_i P_i(n+1)P_k(n) - q_k P_k(n+1)P_i(n)\big) q_i^n,$$

d'où une relation linéaire :

$$\forall n \in \mathbb{N}\ ,\ \sum_{i=1}^{k-1} Q_i(n) q_i^n = 0, \tag{36}$$

où $Q_i(X) = q_i P_i(X+1)P_k(X) - q_k P_k(X+1)P_i(X)$ est un polynôme non nul : son coefficient dominant (voir le module II.6, section 1.2) est en effet $\operatorname{cd}(Q_i) = (q_i - q_k)\operatorname{cd}(P_i)\operatorname{cd}(P_k)$. La relation (36) est strictement plus courte que la relation (35), ce qui contredit la minimalité de k.

II.3.19 Soient $\underline{u}$, $\underline{v}$ deux éléments de V et λ, μ deux scalaires. Notons $\underline{w} := \lambda\underline{u} + \mu\underline{v}$. Alors,

quel que soit $n \in \mathbb{N}$:

$$\begin{aligned} w_{n+p} &= \lambda u_{n+p} + \mu u_{n+p} \\ &= \lambda(a_1 u_{n+p-1} + \cdots + a_p u_n) + \mu(a_1 v_{n+p-1} + \cdots + a_p v_n) \\ &= a_1(\lambda u_{n+p-1} + \mu v_{n+p-1}) + \cdots + a_p(\lambda u_n + \mu v_n) \\ &= a_1 w_{n+p-1} + \cdots + a_p w_n, \end{aligned}$$

d'où l'on déduit que $\underline{w} \in V$. Ainsi, V est un sous–espace vectoriel de $K^{\mathbb{N}}$.
(ii) Le principe de définition d'une suite par récurrence à p pas entraîne que, $(u_0, \ldots, u_{p-1}) \in K^p$ étant donné, il existe une unique suite $\underline{u} \in K^{\mathbb{N}}$ telle que $\forall n \in \mathbb{N}\ ,\ u_{n+p} = a_1 u_{n+p-1} + \cdots + a_p u_n$. Cela signifie précisément que l'application indiquée est bijective. Par définition des opérations sur les suites, l'image de $\lambda\underline{u} + \mu\underline{v}$ est $(\lambda u_0 + \mu v_0, \ldots, \lambda u_{p-1} + \mu v_{p-1}) = \lambda(u_0, \ldots, u_{p-1}) + \mu(v_0, \ldots, v_{p-1})$, et cette application est linéaire. C'est donc un isomorphisme. Ainsi, l'espace vectoriel V est isomorphe à K^p ; il est donc de dimension p.

Remarque. On utilise ce résultat en combinaison avec celui de l'exercice précédent. Si l'on trouve p couples distincts $(q, k) \in K \times \mathbb{N}$ tels que $g^{(q,k)} \in V$, on sait qu'il forment une base de V (voir par exemple l'exercice II.5.6 de la page 276).

II.3.20 Bien que l'énoncé ne le dise pas explicitement, on a évidemment $\mathcal{B} = (x_i)_{i\in I}$.
Supposons f injective et montrons que la famille $f(\mathcal{B}) = (f(x_i))_{i\in I}$ de V' est libre. Si $\sum_{i\in I} \lambda_i f(x_i) = 0$ est une relation linéaire entre les éléments de cette famille, on en tire, par linéarité, $f\big(\sum_{i\in I} \lambda_i x_i\big) = 0$, d'où, f étant injective, $\sum_{i\in I} \lambda_i x_i = 0$, d'où, $\mathcal{B}$ étant libre, $\forall i \in I\ ,\ \lambda_i = 0$. La famille $f(\mathcal{B})$ est donc bien libre. Supposons réciproquement que la famille $f(\mathcal{B})$ est libre et montrons que f est injective. Soit $x \in V$ tel que $f(x) = 0$. On écrit x dans la base $\mathcal{B}$: $x = \sum_{i\in I} \lambda_i x_i$. On a donc $0 = f(x) = \sum_{i\in I} \lambda_i f(x_i)$. La famille $f(\mathcal{B})$ étant libre, on en déduit $\forall i \in I\ ,\ \lambda_i = 0$, donc $x = 0$, et f est bien injective.
Supposons f surjective et montrons que $f(\mathcal{B})$ est génératrice. Soit $y \in V'$. Alors $y = f(x)$ (surjectivité de f) et $x = \sum_{i\in I} \lambda_i x_i$ ($\mathcal{B}$ est une base), donc $y = \sum_{i\in I} \lambda_i f(x_i)$, une combinaison linéaire des éléments de $f(\mathcal{B})$ qui est donc bien génératrice. Supposons réciproquement que $f(\mathcal{B})$ est génératrice et montrons que f est surjective. Soit $y \in V'$. On l'écrit comme combinaison linéaire des éléments de la famille génératrice $f(\mathcal{B})$: $y = \sum_{i\in I} \lambda_i f(x_i)$, d'où, par linéarité, $y = f\left(\sum_{i\in I} \lambda_i x_i\right) \in \operatorname{Im} f$, et f est bien surjective.
La dernière équivalence découle des deux précédentes :

$$\begin{aligned} f(\mathcal{B}) \text{ est une base} &\iff f(\mathcal{B}) \text{ est libre et génératrice} \\ &\iff f \text{ est injective et surjective} \\ &\iff f \text{ est bijective .} \end{aligned}$$

II.3.21 Soient $\underline{x}_1, \ldots, \underline{x}_n$ des éléments de $K^{(I)}$; nous allons démontrer qu'ils n'engendrent pas $K^{(I)}$ (et celui-ci n'admet donc pas de système générateur fini). Pour cela, nous noterons $\underline{x}_k = (x_i^{(k)})_{i\in I}$ pour $k \in [\![1, n]\!]$.

Rappelons que le *support* d'un élément $\underline{x} := (x_i)_{i\in I}$ de $K^{(I)}$ est l'ensemble $A := \{i \in I \mid x_i \neq 0\}$. Ce support peut être vide (dans le cas de la famille identiquement nulle), mais surtout, par définition de $K^{(I)}$ (section 1.3), c'est un ensemble fini. On vérifie de plus aisément les deux propriétés suivantes :

- Le support de $\lambda\underline{x}$ est égal au support de $\underline{x}$, sauf dans le cas particulier où $\lambda = 0$ (et le support de $\lambda\underline{x}$ est alors vide).
- Notons A le support de $\underline{x}$ et B celui de $\underline{y}$. Le support de $\underline{x} + \underline{y}$ est inclus dans la réunion $A \cup B$: en effet, $x_i + y_i \neq 0$ implique $x_i \neq 0$ ou $y_i \neq 0$, c'est-à-dire $i \in A$ ou $i \in B$.

Notons donc $A_1, \ldots, A_n$ les supports respectifs de $\underline{x}_1, \ldots, \underline{x}_n$. En vertu des deux règles ci-dessus, le support de toute combinaison linéaire des $\underline{x}_k$ est inclus dans l'ensemble fini $A := A_1 \cup \cdots \cup A_n$. Soit $i \in I \setminus A$ (il en existe puisque A est fini et I infini). L'élément $\delta^{(i)}$ de K^I (dont la composante d'indice i vaut 1 et dont toutes les autres composantes valent 0, voir 1.3) a pour support $\{i\}$, qui n'est pas inclus dans A. Ce n'est donc pas une combinaison linéaire des $\underline{x}_k$ et la famille $(\underline{x}_1, \ldots, \underline{x}_n)$ n'est donc pas génératrice.

II.3.22 Observons tout d'abord qu'une famille $(\lambda_{i,j})_{i\in I, j\in J}$ de $K^{I\times J}$ est à support fini si, et seulement si,, quel que soit $i \in I$, la famille $L_j := (\lambda_{i,j})_{i\in I}$ de K^I est à support fini et la famille $(L_j)_{j\in J}$ d'éléments de $K^{(I)}$, indexée par J, est à support fini. Cette remarque justifie les écritures de combinaisons linéaires indexées par I, J et $I \times J$ qui vont suivre : rappelons en effet qu'une combinaison linéaire n'a de sens que si la famille de scalaires qui y apparaît est à support fini.

Montrons que la famille des $x_i y_j$ est libre sur K. Soit $\sum\limits_{i\in I, j\in J} \lambda_{i,j} x_i y_j = 0$ une relation linéaire dans cette famille, où les scalaires $\lambda_{i,j}$ forment une famille à support fini dans $K^{I\times J}$. D'après la remarque qui précède, on peut alors écrire une relation linéaire $\sum\limits_{j\in J} \mu_j y_j = 0$, où, pour $j \in J$, on a noté $\mu_j := \sum\limits_{i\in I} \lambda_{i,j} x_i$. C'est un élément bien défini de L et l'on a donc une relation linéaire entre les y_j à coefficients $\mu_j \in L$. Comme, par hypothèse, les y_j sont linéairement indépendants sur L, on en tire $\forall j \in J\ ,\ \mu_j = 0$, c'est-à-dire $\sum\limits_{i\in I} \lambda_{i,j} x_i = 0$. Comme, par hypothèse, les x_i sont linéairement indépendants sur K, on en tire $\forall j \in J\ ,\ \forall i \in I\ ,\ \lambda_{i,j} = 0$. La famille des $x_i y_j$ est donc bien libre sur K.

Montrons maintenant que la famille des $x_i y_j$ de M est K-génératrice. Tout élément $z \in M$ s'écrit $z = \sum\limits_{j\in J} \mu_j y_j$, où $\forall j \in J\ ,\ \mu_j \in L$, et chacun des $\mu_j \in L$ s'écrit $\mu_j = \sum\limits_{i\in I} \lambda_{i,j} x_i$, où $\forall i \in I\ ,\ \lambda_{i,j} \in K$. On en tire l'écriture $z = \sum\limits_{i\in I, j\in J} \lambda_{i,j} x_i y_j$, ce qui achève la démonstration.

II.3.23 (i) Soient $x_1, \ldots, x_p$ des éléments deux à deux distincts de $\bigcup\limits_{i\in I} B_i$. Il existe donc $i_1, \ldots, i_p \in I$ tels que $x_k \in B_{i_k}$ pour $k \in [\![1, p]\!]$. Les B_i étant comparables pour l'inclusion, il existe $i \in \{i_1, \ldots, i_p\}$ tel que les B_{i_k} sont tous inclus dans B_i. Les x_k sont donc tous

éléments de B_i. Comme ils sont deux à deux distincts et que B_i est une partie libre de V, les x_k sont linéairement indépendants. On a donc prouvé que $\bigcup_{i\in I} B_i$ est une partie libre de V.

(ii) Une chaîne de E est une famille $\mathcal{C} = (B_i)_{i\in I}$ de parties libres de V deux à deux comparables pour l'inclusion et telles que $A \subset B_i \subset C$ quel que soit $i \in I$. L'ensemble $B := \bigcup_{i\in I} B_i$ est alors une partie libre de V d'après la question précédente, et l'on a évidemment $A \subset B \subset C$. C'est donc un majorant de $\mathcal{C}$ dans E. L'ensemble ordonné E est donc inductif.

L'ensemble E est de plus non vide, car la famille réduite à A en est élément. D'après le lemme de Zorn (module I.1, section 6), il admet un élément maximal, c'est-à-dire une partie libre maximale B telle que $A \subset B \subset C$, ce qui démontre le lemme 29.

II.3.24 Remarquons qu'en vertu du théorème 30 de la page 193, il existe des bases de Hamel ! Selon l'exercice II.3.21, tout $\mathbb{Q}$-espace vectoriel admettant une famille génératrice dénombrable est lui-même dénombrable (et c'est *a fortiori* le cas s'il admet une famille génératrice finie). Comme $\mathbb{R}$ n'est pas dénombrable (module I.1, section 6), par contraposition, il n'admet donc pas de famille génératrice dénombrable ; en particulier, une base de Hamel ne peut être finie ou dénombrable.

Soit $\mathcal{B}$ une base de Hamel et soit e un élément de cette base. Parmi les formes linéaires coordonnées relatives à la base $\mathcal{B}$ (module II.3, section 3.3), notons π celle relative à e. On sait que l'application $x \mapsto \pi(x)e$ est une projection sur la droite vectorielle $\mathrm{Vect}(e)$. C'est donc un endomorphisme non nul et non bijectif du $\mathbb{Q}$-espace vectoriel $\mathbb{R}$, en particulier, c'est bien un morphisme de groupe non trivial $\mathbb{R} \to \mathbb{R}$ qui n'est pas bijectif.

Nous allons démontrer que tout morphisme de groupe $\mathbb{R} \to \mathbb{R}$ qui est continu est nul ou bijectif. Il en découlera que l'endomorphisme ci-dessus n'est pas continu. Soit donc $f : \mathbb{R} \to \mathbb{R}$ un morphisme de groupe qui est une application continue. D'après l'exercice II.3.8, f est $\mathbb{Q}$-linéaire, et l'on a donc, pour tout rationnel r, $f(r) = rf(1)$. Soit x un réel quelconque. Il est limite d'une suite $(r_n)_{n\in\mathbb{N}}$ de rationnels (module IV.1). Par continuité de f (module IV.2), on a les égalités :

$$f(x) = \lim_{n\to+\infty} f(r_n) = \lim_{n\to+\infty} r_n f(1) = xf(1).$$

Ainsi, f est l'application $x \mapsto \lambda x$, où $\lambda = f(1)$. En particulier, f est nulle si $\lambda = 0$ et bijective si $\lambda \neq 0$.

Notons $\aleph$ le cardinal de la base $\mathcal{B}$. Soient I et J deux ensembles disjoints équipotents à $\mathcal{B}$. On a donc des isomorphismes de $\mathbb{Q}$-espace vectoriels de $\mathbb{R}$ avec $\mathbb{Q}^{(I)}$ et avec $\mathbb{Q}^{(J)}$. Par ailleurs, on a prouvé, dans l'exercice V, l'égalité $\aleph + \aleph = \aleph$. Cela signifie qu'il existe une bijection de $I \cup J$ sur $\mathcal{B}$, donc un isomorphisme de $\mathbb{Q}^{(I\cup J)}$ sur $\mathbb{R}$, donc un isomorphisme de $\mathbb{Q}^{(I)} \times \mathbb{Q}^{(J)}$ sur $\mathbb{R}$, donc un isomorphisme de $\mathbb{R} \times \mathbb{R}$ sur $\mathbb{R}$. Il s'agit d'un isomorphisme de $\mathbb{Q}$-espace vectoriels, donc en particulier d'un isomorphisme de groupes !

> ***Remarque***. Ce raisonnement peut sembler étrange, mais le détour par les $\mathbb{Q}$-espace vectoriels est la méthode la plus simple pour démontrer que les groupes $\mathbb{R} \times \mathbb{R}$ et $\mathbb{R}$ sont isomorphes.

II.3.25 Ces droites étant distinctes, on a $D \cap D' = D \cap D'' = D' \cap D'' = \{0\}$ et $D + D' = D + D'' = D' + D'' = \mathbb{R}^2$. Pour tout $x \in V$, on a donc des écritures

$x = u + u' = v + v'' = w' + w''$ avec $u, v \in D$, $u', w' \in D'$ et $v'', w'' \in D''$. On peut également écrire : $x = u + u' + 0 = v + 0 + v'' = 0 + w' + w''$, ce qui donne trois écritures de la forme $x = y + y' + y''$ avec $y \in D$, $y' \in D'$ et $y'' \in D''$. En général, x n'appartient à aucune des droites D, D', D'', donc aucun des vecteurs u, u', v, v'', w', w'' n'est nul. Les trois écritures mentionnées sont donc distinctes. Il n'y a donc pas unicité de l'écriture $x = y + y' + y''$ avec $y \in D$, $y' \in D'$ et $y'' \in D''$, et l'on ne peut parler de somme directe $D \oplus D' \oplus D''$. Un critère correct permettant de reconnaître les sommes directes de plusieurs sous–espace vectoriels sera donné dans le cours de L2.

II.3.26 Soit W un sous–espace vectoriel de V distinct de $\{0\}$ et de V. Remarquons que l'hypothèse que le corps de base K est infini entraîne que W est infini. Soit $x \in V \setminus W$. Pour tout $w \in W$, on a $x + w \notin W$ et il existe donc au moins un supplémentaire de W qui contient $x+w$; cela découle de la démonstration du théorème 35 de la page 196, mais on peut également le déduire de la conclusion de ce théorème : si W'' est un supplémentaire de $W + \mathrm{Vect}(x+w)$, alors $W' := W'' + \mathrm{Vect}(x + w)$ est un supplémentaire de W qui contient $x + w$.
Notons donc W'_w un tel supplémentaire. L'application $w \mapsto W'_w$ est injective. en effet, si $W'_{w_1} = W'_{w_1} = W'$, alors $x + w_1, x + w_2 \in W'$, d'où $w_1 - w_2 \in W' \cap W = \{0\}$. Il y a donc au moins autant de supplémentaires de W que d'éléments de W, donc une infinité.

II.3.27 Il s'agit, bien sûr, dans tout l'exercice, d'applications *linéaires* !
(i) Si f est injective, elle induit un isomorphisme f_1 de V sur $W' := \mathrm{Im}\, f$. Soit p un projecteur de V' sur W'. Alors $g := f_1^{-1} \circ p : V' \to V$ est linéaire et vérifie $g \circ f = f_1^{-1} \circ p \circ f = f_1^{-1} \circ f_1 = \mathrm{Id}_V$ car $p \circ f = f_1$. Réciproquement, si $g \circ f = \mathrm{Id}_V$, tout $x \in \mathrm{Ker}\, f$ vérifie $x = g\big(f(x)\big) = g(0) = 0$, et f est bien injective.
(ii) Supposons f surjective et soit W un supplémentaire de $\mathrm{Ker}\, f$ dans V. La restriction f_W est un isomorphisme de W sur V' (théorème 36 de la page 196). Soit $h : V' \to W$ sa réciproque : il est clair que $f \circ h = \mathrm{Id}_{V'}$. Réciproquement, si $f \circ h = \mathrm{Id}_{V'}$, tout $y \in V'$ est l'image de $h(y) \in V$ et f est bien surjective.
(iii) Si f est bijective et si f^{-1} est son application réciproque , on a les implications :

$$g \circ f = \mathrm{Id}_V \Longrightarrow g \circ f \circ f^{-1} = f^{-1} \Longrightarrow g = f^{-1}$$

et

$$f \circ h = Id_{V'} \Longrightarrow f^{-1} \circ f \circ h = f^{-1} \Longrightarrow h = f^{-1}.$$

II.3.28 L'égalité $(x_1, x_2) = (y, 0) + (0, z)$ équivaut à $x_1 = y, x_2 = z$. Tout élément de $V_1 \times V_2$ se décompose donc de manière unique en somme d'un élément de $V_1 \times \{0\}$ et d'un élément de $\{0\} \times V_2$ qui sont donc supplémentaires. De plus, les projections de $x := (x_1, x_2)$ sont $(x_1, 0)$ et $(0, x_2)$; or $(x_1, 0) = s_1(x_1) = s_1\big(p_1(x)\big)$ et $(0, x_2) = s_2(x_2) = s_2\big(p_2(x)\big)$: les projections de $V_1 \times V_2$ sur $V_1 \times \{0\}$ et $\{0\} \times V_2$ sont donc respectivement $s_1 \circ p_1$ et $s_2 \circ p_2$.

II.3.29 Soit $\mathcal{B}$ une base de V. Par hypothèse, elle a au moins deux éléments distincts. Soit π l'une des formes linéaires coordonnées associées : c'est un endomorphisme qui n'est ni nul ni bijectif, ce n'est donc pas une homothétie.

II.3.30 Comme l'énoncé le suggère fortement, on prend pour V un plan vectoriel de base (u, v) et l'on définit l'endomorphisme f par son effet sur cette base : $f(u) = u$ et $f(v) = u + v$. Comme $(u, u + v)$ est une base de V, l'endomorphisme f est un automorphisme. Soit W un sous–espace vectoriel de V. Si $W = \{0\}$ ou V, c'est un sous–espace vectoriel stable par f. Sinon, c'est une droite vectorielle : $W = \mathrm{Vect}(w)$, avec $w \neq 0$. On écrit $w = \lambda u + \mu v$, où $(\lambda, \mu) \neq (0, 0)$. On a donc $f(w) = \lambda u + \mu(u + v) = (\lambda + \mu)u + \mu v$. Le sous–espace vectoriel W est stable si, et seulement si, $f(w) \in W$, c'est-à-dire si, et seulement si, w et $f(w)$ sont proportionnels. Or, on sait que $au + bv$ et $cu + dv$ sont proportionnels si, et seulement si, $ad - bc = 0$. Dans notre cas, cela équivaut à $\lambda\mu - \mu(\lambda + \mu) = 0$, c'est-à-dire à $\mu = 0$. La seule droite vectorielle stable par f est donc $E := \mathrm{Vect}(u)$. Comme tous les supplémentaires de E sont des droites vectorielles distinctes de E, aucun n'est stable par f.

II.3.31 Soient $\mathcal{C}$ et $\mathcal{C}'$ des bases de E et F'. Ce sont des parties libres disjointes et telles que, de plus, $A := \mathcal{C} \cup \mathcal{C}'$ est libre (car $E \cap F' = \{0\}$). Il découle du théorème 30 que A est contenue dans une base $\mathcal{B}$ de V. Alors le sous–espace vectoriel F de V de base $\mathcal{B} \setminus \mathcal{C}$ est un supplémentaire de E tel que $F' \subset F$.
Soit $x \in V \setminus E$. On applique ce qui précède à $F' = \mathrm{Vect}(x)$. Soit par ailleurs F'' un supplémentaire de F' dans F : on a donc $V = E \oplus (F' \oplus F'')$, et tout élément v de V s'écrit de manière unique $v = e + (\lambda_v x + f'')$, où $e \in E$, $F'' \in F''$ et λ_v est un scalaire. L'application $f : v \mapsto \lambda_v$ est une forme linéaire sur V nulle sur E et telle que $f(x) = 1$.
Il est évident que E est inclus dans l'intersection des hyperplans qui le contiennent. Pour démontrer l'inclusion réciproque, on raisonne par contraposée. Soit $x \notin E$. Il existe donc une forme linéaire f sur V nulle sur E et telle que $f(x) = 1$. L'hyperplan $H = \mathrm{Ker}\, f$ contient donc E mais pas x. Ce dernier n'est donc pas contenu dans l'intersection des hyperplans qui contiennent E.

II.3.32 Rappelons que $E = \mathrm{Im}\, p = \mathrm{Ker}\, q$ et $F = \mathrm{Ker}\, p = \mathrm{Im}\, q$. Supposons d'abord E stable par f, c'est-à-dire $f(E) \subset E$. On a alors les implications suivantes :

$$\forall x \in V\ ,\ p(x) \in E \Longrightarrow f\big(p(x)\big) \in E \Longrightarrow q\left(f\big(p(x)\big)\right) = 0,$$

ce qui entraîne que $q \circ f \circ p = 0$. Supposons réciproquement que $q \circ f \circ p = 0$. On a alors les implications suivantes :

$$\forall x \in E\ ,\ p(x) = x \Longrightarrow q\big(f(x)\big) = q\left(f\big(p(x)\big)\right) = 0 \Longrightarrow f(x) \in \mathrm{Ker}\, q = E,$$

ce qui entraîne que $f(E) \subset E$, *i.e.* que E est stable par f.

Module II.4 : Calcul matriciel élémentaire

II.4.1 Écrivons $A = \lambda I_n + N$, où N est une matrice triangulaire supérieure stricte. Les matrices λI_n et N commutent, et l'on peut appliquer la formule du binôme :

$$\forall p \in \mathbb{N}\ ,\ A^p = \sum_{k=0}^{p} \binom{p}{k} (\lambda I_n)^{p-k} N^k.$$

Par ailleurs, d'après le cours, la matrice N est nilpotente d'ordre n : on a $N^n = 0$. Si $p \geqslant n$, cette somme peut donc être tronquée. La formule générale est la suivante :

$$\forall p \in \mathbb{N}\ ,\ A^p = \sum_{k=0}^{\min(p,n-1)} \binom{p}{k} \lambda^{p-k} N^k.$$

Lorsque p est grand, elle ne comporte donc que n termes. À titre d'exemple, on trouve :

$$\forall p \in \mathbb{N}\ ,\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^p = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\}^p = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + p \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}.$$

II.4.2 Supposons A et B d'ordres de nilpotence respectifs a et b : on a donc $A^a = B^b = 0$. Cela entraîne que, pour $k \geqslant a$ et pour $l \geqslant b$, on a $A^k = B^l = 0$. Puisque les matrices A et B commutent, on peut appliquer la formule du binôme :

$$\forall p \in \mathbb{N}\ ,\ (A+B)^p = \sum_{k=0}^{p} \binom{p}{k} A^k B^{p-k}.$$

Prenons $p := a + b - 1$. Alors, pour tout $k \in [\![0, p]\!]$, on a $k \geqslant a$ ou $p - k \geqslant b$: en effet, la négation de cette affirmation serait $k \leqslant a - 1$ et $p - k \leqslant b - 1$, qui entraînerait (en additionnant), $p \leqslant a + b - 2$, ce qui contredirait le choix de p. Puisque $k \geqslant a$ ou $p - k \geqslant b$, on a aussi $A^k = 0$ ou $B^{p-k} = 0$, donc, dans tous les cas, $A^k B^{p-k} = 0$. Tous les termes de la formule ci-dessus sont donc nuls, et l'on a finalement : $(A+B)^{a+b-1} = 0$.

Prenons $A := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $B := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. On vérifie sans peine les égalités $A^2 = B^2 = 0$. Mais la matrice $C := A + B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ a pour carré $C^2 = I_2$: elle est inversible, donc pas nilpotente (en fait, ses puissances paires valent I_2 et ses puissances impaires valent C, donc aucune de ces puissances n'est nulle). Naturellement, A et B ne commutent pas : $AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $BA = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

II.4.3 Écrivons $A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, de sorte que $A^2 = \begin{pmatrix} a^2 + bc & ab + bd \\ ca + dc & bc + d^2 \end{pmatrix}$. L'égalité désirée $A^2 = \tau A - \delta I_2$ équivaut donc au système :

$$\begin{cases} \tau a - \delta = a^2 + bc \\ \tau b \quad\ = ab + bd \\ \tau c \quad\ = ca + dc \\ \tau d - \delta = bc + d^2 \end{cases}$$

dont une solution évidente est $\tau = a + d$ (suggérée par la deuxième et la troisième égalité) et $\delta = ad - bc$ (imposée par la première et la quatrième égalité lorsque l'on a trouvé τ). Notons $\mathrm{Tr}(A) := a + d$ la *trace* de A (elle sera étudiée en L2) et $\det(A) := ad - bc$ le *déterminant* de A (voir le module II.7), on peut écrire :

$$\forall A \in M_2(K)\ ,\ A^2 - \mathrm{Tr}(A)A + \det(A)I_2 = 0.$$

C'est un cas particulier du *théorème de Cayley-Hamilton*, qui sera démontré dans le cours de L2.

Si l'on veut définir deux suites $(\alpha_n)_{n\in\mathbb{N}}$ et $(\beta_n)_{n\in\mathbb{N}}$ d'éléments de K telles que $\forall n \in \mathbb{N}, A^n = \alpha_n A + \beta_n I_2$, il est naturel de les initialiser en posant $\alpha_0 := 0, \beta_0 := 1$ et $\alpha_1 := 1, \beta_1 := 0$. On remarque ensuite que l'égalité $A^2 = \tau A - \delta I_2$ entraîne (en multipliant par A^n), pour tout entier $n \in \mathbb{N}$, l'égalité $A^{n+2} = \tau A^{n+1} - \delta A^n$. On pose donc, pour tout entier $n \in \mathbb{N}$, $\alpha_{n+2} = \tau\alpha_{n+1} - \delta\alpha_n$ et $\beta_{n+2} = \tau\beta_{n+1} - \delta\beta_n$. On vérifie alors immédiatement, par récurrence à deux pas, que l'on a bien $\forall n \in \mathbb{N}, A^n = \alpha_n A + \beta_n I_2$.

II.4.4 Si $a_1 = \cdots = a_m = 0$ ou $b_1 = \cdots = b_n = 0$, il est clair que tous les $a_i b_j$ sont nuls et donc $A = 0$. Pour démontrer la réciproque, on raisonne par contraposée : on suppose donc la négation de "$a_1 = \cdots = a_m = 0$ ou $b_1 = \cdots = b_n = 0$", c'est-à-dire que l'un au moins des coefficients a_i est non nul, soit $a_{i_0} \neq 0$, et également que l'un au moins des coefficients b_j est non nul, soit $b_{j_0} \neq 0$. Alors $a_{i_0} b_{j_0} \neq 0$, ce qui entraîne que $A \neq 0$.

Supposons maintenant A non nulle, et soient i_0, j_0 comme ci-dessus. En écrivant $a_i b_j = \dfrac{b_j}{b_{j_0}} a_i b_{j_0}$, on constate que les colonnes $C_1, \ldots, C_n$ de A sont proportionnelles : $C_j = \dfrac{b_j}{b_{j_0}} C_{j_0}$. Le sous–espace vectoriel $\mathrm{Vect}(C_1, \ldots, C_n)$ est donc engendré par C_{j_0}, qui n'est pas nulle (puisque $a_{i_0} b_{j_0} \neq 0$) ; c'est donc une droite vectorielle, et la matrice A est donc de rang 1.

Supposons enfin que $A \in M_{m,n}(K)$ est une matrice de rang 1. Le sous–espace vectoriel $\mathrm{Vect}(C_1, \ldots, C_n)$ est donc engendré par une colonne non nulle C_{j_0}, et l'on a $C_j = b_j C_{j_0}$ pour des scalaires $b_j \in K$ (et nécessairement $b_{j_0} = 1$). Notons $a_1, \ldots, a_m$ les coefficients de la colonne C_{j_0}. Il est immédiat que A est la matrice dont les coefficients sont les $a_i b_j$.

II.4.5 On sait déjà que les matrices scalaires λI_n commutent à toutes les matrices de $M_n(K)$; en particulier, les matrices scalaires inversibles $\lambda I_n, \lambda \in K^*$ commutent à toutes les matrices de $GL_n(K)$, autrement dit, elles appartiennent au centre de $GL_n(K)$.

Soit réciproquement A un élément du centre de $GL_n(K)$, autrement dit, une matrice inversible telle que $\forall B \in GL_n(K)\ ,\ AB = BA$. Nous allons démontrer que A est une matrice scalaire. Notant $a_{i,j}$ les coefficients de A, cela revient à dire que les $a_{i,i}$ sont tous égaux et que les $a_{i,j}$ tels que $i \neq j$ sont tous nuls. Soient i, j deux indices distincts dans $[\![1, n]\!]$. La matrice élémentaire $E_{i,j}$ est nilpotente d'ordre 2 (*i.e.* de carré nul), donc telle que $(I_n - E_{i,j})(I_n + E_{i,j}) = I_n^2 - 0 = I_n$. La matrice $B := I_n + E_{i,j}$ est donc inversible, et, de la relation $AB = BA$, on déduit que $AE_{i,j} = E_{i,j}A$. Notons $L_1, \ldots, L_n$ (resp. $C_1, \ldots, C_n$) les lignes (resp. les colonnes) de A. La matrice $AE_{i,j}$ a une seule colonne non nulle, sa $j^{ème}$, qui vaut C_i. La matrice $E_{i,j}A$ a une seule ligne non nulle, sa $i^{ème}$, qui vaut L_j. L'égalité $AE_{i,j} = E_{i,j}A$ entraîne donc en particulier que $a_{i,j} = 0$ et que $a_{i,i} = a_{j,j}$. Comme c'est vrai quels que soient les indices $i \neq j$, la matrice A est bien scalaire.

II.4.6 Les matrices du groupe G considéré sont de la forme $I_3 + N$, où N est triangulaire supérieure stricte, donc nilpotentes d'ordre 3 (c'est le lemme qui précède la proposition 11 de la page 219 du module II.4). Selon l'exercice II.4.1, $(I_3+N)^3 = I_3+3N+3N^2 = I_3$, puisque, pour tout $a \in \mathbb{Z}/3\mathbb{Z}$, on a $3a = 0$. On a donc bien, dans le groupe G, la relation $\forall x\ ,\ x^3 = 1$. Par ailleurs, ce groupe n'est pas commutatif :

$$\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix} = \begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix} \quad \text{et} \quad \begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix} = \begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}$$

II.4.7 Pour la première assertion, voir l'exercice II.3.27 de la page 204. On l'applique à l'application linéaire $\Phi_A : X \mapsto AX$ de K^n dans K^m. Comme toute application linéaire de K^m dans K^n est de la forme Φ_B, où $\in\ M_{n,m}(K)$, que $\Phi_B \circ \Phi_A = \Phi_{BA}$ et que $\Phi_{BA} = \mathrm{Id}_{K^n} \Leftrightarrow BA = I_n$, on en déduit que l'application linéaire Φ_A est injective si, et seulement si, A est inversible à gauche.

> ***Remarque***. Le terme "inversible à gauche" est ici légèrement abusif, car on n'a pas affaire à une loi de composition interne.

II.4.8 Soient σ, τ deux permutations de $[\![1, n]\!]$, et notons $A_\sigma = (a_{i,j})$ et $A_\tau = (b_{i,j})$. Alors le produit $A_\sigma A_\tau = (c_{i,j})$ est donné par les formules :

$$c_{i,j} = \sum_{k=1}^{n} a_{i,k}b_{k,j} = b_{\sigma(i),j} = \begin{cases}1 \text{ si } j = \tau\big(\sigma(i)\big)\\0 \text{ si } j \neq \tau\big(\sigma(i)\big)\end{cases}$$

de sorte que $A_\sigma A_\tau = A_{\tau\sigma}$. Si l'on note temporairement e la permutation identique de $[\![1, n]\!]$, on a bien sûr $A_e = I_n$. Ainsi, A_σ est inversible d'inverse $A_{\sigma^{-1}}$ et l'ensemble de ces matrices est bien un sous-groupe de $GL_n(K)$. Notons-le G.
L'application $\sigma \mapsto A_\sigma$ est une bijection du groupe symétrique sur G, mais n'est pas un morphisme de groupes. En revanche, en utilisant les relations $(A\,B)^{-1} = B^{-1}\,A^{-1}$ et ${}^t\!A\,B = {}^t\!B\,{}^t\!A$, on trouve que chacune des applications : $\sigma \mapsto A_\sigma^{-1}$ et $\sigma \mapsto {}^t\!A_\sigma$ est un isomorphisme. Le lecteur vérifiera sans peine qu'il s'agit du même isomorphisme : pour toute permutation σ, on a en effet $A_\sigma^{-1} = {}^t\!A_\sigma$.

II.4.9 Pour la première matrice, on suppose a, b, c deux à deux distincts (sinon la matrice a deux lignes égales et n'est donc pas inversible). On appliquera les mêmes opérations élémentaires sur les lignes aux matrices :

$$\begin{pmatrix}1&a&a^2\\1&b&b^2\\1&c&c^2\end{pmatrix} \quad \text{et} \quad \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}.$$

Les transvections $L_2 \leftarrow L_2 - L_1$ et $L_3 \leftarrow L_3 - L_1$ (dans n'importe quel ordre) donnent :

$$\begin{pmatrix}1&a&a^2\\0&b-a&b^2-a^2\\0&c-a&c^2-a^2\end{pmatrix} \quad \text{et} \quad \begin{pmatrix}1&0&0\\-1&1&0\\-1&0&1\end{pmatrix}.$$

Dorénavant, nous sommes contraints de n'employer que des opérations élémentaires sur les lignes (et non sur les colonnes). La transvection $L_3 \leftarrow L_3 - \dfrac{c-a}{b-a}L_2$ donne :

$$\begin{pmatrix} 1 & a & a^2 \\ 0 & b-a & b^2-a^2 \\ 0 & 0 & (c-a)(c-b) \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ \dfrac{c-b}{b-a} & -\dfrac{c-a}{b-a} & 1 \end{pmatrix}.$$

Les transvections $L_1 \leftarrow L_1 - \dfrac{a^2}{(c-a)(c-b)}L_3$ et $L_2 \leftarrow L_2 - \dfrac{b^2-a^2}{(c-a)(c-b)}L_3$ donnent :

$$\begin{pmatrix} 1 & a & 0 \\ 0 & b-a & 0 \\ 0 & 0 & (c-a)(c-b) \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} \dfrac{cb-(c+b)a}{(c-a)(b-a)} & \dfrac{-a^2}{(c-b)(a-b)} & \dfrac{-a^2}{(c-a)(c-b)} \\ \dfrac{b+c}{a-c} & \dfrac{c+a}{c-b} & \dfrac{a^2-b^2}{(c-a)(c-b)} \\ \dfrac{c-b}{b-a} & -\dfrac{c-a}{b-a} & 1 \end{pmatrix}.$$

La transvection $L_1 \leftarrow L_1 - \dfrac{a}{b-a}L_2$ donne :

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & b-a & 0 \\ 0 & 0 & (c-a)(c-b) \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} \dfrac{bc}{(c-a)(b-a)} & \dfrac{ac}{(c-b)(a-b)} & \dfrac{ab}{(c-a)(c-b)} \\ \dfrac{b+c}{a-c} & \dfrac{c+a}{c-b} & \dfrac{a^2-b^2}{(c-a)(c-b)} \\ \dfrac{c-b}{b-a} & -\dfrac{c-a}{b-a} & 1 \end{pmatrix}.$$

Enfin, les dilatations $L_2 \leftarrow \dfrac{1}{b-a}L_2$ et $L_3 \leftarrow \dfrac{1}{(c-a)(c-b)}L_3$ donnent :

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} \dfrac{bc}{(a-b)(a-c)} & \dfrac{ca}{(b-a)(b-c)} & \dfrac{ab}{(c-a)(c-b)} \\ \dfrac{-(b+c)}{(a-b)(a-c)} & \dfrac{-(c+a)}{(b-a)(b-c)} & \dfrac{-(a+b)}{(c-a)(c-b)} \\ \dfrac{1}{(a-b)(a-c)} & \dfrac{1}{(b-a)(b-c)} & \dfrac{1}{(c-a)(c-b)} \end{pmatrix}.$$

Cette dernière matrice est l'inverse recherché. Après lecture du module II.6, le lecteur pourra y reconnaître les coefficients des polynômes d'interpolation de Lagrange aux points a, b, c. Ces derniers sont en effet les polynômes :

$$\begin{aligned} \frac{(X-b)(X-c)}{(a-b)(a-c)} &= \frac{1}{(a-b)(a-c)}\,(X^2-(b+c)X+bc), \\ \frac{(X-c)(X-a)}{(b-c)(b-a)} &= \frac{1}{(b-c)(b-a)}\,(X^2-(c+a)X+ca) \quad \text{et} \\ \frac{(X-a)(X-b)}{(c-a)(c-b)} &= \frac{1}{(c-a)(c-b)}\,(X^2-(a+b)X+ab). \end{aligned}$$

Pour la deuxième matrice de l'énoncé, pour changer un peu, on appliquera plutôt les mêmes

opérations élémentaires sur les colonnes aux matrices :

$$\begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

Les transvections $C_2 \leftarrow C_2 - C_1$, $C_3 \leftarrow C_3 - C_2, \dots, C_n \leftarrow C_n - C_{n-1}$, effectuées *dans cet ordre* transforment la première matrice en I_n (c'est évident). La deuxième matrice est successivement transformée en :

$$\begin{pmatrix} 1 & -1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}, \text{ puis } \begin{pmatrix} 1 & -1 & 1 & \dots & 0 & 0 \\ 0 & 1 & -1 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}, \text{ puis } \dots$$

$$\begin{pmatrix} 1 & -1 & 1 & \dots & (-1)^{n-2} & 0 \\ 0 & 1 & -1 & \dots & (-1)^{n-3} & 0 \\ 0 & 0 & 1 & \dots & (-1)^{n-4} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}, \text{ puis } \begin{pmatrix} 1 & -1 & 1 & \dots & (-1)^{n-2} & (-1)^{n-1} \\ 0 & 1 & -1 & \dots & (-1)^{n-3} & (-1)^{n-2} \\ 0 & 0 & 1 & \dots & (-1)^{n-4} & (-1)^{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -1 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix},$$

qui est l'inverse recherché ; son coefficient général est donc donné par les formules :

$$a_{i,j} = \begin{cases} 0 \text{ si } i > j \\ (-1)^{j-i} \text{ si } i \leqslant j \end{cases}.$$

On retrouve le résultat obtenu (de deux façons) dans le cours.

II.4.10 Si $x_i = x_j$, les lignes d'indices i et j sont égales. Pour que la matrice soit inversible, il est donc nécessaire que les x_i soient deux à deux distincts. Le but de l'exercice est de démontrer la réciproque. Nous noterons, pour tout $i \in [\![1, n]\!]$:

$$P_i := (X - x_1) \cdots (X - x_i) = X^i + \sum_{j=0}^{i-1} \lambda_{i,j} X^j.$$

(i) Le principe général est le suivant. Soit $\lambda \in K$. Si $i \neq n$, les contenus des colonnes de A après la transvection $C_n \leftarrow C_n + \lambda C_i$ sont respectivement $C'_1 = C_1, \dots, C'_{n-1} = C_{n-1}$ et $C'_n = C_n + \lambda C_i$. Si l'on effectue les transvections $C_n \leftarrow C_n + \lambda_{n-1,i-1} C_i$ pour $i = 1, \dots, n-1$, les colonnes $C_1, \dots, C_{n-1}$ ne sont pas affectées et la colonne C_n est successivement transformée en $C'_n = C_n + \lambda_{n-1,0} C_1$, puis $C''_n = C_n + \lambda_{n-1,0} C_1 + \lambda_{n-1,1} C_2$, etc. Après k transvections, on a, de manière générale : $C_n^{(k)} = C_n + \lambda_{n-1,0} C_1 + \lambda_{n-1,1} C_2 + \cdots + \lambda_{n-1,k-1} C_k$. Le contenu final de C_n après les n transvections indiquées est donc bien $C_n + \lambda_{n-1,0} C_1 + \cdots + \lambda_{n-1,n-2} C_{n-1}$.

À l'issue de cette opération (composée de n transvections), les $a_{i,k}, k < n$ n'ont pas été modifiés. Le $i^{ème}$ coefficient $a_{i,n}$ de C_n a été remplacé par :

$$\begin{aligned} a_{i,n} + \lambda_{n-1,0}\, a_{i,1} + \cdots + \lambda_{n-1,n-2}\, a_{i,n-1} &= x_i^{n-1} + \lambda_{n-1,0} + \cdots + \lambda_{n-1,n-2}\, x_i^{n-2} \\ &= P_{n-1}(x_i). \end{aligned}$$

Or, les racines de P_{n-1} sont $x_1, \ldots, x_{n-1}$. La dernière colonne a donc maintenant tous ses coefficients nuls, sauf le dernier qui vaut $P_{n-1}(x_n) = (x_n - x_1)\cdots(x_n - x_{n-1})$. Le contenu de C_n après l'opération indiquée est donc $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ P_{n-1}(x_n) \end{pmatrix}$.

(ii) Pour chaque k de $n-1$ à 2, l'opération indiquée dans l'énoncé est le produit des transvections $C_k \leftarrow C_k + \lambda_{k-1,i-1} C_i$ $(i = 1, \ldots, k-1)$. Cette opération ne modifie que la colonne C_k et ne met en jeu que les colonnes C_i $(i = 1, \ldots, k-1)$, qui n'ont pas encore été modifiées et sont donc dans leur état initial. Après cette opération, le contenu de la colonne C_k est donc $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ P_{k-1}(x_k) \\ \vdots \\ P_{k-1}(x_n) \end{pmatrix}$. Remarquons que le $k^{ème}$ coefficient de cette colonne (celui qui figure sur la diagonale) est $P_{k-1}(x_k) = (x_k - x_1)\cdots(x_k - x_{k-1})$.

Après toutes ces opérations, A a été transformée en une matrice triangulaire inférieure dont les coefficients diagonaux sont : $P_0(x_1), P_1(x_2), \ldots, P_{n-1}(x_n)$. Le produit de ces coefficients diagonaux est $\prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)$: c'est donc le déterminant de A (module II.7), puisque les transvections ne modifient pas le déterminant. Dans tous les cas, si les x_i sont deux à deux distincts, on a obtenu une matrice triangulaire à coefficients diagonaux non nuls, donc inversible : la matrice A de départ est donc elle-même inversible.

II.4.11 Pour la description donnée ici de l'algorithme d'Euclide, le lecteur pourra lire les modules II.6 et II.8. Comme l'indique l'énoncé, on a $x_{i+1} = x_{i-1} - q_i x_i$, où $q_i := x_{i-1}\text{div}x_i$. On en tire :

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} x_{i-1} \\ x_i \end{pmatrix} = \begin{pmatrix} 0.x_{i-1} + 1.x_i \\ 1.x_{i-1} - q_i x_i \end{pmatrix} = \begin{pmatrix} x_i \\ x_{i-1} - q_i x_i \end{pmatrix} = \begin{pmatrix} x_i \\ x_{i+1} \end{pmatrix},$$

comme demandé.

On itère l'égalité obtenue :

$$\begin{pmatrix} x_i \\ x_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} x_{i-1} \\ x_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{i-1} \end{pmatrix} \begin{pmatrix} x_{i-2} \\ x_{i-1} \end{pmatrix} = \cdots$$

$$\cdots = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{i-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}.$$

Notons donc :

$$\begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} := \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{i-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}.$$

On a alors :

$$\begin{pmatrix} x_i \\ x_{i+1} \end{pmatrix} = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix},$$

puisque, par initialisation, $x_0 = u$ et $x_1 = v$. En particulier, $x_i = a_i u + b_i v$ (et $x_{i+1} = c_i u + d_i v$). Par définition :

$$\begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} a_{i+1} & b_{i+1} \\ c_{i+1} & d_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{pmatrix} \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$$

De cette dernière égalité, on déduit que $a_{i+1} = c_i$ et $b_{i+1} = d_i$. Les $\star$ de la deuxième ligne de la matrice $\begin{pmatrix} a_i & b_i \\ \star & \star \end{pmatrix}$ sont donc $c_i = a_{i+1}$ et $d_i = b_{i+1}$ (ce qui rend cohérentes les deux égalités $x_i = a_i u + b_i v$ et $x_{i+1} = c_i u + d_i v$). Les relations ci-dessus se réécrivent comme suit :

$$\begin{pmatrix} a_0 & b_0 \\ a_1 & b_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} a_{i+1} & b_{i+1} \\ a_{i+2} & b_{i+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{pmatrix} \begin{pmatrix} a_i & b_i \\ a_{i+1} & b_{i+1} \end{pmatrix}$$

On peut donc définir les suites (a_i) et (b_i) par les initialisations $a_0 = 1$, $a_1 = 0$, $b_0 = 0$, $b_1 = 1$ et les relations de récurrence à deux pas : $a_{i+2} = a_i - q_{i+1} a_{i+1}$, $b_{i+2} = b_i - q_{i+1} b_{i+1}$. Lorsque $x_k \neq 0$ et $x_{k+1} = 0$, on sait que $\delta := x_k$ est un pgcd de u et v. La relation de Bézout s'écrit alors $\delta = au + bv$, les coefficients $a := a_k$ et $b := b_k$ ayant été obtenus par la récurrence indiquée, ou bien comme la première ligne de la matrice $\begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{k-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}$.

Module II.5 : Le corps des nombres complexes

II.5.1 Supposons $\mathbb{C}$ muni d'un ordre total $\leqslant$, compatible avec l'addition et la multiplication (au sens du module I.1). L'ordre étant total, tout élément de $\mathbb{C}$ est comparable à 0. On en déduit que *tout carré est positif*. En effet, l'ordre étant total, pour tout $x \in \mathbb{C}$, on a soit $x \geqslant 0$, soit $x \leqslant 0$. Dans le premier cas, $x^2 = x.x$ est positif comme produit de deux éléments positifs ; dans le second cas, $x \leqslant 0 \Rightarrow -x \geqslant 0$, et $x^2 = (-x).(-x)$ est encore positif comme produit de deux éléments positifs.

Appliquant ce principe à $x = 1$, on conclut d'abord que $1^2 = 1$ est positif : $0 \leqslant 1$. Appliquant ce principe à $x = \mathrm{i}$, on conclut ensuite que $\mathrm{i}^2 = -1$ est également positif : $-1 \geqslant 0$, d'où $1 \leqslant 0$ (ici, on a utilisé la compatibilité de $\leqslant$ avec l'addition). Des deux inégalités $0 \leqslant 1$ et $1 \leqslant 0$, on tire $0 = 1$, ce qui est une contradiction.

> ***Remarque***. Soit K un corps commutatif. Il est facile de voir que, s'il existe sur K une relation d'ordre total compatible avec l'addition et la multiplication, alors *toute somme de carrés non tous nuls est non nulle* (même méthode que ci-dessus). On peut en fait démontrer que la réciproque est vraie (c'est un théorème dû au mathématicien allemand Emil Artin).

II.5.2 (i) Avec la notation $\tilde{\mathrm{i}} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ de la question (ii), on observe tout d'abord que $\tilde{\mathbb{C}} = \{aI_2 + b\tilde{\mathrm{i}} \mid a, b \in \mathbb{R}\}$, qui est le sous $\mathbb{R}$-espace vectoriel de $M_2(\mathbb{R})$ engendré par I_2 et $\tilde{\mathrm{i}}$; en particulier, c'est un sous-groupe du groupe additif $M_2(\mathbb{R})$. Il contient l'élément neutre I_2 de la multiplication (prendre $a = 1$, $b = 0$). De plus :

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} a'' & b'' \\ -b'' & a'' \end{pmatrix}, \text{ où } a'' = aa' - bb' \quad \text{et} \quad b'' = ab' + ba'. \tag{37}$$

Cela se vérifie par calcul direct, ou bien en remarquant que $\tilde{\mathrm{i}}^2 = -I_2$ (voir calcul plus bas). Il en découle que $\tilde{\mathbb{C}}$ est stable pour la multiplication ; c'est donc un sous-anneau de $M_2(\mathbb{R})$. Par ailleurs, l'application $a \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI_2$ est l'unique application $\mathbb{R}$-linéaire de $\mathbb{R}$ dans $\tilde{\mathbb{C}}$ telle que $1 \mapsto I_2$, en particulier, c'est un morphisme de groupes. On a $1 \mapsto I_2$ (éléments neutres de la multiplication des deux anneaux), et l'égalité $abI_2 = (aI_2)(bI_2)$ achève de montrer que c'est un morphisme d'anneaux. Son noyau est formé des $a \in \mathbb{R}$ tels que $aI_2 = 0$, c'est-à-dire $a = 0$. Le morphisme est donc injectif, et c'est un isomorphisme de $\mathbb{R}$ sur son image, qui est un sous-anneau de $\tilde{\mathbb{C}}$. Il est donc légitime d'identifier $\mathbb{R}$ au sous-anneau $\left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R}\right\}$ de $\tilde{\mathbb{C}}$, et tout réel a à l'élément aI_2 de $\tilde{\mathbb{C}}$.

(ii) On vérifie d'abord que $\tilde{\mathrm{i}}^2 = -I_2$:

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0^2 + 1.(-1) & 0.1 + 1.0 \\ -1.0 + 0.(-1) & (-1).1 + 0^2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Modulo l'identification décidée à la question précédente, on peut donc écrire $\tilde{\mathrm{i}}^2 = -1$. On a déjà vu que I_2 et $\tilde{\mathrm{i}}$ engendrent le $\mathbb{R}$-espace vectoriel $\tilde{\mathbb{C}}$, et il est clair qu'ils sont linéairement indépendants, donc qu'ils en forment une base. Autrement dit, tout élément de $\tilde{\mathbb{C}}$ s'écrit

de manière unique $a + b\tilde{\mathrm{i}}$, avec $a, b \in \mathbb{R}$, et l'application $a + b\mathrm{i} \mapsto a + b\tilde{\mathrm{i}}$ définit un isomorphisme de $\mathbb{R}$-espace vectoriels de $\mathbb{C}$ dans $\tilde{\mathbb{C}}$ dont la restriction à $\mathbb{R}$ est l'identité. Il reste à voir que c'est un morphisme d'anneaux. On sait déjà que $1 \mapsto I_2$ (éléments neutres de la multiplication des deux anneaux). Il reste à vérifier la compatibilité avec la multiplication, c'est-à-dire que $a'' + b''\mathrm{i} := (a + b\mathrm{i})(a' + b'\mathrm{i})$ a pour image $a'' + b''\tilde{\mathrm{i}} := (a + b\tilde{\mathrm{i}})(a' + b'\tilde{\mathrm{i}})$. Mais c'est une conséquence immédiate de l'égalité 37 de la page précédente.

II.5.3 Supposons que l'on a trouvé un tel morphisme ψ. Alors, pour tout complexe $z = x + \mathrm{i}y$, on a : $\psi(x + \mathrm{i}y) = \psi(x) + \psi(\mathrm{i})\psi(y) = \varphi(x) + \alpha\varphi(y)$. S'il existe, le morphisme ψ est donc unique.

Réciproquement, pour tout complexe $z = x + \mathrm{i}y$, posons : $\psi(x + \mathrm{i}y) = \varphi(x) + \alpha\varphi(y)$. Il vient d'abord $\psi(x) = \varphi(x)$ et $\psi(\mathrm{i}) = \alpha$; nous devons vérifier que ψ est un morphisme d'anneaux. Avec des notations évidentes :

$$\begin{aligned} \psi(z + z') &= \varphi(x + x') + \alpha\varphi(y + y'), \\ \psi(z) + \psi(z') &= \big(\varphi(x) + \alpha\varphi(y)\big) + \big(\varphi(x') + \alpha\varphi(y')\big), \end{aligned}$$

et l'égalité $\psi(z + z') = \psi(z) + \psi(z')$ vient de ce que φ est un morphisme de groupes. Il est évident que $\psi(1) = 1$. Reste le produit :

$$\begin{aligned} \psi(zz') &= \varphi(xx' - yy') + \alpha\varphi(xy' + yx'), \\ \psi(z)\psi(z') &= \big(\varphi(x) + \alpha\varphi(y)\big)\big(\varphi(x') + \alpha\varphi(y')\big) \\ &= \big(\varphi(x)\varphi(x') - \varphi(y)\varphi(y')\big) + \alpha\big(\varphi(x)\varphi(y') + \varphi(y)\varphi(x')\big); \end{aligned}$$

pour ce dernier calcul, on a utilisé pour la première fois le fait que $\alpha^2 = -1$. Du fait que φ est un morphisme d'anneaux, on déduit successivement :

$$\varphi(xx' - yy') = \varphi(x)\varphi(x') - \varphi(y)\varphi(y'), \qquad \varphi(xy' + yx') = \varphi(x)\varphi(y') + \varphi(y)\varphi(x')$$

et, enfin $\psi(zz') = \psi(z)\psi(z')$. Donc ψ est un morphisme d'anneaux.

II.5.4 (i) La propriété "$\mathbb{R}$ est central dans $\mathcal{H}$" signifie :

$$\forall x, a, b, c, d \in \mathbb{R}\ ,\ x(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})x.$$

Comme $\mathbb{R}$ est commutatif, il suffit de vérifier les égalités $x\mathbf{i} = \mathbf{i}x$, $x\mathbf{j} = \mathbf{j}x$ et $x\mathbf{k} = \mathbf{k}x$. Les deux premières font partie des règles postulées. Pour la troisième, on calcule :

$$x\mathbf{k} = x(\mathbf{ij}) = (x\mathbf{i})\mathbf{j} = (\mathbf{i}x)\mathbf{j} = \mathbf{i}(x\mathbf{j}) = \mathbf{i}(\mathbf{j}x) = (\mathbf{ij})x = \mathbf{k}x,$$

en invoquant plusieurs fois l'associativité de la multiplication dans l'anneau $\mathbf{H}$. Nous utiliserons dorénavant l'associativité de manière plus implicite, ainsi que le fait que tout réel commute avec tous les quaternions. Pour le calcul qui suit, rappelons l'égalité valable dans tout anneau : $-u = (-1)u$. Démontrons que $\mathbf{k}^2 = -1$:

$$\mathbf{k}^2 = (\mathbf{ij})^2 = \mathbf{i}(\mathbf{ji})\mathbf{j} = \mathbf{i}(-\mathbf{ij})\mathbf{j} = -\mathbf{i}^2\mathbf{j}^2 = -(-1)^2 = -1.$$

De même :

$$\mathbf{jk} = \mathbf{jij} = -\mathbf{ij}^2 = \mathbf{i} \quad \text{et} \quad \mathbf{kj} = \mathbf{ijj} = \mathbf{ij}^2 = -\mathbf{i}.$$

Enfin :

$$\mathbf{ki} = \mathbf{iji} = -\mathbf{ji}^2 = \mathbf{j} \quad \text{et} \quad \mathbf{ik} = \mathbf{i}^2\mathbf{j} = -\mathbf{j}.$$

On trouve sans peine :

$$(a_1+b_1\mathbf{i}+c_1\mathbf{j}+d_1\mathbf{k})+(a_2+b_2\mathbf{i}+c_2\mathbf{j}+d_2\mathbf{k}) = (a_1+a_2)+(b_1+b_2)\mathbf{i}+(c_1+c_2)\mathbf{j}+(d_1+d_2)\mathbf{k}.$$

Pour le produit, grâce à la distributivité, aux trois formules $\mathbf{i}^2 = -1$, etc, et aux six formules $\mathbf{ij} = \mathbf{k}$, etc, on trouve (avec peine mais sans difficulté) :

$$(a_1 + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k})(a_2 + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) = (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)+$$

$$(a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)\mathbf{i} + (a_1c_2 + c_1a_2 + d_1b_2 - b_1d_2)\mathbf{j} + (a_1d_2 + d_1a_2 + b_1c_2 - c_1b_2)\mathbf{k}.$$

En prenant $a_2 = a_1$, $b_2 = -b_1$, $c_2 = -c_1$ et $d_2 = -d_1$, on trouve que seul le terme réel demeure :

$$(a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k})(a-b\mathbf{i}-c\mathbf{j}-d\mathbf{k}) = (a^2+b^2+c^2+d^2)+0\mathbf{i}+0\mathbf{j}+0\mathbf{k} = a^2+b^2+c^2+d^2.$$

Ainsi, l'égalité $a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} = 0$ entraîne $a^2+b^2+c^2+d^2 = 0$, donc $a = b = c = d = 0$, car ce sont des réels. On en déduit notamment que $(1, \mathbf{i}, \mathbf{j}, \mathbf{k})$ est une base du $\mathbb{R}$-espace vectoriel $\mathbf{H}$.

Pour vérifier que $\mathbf{H}$ est un corps, il suffit de prouver que tout élément non nul est inversible. Mais il résulte du dernier calcul (et de la centralité de $\mathbb{R}$) que, si $a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} \neq 0$, alors il admet pour inverse :

$$\frac{a}{a^2+b^2+c^2+d^2} + \frac{-b}{a^2+b^2+c^2+d^2}\mathbf{i} + \frac{-c}{a^2+b^2+c^2+d^2}\mathbf{j} + \frac{-d}{a^2+b^2+c^2+d^2}\mathbf{k}.$$

Anticipant les notations qui seront introduites à la question (iii), et généralisant la terminologie des nombres complexes, on appelle *conjugué* du quaternion $x := a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ le quaternion $\sigma(x) := a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$; de même, on appelle *norme algébrique* de x le produit $N(x) := x\sigma(x)$.

Il résulte des calculs précédents que $N(x) = N(\sigma(x)) = a^2+b^2+c^2+d^2 \in \mathbb{R}$ et que l'inverse de x est $\dfrac{1}{N(x)}\sigma(x)$.

Il découle de l'exercice précédent, appliqué à $\varphi : a \mapsto a$ et à $\alpha = \mathbf{i}$, que l'application $a+b\mathrm{i} \mapsto a+b\mathbf{i}$ définit un morphisme d'anneaux de $\mathbb{C}$ dans $\mathbf{H}$ dont la restriction à $\mathbb{R}$ est l'identité. Comme $a+b\mathbf{i} \Rightarrow a = b = 0$, il est clair que ce morphisme est injectif.

(ii) Plagiant la construction de $\mathbb{C}$, on peut poser $\mathbf{H} = \mathbb{R}^4$, que l'on munit de la structure de groupe produit. Le produit $(a_1, b_1, c_1, d_1)(a_2, b_2, c_2, d_2)$ est donné par la formule :

$$(a_1a_2-b_1b_2-c_1c_2-d_1d_2, a_1b_2+b_1a_2+c_1d_2-d_1c_2, a_1c_2+c_1a_2+d_1b_2-b_1d_2, a_1d_2+d_1a_2+b_1c_2-c_1b_2)$$

On identifie alors 1 à $(1,0,0,0)$ et l'on note $\mathbf{i} = (0,1,0,0)$, $\mathbf{j} = (0,0,1,0)$ et $\mathbf{k} = (0,0,0,1)$.

(iii) L'application σ est l'automorphisme du $\mathbb{R}$-espace vectoriel qui transforme la base $(1, \mathbf{i}, \mathbf{j}, \mathbf{k})$ en la $(1, -\mathbf{i}, -\mathbf{j}, -\mathbf{k})$. C'est donc en particulier un automorphisme de groupe. Pour démontrer l'égalité $\sigma(xy) = \sigma(y)\sigma(x)$, observons d'abord que les applications $x \mapsto \sigma(xy)$ et $x \mapsto \sigma(y)\sigma(x)$ sont toutes deux $\mathbb{R}$-linéaires ; il suffit donc d'examiner le cas où x est élément de la base $(1, \mathbf{i}, \mathbf{j}, \mathbf{k})$ (théorème 26 de la page 192 du module II.3). De même, les applications $y \mapsto \sigma(xy)$ et $y \mapsto \sigma(y)\sigma(x)$ étant $\mathbb{R}$-linéaires, il suffit d'examiner le cas où $y \in (1, \mathbf{i}, \mathbf{j}, \mathbf{k})$. Si x ou y vaut 1, l'égalité à vérifier est triviale ; de même si $x = y$. Il reste donc les six cas $(\mathbf{i}, \mathbf{j})$, $(\mathbf{i}, \mathbf{k})$, $(\mathbf{j}, \mathbf{i})$, $(\mathbf{j}, \mathbf{k})$, $(\mathbf{k}, \mathbf{i})$ et $(\mathbf{k}, \mathbf{j})$: nous les laissons au plaisir du lecteur.

On peut alors calculer :

$$N(xy) = xy\sigma(xy) = xy\sigma(y)\sigma(x) = xN(y)\sigma(x) = x\sigma(x)N(y) = N(x)N(y).$$

On a utilisé le fait que $N(y) \in \mathbb{R}$ est central, donc commute avec $\sigma(x)$.
Notons $x := a_1 + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k}$ et $y := a_2 + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}$. La formule précédente donne alors :

$$(a_1^2 + b_1^2 + c_1^2 + d_1^2)(a_2^2 + b_2^2 + c_2^2 + d_2^2) = (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)^2 +$$

$(a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)^2 + (a_1c_2 + c_1a_2 + d_1b_2 - b_1d_2)^2 + (a_1d_2 + d_1a_2 + b_1c_2 - c_1b_2)^2$.
Si l'on pose maintenant :

$$\mathcal{N} := \{a^2 + b^2 + c^2 + d^2 \mid a, b, c, d \in \mathbb{Z}\},$$

on déduit de ce qui précède que $\mathcal{N}$ est un sous-ensemble de $\mathbb{N}$ stable pour la multiplication. Si l'on arrivait à démontrer que $\mathcal{N}$ contient les nombres premiers, on en déduirait que $\mathcal{N} = \mathbb{N}$, c'est-à-dire le théorème de Lagrange. En réalité, c'est bien sûr le fait que $\mathcal{N}$ contient les nombres premiers (autrement dit, que tout nombre premier est somme de quatre carrés) qui est difficile à démontrer !

II.5.5 Si l'on part d'une équation générale du quatrième degré :

$$P(Z) := AZ^4 + BZ^3 + CZ^2 + DZ + E = 0 \qquad \text{avec} \qquad A \neq 0,$$

on peut poser $z = Z + \dfrac{B}{4A}$ dans le but de faire disparaître le terme de degré 3 ; l'idée est que l'on considère $AZ^4 + BZ^3$ comme le début du développement de $A\left(Z + \dfrac{B}{4A}\right)^4$. Ce changement de variable, qui généralise la mise sous forme canonique du trinôme du second degré, est appelée *transformation de Tschirnhaus*. On obtient alors l'équation $Q(z) = z^4 + az^2 + bz + c = 0$ avec $Q(z) := \dfrac{1}{A}P\left(z - \dfrac{B}{4A}\right)$. Pour déterminer les coefficients a, b, c, on peut calculer "à la brute" ou bien appliquer la formule de Taylor (théorème 35 de la page 302, module II.6) à $P\left(z - \dfrac{B}{4A}\right)$, ce qui donne :

$$P\left(-\frac{B}{4A}\right) + P'\left(-\frac{B}{4A}\right)z + \frac{1}{2}P''\left(-\frac{B}{4A}\right)z^2 + \frac{1}{6}P'''\left(-\frac{B}{4A}\right)z^3 + \frac{1}{24}P^{(iv)}\left(-\frac{B}{4A}\right)z^4.$$

En divisant par A, on obtient bien $z^4 + az^2 + bz + c$, où :

$$a = -\frac{3B^2}{8A^3} + \frac{C}{A^2}\,,\ b = \frac{B^3}{8A^4} - \frac{2BC}{A^3}Z + \frac{D}{A^2} \quad \text{et} \quad c = \frac{-3B^4}{256A^5} + \frac{CB^2}{16A^3} - \frac{BD}{4A^2} + \frac{E}{A}$$

(on a $P''' = 24Z + 6\dfrac{B}{A}$, d'où $P'''\left(-\dfrac{B}{4A}\right) = 0$, ce qui confirme l'absence du terme en z^3).

(ii) L'égalité $(z^2 + w)^2 = a'z^2 + b'z + c'$ équivaut à $z^4 + (2w - a')z^2 - b'z + (w^2 - c') = 0$. On demande donc (par identification) que $2w - a' = a$, $-b' = b$ et $w^2 - c' = c$. En posant $a' := 2w - a$, $b' := -b$ et $c' := w^2 - c$, on ramène donc l'équation de départ à celle-ci.

(iii) Le trinôme $a'z^2 + b'z + c'$ est un carré si, et seulement si, $b'^2 - 4a'c' = 0$, c'est-à-dire $b^2 - 4(2w - a)(w^2 - c) = 0$, ce qui se ramène à l'équation : $w^3 - \dfrac{a}{2}w^2 - cw + \dfrac{4ac - b^2}{8} = 0$. Une fois celle-ci résolue (on choisit l'une quelconque de ses racines, cela n'a pas

d'importance), selon la méthode de Cardan (ou de Scipion del Ferro), on doit résoudre : $(z^2+w)^2 = a'\left(z+\dfrac{b'}{2a'}\right)^2$. Pour chacune des deux racines carrées α de a', on doit alors résoudre l'équation du second degré $z^2+w=\alpha\left(z+\dfrac{b'}{2a'}\right)$: on obtient au total quatre racines (en général distinctes).

II.5.6 (i) C'est un cas particulier de l'exercice II.3.19 de la page 203 , où l'on a de plus démontré que l'application $\underline{u}\mapsto(u_0,u_1)$ est un isomorphisme de E sur $\mathbb{C}^2$, et donc que $\dim E=2$.
(ii) Si la suite des $u_n=x^n$ est élément de E, la relation de récurrence, écrite pour $n=0$, entraîne que $x^2=px+q$. Réciproquement, si $x^2=px+q$, en multipliant par x^n on voit que $x^{n+2}=px^{n+1}+qx^n$ (pour tout entier n), donc que la suite des $u_n=x^n$ est élément de E. Ainsi, si $p^2+4q\neq 0$, il y a deux suites de cette forme dans E (correspondant aux deux racines de l'équation). Supposons maintenant que $p^2+4q=0$, notons x la racine double (donc la la suite des x^n est élément de E) et considérons la suite de terme général $u_n=nx^n$. Alors, pour tout entier n :

$$u_{n+2}-pu_{n+1}-qu_n=nx^n(x^2-px-q)+x^{n+1}(2x-p).$$

Comme x est racine double, on a $x^2-px-q=2x-p=0$, et la suite des $u_n=nx^n$ est élément de E.
(iii) Soit $\underline{u}\in E$. Puisque les suites $\underline{u}$, $\underline{v}$ et $\underline{w}$ vérifient la même relation de récurrence linéaire à deux pas, pour que l'égalité $\underline{u}=a\underline{v}+b\underline{w}$, soit vérifiée, il faut, et il suffit, que l'on ait $u_0=av_0+bw_0$ et $u_1=av_1+bw_1$; c'est d'ailleurs aussi une conséquence de l'isomorphisme évoqué à la question (i). Dans le cas où $p^2+4q\neq 0$, soient y et z les deux racines : on a donc $v_n=y^n$ et $w_n=z^n$, et il s'agit de résoudre le système $a+b=u_0$, $ay+bz=u_1$. L'unique solution est $a=\dfrac{u_1-u_0z}{y-z}$, $b=\dfrac{u_1-u_0y}{z-y}$.
Dans le cas où $p^2+4q=0$, soit x la racine double : on a donc $v_n=x^n$ et $w_n=nx^n$, et il s'agit de résoudre le système $a=u_0$, $ax+bx=u_1$. L'unique solution est évidemment $a=u_0$, $b=\dfrac{u_1-u_0x}{x}$.
Il faut toutefois traiter à part le cas où $x=0$ est racine double, qui correspond à $p=q=0$. Le calcul précédent est alors incorrect ; d'ailleurs, la suite des nx^n est identiquement nulle et ne peut donc faire partie d'une base. En fait, dans ce cas, E est formé des suites nulles à partir du rang 2, dont une base est formée de la suite $(1,0,0,\ldots)$ (c'est la suite des $v_n=x^n$) et de la suite $(0,1,0,\ldots)$.
(iv) Notons que le raisonnement de la question (i), c'est-à-dire la solution de l'exercice II.3.19 de la page 203, est indépendant du corps de base : le $\mathbb{R}$-espace vectoriel F est donc de dimension 2.
Si $p^2+4q>0$ ou $p^2+4q=0$, les suites $\underline{v}$ et $\underline{w}$ étudiées à la question (iii) sont à termes réels et les mêmes arguments que précédemment montrent qu'elles forment une base de F.
Si $p^2+4q<0$, les racines y et z sont complexes conjuguées et l'on peut les écrire : $y=r\mathrm{e}^{\mathrm{i}\theta}$ et $z=r\mathrm{e}^{-\mathrm{i}\theta}$ avec $r>0$ et (par exemple) $\theta\in]0,\pi[$. Les suites $\underline{c}:=\dfrac{1}{2}(\underline{v}+\underline{w})$ et $\underline{s}:=\dfrac{1}{2\mathrm{i}}(\underline{v}-\underline{w})$ forment une base de E, donc sont $\mathbb{C}$-linéairement indépendantes. Elles ont respectivement pour terme général $c_n=r^n\cos n\theta$ et $s_n=r^n\sin n\theta$: ce sont donc des

éléments de F ; comme ces suites sont $\mathbb{C}$-linéairement indépendantes, elles sont *a fortiori* $\mathbb{R}$-linéairement indépendantes et forment donc une base de F.

Exemples.

1. La suite de Fibonacci est définie par $F_0 = 0$, $F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$. L'équation associée $x^2 = x + 1$ a deux racines réelles $\dfrac{1 \pm \sqrt{5}}{2}$. On trouve que $F_n = \dfrac{1}{\sqrt{5}} \left(\left(\dfrac{1+\sqrt{5}}{2} \right)^n - \left(\dfrac{1-\sqrt{5}}{2} \right)^n \right)$.
2. Toute suite $(u_n)_{n \geqslant 0}$ de réels telle que $\forall n \geqslant 0$, $u_{n+2} + u_{n+1} + u_n = 0$ est combinaison linéaire des suites $(\cos 2n\pi/3))_{n \geqslant 0}$ et $(\sin 2n\pi/3)$. En effet, l'équation associée est $x^2 = -x - 1$, dont les racines sont $\mathrm{e}^{\pm \mathrm{i} 2\pi/3}$.
3. Toute suite $(u_n)_{n \geqslant 0}$ de réels telle que $\forall n \geqslant 0$, $u_{n+2} = 2u_{n+1} - u_n$ est de la forme $u_n = a + bn$. En effet, l'équation associée est $x^2 - 2x + 1 = 0$, qui admet 1 pour racine double.

II.5.7 Les éléments neutres $0 = 0 + 0\mathrm{i}$ et $1 = 1 + 0\mathrm{i}$ sont dans $\mathbb{Z}[\mathrm{i}]$.

La différence $(a + \mathrm{i}b) - (a' + \mathrm{i}b') = (a - a') + \mathrm{i}(b - b')$ et le produit $(a + \mathrm{i}b)(a' + \mathrm{i}b') = (aa' - bb') + \mathrm{i}(ab' + a'b)$ de deux éléments de $\mathbb{Z}[\mathrm{i}]$ sont dans $\mathbb{Z}[\mathrm{i}]$. C'est donc bien un sous-anneau de $\mathbb{C}$. Comme $a + \mathrm{i}b \in \mathbb{Z}[\mathrm{i}] \Leftrightarrow a - \mathrm{i}b \in \mathbb{Z}[\mathrm{i}]$, ce sous-anneau est stable par conjugaison. Les normes algébriques des éléments de $\mathbb{Z}[\mathrm{i}]$ forment l'ensemble :

$$\{N(a + \mathrm{i}b) \mid a, b \in \mathbb{Z}\} = \{a^2 + b^2 \mid a, b \in \mathbb{Z}\};$$

ce sont donc exactement les sommes de deux carrés dans $\mathbb{N}$.
Puisque $\mathbb{Z}[\mathrm{i}]$ est stable par multiplication, on déduit de la propriété $N(zz') = N(z)N(z')$ que l'ensemble $\{N(a + \mathrm{i}b) \mid a, b \in \mathbb{Z}\}$ est également stable par multiplication. Pratiquement :

$$(a^2 + b^2)(a'^2 + b'^2) = (aa' - bb')^2 + (ab' + a'b)^2.$$

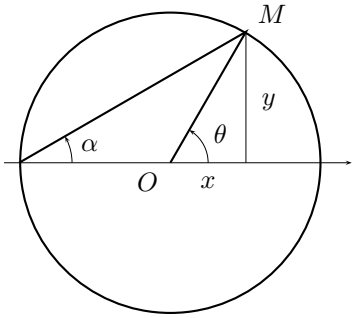
Soit $z \in \mathbb{Z}[\mathrm{i}]$ un entier de Gauß inversible, et soit $z' \in \mathbb{Z}[\mathrm{i}]$ son inverse. Alors $N(z), N(z') \in \mathbb{N}$ et $N(z)N(z') = N(zz') = N(1) = 1$. On a donc $N(z) = 1$. Soit réciproquement $z \in \mathbb{Z}[\mathrm{i}]$ tel que $z\overline{z} = N(z) = 1$. Alors $\overline{z} \in \mathbb{Z}[\mathrm{i}]$, et c'est l'inverse de z, qui est donc un entier de Gauß inversible.
En écrivant $z = a + \mathrm{i}b$, on est conduits à chercher les solutions dans $\mathbb{Z}$ de l'équation $a^2 + b^2 = 1$. On trouve exactement quatre couples : $(\pm 1, 0)$ et $(0, \pm 1)$. Les entiers de Gauß inversibles sont donc ± 1, $\pm \mathrm{i}$.

II.5.8 Les éléments neutres $0 = 0 + 0j$ et $1 = 1 + 0j$ sont dans $\mathbb{Z}[j]$.

La différence $(a + bj) - (a' + b'j) = (a - a') + (b - b')j$ de deux éléments de $\mathbb{Z}[j]$ est dans $\mathbb{Z}[j]$. De l'égalité $j^2 = -j - 1$, on déduit que le produit $(a + bj)(a' + b'j) = (aa' - bb') + (ab' + a'b - bb')j$ de deux éléments de $\mathbb{Z}[j]$ est dans $\mathbb{Z}[j]$. C'est donc bien un sous-anneau de $\mathbb{C}$. De l'égalité $\overline{j} = -j - 1$, on déduit que le conjugué $\overline{a + bj} = (a - b) - bj$ est dans $\mathbb{Z}[j]$, qui est donc stable par conjugaison.
Des égalités $j + \overline{j} = -1$, $j\overline{j} = 1$, on déduit que $N(a + bj) = (a + bj)(a + b\overline{j}) = a^2 - ab + b^2$.

Les normes algébriques des éléments de $\mathbb{Z}[j]$ sont donc exactement les $a^2 - ab + b^2$ pour $a, b \in \mathbb{Z}$, ou encore (quitte à changer b en $-b$), les $a^2 + ab + b^2$ pour $a, b \in \mathbb{Z}$. Comme dans l'exercice précédent, on conclut que l'ensemble des entiers de la forme $a^2 + ab + b^2$ avec $a, b \in \mathbb{Z}$ est stable par multiplication.

II.5.9 Le plus simple est de mettre z sous forme trigonométrique : $z = \rho e^{i\theta}$, $\rho > 0$, $\theta \in]-\pi, \pi[$. On a alors $\operatorname{Arg} z = \theta$, $|z| = \rho$, $\operatorname{Im} z = \rho \sin\theta$ et $\operatorname{Re} z = \rho\cos\theta$. L'égalité à démontrer se réécrit : $2\arctan \dfrac{\rho\sin\theta}{\rho + \rho\cos\theta} = \theta$, soit encore : $\arctan \dfrac{\sin\theta}{1+\cos\theta} = \dfrac{\theta}{2}\cdot$ On observe, d'une part, que $\dfrac{\theta}{2} \in \left]-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right[$; d'autre part, que les égalités $\sin\theta = 2\sin\dfrac{\theta}{2}\cos\dfrac{\theta}{2}$ et $\cos\theta = 2\cos^2\dfrac{\theta}{2} - 1$ entraînent $\dfrac{\sin\theta}{1+\cos\theta} = \tan\dfrac{\theta}{2}$ (on peut simplifier par $\cos\dfrac{\theta}{2}$ car celui-ci est non nul). Comme la fonction $\arctan$ est la réciproque de $\tan : \left]-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right[\to \mathbb{R}$, l'égalité voulue en découle. Cette égalité admet d'ailleurs une interprétation géométrique :



Dans cette figure, $\operatorname{Aff}(M) = z = x + iy$, $\rho = OM$ et $\alpha = \dfrac{\theta}{2}$.

II.5.10 (i) Fixons l'entier n et notons $C(\theta) := \sum_{k=0}^{n} \cos k\theta$ et $S(\theta) := \sum_{k=0}^{n} \sin k\theta$. Alors :

$$W(\theta) := C(\theta) + iS(\theta) = \sum_{k=0}^{n} (\cos k\theta + i\sin k\theta) = \sum_{k=0}^{n} w^k,$$

où l'on a posé $w := \cos\theta + i\sin\theta = e^{i\theta}$. Si $w = 1$, c'est-à-dire si $\theta \equiv 0 \pmod{2\pi}$, la somme vaut $n+1$ et l'on en déduit $C(\theta) = n+1$ et $S(\theta) = 0$. Sinon, on reconnaît la somme partielle d'une série géométrique :

$$W(\theta) = \frac{w^{n+1} - 1}{w - 1} = \frac{e^{i(n+1)\theta} - 1}{e^{i\theta} - 1}\cdot$$

Rappelons la formule bien commode : $e^{i\alpha} - 1 = e^{i\alpha/2}(2i\sin\alpha/2)$; on en déduit ici :

$$W(\theta) = \frac{e^{i(n+1)\theta} - 1}{e^{i\theta} - 1} = \frac{e^{i(n+1)\theta/2}}{e^{i\theta/2}} \frac{2i\sin(n+1)\theta/2}{2i\sin\theta/2} = e^{in\theta/2}\frac{\sin(n+1)\theta/2}{\sin\theta/2}\cdot$$

Notons que les dénominateurs sont non nuls car on a supposé $w \neq 1$, c'est-à-dire $\theta \not\equiv 0 \pmod{2\pi}$. On conclut enfin :

$$C(\theta) = \frac{\cos n\theta/2\ \sin(n+1)\theta/2}{\sin\theta/2} \qquad \text{et} \qquad S(\theta) = \frac{\sin n\theta/2\ \sin(n+1)\theta/2}{\sin\theta/2}\cdot$$

II.5.11 L'expression $\cos^2 x \sin^3 x$ est une fonction impaire de x, sa forme linéarisée ne comportera donc que des sinus. Écrivons $w := \mathrm{e}^{\mathrm{i}x}$. Alors :

$$\cos^2 x \sin^3 x = \left(\frac{w+w^{-1}}{2}\right)^2 \left(\frac{w-w^{-1}}{2\mathrm{i}}\right)^3 = \frac{\mathrm{i}}{32}(w^2+2+w^{-2})(w^3-3w+3w^{-1}-w^{-3}) =$$

$$\frac{\mathrm{i}}{32}(w^5 - w^3 - 2w + 2w^{-1} + w^{-3} - w^{-5}) = \frac{1}{16}(-\sin 5x + \sin 3x + 2\sin x).$$

II.5.12 Il s'agit de démontrer que *la fonction* $\exp$ *est un morphisme surjectif du groupe additif* $\mathbb{C}$ *sur le groupe multiplicatif* $\mathbb{C}^*$*, de noyau* $2\mathrm{i}\pi\mathbb{Z}$, sachant que *la* fonction exponentielle complexe $z \mapsto \exp z = \mathrm{e}^z$ *de* $\mathbb{C}$ *dans* $\mathbb{C}^*$ *est définie par la formule :*

$$\exp(x + \mathrm{i}y) := \mathrm{e}^x\,(\cos y + \mathrm{i}\sin y).$$

Pour vérifier que $\exp$ est un morphisme, on doit prouver la formule :

$$\exp(z + z') = \exp(z)\exp z'.$$

Notant $z = x + \mathrm{i}y$ et $z' = x' + \mathrm{i}y'$, on est ramené à prouver l'égalité :

$$\mathrm{e}^{x+x'}\,(\cos(y+y') + \mathrm{i}\sin(y+y')) = \mathrm{e}^x\,(\cos y + \mathrm{i}\sin y)\,\mathrm{e}^{x'}\,(\cos y' + \mathrm{i}\sin y')\,.$$

Or, on sait que $\mathrm{e}^{x+x'} = \mathrm{e}^x\mathrm{e}^{x'}$ (cours de terminale) ; et l'égalité :

$$(\cos(y+y') + \mathrm{i}\sin(y+y')) = (\cos y + \mathrm{i}\sin y)\,(\cos y' + \mathrm{i}\sin y')$$

découle des formules d'addition :

$$\cos(y+y') = \cos y\cos y' - \sin y \sin y' \qquad \text{et} \qquad \sin(y+y') = \sin y\cos y' + \cos y \sin y'.$$

Pour vérifier que ce morphisme est surjectif, on doit prouver que, pour tout couple (X, Y) de réels non tous deux nuls, il existe $x, y \in \mathbb{R}$ tels que $X = \mathrm{e}^x \cos y$ et $Y = \mathrm{e}^x \sin y$. Ces égalités équivalent à $\mathrm{e}^x = \sqrt{X^2+Y^2}$ et $\cos y = X' := \dfrac{X}{\sqrt{X^2+Y^2}}$, $\sin y = Y' := \dfrac{Y}{\sqrt{X^2+Y^2}}$ (on peut en effet diviser par $\sqrt{X^2+Y^2}$). On prendra donc $x = \log\sqrt{X^2+Y^2}$, puis l'on résoudra $\cos y = X'$, $\sin y = Y'$, ce qui est possible puisque $X'^2 + Y'^2 = 1$.
Reste à déterminer le noyau, c'est-à-dire à résoudre l'équation $\exp z = 1$, ou encore le système $\mathrm{e}^x\cos y = 1$, $\mathrm{e}^x \sin y = 0$. D'après le calcul ci-dessus, $x = \log 1 = 0$, et $\cos y = 1$, $\sin y = 0$, d'où $y \equiv 0 \pmod{2\pi}$. Les éléments du noyau sont donc les complexes $x + \mathrm{i}y = 0 + \mathrm{i}(2k\pi)$, $k \in \mathbb{Z}$, et le noyau est bien le groupe $2\mathrm{i}\pi\mathbb{Z}$.

II.5.13 Posons, comme le suggère l'énoncé, $f(z) := \mathrm{e}^{\mathrm{i}\theta(z)/2}$.

On aurait alors $\big(f(z)\big)^2 = \mathrm{e}^{\mathrm{i}\theta(z)} = z$ et :

$$f(zz') = \mathrm{e}^{\mathrm{i}\theta(zz')} = \mathrm{e}^{\mathrm{i}\left(\theta(z)+\theta(z')\right)} = \mathrm{e}^{\mathrm{i}\theta(z)}\mathrm{e}^{\mathrm{i}\theta(z')} = f(z)f(z'),$$

autrement dit, on a une fonction « racine carrée » qui est un morphisme. On a vu dans le cours que cela n'est pas possible.
Voici une preuve directe inspirée de la discussion du cours : on écrit d'abord que $\theta(1) = \theta(1.1) = \theta(1) + \theta(1) = 2\theta(1)$, d'où $\theta(1) = 0$; puis :

$$0 = \theta(1) = \theta\big((-1).(-1)\big) = \theta(-1) + \theta(-1) = 2\theta(-1),$$

d'où $\theta(-1) = 0$. Mais cela contredit l'égalité $\mathrm{e}^{\mathrm{i}\theta(-1)} = -1$.

II.5.14 (i) Notons $\varphi(z) := \dfrac{z-\mathrm{i}}{z+\mathrm{i}}$ et $\psi(w) := \mathrm{i}\dfrac{1+w}{1-w}$. L'application φ est définie sur $\mathbb{C}\setminus\{-\mathrm{i}\}$, et son image est incluse dans $\mathbb{C}\setminus\{1\}$, car $\varphi(z)-1 = \dfrac{-2\mathrm{i}}{z+\mathrm{i}} \neq 0$. De même, l'application ψ est définie sur $\mathbb{C}\setminus\{1\}$, et son image est incluse dans $\mathbb{C}\setminus\{-\mathrm{i}\}$, car $\psi(w)+\mathrm{i} = \dfrac{2\mathrm{i}}{1-w} \neq 0$. On peut donc composer ψ et φ dans n'importe quel ordre ; on trouve :

$$\psi\big(\varphi(z)\big) = \mathrm{i}\frac{1+\dfrac{z-\mathrm{i}}{z+\mathrm{i}}}{1-\dfrac{z-\mathrm{i}}{z+\mathrm{i}}} = \mathrm{i}\frac{2z}{2\mathrm{i}} = z$$

et

$$\varphi\big(\psi(w)\big) = \frac{\mathrm{i}\dfrac{1+w}{1-w}-\mathrm{i}}{\mathrm{i}\dfrac{1+w}{1-w}+\mathrm{i}} = \frac{(1+w)-(1-w)}{(1+w)+(1-w)} = w,$$

ce qui montre que φ et ψ sont des bijections réciproques l'une de l'autre entre les ensembles $\mathbb{C}\setminus\{-\mathrm{i}\}$ et $\mathbb{C}\setminus\{1\}$.
(ii) Notons A et B les points du plan d'affixes respectives i et $-\mathrm{i}$. La médiatrice Δ du segment AB est l'axe des réels, et un point M est plus proche de A que de B si, et seulement s'il est dans le demi-plan bordé par Δ qui contient A. Autrement dit, $|z-\mathrm{i}| < |z+\mathrm{i}| \Leftrightarrow z \in \mathcal{H}$. On a donc démontré l'équivalence : $|\varphi(z) \in \mathcal{D}| \in\!\!\Leftrightarrow z \in \mathcal{H}$. Ainsi, φ réalise une bijection de $\mathcal{H}$ sur $\mathcal{D}$ (et ψ réalise la bijection réciproque).

II.5.15 (i) Notons A et B les points du plan d'affixes respectives 1 et -1. La médiatrice Δ du segment AB est l'axe des imaginaires, et le point M d'affixe $\mathrm{i}x$ est équidistant de A et de B (*i.e.* $\left|\dfrac{1+\mathrm{i}x}{1-\mathrm{i}x}\right| = 1$) si, et seulement si, $\mathrm{i}x$ est imaginaire pur, c'est-à-dire si, et seulement si, x est réel.

(ii) Puisque a est réel, $\left|\dfrac{1+\mathrm{i}a}{1-\mathrm{i}a}\right| = 1$, et toute racine x de l'équation vérifie de même $\left|\dfrac{1+\mathrm{i}x}{1-\mathrm{i}x}\right| = 1$, donc est réelle d'après la question (i).

On peut écrire $a = \tan\alpha$, $\alpha \in]-\pi/2, \pi/2[$, d'où $\dfrac{1+\mathrm{i}a}{1-\mathrm{i}a} = \mathrm{e}^{2\mathrm{i}\alpha}$.

De même, on peut écrire $x = \tan\theta$, $\theta \in]-\pi/2, \pi/2[$, d'où $\dfrac{1+\mathrm{i}x}{1-\mathrm{i}x} = \mathrm{e}^{2\mathrm{i}\theta}$.

Les racines x vérifient donc $\mathrm{e}^{2\mathrm{i}n\theta} = \mathrm{e}^{2\mathrm{i}\alpha}$, soit $2\theta \equiv 2\alpha/n + 2k\pi/n \pmod{2\pi}$, $k \in [\![0, n-1]\!]$. Notons $x_k = \tan\dfrac{\alpha+k\pi}{n}$. Pour $k \in [\![0, n-1]\!]$, les $\dfrac{\alpha+k\pi}{n}$ sont deux à deux distincts dans l'intervalle $[\alpha/n, \alpha/n+\pi[$ et les $x_k = \tan\dfrac{\alpha+k\pi}{n}$ sont deux à deux distincts (car la fonction $\tan$ est injective sur un tel intervalle). Si tous les x_k sont définis, l'équation donnée a donc n racines (qui sont $x_0, \ldots, x_{n-1}$).

Le seul cas où l'un des x_k n'est pas défini est celui où l'un des $\dfrac{\alpha+k\pi}{n}$ vaut $\pi/2$

$(\mathrm{mod}\ \pi)$; vu le choix de α, cela équivaut à $\dfrac{\alpha + k\pi}{n} = \dfrac{\pi}{2}$, soit $\alpha = n\pi/2 - k\pi$, soit encore $\dfrac{1+\mathrm{i}a}{1-\mathrm{i}a} = \mathrm{e}^{2\mathrm{i}\alpha} = (-1)^n$. Dans ce cas, parmi les racines $n^{\textit{èmes}}$ de $(-1)^n$, figure -1 qui n'est pas de la forme $\dfrac{1+\mathrm{i}x}{1-\mathrm{i}x}$. Il n'y a alors que $n-1$ racines, qui sont ceux des x_k qui sont bien définis. Comme la limite de $\dfrac{1+\mathrm{i}x}{1-\mathrm{i}x}$ est -1 lorsque x tend vers l'infini, on dit parfois par abus qu'il y a encore n racines mais que l'une d'entre elles est infinie.

II.5.16 Notons $\varphi_{a,b}(z) := az + b$.

Le groupe des similitudes est donc $G := \{\varphi_{a,b} \mid a \in \mathbb{C}^*, b \in \mathbb{C}\}$. L'application $(a,b) \mapsto \varphi_{a,b}$ est une bijection de $\mathbb{C}^* \times \mathbb{C}$ sur G. De plus, $\varphi_{a,b}\big(\varphi_{a',b'}(z)\big) = a(a'z+b')+b = aa'z+(ab'+b)$, d'où $\varphi_{a,b} \circ \varphi_{a',b'} = \varphi_{aa',ab'+b} = \varphi_{(a,b)\star(a',b')}$. L'application $(a,b) \mapsto \varphi_{a,b}$ est donc un isomorphisme de $(\mathbb{C}^* \times \mathbb{C}, \star)$ sur le groupe G ; cela entraîne d'ailleurs automatiquement que $(\mathbb{C}^* \times \mathbb{C}, \star)$ est bien un groupe.

II.5.17 L'inégalité donnée est obtenue à partir de l'inégalité :

$$\left|\sum_{n=0}^{N} \frac{z^n}{(n+2)!}\right| \leqslant \sum_{n=0}^{N} \left|\frac{z^n}{(n+2)!}\right|$$

(qui découle de l'inégalité du triangle) par passage à la limite lorsque $N \to +\infty$. La majoration à démontrer est :

$$\forall z \in \mathbb{C}^*\ ,\ 0 < |z| \leqslant M \quad \Longrightarrow \quad \left|\frac{\exp z - 1 - z}{z^2}\right| \leqslant \exp M. \tag{38}$$

Le membre gauche de cette inégalité est $\left|\sum\limits_{n\geqslant 0} \dfrac{z^n}{(n+2)!}\right|$, qui est donc majoré par $\sum\limits_{n\geqslant 0} \left|\dfrac{z^n}{(n+2)!}\right|$, donc par $\sum\limits_{n\geqslant 0} \dfrac{M^n}{(n+2)!}$ (hypothèse $|z| \leqslant M$), donc par $\exp M = \sum\limits_{n\geqslant 0} \dfrac{M^n}{n!}$ (car $\dfrac{1}{(n+2)!} \leqslant \dfrac{1}{n!}$).

II.5.18 Supposons que la fonction $f : \mathbb{R} \to \mathbb{R}$ est telle que $f(0) = 1$ et $f' = f$ et posons $g(x) = f(x)\mathrm{e}^{-x}$. Alors $g(0) = 1$ et $g'(x) = \big(f'(x) - f(x)\big)\mathrm{e}^{-x} = 0$; l'application g est donc la constante 1 et f la fonction exponentielle.

II.5.19 La proposition dit : *La fonction* $\exp$ *est un morphisme surjectif du groupe additif* $\mathbb{C}$ *sur le groupe multiplicatif* $\mathbb{C}^*$*, de noyau* $2\mathrm{i}\pi\mathbb{Z}$. Nous invoquons le théorème 21 de la page 270 : il entraîne que la fonction $\exp$ est un morphisme. On a donc en particulier $\exp(x + \mathrm{i}y) = \exp(x)\exp(\mathrm{i}y)$. D'après le théorème 22 de la page 270, $\exp x = \mathrm{e}^x$ (exponentielle réelle) : on sait que cette fonction prend toute valeur réelle strictement positive. D'après le théorème suivant du cours, $\exp(\mathrm{i}y)$ prend toute valeur de module 1. Comme

tout complexe non nul s'écrit comme produit d'un réel strictement positif et d'un complexe de module 1, la fonction $\exp$ est surjective de $\mathbb{C}$ sur $\mathbb{C}^*$. Pour déterminer son noyau, on résout $\exp(x+\mathrm{i}y) = \exp(x)\exp(\mathrm{i}y) = 1$. D'après ce qui précède, cela entraîne $\mathrm{e}^x = 1$, donc $x = 0$, et $\exp(\mathrm{i}y) = 1$, donc, d'après le dernier théorème invoqué, $y \in 2\pi\mathbb{Z}$. Le noyau est donc $2\mathrm{i}\pi\mathbb{Z}$.

Module II.6 : Polynômes et fractions rationnelles

II.6.1 Tout d'abord, l'application $\varphi_a : P \mapsto P(X+a)$ est évidemment linéaire et admet φ_{-a} pour réciproque ; de plus, elle ne change pas le degré. C'est donc bien un automorphisme du K-espace vectoriel $K_n[X]$, et l'application $\Phi : a \mapsto \varphi_a$ va de K dans $\mathcal{GL}(K_n[X])$. Comme $\varphi_{a+b}(P) = P(X+a+b)$ et comme $\varphi_a \circ \varphi_b(P) = \varphi_a\big(P(X+b)\big) = P(X+a+b)$, on a $\varphi_{a+b} = \varphi_a \circ \varphi_b$ et Φ est un morphisme du groupe $(K,+)$ dans le groupe $(\mathcal{GL}(K_n[X]), \circ)$. On reconnaît dans M_a la matrice de l'automorphisme φ_a dans la base canonique $\mathcal{B} := (1, X, \dots, X^n)$ de $K_n[X]$ (module II.7).

Du développement du binôme : $(X+a)^k = \sum_{i=0}^{k} \binom{k}{i} a^{k-i} X^i$, on tire :

$$M_a = \begin{pmatrix} 1 & a & a^2 & \dots & a^n \\ 0 & 1 & 2a & \dots & na^{n-1} \\ 0 & 0 & 1 & \dots & \dfrac{n(n-1)}{2} a^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Il sera commode d'indexer ces coefficients par $[\![0,n]\!]^2$; pour $0 \leqslant i,j \leqslant n$, le coefficient d'indices (i,j) de M_a vaut donc 0 si $i > j$, et $\binom{j}{i} a^{j-i}$ si $i \leqslant j$.

Puisque $\varphi_{a+b} = \varphi_a \circ \varphi_b$, on a $M_{a+b} = M_a M_b$, et l'application $a \mapsto M_a$ est un morphisme du groupe additif K dans le groupe linéaire $GL_{n+1}(K)$. On peut le vérifier par le calcul. Le coefficient d'indices (i,j) de $M_a M_b$ est :

$$(M_a M_b)_{i,j} = \sum_{k=0}^{n} (M_a)_{i,k} (M_b)_{k,j} = \sum_{i \leqslant k \leqslant j} \binom{k}{i} a^{k-i} \binom{j}{k} b^{j-k},$$

qui est nul si $j < i$ et vaut $\left(\sum_{i \leqslant k \leqslant j} \binom{k}{i}\binom{j}{k} \right) a^{k-i} b^{j-k}$ si $i \leqslant j$. Pour ce calcul, nous ferons les changements d'indice $l := k - i$ et $p := j - i$ (qui est donc positif ou nul) :

$$\begin{aligned} \sum_{i \leqslant k \leqslant j} \binom{k}{i}\binom{j}{k} a^{k-i} b^{j-k} &= \sum_{i \leqslant k \leqslant j} \frac{k!}{i!(k-i)!} \frac{j!}{k!(j-k)!} a^{k-i} b^{j-k} \\ &= \sum_{i \leqslant k \leqslant j} \frac{j!}{i!(k-i)!(j-k)!} a^{k-i} b^{j-k} \\ &= \frac{j!}{i!} \sum_{i \leqslant k \leqslant j} \frac{1}{(k-i)!(j-k)!} a^{k-i} b^{j-k} \\ &= \frac{j!}{i!} \sum_{l=0}^{p} \frac{1}{l!(p-l)!} a^l b^{k-l} \\ &= \frac{j!}{i!(j-i)!} \sum_{l=0}^{p} \frac{p!}{l!(p-l)!} a^l b^{k-l} \\ &= \frac{j!}{i!(j-i)!} (a+b)^p = \binom{j}{i} (a+b)^{j-i}. \end{aligned}$$

On a bien $M_{a+b} = M_a M_b$.

II.6.2 Il est évident que l'application Δ_a est linéaire, et, d'après l'exercice II.6.1, qu'elle envoie l'espace vectoriel $K_n[X]$ dans lui-même. De plus, les polynômes $P(X)$ et $P(X+a)$ ayant même terme dominant, $\deg P \leqslant n \Rightarrow \deg\big(P(X+a)-P(X)\big) \leqslant n-1$, et Δ_a envoie $K_n[X]$ dans $K_{n-1}[X]$.

Si K est de caractéristique nulle, les polynômes de Newton $N_n := \binom{X}{n}$ sont bien définis.

On a $N_0 = 1$, donc $\Delta_1(N_0) = 0$. Pour $n \geqslant 1$:

$$\begin{aligned}\Delta_1(N_n) &= \frac{(X+1)X\cdots(X-n+2)}{n!} - \frac{X(X-1)\cdots(X-n+1)}{n!}\\ &= \big((X+1)-(X-n+1)\big)\frac{X(X-1)\cdots(X-n+2)}{n!}\\ &= n\frac{X(X-1)\cdots(X-n+2)}{n!}\\ &= \frac{X(X-1)\cdots(X-n+2)}{(n-1)!} = N_{n-1}.\end{aligned}$$

L'image de la base $(N_0, N_1, \ldots, N_n)$ de $K_n[X]$ est donc la famille $(0, N_0, \ldots, N_{n-1})$ de $K_{n-1}[X]$. On en déduit que $\operatorname{Ker}\Delta_1 = \operatorname{Vect}(N_0) = K$ et que $\operatorname{Im}\Delta_1 = K_{n-1}[X]$.
Puisque les valeurs du polynôme P_k sont imposées sur l'ensemble infini $\mathbb{N}^*$, il est unique s'il existe. La relation : $\forall n \in \mathbb{N}^*\ ,\ P_k(n) = 1^k + \cdots + n^k$ équivaut à : $P_k(1) = 1$ et $\forall n \in \mathbb{N}^*\ ,\ P_k(n+1) - P_k(n) = (n+1)^k$ (démonstration immédiate par récurrence). La deuxième relation impose les valeurs de $\Delta_1(P_k)$ sur l'ensemble infini $\mathbb{N}^*$, donc elle équivaut à l'égalité $\Delta_1(P_k) = (X+1)^k$. D'après le début de cet exercice, il existe des polynômes de $\mathbb{K}_{k+1}[X]$ dont l'image par Δ_1 est $(X+1)^k$, et ils sont définis à une constante près ; il en existe donc un unique tel que $1 \mapsto 1$, et c'est le polynôme P_k recherché.
Pour préciser son terme dominant, on écrit $(X+1)^k$ dans la base des polynômes de Newton : $(X+1)^k = C_0 N_0 + \cdots + C_k N_k$. La comparaison des coefficients dominants montre que $C_k = k!$. L'étude de Δ_1 montre que $P_k = C + C_0 N_1 + \cdots + C_k N_{k+1}$, où la constante C est à déterminer. Le coefficient dominant est donc $k!\dfrac{1}{(k+1)!} = \dfrac{1}{k+1}$, comme prévu. Pour déterminer la constante, on écrit $1 = P_k(1) = C + C_0 N_1(1) + \cdots + C_k N_{k+1}(1) = C + C_0$ (car $N_1(1) = 1$ et $N_n(1) = 0$ pour $n \geqslant 2$). En fait, on a $C_0 = 1$ (prendre $X = 0$), d'où $C = 0$.
À titre d'exemple, calculons P_2. On trouve d'abord que $(X+1)^2 = N_0 + 3N_1 + 2N_2$, donc $P_2 = N_1 + 3N_2 + 2N_3 = \dfrac{X(X+1)(2X+1)}{6}$, d'où la formule connue :

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

II.6.3 Écrivons $n = qm + r$, avec $q \in \mathbb{N}$ et $r \in [\![0, m-1]\!]$.

Alors $X^n - 1 = X^r \dfrac{X^{qm}-1}{X^m-1}(X^m-1) + X^r - 1$, et le quotient et le reste de la division

euclidienne de X^n-1 par X^m-1 sont respectivement $X^r\dfrac{X^{qm}-1}{X^m-1}$ (qui est bien un polynôme !) et X^r-1.
Soient $n_0:=n$, $n_1:=m$, $\ldots, n_k\neq 0$, $n_{k+1}=0$ les entiers qui apparaissent au cours d'une exécution de l'algorithme d'Euclide appliqué à n et m. Alors les polynômes qui apparaissent au cours d'une exécution de l'algorithme d'Euclide appliqué à X^n-1 et X^m-1 sont $X^{n_0}-1=X^n-1$, $X^{n_1}-1=X^m-1$, $\ldots, X^{n_k}-1$ (le pgcd), $X^{n_{k+1}}-1=0$.

II.6.4 Si A et B ne sont pas étrangers, on peut écrire $A=\Delta A_1$, $B=\Delta B_1$ avec $\deg\Delta\geqslant 1$, donc $\deg A_1\leqslant n-1$ et $\deg B_1\leqslant p-1$. Il suffit alors de prendre $P:=B_1$ et $Q:=-A_1$.
Si A et B sont étrangers, de la relation $AP+BQ=0$, on tire $A\mid BQ$, donc, par hypothèse et d'après le lemme de Gauß, $A\mid Q$. Comme $\deg Q<\deg A$, cela entraîne $Q=0$, puis $AP=0$ et (par intégrité) $P=0$.
Écrivons $P=\lambda_0+\lambda_1X+\cdots+\lambda_{p-1}X^{p-1}$ et $Q=\mu_0+\mu_1X+\cdots+\mu_{n-1}X^{n-1}$. La relation $AP+BQ=0$ équivaut à :

$$\lambda_0A+\lambda_1(XA)+\cdots+\lambda_{p-1}(X^{p-1}A)+\mu_0B+\mu_1(XB)+\cdots+\mu_{n-1}(X^{n-1}B)=0,$$

ce qui est la relation linéaire voulue (en rectifiant le q de l'énoncé, qui est en fait n) ; et l'on a $(\lambda_0,\lambda_1,\ldots,\lambda_{p-1},\mu_0,\mu_1,\ldots,\mu_{n-1})\neq 0$ si, et seulement si, P et Q ne sont pas tous deux nuls.
La matrice de la famille $(A,XA,\ldots,X^{p-1}A,B,XB,\ldots,X^{q-1}B)$ dans la base canonique de $K_{n+p-1}[X]$ est la matrice $S(A,B)$, et il découle du cours d'algèbre linéaire qu'elle est inversible si, et seulement si, cette famille est libre, c'est-à-dire si A et B sont premiers entre eux.

> ***Remarque***. La matrice $S(A,B)$ est également celle de l'application linéaire $(P,Q)\mapsto AP+BQ$ de $K_{p-1}[X]\times K_{n-1}[X]$ dans $K_{n+p-1}[X]$, l'espace but étant muni de la base canonique et l'espace source étant muni de la base obtenue à partir des bases canoniques, *i.e.* $\big((1,0),\ldots,(X^{p-1},0),(0,1),\ldots,(0,X^{n-1})\big)$.

II.6.5 Suivant les indications, on écrit $x=\dfrac{p}{q}$ avec $p\in\mathbb{Z}$, $q\in\mathbb{N}^*$ et $p\wedge q=1$. La relation $P(x)=0$ entraîne (en chassant les dénominateurs) $p^n+a_{n-1}p^{n-1}q+\cdots+a_nq^n=0$, d'où $q\mid p^n$. Comme $p\wedge q=1$, l'application répétée du lemme de Gauß permet de déduire que $q=1$, donc $x\in\mathbb{Z}$.
Les nombres donnés sont respectivement racines des polynômes unitaires et à coefficients entiers X^2-2, X^2-3 et $(X^2-5)^2-24$. Si $\sqrt{2}$, $\sqrt{3}$ ou $\sqrt{2}+\sqrt{3}$ étaient rationnels, ils seraient donc entiers. Or, les calculs approchés $\sqrt{2}\approx 1{,}414$, $\sqrt{3}\approx 1{,}732$ et $\sqrt{2}+\sqrt{3}\approx 3{,}146$ *démontrent* que $1<\sqrt{2}<2$, $1<\sqrt{3}<2$ et $3<\sqrt{2}+\sqrt{3}<4$: ce ne sont donc pas des entiers.

II.6.6 (i) Si $P\in\mathbb{Q}[X]$, il est évident que $P(\mathbb{Z})\subset\mathbb{Q}$. Soit réciproquement $P\in\mathbb{C}[X]$ tel que $P(\mathbb{Z})\subset\mathbb{Q}$, et notons $n:=\deg P$ et $L_0,\ldots,L_n$ les polynômes d'interpolation de Lagrange aux points $0,1,\ldots,n$: il est clair, d'après les formules données dans le cours, que $L_0,\ldots,L_n\in\mathbb{Q}[X]$. Comme $P=\sum_{i=0}^{n}P(i)L_i$, on a bien $P\in\mathbb{Q}[X]$.

(ii) Notons $\binom{X}{n}(k)$ la valeur du polynôme de Newton $\binom{X}{n}$ en k et $\binom{p}{q} := \dfrac{p!}{q!(p-q)!}$ les coefficients binomiaux, *a priori* définis pour $0 \leqslant q \leqslant p$. Le lecteur prouvera sans peine les (utiles) égalités suivantes :

$$\forall n \in \mathbb{N}\ ,\ \forall k \in \mathbb{Z}\ ,\ \binom{X}{n}(k) = \begin{cases} \binom{k}{n} \text{ si } k \geqslant n, \\ 0 \text{ si } 0 \leqslant k < n, \\ (-1)^n \binom{-k+n-1}{n} \text{ si } k < 0. \end{cases}$$

Ainsi, chaque polynôme de Newton $\binom{X}{n}$ prend sur $\mathbb{Z}$ des valeurs entières. Avec les notations de l'énoncé, si les $a_n \in \mathbb{Z}$, on a donc bien $P(\mathbb{Z}) \subset \mathbb{Z}$.
Supposons réciproquement que $P(\mathbb{Z}) \subset \mathbb{Z}$. On calcule d'abord $P(0) = a_0 \in \mathbb{Z}$: le polynôme $P_1 := \sum\limits_{n \geqslant 1} a_n \binom{X}{n}$ envoie donc également $\mathbb{Z}$ dans $\mathbb{Z}$. On calcule alors $P(1) = a_1 \in \mathbb{Z}$: le polynôme $P_2 := \sum\limits_{n \geqslant 2} a_n \binom{X}{n}$ envoie donc également $\mathbb{Z}$ dans $\mathbb{Z}$. Itérant ce procédé, on trouve que tous les a_k sont entiers.

II.6.7 Si C désigne le vecteur colonne des coefficients d'un polynôme P de $K_{n-1}[X]$, c'est-à-dire le vecteur colonne de ses coordonnées dans la base canonique de $K_{n-1}[X]$, on a $AC = \begin{pmatrix} P(x_1) \\ \vdots \\ P(x_n) \end{pmatrix}$. La $j^{ème}$ colonne de AB est donc $\begin{pmatrix} L_j(x_1) \\ \vdots \\ L_j(x_n) \end{pmatrix}$, qui est le $j^{ème}$ vecteur de la base canonique de K^n. On a donc bien $AB = I_n$.

II.6.8 Le polynôme $\sum\limits_{i=1}^{n} P(x_i)L_i$ est de degré inférieur ou égal à $n-1$ et prend les mêmes valeurs que P en $x_1, \ldots, x_n$. Si $\deg P \leqslant n-1$, on a donc $P = \sum\limits_{i=1}^{n} P(x_i)L_i$.

Si $\deg P \leqslant n-2$, on voit que le terme de degré $n-1$ de $\sum\limits_{i=1}^{n} P(x_i)L_i$ est nul. Comme le coefficient de degré $n-1$ de L_i est $\dfrac{1}{\omega'(x_i)}$, on a bien $\sum\limits_{i=1}^{n} \dfrac{P(x_i)}{\omega'(x_i)} = 0$.
Le même raisonnement appliqué à X^{n-1} (identification des coefficients de degré $n-1$) donne l'égalité : $\sum\limits_{i=1}^{n} \dfrac{x_i^{n-1}}{\omega'(x_i)} = 1$.
Le lecteur est invité à vérifier ces égalités lorsque $\omega := (X-a)(X-b)$ et lorsque $\omega := (X-a)(X-b)(X-c)$.

II.6.9 Les racines de $X^2 - 2X\cos\theta + 1 = (X - \cos\theta)^2 + \sin^2\theta$ sont $\mathrm{e}^{\mathrm{i}\theta}$ et $\mathrm{e}^{-\mathrm{i}\theta}$. Si $\theta \not\equiv 0 \pmod{\pi}$, elles sont distinctes, et, pour qu'un polynôme P soit multiple de $X^2 - 2X\cos\theta + 1$, il faut, et il suffit, que $P(\mathrm{e}^{\mathrm{i}\theta}) = P(\mathrm{e}^{-\mathrm{i}\theta}) = 0$. Pour un polynôme à coefficients réels, il suffit

même de vérifier que $P(\mathrm{e}^{\mathrm{i}\theta}) = 0$ (puisque $\mathrm{e}^{-\mathrm{i}\theta}$ est le conjugué de $\mathrm{e}^{\mathrm{i}\theta}$). Appliquons ce critère à $X^n \sin\theta - X \sin n\theta + \sin(n-1)\theta$, qui est un polynôme à coefficients réels :

$$\begin{aligned}\mathrm{e}^{ni\theta}\sin\theta - \mathrm{e}^{\mathrm{i}\theta}\sin n\theta + \sin(n-1)\theta = \ & (\cos n\theta \sin\theta - \cos\theta \sin n\theta + \sin(n-1)\theta) \\ & + \mathrm{i}(\sin n\theta \sin\theta - \sin\theta \sin n\theta) = 0,\end{aligned}$$

en vertu de la formule $\sin(a-b) = \sin a \cos b - \cos a \sin b$, appliquée à $a = n\theta$ et $b = \theta$.
Si $\theta \not\equiv 0 \pmod{\pi}$, les deux racines sont confondues et le critère précédent n'est plus correct : il faudrait en principe utiliser la condition $P(\mathrm{e}^{\mathrm{i}\theta}) = P'(\mathrm{e}^{\mathrm{i}\theta}) = 0$. En fait, dans ce cas, $\sin\theta = \sin n\theta = \sin(n-1)\theta = 0$ et $X^n \sin\theta - X \sin n\theta + \sin(n-1)\theta$ est nul.

II.6.10 Comme p est premier, les $\binom{p}{n}$ sont multiples de p pour $1 \leqslant n \leqslant p-1$. On a donc $(X+1)^p = X^p + 1$ dans $K[X]$, d'où :

$$\Delta_1(X^p - X) = \big((X+1)^p - (X+1)\big) - (X^p - X) = 0.$$

Par ailleurs, si $P = \sum a_i X^i$, un calcul direct permettrait de prouver que l'on ne peut avoir $\Delta_1(P) = X^{p-1}$. Voici une méthode plus amusante. De manière générale, si $\Delta_1(P) = Q$, on a :

$$\sum_{i=0}^{p-1} Q(i) = \sum_{i=0}^{p-1} \big(P(i+1) - P(i)\big) = P(p) - P(0) = 0,$$

puisque $p = 0$ dans K. Mais, si $Q = X^{p-1}$:

$$\sum_{i=0}^{p-1} Q(i) = \sum_{i=0}^{p-1} i^{p-1} = \sum_{i=1}^{p-1} 1 = p - 1 = -1,$$

puisque les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ vérifient $x^{p-1} = 1$.
On ne peut donc avoir $\Delta_1(P) = X^{p-1}$.

II.6.11 *Il faut légèrement rectifier l'exposant de* $\mathrm{cd}(A)$ *; la formule correcte est :* $\big(\mathrm{cd}(A)\big)^k B = QA + R$, *où* $k := \max(0, \deg B - \deg A + 1)$.

Écrivons $A = aX^n + \cdots$ et $B = bX^p + \cdots$ (les points désignent des termes de degrés inférieurs). Si $p < n$, on peut prendre $Q := 0$ et $R := B$. Sinon, on fait une récurrence sur $p - n$. Si $p - n = 0$, on voit que $\deg(aB - b_p A) < n$, et l'on peut prendre $k := 1$, $Q := b$ et $R := aB - bA$. Si $p - n \geqslant 1$, on voit de même que $\deg(aB - bX^{p-n}A) < p$, et l'on peut appliquer l'hypothèse de récurrence à $B_1 := aB - bX^{p-n}A$. On écrit $a^{p-n}B_1 = Q_1 A + R_1$, avec $\deg R_1 < n$, et l'on en déduit $a^{p-n+1}B = QA + R$, avec $Q = a^{p-n}bX^{p-n} + Q_1$ et $R := R_1$.

Si $\mathrm{cd}(A)$ est inversible, on a bien sûr $B = \big(\mathrm{cd}(A)\big)^{-k} Q + \big(\mathrm{cd}(A)\big)^{-k} R$, qui répond aux conditions. Si l'on avait deux telles écritures $B = Q_1 A + R_1 = Q_2 A + R_2$, on aurait $\deg A(Q_1 - Q_2) < \deg A$; mais, si $Q_1 - Q_2 \neq 0$, le coefficient dominant de $A(Q_1 - Q_2)$ est $\mathrm{cd}(A)\,\mathrm{cd}(Q_1 - Q_2)$, car $\mathrm{cd}(A)$ n'est pas un diviseur de 0, le degré de $A(Q_1 - Q_2)$ est au moins celui de A ; on a donc nécessairement $Q_1 = Q_2$ puis $R_1 = R_2$, d'où l'unicité.

II.6.12 De l'égalité $(X+P)^n - X^n = P\sum_{i=1}^{n}\binom{n}{i}P^{i-1}X^{n-i}$, on tire, par combinaison linéaire, que $P(X+P)-P(X)$ est un multiple de $P = P(X)$, donc que $P \mid P(X+P)$. Si $\deg P \geqslant 2$, alors $\deg P(X+P) = (\deg P)^2 > \deg P$, et $P(X+P)$ ne peut donc être irréductible. Si $P = aX + b$, $P(X+P) = a(a+1)X + (ab+b)$, qui est constant (et donc n'est pas irréductible) si $a \in \{0, -1\}$. Ainsi, $P(X+P)$ est irréductible si, et seulement si, P est de degré 1 et de coefficient dominant différent de -1.

II.6.13 Dans l'exercice sur les quaternions (module II.5), nous avons calculé la norme algébrique $z\overline{z}$; il résulte de ce calcul que, si $z := b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, alors $z^2 = -(b^2+c^2+d^2)$. Tous les $b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ tels que $b^2+c^2+d^2 = -1$ sont donc racines du polynôme X^2+1.
Le calcul des produits $\mathbf{ij}$, etc, montre que $G := \{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ est un sous-groupe d'ordre 8 du groupe multiplicatif $\mathbf{H}^*$. Mais ses éléments autres que 1 sont d'ordre 2 (pour -1) ou 4 (pour $\pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}$) ; aucun n'est donc générateur, et G n'est pas cyclique. En fait, G n'est même pas commutatif, puisque $\mathbf{ij} \neq \mathbf{ji}$.

II.6.14 (i) Rappelons que, le groupe K^* ayant $q-1$ éléments, chaque élément a de ce groupe vérifie $a^{q-1} = 1$. Le polynôme unitaire $X^{q-1}-1$, qui est de degré $q-1$, admet donc les $q-1$ éléments de K^* comme racines ; il n'a donc pas d'autres racines, toutes ses racines sont simples, et l'on a la factorisation : $X^{q-1} - 1 = \prod_{a\in K^*}(X-a)$. C'est (avec les notations du cours) le polynôme ω correspondant aux $q-1$ points $a \in K^*$. Indexons par K^* les polynômes d'interpolation de Lagrange : on a donc $L_a = \dfrac{\omega}{(X-a)\omega'(a)}$. On a $\omega' = (q-1)X^{q-2} = -X^{q-2}$ car $q = 0$ dans K (premier argument : q est une puissance non triviale, donc un multiple, de p, caractéristique du corps K ; deuxième argument : l'élément 1 du groupe additif K a un ordre qui divise le cardinal q de ce groupe). Pour $a \in K^*$, on a $a^{q-1} = 1$, donc $\omega'(a) = -a^{-1}$. Enfin, de l'identité remarquable

$$X^{q-1} - 1 = X^{q-1} - a^{q-1} = (X-a)\sum_{i+j=q-2} a^i X^j$$

et de l'égalité $a^{q-2-j}a^{-1-j}$, on tire :

$$L_a = \frac{\omega}{(X-a)\omega'(a)} = -a\sum_{j=0}^{q-2} a^{-j-1}X^j = -\sum_{j=0}^{q-2} a^{-j}X^j.$$

(ii) Si, dans l'égalité $X^{q-1} - 1 = \prod_{a\in K^*}(X-a)$, on remplace X par 0, on trouve $-1 = (-1)^{q-1}\prod_{a\in K^*} a$, donc $(-1)^q = \prod_{a\in K^*} a$. Appliquant cela au corps $\mathbb{Z}/p\mathbb{Z}$, on obtient la congruence $(p-1)! \equiv (-1)^p \pmod p$, qui est celle de l'énoncé lorsque p est impair ; lorsque $p = 2$, on a $-1 \equiv 1$ et la conclusion demeure.

II.6.15 (i) Il s'agit simplement de conditionner par la valeur de D_k : la probabilité que $D_{k+1} = m$ sachant que $D_k = a$ est nulle si $a \notin \{m, m-1\}$; si $a = m$, elle vaut $\dfrac{m}{n}$ (choix d'un entier

de $[\![1,n]\!]$ parmi les m valeurs déjà tirées) ; si $a=m-1$, elle vaut $\dfrac{n-(m-1)}{n}$ (choix d'un entier de $[\![1,n]\!]$ parmi les $n-(m-1)$ valeurs pas encore tirées). Pour $m=0$, la formule reste valable avec un raisonnement direct, sachant que $\mathbb{P}(D_k=-1)=0$ quel que soit $k\geqslant 0$. La formule reste d'ailleurs également valable pour $m>n$,avec la remarque que $\mathbb{P}(D_k=m)=0$ quel que soit $k\geqslant 0$.

(ii) On a $P_k(1)=\sum_{m=0}^{n}\mathbb{P}(D_k=m)=1$ (tous les cas possibles) et

$$P_k'=\sum_{m=1}^{n}m\mathbb{P}(D_k=m)X^{m-1}\qquad\text{d'où}\qquad P_k'(1)=\sum_{m=1}^{n}m\mathbb{P}(D_k=m),$$

qui est bien l'espérance de la variable aléatoire D_k.

(iii) Comme D_0 et D_1 valent respectivement 0 et 1 avec probabilité 1, on a $P_0=1X^0+\sum_{m\geqslant 1}0X^m=1$ et $P_1=1X^1+\sum_{m\neq 0}0X^m=X$.

Dans le calcul qui suit, on notera, pour simplifier, $p_{k,m}:=\mathbb{P}(D_k=m)$. Remarquons par ailleurs que l'on peut écrire $P_k=\sum_{m\geqslant 0}p_{k,m}X^m$ puisque les $p_{k,m}$ sont nuls dès que $m>n$.

$$\begin{aligned}
P_{k+1}=\sum_{m\geqslant 0}p_{k+1,m}X^m&=\sum_{m\geqslant 0}\left(\frac{m}{n}p_{k,m}+\frac{n-m+1}{n}p_{k,m-1}\right)X^m\\
&=\frac{1}{n}\sum_{m\geqslant 0}mp_{k,m}X^m+\frac{1}{n}\sum_{m\geqslant 0}(n-m+1)p_{k,m-1}X^m\\
&=\frac{1}{n}\sum_{m\geqslant 0}mp_{k,m}X^m+\sum_{m\geqslant 0}p_{k,m-1}X^m-\frac{1}{n}\sum_{m\geqslant 0}(m-1)p_{k,m-1}X^m\\
&=\frac{1}{n}XP_k'+XP_k-\frac{1}{n}X^2P_k'\\
&=XP_k+\frac{X-X^2}{n}P_k'.
\end{aligned}$$

(iv) il est clair que Φ est linéaire de $K_n[X]$ dans $K_{n+1}[X]$, car, si $\deg P=k\leqslant n$, chacun des polynômes XP et $\dfrac{X-X^2}{n}P'$ est de degré $k+1\leqslant n+1$. Mais $\Phi(X^n)=X^n$, et l'on voit que, si $\deg P\leqslant n$, alors $\deg\Phi(P)\leqslant n$: c'est donc un endomorphisme de $K_n[X]$.

Notons $Q_k:=X^k(1-X)^{n-k}$; on sait que les Q_k forment une base (famille à valuations échelonnées). Pour calculer $\Phi(Q_k)$, le moins fatigant est d'utiliser la dérivée logarithmique : $\dfrac{Q_k'}{Q_k}=\dfrac{k}{X}+\dfrac{n-k}{X-1}$, d'où l'on tire immédiatement : $\Phi(Q_k)=\dfrac{k}{n}Q_k$. On a donc *diagonalisé* l'endomorphisme Φ.

Du développement du binôme de $1^n=\big(X+(1-X)\big)^n$, on tire l'égalité $1=\sum_{j=0}^{n}\binom{n}{j}Q_j$. De la question précédente, on déduit que $P_k=\Phi^k(P_0)$, donc $P_k=\sum_{j=0}^{n}\left(\dfrac{j}{n}\right)^k\binom{n}{j}Q_j$. Comme Q_j est exactement divisible par $(1-X)^{n-j}$, on voit que $P_k(1)=Q_n(1)=1$ (qui n'est qu'une

vérification), et :

$$P_k'(1) = \sum_{j=0}^{n} \left(\frac{j}{n}\right)^k \binom{n}{j} Q_j'(1) = Q_n'(1) - n\left(\frac{n-1}{n}\right)^k = n\left(1 - \left(\frac{n-1}{n}\right)^k\right),$$

qui tend vers n en croissant strictement, comme on pouvait s'y attendre.

Remarque. Ce problème est appelé « problème (direct) du collectionneur de coupons » , mais on considère comme plus intéressant pratiquement le « problème inverse » : à combien de tirages doit-on s'attendre avant d'avoir constitué une collection complète ?

II.6.16 Soit $u := \mathrm{e}^{2\mathrm{i}\pi/n}$, d'où $\mu_n = \{u^0, u^1, \ldots, u^{n-1}\}$. Alors :

$$\omega := \prod_{x\in\mu_n} (X - x) = \prod_{k=0}^{n-1} (X - u^k) = X^n - 1,$$

et $\omega' = nX^{n-1}$, d'où $\omega'(u^k) = nu^{-k}$. Enfin :

$$L_k = \frac{\omega}{(X-u^k)\omega'(u^k)} = \frac{1}{n}\sum_{j=0}^{n-1} u^{-jk} X^k.$$

Les calculs ressemblent à ceux de l'exercice II.6.14 de la page 325.

II.6.17 Les racines du polynôme $(X+1)^n - \mathrm{e}^{2\mathrm{i}n\theta}$ sont les

$$\mathrm{e}^{2\mathrm{i}(\theta+k\pi/n)} - 1 = 2\mathrm{i}\mathrm{e}^{\mathrm{i}(\theta+k\pi/n)} \sin(\theta + k\pi/n) \quad \text{pour} \quad k \in [\![0, n-1]\!].$$

Leur produit est $(-1)^n(1 - \mathrm{e}^{2\mathrm{i}n\theta})$, d'où :

$$\prod_{k=0}^{n-1} \sin(\theta + k\pi/n) = \frac{(-1)^n(1-\mathrm{e}^{2\mathrm{i}n\theta})}{(2\mathrm{i}\mathrm{e}^{\mathrm{i}\theta})^n \mathrm{e}^{\mathrm{i}\pi(n-1)/2}} = \frac{(-1)^n(-2\mathrm{i}\sin n\theta)}{(2\mathrm{i})^n \mathrm{i}^{n-1}} = \frac{1}{2^{n-1}} \sin n\theta.$$

En remplaçant θ par $\theta + \pi/2$, on trouve :

$$\prod_{k=0}^{n-1} \cos(\theta + k\pi/n) = \frac{1}{2^{n-1}} \sin n(\theta + \pi/2) = \begin{cases} \dfrac{(-1)^k}{2^{n-1}} \sin n\theta \text{ si } n = 2k, \\ \dfrac{(-1)^k}{2^{n-1}} \cos n\theta \text{ si } n = 2k+1. \end{cases}$$

II.6.18 On part de la factorisation : $X^{2p} - 1 = (X^2 - 1)\prod_{k=1}^{p-1}(X^2 - 2X\cos k\pi/p + 1)$.

Pour $X = \mathrm{e}^{\mathrm{i}\theta}$, on a $X^2 - 2X\cos k\pi/p + 1 = 2\mathrm{e}^{\mathrm{i}\theta}(\cos\theta - \cos k\pi/p)$, d'où :

$$\frac{\sin p\theta}{\sin\theta} = 2^{p-1} \prod_{k=1}^{p-1} (\cos\theta - \cos k\pi/p).$$

On reconnaît l'expression factorisée de $U_{p-1}(\cos\theta)$.

II.6.19 (i) En intégrant les inégalités $\cos t \leqslant 1 \leqslant 1 + \tan^2 t$ sur $[0, x]$ (pour tout $x \geqslant 0$), on trouve $\sin x \leqslant x \leqslant \tan x$. Par ailleurs :

$$\operatorname{cotan}^2 x + 1 = \frac{\cos^2 x}{\sin^2 x} + 1 = \frac{\cos^2 x + \sin^2 x}{\sin^2 x} = \frac{1}{\sin^2 x}$$
$$\operatorname{cotan}(\pi - x) = \frac{\cos(\pi - x)}{\sin(\pi - x)} = \frac{-\cos x}{\sin x} = -\operatorname{cotan} x.$$

(ii) La formule donnée a été démontrée lors de l'étude de la cyclotomie. Si $n = 2p$, en exploitant les égalités $\operatorname{cotan}(\pi - x) = -\operatorname{cotan} x$ et $\operatorname{cotan} \pi/2 = 0$, on en tire : $\sum_{k=1}^{p} \operatorname{cotan}^2 \frac{k\pi}{n} = \frac{(n-1)(n-2)}{6}$. De l'encadrement $\sin x \leqslant x \leqslant \tan x$ appliqué en $x = k\pi/n$, on tire $\operatorname{cotan}^2 k\pi/n \leqslant \frac{n^2}{k^2\pi^2} \leqslant 1 + \operatorname{cotan}^2 k\pi/n$, puis :

$$\frac{(n-1)(n-2)}{6} \leqslant \frac{n^2}{\pi^2} \sum_{k=1}^{p} \frac{1}{k^2} \leqslant \frac{n}{2} + \frac{(n-1)(n-2)}{6},$$

d'où

$$\frac{\pi^2}{6}\frac{(n-1)(n-2)}{n^2} \leqslant \sum_{k=1}^{p} \frac{1}{k^2} \leqslant \frac{\pi^2}{6}\frac{(n-1)(n-2)}{n^2} + \frac{\pi^2}{2n}\,.$$

Lorsque $p \to +\infty$, on obtient la formule, due à Euler : $\sum_{k=1}^{+\infty} \frac{1}{k^2} = \frac{\pi^2}{6}$.

II.6.20 Suivant l'exercice II.5.6 de la page 276, on résout d'abord l'équation caractéristique associée : $X^2 - 2xX + 1 = 0$. Selon le signe de $x^2 - 1$, on trouve les cas suivants :

1. Si $|x| < 1$, notons $x = \cos\theta$. L'espace vectoriel E des suites solutions de la récurrence admet pour base $(\cos n\theta)_{n\geqslant 0}$, $(\sin n\theta)_{n\geqslant 0}$. Par identification des deux premiers termes, on trouve les coefficients nécessaires et : $t_n = \cos n\theta$, $u_n = \frac{\sin(n+1)\theta}{\sin\theta}$, ce qui était prévisible d'après l'étude des polynômes de Tchebychef.
2. Si $x = 1$, l'espace vectoriel E admet pour base $\big((1)^n\big)_{n\geqslant 0}$, $\big(n(1)^n\big)_{n\geqslant 0}$. Cela donne $t_n = 1$, $u_n = n + 1$.
3. Si $x = -1$, l'espace vectoriel E admet pour base $\big((-1)^n\big)_{n\geqslant 0}$, $\big(n(-1)^n\big)_{n\geqslant 0}$. Cela donne $t_n = (-1)^n$, $u_n = (n+1)(-1)^n$.
4. Si $|x| > 1$, l'espace vectoriel E admet pour base :

   $$\big((x + \sqrt{x^2-1})^n\big)_{n\geqslant 0}, \big((x - \sqrt{x^2-1})^n\big)_{n\geqslant 0}.$$

   On trouve facilement

   $$t_n = \frac{(x + \sqrt{x^2-1})^n + (x - \sqrt{x^2-1})^n}{2},$$
   $$u_n = \frac{(x + \sqrt{x^2-1})^{n+1} - (x - \sqrt{x^2-1})^{n+1}}{(x + \sqrt{x^2-1}) - (x - \sqrt{x^2-1})}.$$

En fait, avec un peu de trigonométrie hyperbolique, on peut rapprocher ce cas du premier. Rappelons que $\cosh t = \dfrac{\mathrm{e}^t + \mathrm{e}^{-t}}{2}$ et $\sinh t = \dfrac{\mathrm{e}^t + \mathrm{e}^{-t}}{2}$. Si $x = \cosh t$, avec $t > 0$, le lecteur vérifiera que $t_n = \cosh nt$, $u_n = \dfrac{\sinh(n+1)t}{\sinh t}$.

II.6.21 Si l'on applique le polynôme $T_n^2 + (1 - X^2)U_{n-1}^2 - 1$ en $\cos\theta$, $\theta \notin \pi\mathbb{Z}$, compte tenu des égalités $T_n(\cos\theta) = \cos n\theta$ et $U_{n-1}(\cos\theta) = \dfrac{\sin n\theta}{\sin\theta}$, on trouve $\cos^2 n\theta + \sin^2 n\theta - 1 = 0$. Ce polynôme ayant une infinité de racines, il est nul.
On démontre de même les relations : $T_{n+1} = XT_n + (X^2 - 1)U_{n-1}$ et $U_n = T_n + XU_{n-1}$. En effet, par la substitution $X = \cos\theta$, elles se ramènent respectivement aux formules $\cos(n+1)\theta = \cos n\theta\cos\theta - \sin n\theta\sin\theta$ et $\dfrac{\sin(n+1)\theta}{\sin\theta} = \cos n\theta + \dfrac{\sin n\theta}{\sin\theta}\cos\theta$ (formules d'addition). On en déduit : $\begin{pmatrix} T_{n+1} \\ U_n \end{pmatrix} = \begin{pmatrix} X & X^2 - 1 \\ 1 & X \end{pmatrix} \begin{pmatrix} T_n \\ U_{n-1} \end{pmatrix}$, d'où, en itérant :

$$\begin{pmatrix} T_{n+1} \\ U_n \end{pmatrix} = \begin{pmatrix} X & X^2 - 1 \\ 1 & X \end{pmatrix}^n \begin{pmatrix} T_1 \\ U_0 \end{pmatrix} = \begin{pmatrix} X & X^2 - 1 \\ 1 & X \end{pmatrix}^n \begin{pmatrix} X \\ 1 \end{pmatrix}.$$

II.6.22 On écrit $P = \sum_{l=0}^{n} b_l X^l$, d'où $Q = \sum_{l=0}^{n} b_l X^l (1+X)^{n-l} \in K_n[X]$.
Si l'on remplace X par $\dfrac{X}{1-X}$, on trouve $P = (1-X)^n Q\left(\dfrac{X}{1-X}\right) \in K_n[X]$ par un calcul similaire.
Si $P = X^i = \sum_{k=0}^{n} a_k X^k (1-X)^{n-k}$, on a donc $Q = (1+X)^n \left(\dfrac{X}{1+X}\right)^i = X^i(1+X)^{n-i}$, donc a_k est le coefficient de X^k dans $X^i(1+X)^{n-i}$, qui est nul si $k < i$ ou $k > n$, et vaut $\binom{n-i}{n-k}$ si $i \leqslant k \leqslant n$.

II.6.23 Définissons les suites de polynômes $(A_n)_{n\in\mathbb{N}}$, $(B_n)_{n\in\mathbb{N}}$ par les relations $A_0 = 0$, $B_0 = 1$, et, pour tout $n \in \mathbb{N}$, $A_{n+1} = A_n + XB_n$ et $B_{n+1} = B_n - XA_n$. Alors $B_0 + \mathrm{i}A_0 = 1$ et $B_{n+1} + \mathrm{i}A_{n+1} = (1 + \mathrm{i}X)(B_n + \mathrm{i}A_n)$ (calcul facile). On a donc bien $B_n + \mathrm{i}A_n = (1 + \mathrm{i}X)^n = \sum_{k=0}^{n} \binom{n}{k} \mathrm{i}^k X^k$, donc $B_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} (-1)^k X^{2k}$ et $A_n = \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n}{2k+1} (-1)^k X^{2k+1}$, où $\lfloor x \rfloor$ désigne la partie entière de x. Cela implique en particulier que A_n n'est pas le polynôme nul, et l'on voit que les fractions rationnelles $G_n := \dfrac{A_n}{B_n}$ vérifient les relations $G_0 := 0$ et, pour tout $n \in \mathbb{N}$, $G_{n+1} := \dfrac{G_n + X}{1 - XG_n}$: on a donc $G_n = F_n$ pour tout $n \in \mathbb{N}$; on voit du même coup que les F_n sont tous bien définis.
Soit $\theta \in]-\pi/2, \pi/2[$. Alors :

$$(B_n + \mathrm{i}A_n)(\tan\theta) = (1 + \mathrm{i}\tan\theta)^n = \frac{\mathrm{e}^{\mathrm{i}n\theta}}{\cos^n\theta},$$

d'où $B_n(\tan\theta) = \dfrac{\cos n\theta}{\cos^n\theta}$ et $A_n(\tan\theta) = \dfrac{\sin n\theta}{\cos^n\theta}$. Si $\cos n\theta \neq 0$, on a donc $F_n(\tan\theta) = \tan n\theta$; par π-périodicité de la fonction $\tan$, cela reste vrai pour tout θ tel que $\cos\theta, \cos n\theta \neq 0$.
Des formules donnant $B_n(\tan\theta)$ et $A_n(\tan\theta)$, on déduit que les zéros de F_n sont les $\tan k\pi/n$ et ses pôles les $\tan(2k+1)\pi/2n$. On peut imposer à k de varier dans un intervalle (d'entiers) de longueur n ; il faut de plus exclure les valeurs $\pm\pi/2$ des arguments de $\tan$.
Le lecteur vérifiera (discussion selon la parité de n) que le nombre de zéros de F_n (resp. son nombre de pôles) est égal au degré de B_n (resp. de A_n).

II.6.24 On a *a priori* $(c,d) \neq (0,0)$, sans quoi l'écriture $\dfrac{aX+b}{cX+d}$ n'aurait aucun sens. L'égalité $\dfrac{aX+b}{cX+d} = \lambda$, $\lambda \in K$ équivaut à $(a,b) = \lambda(c,d)$; l'existence d'un tel λ équivaut donc, d'après le cours d'algèbre linéaire, à $ad - bc = 0$.
Notons $A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$ et $A' := \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in GL_2(K)$. Alors :

$$H_{A'} \circ H_A = \frac{a'\dfrac{aX+b}{cX+d} + b'}{c'\dfrac{aX+b}{cX+d} + d'} = \frac{a'(aX+b) + b'(cX+d)}{c'(aX+b) + d'(cX+d)} = \frac{(a'a+b'c)X + (a'b+b'd)}{(c'a+d'c)X + (c'b+d'd)} = H_B,$$

où $B := \begin{pmatrix} a'a+b'c & a'b+b'd \\ c'a+d'c & c'b+d'd \end{pmatrix}$. On reconnaît que $B = A'A$, d'où l'égalité $H_{A'} \circ H_A = H_{A'A}$. Par ailleurs, $H_{I_2} = \dfrac{1X+0}{0X+1} = X$.
On en déduit que la loi $\circ$ est interne sur l'ensemble des homographies et que $A \mapsto H_A$ est un morphisme, par définition surjectif, de $GL_2(K)$ sur cet ensemble muni de cette loi. Il est alors clair que les homographies forment un groupe pour la composition, dont $H_{I_2} = X$ est l'élément neutre et tel que l'inverse de H_A est $H_{A^{-1}}$.
La matrice H_A appartient au noyau si, et seulement si, $H_A = X$. Avec les notations ci-dessus, cela équivaut à $\dfrac{aX+b}{cX+d} = X$, c'est-à-dire à $cX^2 + (d-a)X + b = 0$, ou encore à $c = b = d - a = 0$, *i.e.* à $A = aI_2$ (et $a \neq 0$, puisque $A \in GL_2(K)$). Le noyau est donc K^*I_2.

II.6.25 Rappelons que, si $P := \prod_{a\in A}(X-a)$, alors la décomposition en éléments simples de $\dfrac{1}{P}$ est :

$$\frac{1}{P} = \sum_{a\in A} \frac{1}{P'(a)} \frac{1}{X-a}.$$

De la factorisation $T_n = 2^{n-1} \prod_{k=1}^{n} \left(X - \cos\dfrac{(2k-1)\pi}{2n} \right)$, et de l'égalité $T_n' = nU_{n-1}$, on tire :

$$\frac{1}{T_n} = \frac{1}{n} \sum_{k=1}^{n} \frac{(-1)^{k-1} \sin\dfrac{(2k-1)\pi}{2n}}{X - \cos\dfrac{(2k-1)\pi}{2n}};$$

en effet :

$$U_{n-1}\left(\cos\frac{(2k-1)\pi}{2n}\right)=\frac{\sin\dfrac{(2k-1)\pi}{2}}{\sin\dfrac{(2k-1)\pi}{2n}}=\frac{(-1)^{k-1}}{\sin\dfrac{(2k-1)\pi}{2n}}\cdot$$

On trouve de même :

$$\frac{1}{X^n-1}=\sum_{j\in\mu_n}\frac{1}{nj^{n-1}}\frac{1}{X-j}=\frac{1}{n}\sum_{j\in\mu_n}\frac{j}{X-j},$$

et :

$$\frac{1}{X^q-X}=\sum_{a\in K}\frac{1}{qa^{q-1}-1}\frac{1}{X-a}=-\sum_{a\in K}\frac{1}{X-a}\cdot$$

II.6.26 Écrivons $B=(X-\alpha)C$, où $C(\alpha)=B'(\alpha)\neq 0$. Alors $\dfrac{A}{B}=\dfrac{r}{X-\alpha}+\dfrac{D}{C}$, où r est le résidu recherché. Appliquant l'égalité $A=rC+(X-\alpha)D$ en α, on trouve $r=\dfrac{A(\alpha)}{C(\alpha)}=\dfrac{A(\alpha)}{B'(\alpha)}$, comme désiré.

II.6.27 Il s'agit, bien sûr, de décomposer la fraction rationnelle $\dfrac{1}{X+1}\cdots\dfrac{1}{X+p}$ (sinon, la question n'aurait aucun sens), et d'étudier la somme de la série $\displaystyle\sum_{n\geqslant 0}\left(\frac{1}{n+1}\cdots\frac{1}{n+p}\right)$ (sinon, il n'y aurait pas convergence).

On écrit $\dfrac{1}{X+1}\cdots\dfrac{1}{X+p}=\dfrac{a_1}{X+1}+\cdots+\dfrac{a_p}{X+p}$, on multiplie par $X+i$ et l'on évalue en $-i$, ce qui donne $a_i=\dfrac{(-1)^{i-1}}{(i-1)!(p-i)!}$. On calcule ensuite les sommes partielles :

$$\begin{aligned}\sum_{n=0}^{N}\frac{1}{n+1}\cdots\frac{1}{n+p}&=\sum_{i=1}^{p}\frac{(-1)^{i-1}}{(i-1)!(p-i)!}\sum_{n=0}^{N}\frac{1}{n+i}=\sum_{i=1}^{p}\frac{(-1)^{i-1}}{(i-1)!(p-i)!}(H_{N+i}-H_{i-1})\\&=\sum_{i=1}^{p}\frac{(-1)^{i-1}}{(i-1)!(p-i)!}\big(\log(N+i)+\gamma+\mathrm{o}(1)\big)-\sum_{i=1}^{p}\frac{(-1)^{i-1}}{(i-1)!(p-i)!}H_{i-1}\\&=\left(\sum_{i=1}^{p}\frac{(-1)^{i-1}}{(i-1)!(p-i)!}\right)(\log N+\gamma)-\sum_{i=1}^{p}\frac{(-1)^{i-1}}{(i-1)!(p-i)!}H_{i-1}+\mathrm{o}(1).\end{aligned}$$

Comme $p\geqslant 2$, on sait *a priori* que la série converge ; pour cela, il est nécessaire que l'entier $\displaystyle\sum_{i=1}^{p}\frac{(-1)^{i-1}}{(i-1)!(p-i)!}$ soit nul, sans quoi l'expression ci-dessus aurait une limite infinie. La somme de la série est donc le rationnel :

$$-\sum_{i=1}^{p}\frac{(-1)^{i-1}}{(i-1)!(p-i)!}H_{i-1}=\frac{-1}{(p-1)!}\sum_{j=0}^{p-1}\binom{p-1}{j}(-1)^jH_j.$$

En fait, $\displaystyle\sum_{i=1}^{p}\frac{(-1)^{i-1}}{(i-1)!(p-i)!}=(p-1)!(1-1)^{p-1}$ (formule du binôme) est bien nul, puisque $p-1\geqslant 1$.

II.6.28 Par parité et 2π-périodicité de la fonction $\cos$, on peut supposer que $\theta \in [0, \pi]$.

Si $\theta = 0$, la fraction est $\dfrac{1}{(X-1)^2}$, qui est déjà décomposée, et dont on connaît la dérivée $n^{ème}$: c'est $\dfrac{(n+1)!(-1)^n}{(X-1)^{n+2}}$. Si $\theta = \pi$, la fraction est $\dfrac{1}{(X+1)^2}$, qui est déjà décomposée, et dont on connaît la dérivée $n^{ème}$: c'est $\dfrac{(n+1)!(-1)^n}{(X+1)^{n+2}}$.

Si $\theta \in]0, \pi[$, la fraction est :

$$\frac{1}{(X-\mathrm{e}^{\mathrm{i}\theta})(X-\mathrm{e}^{-\mathrm{i}\theta})} = \frac{1}{2\mathrm{i}\sin\theta}\left(\frac{1}{X-\mathrm{e}^{\mathrm{i}\theta}} - \frac{1}{X-\mathrm{e}^{-\mathrm{i}\theta}}\right),$$

dont la dérivée $n^{ème}$ est :

$$\frac{(-1)^n n!}{2\mathrm{i}\sin\theta}\left(\frac{1}{(X-\mathrm{e}^{\mathrm{i}\theta})^{n+1}} - \frac{1}{(X-\mathrm{e}^{-\mathrm{i}\theta})^{n+1}}\right).$$

II.6.29 On factorise le numérateur avec les « racines inverses » , car cela facilite le calcul des développements limités. En effet, on a : $\dfrac{1}{1-rX} = \sum\limits_{m=0}^{n} r^m X^m \pmod{X^{n+1}}$. Ici, cela donne :

$(1-X^2)(1-X^3) = (1-X)^2(1+X)(1+X+X^2) = (1-X)^2(1+X)(1-jX)(1-kX)$,

où $j := \mathrm{e}^{2\mathrm{i}\pi/3}$ et $k := \mathrm{e}^{-2\mathrm{i}\pi/3}$. La décomposition en éléments simples est alors :

$$\frac{1}{(1-X^2)(1-X^3)} = \frac{a}{1-X} + \frac{b}{(1-X)^2} + \frac{c}{1+X} + \frac{d}{1-jX} + \frac{e}{1-kX},$$

où, par application des méthodes du cours, on trouve : $a = \dfrac{1}{4}$, $b = \dfrac{1}{6}$, $c = \dfrac{1}{4}$, $d = \dfrac{1-k}{9}$ et $e = \dfrac{1-j}{9}$. Le développement limité à l'ordre n de notre fraction rationnelle est donc :

$$\frac{1}{(1-X^2)(1-X^3)} \equiv \sum_{m=0}^{n} \big(a + b(m+1) + c(-1)^m + dj^m + ek^m\big) \pmod{X^{n+1}}.$$

Par ailleurs, des développements limités suivants : $\dfrac{1}{1-X^2} = \sum\limits_{p=0}^{n} X^{2p} \pmod{X^{2n+1}}$ et $\dfrac{1}{1-X^3} = \sum\limits_{q=0}^{n} X^{3q} \pmod{X^{3n+1}}$, on déduit que, pour $n \geqslant m$, le coefficient du terme de degré m dans le développement limité à l'ordre n de $\dfrac{1}{(1-X^2)(1-X^3)}$ est le nombre u_m des couples $(p, q) \in \mathbb{N} \times \mathbb{N}$ tels que $2p + 3q = m$. Ce calcul utilise la règle sur les développements limités d'un produit de deux fonctions rationnelles.

Par unicité du développement limité, on en déduit la formule :

$$u_m := \operatorname{card}\{(p,q) \in \mathbb{N}\times\mathbb{N} \mid 2p+3q = m\} = \frac{1}{4} + \frac{1}{6}(m+1) + \frac{1}{4}(-1)^m + \frac{1-k}{9}j^m + \frac{1-j}{9}k^m.$$

II.6.30 On a, par hypothèse, $\deg F_0 = \deg P_0$. Si $\deg F_n = \deg P_n$, alors $\deg \dfrac{1}{F_n} = -\deg P_n < 0$, donc $\deg\left(P_{n+1} + \dfrac{1}{F_n}\right) = \deg P_{n+1}$.

L'égalité des degrés est donc démontrée par récurrence. Il en découle en particulier qu'aucun F_n ne s'annule et que la relation de récurrence est bien définie.
Supposons les A_n et les B_n définis comme dans l'énoncé (initialisation et récurrence). On a $A_1 = A_0P_1 + 1$, donc $\deg A_1 > \deg A_0$; puis, si $\deg A_n > \deg A_{n-1}$, alors $\deg A_{n+1} = \deg(A_nP_{n+1} + A_{n-1}) > \deg A_n$. La suite des $\deg A_n$ est donc strictement croissante, et les A_n ne s'annulent pas, donc les $B_n = A_{n+1}$ non plus. On peut donc poser $G_n := \dfrac{A_n}{B_n}$. Il est alors immédiat que $G_0 = P_0$ et que $G_{n+1} := P_{n+1} + \dfrac{1}{G_n}\cdot$ Comme la suite des G_n et la suite des A_n ont même initialisation et même relation de récurrence, elles sont égales : on a donc bien $F_n = G_n = \dfrac{A_n}{B_n}$ pour tout entier n.
Des relations $A_{n+1} = A_nP_{n+1} + B_n$ et $B_{n+1} = A_n$, on déduit sans peine l'égalité des pgcd : $A_{n+1} \wedge B_{n+1} = A_n \wedge B_n$, donc, par récurrence, $A_n \wedge B_n = A_1 \wedge B_1 =$ ‘. La fraction rationnelle $\dfrac{A_n}{B_n}$ est donc irréductible.

II.6.31 Supposons d'abord $F \neq 0$ et écrivons $F = \dfrac{A}{B}$, où :

$$A = a_0X^n + \cdots + a_n, \qquad B = b_0X^p + \cdots + b_p \qquad \text{et} \qquad a_0, b_0 \neq 0.$$

On a donc $\deg F = n - p$. D'autre part :

$$F\left(\frac{1}{X}\right) = X^{p-n}\frac{a_0 + \cdots + a_nX^n}{b_0 + \cdots + b_pX^p}, \text{ avec } a_0, b_0 \neq 0,$$

et l'ordre de $F(1/X)$ en 0 est $p - n = -\deg F$ (et non $\deg F$ comme l'affirme l'énoncé par erreur). Si $F = 0$, le degré est $-\infty$ et l'ordre $+\infty$: la relation est encore valable.

II.6.32 Écrivons $F_0 = \dfrac{A_0}{A_1}$ (forme irréductible). Si l'on a, pour $n \geqslant 1$ quelconque, une telle écriture $F_{n-1} = \dfrac{A_{n-1}}{A_n}$, et si F_{n-1} n'est pas un polynôme, alors la partie entière de F_{n-1} est le quotient Q_{n-1} de la division euclidienne : $A_{n-1} = Q_{n-1}A_n + R_n$. On a alors $F_n = \dfrac{A_n}{R_n}$, et l'on peut poser $A_{n+1} := R_n$. De plus, le pgcd de A_n et A_{n+1} est celui de A_{n-1} et de A_n, donc, par récurrence, ils sont premiers entre eux. Finalement, on a bien des écritures irréductibles $F_n = \dfrac{A_n}{A_{n+1}}$, où les A_n sont définis comme dans l'énoncé.
Mais ces A_n sont les termes qui apparaissent au cours d'une exécution de l'algorithme d'Euclide appliqué à A_0, A_1 : la suite est donc finie.

II.6.33 On a vu dans le cours que $K(X) = K[X] \oplus K_{-1}(X)$. Soit $F = G + H$ une telle décomposition : il s'agit de voir que $F \in K_n(X) \Leftrightarrow G \in K_n(X)$. Il suffit, pour cela, d'observer que, si $\deg(F - G) \leqslant -1$ et si $n \geqslant 0$, alors $\deg F \leqslant n \Leftrightarrow \deg G \leqslant n$.

Module II.7 : Espaces vectoriels de dimension finie

II.7.1 Soient $V := E \times \{0\}$ et $W := \{0\} \times F$. Ce sont deux sous-espaces vectoriels supplémentaires de $E \times F$. En effet, leur intersection est réduite à $\{0\}$, et tout $(x, y) \in E \times F$ s'écrit : $(x, y) = (x, 0) + (0, y)$, donc appartient à $V + W$, de sorte que $V + W = E \times F$. L'application $x \mapsto (x, 0)$ est un isomorphisme de E sur V, donc V est de dimension finie et $\dim(V) = \dim(E)$. De même W est de dimension finie et $\dim(W) = \dim(F)$. Le théorème 12 de la page 335 montre alors que $E \times F$ est de dimension finie, à savoir :

$$\dim(E \times F) \;=\; \dim(V) + \dim(W) \;=\; \dim(E) + \dim(F).$$

Cela donne une autre preuve de la proposition 13 de la page 336.

II.7.2 Puisque u est surjective, *i.e.* $u(E') = E$, on a :

$$\operatorname{Im} f \;=\; f(E) \;=\; f\big(u(E')\big) \;=\; \operatorname{Im}(f \circ u).$$

Par ailleurs, v est injective, elle induit donc un isomorphisme de F sur $\operatorname{Im} v = v(F)$. Pour tout sous-espace vectoriel F_1 de F, la restriction dudit isomorphisme à F_1 est un isomorphisme de F_1 sur $v(F_1)$. Soit en particulier $F_1 := \operatorname{Im} f$. Nous avons donc un isomorphisme de $\operatorname{Im} f$ sur le sous-espace vectoriel de F' suivant :

$$v(\operatorname{Im} f) \;=\; v\big(\operatorname{Im}(f \circ u)\big) \;=\; v\left(f\big(u(E')\big)\right) \;=\; \operatorname{Im}(v \circ f \circ u).$$

Ainsi les images de f et de $v \circ f \circ u$ sont isomorphes. La conclusion résulte alors du théorème 6 de la page 332.

II.7.3 L'égalité $f \circ f = 0$, c'est-à-dire $f\big(f(x)\big) = 0$ pour tout $x \in E$, est équivalente à l'inclusion $\operatorname{Im} f \subset \operatorname{Ker} f$. Soient p, q les dimensions respectives de $\operatorname{Im} f$ et $\operatorname{Ker} f$. L'inclusion précédente implique $p \leqslant q$. D'un autre côté, le théorème du rang donne l'égalité $p + q = n$. Ainsi $p \leqslant n - p$, soit $p \leqslant n/2$. Enfin p est, par définition, le rang de f, donc $\operatorname{rang}(f) \leqslant n/2$.

II.7.4 1) L'image de $g \circ f$, à savoir $g\big(f(E)\big)$, est contenue dans $g(F) = \operatorname{Im} g$. Comme g est de rang fini, *i.e.* $\operatorname{Im} g$ est de dimension finie, l'image de $g \circ f$ est de dimension finie au plus égale à $\dim(\operatorname{Im} g) = \operatorname{rang}(g)$. Ainsi $g \circ f$ est de rang fini, et $\operatorname{rang}(g \circ f) \leqslant \operatorname{rang}(g)$.

La restriction de g à $\operatorname{Im} f$ est une application linéaire surjective de $\operatorname{Im} f$ sur $g(\operatorname{Im} f) = \operatorname{Im}(g \circ f)$. Mais $\operatorname{Im} f$ est de dimension finie, donc le théorème du rang montre que $\operatorname{Im}(g \circ f)$ est de dimension finie et donne l'inégalité $\dim\big(\operatorname{Im}(g \circ f)\big) \leqslant \dim(\operatorname{Im} f)$. Autrement dit, $g \circ f$ est de rang fini (nous le savions), et $\operatorname{rang}(g \circ f) \leqslant \operatorname{rang}(f)$.

2) Soit donc u la restriction de g à $\operatorname{Im} f$. Nous avons vu que $\operatorname{Im} u = \operatorname{Im}(g \circ f)$. Par ailleurs, il est clair que $\operatorname{Ker} u = \operatorname{Ker} g \cap \operatorname{Im} f$. Comme $\operatorname{Im} f$ est de dimension finie, nous pouvons appliquer le théorème du rang à u :

$$\operatorname{rang}(g \circ f) \;=\; \dim(\operatorname{Im} u) \;=\; \dim(\operatorname{Im} f) - \dim(\operatorname{Ker} g \cap \operatorname{Im} f).$$

Comme $\operatorname{Ker} g \cap \operatorname{Im} f \subset \operatorname{Ker} g$, on a $\dim(\operatorname{Ker} g \cap \operatorname{Im} f) \leqslant \dim(\operatorname{Ker} g)$, d'où, en appliquant le théorème du rang à g :

$$\operatorname{rang}(g \circ f) \;\geqslant\; \dim(\operatorname{Im} f) - \dim(\operatorname{Ker} g) \;=\; \dim(\operatorname{Im} f) + \dim(\operatorname{Im} g) - \dim(F)\,,$$

soit $\operatorname{rang}(g \circ f) \geqslant \operatorname{rang}(f) + \operatorname{rang}(g) - n$, comme désiré.

Revenons à l'exercice précédent. Ici $F := E$, $G := E$ et $g := f$. Le rang de $g \circ f = f^2 = 0$ est nul. Ce que nous venons de prouver donne l'inégalité $2\,\mathrm{rang}(f) \leqslant n$, *i.e.* nous retrouvons la conclusion obtenue ci-dessus.

II.7.5 1) Soit $k \in \mathbb{N}$. L'égalité $f^{k+1} = f \circ f^k$ implique l'inclusion $V_k \subset V_{k+1}$, d'où $d_k \leqslant d_{k+1}$. La suite $(d_k)_{k\geqslant 0}$ est donc croissante. Comme les d_k sont des entiers majorés par $n := \dim(E)$, cette suite est stationnaire. L'argument utilisé ici est que toute partie non vide et majorée de $\mathbb{N}$ est finie et possède un plus grand élément.

2) Soient donc H un supplémentaire de V_{k+1} dans V_{k+2} et $u : H \to E$ la restriction de f à H. Si $x \in H$, $f^{k+2}(x) = 0$, soit $f^{k+1}\big(u(x)\big) = 0$, autrement dit $u(x) \in V_{k+1}$. De plus u est (linéaire) *injective*. Soit en effet $x \in \mathrm{Ker}\, u$: $x \in H$ et $f(x) = 0$. Alors $x \in \mathrm{Ker}\, f = V_1 \subset V_{k+1}$, donc $x \in H \cap V_{k+1} = \{0\}$.

Ce qui précède montre que u est un isomorphisme de H sur un sous-espace vectoriel de V_{k+1}. Montrons maintenant que $u(H) \cap V_k = \{0\}$. Soit $x \in H$ tel que $f(x) = u(x) \in V_k$. Alors $f^k\big(f(x)\big) = 0$, soit $x \in V_{k+1}$. Là encore $x \in H \cap V_{k+1}$, donc $x = 0$. Puisque $u(H) + V_k \subset V_{k+1}$, le théorème 16 de la page 337 donne :

$$\dim\big(u(H)\big) + \dim(V_k) = \dim\big(u(H) + V_k\big) \leqslant \dim(V_{k+1}) = d_{k+1}\,,$$

d'où $\dim(H) = \dim\big(u(H)\big) \leqslant d_{k+1} - d_k$. Or le théorème 12 de la page 335 montre que $\dim(H) + d_{k+1} = d_{k+2}$, et ainsi $d_{k+2} - d_{k+1} \leqslant d_{k+1} - d_k$, ce qui montre que la suite $(d_{k+1} - d_k)_{k\geqslant 0}$ est décroissante.

II.7.6 Supposons que f soit de rang 1. Alors $D := \mathrm{Im}\, f$ est une droite. Soit b un vecteur non nul de D. Pour tout $x \in E$, $f(x) \in D$, *i.e.* il existe un unique scalaire $\alpha(x)$ tel que $f(x) = \alpha(x) \cdot b$. Si $x, y \in E$, on a :

$$\alpha(x+y)\cdot b = f(x+y) = f(x) + f(y) = \alpha(x)\cdot b + \alpha(y)\cdot b = \big[\alpha(x) + \alpha(y)\big]\cdot b\,,$$

ce qui montre que $\alpha(x+y) = \alpha(x) + \alpha(y)$. On montre de même que $\alpha(\lambda x) = \lambda\alpha(x)$ pour tous $x \in E$ et $\lambda \in K$, donc α est une forme linéaire, évidemment non nulle, sur E.

Supposons inversement qu'il existe un vecteur non nul $b \in F$ et une forme linéaire non nulle α sur E tels que $f(x) = \alpha(x)\cdot b$ pour tout $x \in E$. On a d'abord $\mathrm{Im}\, f = f(E) \subset \mathrm{Vect}(b)$. En fait, il existe $a \in E$ tel que $\alpha(a) \neq 0$, et alors $f(a) = \alpha(a)\cdot b$, d'où $b = f\big(\alpha(a)^{-1}a\big) \in f(E)$. Ainsi $\mathrm{Im}\, f = \mathrm{Vect}(b)$, ce qui montre que f est de rang 1.

Soient b, α comme ci-dessus et $t \in K^*$. Posant $\alpha' := t\alpha$ et $b' := t^{-1}b$, il est clair qu'on a encore $f(x) = \alpha'(x)\cdot b'$ pour tout $x \in E$. Inversement, soient $b'' \in F$ et α'' une forme linéaire sur E tels que $f(x) = \alpha''(x)\cdot b''$ pour tout $x \in E$. L'argument ci-dessus montre que $\mathrm{Vect}(b'') = \mathrm{Im}\, f = \mathrm{Vect}(b)$. Il existe donc $t \in K^*$ tel que $b'' = t^{-1}b$. Pour tout $x \in E$, il vient :

$$\alpha(x)\cdot b = f(x) = \alpha''(x)\cdot b'' = t^{-1}\alpha''(x)\cdot b, \quad \text{d'où} \quad \alpha(x) = t^{-1}\alpha''(x).$$

Cela étant vrai pour tout $x \in E$, il en résulte que $\alpha'' = t\alpha$. En résumé, les couples $(b', \alpha') \in F \times E^*$ ayant la propriété requise sont donnés par $\alpha' = t\alpha$ et $b' = t^{-1}b$, où t est un scalaire non nul arbitraire.

II.7.7 La preuve du théorème 42 de la page 198 montre qu'un endomorphisme g de E est une homothétie si, et seulement si, toute droite est stable par g, ce qui revient à dire que, pour tout $x \in E$, $g(x)$ est colinéaire à x. Puisque f n'est pas une homothétie, il existe un vecteur $x \in E$ tel que la famille $\big(x, f(x)\big)$ soit libre. Posons $e_1 := x$ et $e_2 := f(x)$. La famille (e_1, e_2) étant libre, on peut la compléter en une base $(e_1, e_2, \dots, e_n)$ de E, et l'on a bien $f(e_1) = e_2$.

II.7.8 Supposons donc que $v \in \mathcal{L}(E)$ soit tel que $u \circ v = 0$ et $u + v \in \mathcal{GL}(E)$. La première condition équivaut à l'inclusion $\operatorname{Im} v \subset \operatorname{Ker} u$, *i.e.* $u\big(v(x)\big) = 0$ pour tout $x \in E$. Le fait que $u + v$ soit inversible signifie, puisque nous sommes en dimension finie, que $u + v$ est surjectif. Or, si $x \in E$, $(u + v)(x) = u(x) + v(x)$, donc $(u + v)(x) \in \operatorname{Im} u + \operatorname{Im} v$. Ainsi $E = \operatorname{Im}(u+v) \subset \operatorname{Im} u + \operatorname{Im} v \subset E$, et par suite $\operatorname{Im} u + \operatorname{Im} v = E$. Mais $\operatorname{Im} v \subset \operatorname{Ker} u$, d'où *a fortiori* $\operatorname{Im} u + \operatorname{Ker} u = E$.

D'après le théorème du rang, $\dim\big(\operatorname{Im} u\big) + \dim\big(\operatorname{Ker} u\big) = \dim(E)$. La proposition 17 de la page 337 entraîne alors que E est somme directe de $\operatorname{Im} u$ et $\operatorname{Ker} u$, comme annoncé.

Supposons inversement que E soit somme directe de $\operatorname{Im} u$ et $\operatorname{Ker} u$: $E = \operatorname{Im} u \oplus \operatorname{Ker} u$. Soit $v \in \mathcal{L}(E)$ la projection sur $\operatorname{Ker} u$ parallèlement à $\operatorname{Im} u$. On sait que $\operatorname{Im} v = \operatorname{Ker} u$ et $\operatorname{Ker} v = \operatorname{Im} u$. La première de ces égalités montre que $u \circ v = 0$. Il reste à vérifier que $u + v$ est inversible, c'est-à-dire que $\operatorname{Ker}(u + v) = \{0\}$ (toujours parce qu'il s'agit d'un endomorphisme d'un espace vectoriel de dimension finie). Soit donc $x \in \operatorname{Ker}(u + v)$: $v(x) = -u(x)$. Mais $v(x) \in \operatorname{Im} v = \operatorname{Ker} u$, et $-u(x) \in \operatorname{Im} u$, de sorte que $v(x) \in \operatorname{Ker} u \cap \operatorname{Im} u = \{0\}$. Ainsi $v(x) = 0$. Mais alors $v(x) = 0 = -u(x)$, donc $x \in \operatorname{Ker} v \cap \operatorname{Ker} u = \operatorname{Im} u \cap \operatorname{Ker} u = \{0\}$, d'où $x = 0$. Finalement $u \circ v = 0$ et $u + v \in \mathcal{GL}(E)$, donc v répond à la question.

II.7.9 Supposons que E soit de dimension finie sur $\mathbb{R}$: il existe une partie finie S de E qui engendre E sur $\mathbb{R}$. Autrement dit, tout vecteur de E est combinaison linéaire, à coefficients dans $\mathbb{R}$, donc aussi dans $\mathbb{C}$, des éléments de S. Ainsi S engendre *a fortiori* E sur $\mathbb{C}$, et par suite E est de dimension finie sur $\mathbb{C}$.

Inversement, supposons que $(u_1, \dots, u_n)$ soit une famille génératrice finie de E sur $\mathbb{C}$. Soit $x \in E$. Il existe $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ tels que $x = \sum_{j=1}^{n} \lambda_j u_j$. Pour tout j, posons $\alpha_j := \operatorname{Re} \lambda_j$ et $\beta_j := \operatorname{Im} \lambda_j$. Alors :

$$x = \sum_{j=1}^{n} (\alpha_j + i\beta_j) \cdot u_j = \sum_{j=1}^{n} \alpha_j u_j + \sum_{j=1}^{n} \beta_j (iu_j).$$

Cela montre que la famille $(u_1, \dots, u_n, iu_1, \dots, iu_n)$ engendre E sur $\mathbb{R}$. Ainsi E est de dimension finie sur $\mathbb{R}$.

Supposons enfin que E soit de dimension finie n sur $\mathbb{C}$, et soit ici $(u_1, \dots, u_n)$ une base de E sur $\mathbb{C}$. D'après ce que nous venons de voir, $(u_1, \dots, u_n, iu_1, \dots, iu_n)$ est une famille génératrice de E sur $\mathbb{R}$. La dimension de E sur $\mathbb{R}$ est donc au plus $2n$. En fait cette dimension vaut $2n$, *i.e.* $(u_1, \dots, u_n, iu_1, \dots, iu_n)$ est une base de E sur $\mathbb{R}$. Il suffit de vérifier que cette famille est libre (sur $\mathbb{R}$). Soit $(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n) \in \mathbb{R}^{2n}$ une famille telle

que $\sum_{j=1}^{n} \alpha_j u_j + \sum_{j=1}^{n} \beta_j (iu_j) = 0$. Ainsi $\sum_{j=1}^{n} (\alpha_j + i\beta_j) \cdot u_j = 0$. Comme $(u_1, \dots, u_n)$ est libre sur $\mathbb{C}$, on a, pour tout j, $\alpha_j + i\beta_j = 0$, c'est-à-dire $\alpha_j = \beta_j = 0$. En résumé, avec des notations évidentes, nous avons prouvé ceci :

$$\dim_{\mathbb{R}} E \;=\; 2 \dim_{\mathbb{C}} E.$$

II.7.10 Soit $x \in E$. Il existe $\lambda_1, \dots, \lambda_n \in L$ tels que $x = \sum_{j=1}^{n} \lambda_j \cdot e_j$. Soit $j \in [\![1, n]\!]$. Puisque $(a_1, \dots, a_p)$ engendre le K-espace vectoriel L, il existe une famille $(\alpha_{1,j}, \dots, \alpha_{p,j}) \in K^p$ telle que $\lambda_j = \sum_{i=1}^{p} \alpha_{i,j} a_i$. Alors :

$$x \;=\; \sum_{j=1}^{n} \lambda_j \cdot e_j \;=\; \sum_{j=1}^{n} \left(\sum_{i=1}^{p} \alpha_{i,j} a_i \right) \cdot e_j \;=\; \sum_{(i,j) \in [\![1,p]\!] \times [\![1,n]\!]} \alpha_{i,j} \cdot (a_i \cdot e_j).$$

Cela montre que, lorsque (i, j) décrit $[\![1, p]\!] \times [\![1, n]\!]$, les $a_i \cdot e_j$ forment une famille génératrice de E sur K. Un calcul analogue, en prenant $x := 0$ ci-dessus, montre que cette famille de E est libre sur K. C'est donc une base de E sur K, ce qui montre que la dimension de E sur K est pn :

$$\dim_K(E) \;=\; \dim_K(L) \times \dim_L(E).$$

Supposons seulement que E soit un K-espace vectoriel de dimension finie N. Toute partie génératrice de E sur K est *a fortiori* une partie génératrice de E sur L, de sorte que E est de dimension finie n sur L. Supposons $N \geqslant 1$, et soit u un vecteur non nul de E. Soit $D := \mathrm{Vect}_L(u)$ la droite vectorielle engendrée par u sur L. C'est un sous-L-espace vectoriel, *a fortiori* un sous-K-espace vectoriel de E. Comme E est de dimension finie sur K, D est de dimension finie p sur K. De plus $\lambda \mapsto \lambda \cdot u$ est un L-isomorphisme, et *a fortiori* un K-isomorphisme, de L sur D. Il en résulte que L est de dimension p sur K. Nous retrouvons les hypothèses précédentes, et ainsi $N = pn$. Voici la conclusion obtenue : si E est de dimension finie sur K et si $E \neq \{0\}$, alors d'une part L est de dimension finie sur K, et d'autre part E est de dimension finie sur L. Bien entendu, si $E = \{0\}$, on ne peut rien dire de la dimension de L sur K.

II.7.11 Soit k le plus petit sous-corps de K, au sens de l'inclusion, *i.e.* l'intersection de tous les sous-corps de K. D'après l'exercice II.2.39 de la page 158, la caractéristique de K est un nombre premier p, et k est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, en particulier k est de cardinal p. Comme k-espace vectoriel, K est de dimension finie, parce que K lui-même est une partie génératrice finie de K sur k. Soit donc n la dimension du k-espace vectoriel K. D'abord $n \geqslant 1$, car $0 \neq 1$ dans K, donc $K \neq \{0\}$. Ensuite K est isomorphe, *en tant que k-espace vectoriel*, à k^n. Tout k-isomorphisme de k^n sur K est en particulier une bijection de k^n sur K. Il en résulte que le cardinal q de K est égal au cardinal de k^n, c'est-à-dire à p^n : $q = p^n$.

II.7.12 1) Soient $A, B \in R_n$. Soit $j \in [\![1, n]\!]$. On a :

$$\sum_{i=1}^{n} (A+B)_{i,j} = \sum_{i=1}^{n} (A_{i,j} + B_{i,j}) = \sum_{i=1}^{n} A_{i,j} + \sum_{i=1}^{n} B_{i,j} = \ell(A) + \ell(B).$$

De même, si $i \in [\![1,n]\!]$ est fixé, il vient :

$$\sum_{j=1}^{n}(A+B)_{i,j} = \sum_{j=1}^{n}(A_{i,j}+B_{i,j}) = \sum_{j=1}^{n}A_{i,j} + \sum_{j=1}^{n}B_{i,j} = \ell(A)+\ell(B).$$

Ainsi $A+B \in R_n$, et en outre $\ell(A+B) = \ell(A)+\ell(B)$. Ensuite, pour tout $j \in [\![1,n]\!]$, on a :

$$\sum_{i=1}^{n}(AB)_{i,j} \;=\; \sum_{i=1}^{n}\left(\sum_{k=1}^{n}A_{i,k}B_{k,j}\right) \;=\; \sum_{k=1}^{n}B_{k,j}\left(\sum_{i=1}^{n}A_{i,k}\right) \;=$$

$$= \sum_{k=1}^{n}B_{k,j}\ell(A) \;=\; \ell(A)\sum_{k=1}^{n}B_{k,j} \;=\; \ell(A)\ell(B).$$

On montre de même que, pour tout $i \in [\![1,n]\!]$ fixé, $\sum\limits_{j=1}^{n}(AB)_{i,j} = \ell(A)\ell(B)$. Il en résulte que $AB \in R_n$, et de plus $\ell(AB) = \ell(A)\ell(B)$.

On vérifie aisément que, pour tout $\lambda \in K$, $\lambda A \in R_n$ et $\ell(\lambda A) = \lambda\ell(A)$. Enfin la matrice identité I_n appartient à R_n $\big($et $\ell(I_n) = 1\big)$, donc R_n est à la fois un sous-espace vectoriel et un sous-anneau de $M_n(K)$.

2) Nous venons de montrer que $\ell(I_n) = 1$. Pour toutes matrices $A, B \in R_n$, nous savons que $\ell(A+B) = \ell(A)+\ell(B)$, $\ell(AB) = \ell(A)\ell(B)$ et $\ell(\lambda A) = \lambda\ell(A)$ pour tout $\lambda \in K$. Ainsi $\ell : R_n \to K$ est à la fois un morphisme d'anneaux et une application K-linéaire.

3) Il est clair que $R_1 = M_1(K)$, donc R_1 est de dimension 1. Supposons $n \geqslant 2$. À toute matrice $A \in R_n$, associons le couple $\big(A', \ell(A)\big)$, où A' est la matrice déduite de A par suppression de la dernière ligne et de la dernière colonne. Nous obtenons ainsi une application f, évidemment linéaire (parce que ℓ l'est), de R_n dans $M_{n-1}(K) \times K$. L'espace vectoriel $M_{n-1}(K) \times K$ étant de dimension $(n-1)^2+1 = n^2-2n+2$, il nous suffit de vérifier que f est bijective.

Soit $A \in \operatorname{Ker} f$, montrons que $A = 0$. Puisque $A' = 0$, il suffit de voir que, pour tout $i \in [\![1,n]\!]$ fixé, $A_{i,n} = 0 = A_{n,i}$. Supposons d'abord $i \neq n$. Alors $A_{i,j} = 0$ pour $j = 1, \ldots, n-1$, d'où :

$$0 \;=\; \ell(A) \;=\; \sum_{j=1}^{n}A_{i,j} \;=\; A_{i,n} \quad \text{et} \quad 0 \;=\; \ell(A) \;=\; \sum_{j=1}^{n}A_{j,i} \;=\; A_{n,i}.$$

Enfin $A_{n,n} = 0$, parce que la somme des termes de la dernière colonne de A est nulle. En conclusion, f est injective (elle est linéaire et son noyau est trivial).

Montrons que f est surjective. Soient $M \in M_{n-1}(K)$ et $t \in K$. Définissons une matrice $A \in M_n(K)$ de la façon suivante. Pour tous indices $i, j \in [\![1,n-1]\!]$, nous posons d'abord $A_{i,j} := M_{i,j}$. Ensuite, pour tout $i \in [\![1,n-1]\!]$, nous posons :

$$A_{n,i} := t - \sum_{j=1}^{n-1}M_{j,i} \quad \text{et} \quad A_{i,n} := t - \sum_{j=1}^{n-1}M_{i,j}.$$

Il nous reste à définir $A_{n,n}$:

$$A_{n,n} \;:=\; t - \sum_{i=1}^{n-1}A_{n,i}.$$

La définition de A montre d'abord que M se déduit de A par suppression de la dernière ligne et de la dernière colonne. Ensuite, pour tout $i \in [\![1, n-1]\!]$, la somme des termes de la $i^{ème}$ ligne (respectivement $i^{ème}$ colonne) de A vaut t, par définition de $A_{i,n}$ (respectivement $A_{n,i}$). De même, la somme des termes de la dernière ligne de A vaut t. Calculons la somme des termes de la dernière colonne de A :

$$\begin{aligned}\sum_{k=1}^{n} A_{k,n} &= A_{n,n} + \sum_{k=1}^{n-1} A_{k,n} \\ &= A_{n,n} + \sum_{k=1}^{n-1} \left(t - \sum_{j=1}^{n-1} M_{k,j} \right) \\ &= A_{n,n} + (n-1)t - \sum_{k=1}^{n-1}\sum_{j=1}^{n-1} M_{k,j} \\ &= nt - \sum_{j=1}^{n-1} A_{n,j} - \sum_{k=1}^{n-1}\sum_{j=1}^{n-1} M_{k,j} \\ &= nt - \sum_{j=1}^{n-1} \left(t - \sum_{k=1}^{n-1} M_{k,j} \right) - \sum_{k=1}^{n-1}\sum_{j=1}^{n-1} M_{k,j} = t.\end{aligned}$$

La somme des termes de la dernière colonne de A vaut donc aussi t. Ainsi $A \in R_n$ et $\ell(A) = t$, d'où $f(A) = (M, t)$, ce qui prouve la surjectivité de f.

II.7.13 Comme $\dim(P) + \dim(D) = 2 + 1 = \dim(\mathbb{R}^3)$, l'égalité $P \cap D = \{0\}$ suffira pour montrer que $\mathbb{R}^3 = P \oplus D$ (proposition 17 de la page 337). Or D est formée des vecteurs (t, t, t), t décrivant $\mathbb{R}$, *i.e.* des vecteurs $(x, y, z) \in \mathbb{R}^3$ tels que $x = y = z$. Un tel vecteur n'appartient à P que si $3x = 0$, soit $x = 0$. D'où $\mathbb{R}^3 = P \oplus D$.

Soit $u := (x, y, z) \in \mathbb{R}^3$, calculons $s(u)$. On sait qu'il existe un unique couple $(v, w) \in P \times D$ tel que $u = v + w$, et alors $s(u) = v - w = u - 2w$, par définition de s. On écrit $v := (x', y', z')$, de sorte que $x' + y' + z' = 0$. Par ailleurs, il existe un unique $t \in \mathbb{R}$ tel que $w = (t, t, t)$. Dans ces conditions, $(x, y, z) = (x', y', z') + (t, t, t)$. En faisant la somme des composantes de chacun de ces vecteurs, il vient $x + y + z = 0 + 3t$, ce qui donne $t = (x + y + z)/3$. D'où $s(u)$:

$$s(u) \;=\; u - 2(t, t, t) \;=\; (x, y, z) - (2/3)\big(x + y + z, x + y + z, x + y + z\big)\,,$$

c'est-à-dire :

$$s(u) \;=\; \frac{1}{3}\Big(x - 2y - 2z, -2x + y - 2z, -2x - 2y + z\Big).$$

En prenant successivement pour u chacun des vecteurs de la base canonique de $\mathbb{R}^3$, on obtient la matrice de s dans cette base, à savoir :

$$\frac{1}{3}\begin{pmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ -2 & -2 & 1 \end{pmatrix}.$$

Par exemple, prenant $u := (1, 0, 0)$, il vient $s(u) = (1/3)(1, -2, -2)$, d'où la première colonne de ladite matrice.

II.7.14 Soit $A \in M_3(K)$ la matrice en question. Supposons d'abord qu'il existe une base $\mathcal{B}$ de E dans laquelle la matrice de f soit A. En fait A est la matrice $E_{1,2}$. En général, si $h, i, j, k \in [\![1, n]\!]$, on sait que $E_{h,i}E_{j,k} = \delta_{i,j}E_{h,k}$, où $\delta_{i,j}$ est le symbole de Kronecker. Ainsi $A^2 = E_{1,2}E_{1,2} = 0$. Comme A^2 est la matrice de f^2 dans la base $\mathcal{B}$, $f^2 = 0$.

Supposons inversement que $f^2 = 0$ mais $f \neq 0$. Le théorème du rang donne $\dim(\operatorname{Im} f) + \dim(\operatorname{Ker} f) = \dim(E) = 3$. L'égalité $f \circ f = 0$ équivaut ensuite à l'inclusion $\operatorname{Im} f \subset \operatorname{Ker} f$. Ainsi $\dim(\operatorname{Im} f) \leqslant \dim(\operatorname{Ker} f)$. Par ailleurs $f \neq 0$, autrement dit $\dim(\operatorname{Im} f) \geqslant 1$, ou encore $\dim(\operatorname{Ker} f) < 3$. Il n'y a donc qu'une seule possibilité : $\dim(\operatorname{Im} f) = 1$ et $\dim(\operatorname{Ker} f) = 2$. Soit e_1 un vecteur non nul de $\operatorname{Im} f$; il existe $e_2 \in E$ tel que $f(e_2) = e_1$. D'un autre côté, $e_1 \in \operatorname{Ker} f$ n'est pas nul. D'après le théorème de la base incomplète, il existe un vecteur $e_3 \in \operatorname{Ker} f$ tel que (e_1, e_3) soit une base de $\operatorname{Ker} f$. Comme $f(e_2) = e_1 \neq 0$, $e_2 \notin \operatorname{Ker} f$, et par suite $\mathcal{B} := (e_1, e_2, e_3)$ est libre, *i.e.* est une base de E. Enfin $f(e_1) = 0$, $f(e_2) = e_1$ et $f(e_3) = 0$, donc la matrice de f dans la base $\mathcal{B}$ est bien égale à A.

II.7.15 Notons f l'endomorphisme $P \longmapsto P(X + a)$ de $K_n[X]$. Notons de même g l'endomorphisme $P \longmapsto P(X - a)$ de $K_n[X]$. Il est clair que f et g sont deux automorphismes réciproques l'un de l'autre : si $P \in K_n[X]$, $g\big(f(P)\big) = f(P)(X - a) = P\big((X - a) + a\big) = P(X) = P$, de même $f\big(g(P)\big) = P$. Il en résulte que, si A est la matrice de f dans la base $\mathcal{B} := (1, X, \dots, X^n)$, A est inversible, son inverse étant la matrice de g dans la base $\mathcal{B}$.

Déterminons la matrice A. Soit $j \in [\![0, n]\!]$. La définition de f et la formule du binôme donnent :

$$f(X^j) = (X + a)^j = \sum_{i=0}^{j} \binom{j}{i} a^{j-i} X^i$$

La colonne d'indice j de A (c'est donc la $j + 1^{ème}$ colonne de A) a donc pour coefficients $\binom{j}{i} a^{j-i}$ pour $i = 0, \dots, j$, puis des zéros. Autrement dit :

$$A = \begin{pmatrix} 1 & \binom{1}{0}a & \binom{2}{0}a^2 & \cdots & \binom{n}{0}a^n \\ 0 & \binom{1}{1} & \binom{2}{1}a & \cdots & \binom{n}{1}a^{n-1} \\ 0 & 0 & \binom{2}{2} & \cdots & \binom{n}{2}a^{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \binom{n}{n} \end{pmatrix}.$$

Pour déterminer A^{-1}, matrice de g dans la base $\mathcal{B}$, il suffit de remplacer a par $-a$ dans A :

$$A^{-1} = \begin{pmatrix} 1 & -\binom{1}{0}a & \binom{2}{0}a^2 & \cdots & (-1)^n\binom{n}{0}a^n \\ 0 & \binom{1}{1} & -\binom{2}{1}a & \cdots & (-1)^{n-1}\binom{n}{1}a^{n-1} \\ 0 & 0 & \binom{2}{2} & \cdots & (-1)^{n-2}\binom{n}{2}a^{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \binom{n}{n} \end{pmatrix}.$$

Ainsi d'une part A^{-1} est triangulaire supérieure. D'autre part, si $i, j \in [\![0, n]\!]$ et $i \leqslant j$, le coefficient de A^{-1} situé sur la ligne d'indice i et la colonne d'indice j (*i.e.* sur la $i+1^{ème}$ ligne et la $j+1^{ème}$ colonne) est $(-1)^{j-i}\binom{j}{i}a^{j-i}$.

II.7.16 Soient $Q_1, Q_2 \in K_{n-1}[X]$. Pour $i = 1, 2$, $f(Q_i)$ est, par définition, le seul polynôme appartenant à $K_{n-1}[X]$ tel que P divise $Q_i - f(Q_i)$.

Mais alors P divise $Q_1+Q_2-\big(f(Q_1)+f(Q_2)\big)$, et $f(Q_1)+f(Q_2) \in K_{n-1}[X]$, ce qui montre que $f(Q_1) + f(Q_2) = f(Q_1 + Q_2)$. On montre de même que $f(\lambda Q_1) = \lambda f(Q_1)$ pour tout $\lambda \in K$, ce qui montre que $f : K_{n-1}[X] \to K_{n-1}[X]$ est linéaire : f est un endomorphisme de $K_{n-1}[X]$.

Soit $j \in [\![0, n-2]\!]$. Puisque $j + 1 \leqslant n - 1$, $X \cdot X^j = X^{j+1} \in K_{n-1}[X]$, et par suite $f(X^j)$ vaut simplement X^{j+1}. Calculons ensuite $f(X^{n-1})$. Par définition, c'est le reste dans la division de X^n par P. L'égalité :

$$X^n \;=\; P - \big[a_{n-1}X^{n-1} + \cdots + a_1X + a_0\big]$$

montre que ce reste n'est autre que l'opposé du terme entre crochets $\big($qui appartient bien à $K_{n-1}[X]\big)$. Ainsi :

$$f(X^{n-1}) \;=\; -\big[a_{n-1}X^{n-1} + \cdots + a_1X + a_0\big].$$

La matrice de f dans la base $(1, X, \ldots, X^{n-1})$ est donc la suivante (c'est une matrice à n lignes et n colonnes) :

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}.$$

II.7.17 1) Notons $a_{i,j}$ les coefficients de A. Par définition de la matrice d'un endomorphisme dans une base, on a :

$$f(e_j) \;=\; \sum_{i=1}^{n} a_{i,j}e_i \quad \text{pour tout} \quad j \in [\![1, n]\!]. \qquad (*)$$

Pour un indice j donné, il en résulte que $f(e_j)$ appartient à V_j si, et seulement si, $a_{i,j} = 0$ pour tout $i \in [\![j+1, n]\!]$. Ainsi $A \in T_n(K)$ si, et seulement si, $f(e_j) \in V_j$ pour tout $j \in [\![1, n]\!]$. On en déduit déjà que, si $f(V_k) \subset V_k$ pour tout $k \in [\![1, n]\!]$, A appartient à $T_n(K)$.

Supposons inversement que $A \in T_n(K)$, et soit $k \in [\![1, n]\!]$. Pour tout $j \in [\![1, k]\!]$, on a donc $f(e_j) \in V_j \subset V_k$, d'où $f(e_j) \in V_k$. Comme $(e_1, \ldots, e_k)$ est une famille génératrice de V_k, il en résulte que $f(V_k)$ est inclus dans V_k.

2) Soit A (resp. B) une matrice appartenant à $T_n(K)$ et f (resp. g) l'endomorphisme de K^n canoniquement associé à A (resp. B). La matrice de $f + g$ (resp. $f \circ g$) dans la base $\mathcal{B}$ est donc $A + B$ (resp. AB). Soit $k \in [\![1, n]\!]$. D'après la question 1), $f(V_k) \subset V_k$ et $g(V_k) \subset V_k$. Pour tout $x \in V_k$, $f(x) + g(x) \in V_k$, car $f(x) \in V_k$ et $g(x) \in V_k$; de même $g(x) \in V_k$, donc $(f \circ g)(x) = f\big(g(x)\big) \in f(V_k) \subset V_k$. Ainsi $(f + g)(V_k) \subset V_k$ et $(f \circ g)(V_k) \subset V_k$.

Cela étant vrai pour tout $k \in [\![1,n]\!]$, la question 1) montre que $A+B$ et AB appartiennent à $T_n(K)$. On voit de même que $\lambda A \in T_n(K)$ pour tout $\lambda \in K$, ce qui montre que $T_n(K)$ est un sous-espace vectoriel de $M_n(K)$. Enfin $I_n \in T_n(K)$, et donc $T_n(K)$ est un sous-anneau de $M_n(K)$.

Soit $H := T_n(K) \cap GL_n(K)$. C'est une partie stable de $GL_n(K)$, contenant I_n. Pour prouver que c'est un sous-groupe du groupe multiplicatif $GL_n(K)$, il suffit donc de vérifier que, si $A \in H$, alors A^{-1} appartient à H, c'est-à-dire que $A^{-1} \in T_n(K)$. Soit $f \in \mathcal{L}(K^n)$ l'endomorphisme canoniquement associé à A. D'abord f est un automorphisme de K^n, *i.e.* f est bijectif, en vertu du théorème 29 de la page 345. Soit alors $k \in [\![1,n]\!]$. D'après 1), $f(V_k) \subset V_k$. Mais f est injective, donc sa restriction à V_k est un isomorphisme de V_k sur $f(V_k)$. En particulier, $\dim\big(f(V_k)\big) = \dim(V_k) = k$. Ainsi $f(V_k)$ est un sous-espace vectoriel de V_k, de même dimension finie que V_k, donc $f(V_k) = V_k$, en vertu du théorème 10 de la page 334. Il en résulte que la réciproque f^{-1} de f vérifie : $f^{-1}(V_k) = V_k$. Cela étant vrai pour tout $k \in [\![1,n]\!]$, la question 1) montre que A^{-1}, matrice de f^{-1} dans la base $\mathcal{B}$, appartient à $T_n(K)$, comme désiré.

3) Supposons déjà que $A = (a_{i,j}) \in T_n(K)$, *i.e.* que $f(V_k) \subset V_k$ pour tout $k \in [\![1,n]\!]$. Alors $A \in T_n^*(K)$ si, et seulement si, $a_{k,k} = 0$ pour tout $k \in [\![1,n]\!]$. L'égalité $a_{1,1} = 0$ équivaut à $f(e_1) = 0$, soit $f(V_1) = \{0\}$. Soit $k \in [\![2,n]\!]$. Pour tout $j \in [\![1,k-1]\!]$, on a déjà $f(e_j) \in V_j \subset V_{k-1}$. Ainsi, puisque $f(e_1), \dots, f(e_k)$ engendrent $f(V_k)$, l'inclusion $f(V_k) \subset V_{k-1}$ est vraie si, et seulement si, $f(e_k) \in V_{k-1}$ ce qui, compte tenu de l'égalité $(*)$ (où l'on remplace j par k), signifie que $a_{k,k} = 0$. D'où l'équivalence annoncée.

Soient maintenant $A_1, \dots, A_n \in T_n^*(K)$ et $A = A_1 A_2 \cdots A_n$. Pour tout $j \in [\![1,n]\!]$, notons f_j l'endomorphisme de K^n canoniquement associé à A_j, et de même notons f l'endomorphisme de K^n canoniquement associé à A. Ainsi $f = f_1 \circ f_2 \circ \cdots \circ f_n$. Montrons par récurrence sur $k \in [\![1,n]\!]$ que la restriction de $f_1 \circ f_2 \circ \cdots \circ f_k$ à V_k est nulle. Le début de cette question montre que $f(V_1) = \{0\}$, d'où le cas $k = 1$. Supposons que $k \in [\![2,n]\!]$, et que la restriction de $f_1 \circ f_2 \circ \cdots \circ f_{k-1}$ à V_{k-1} soit nulle. Soit $x \in V_k$. Toujours d'après le début de cette question, $f_k(x) \in V_{k-1}$. D'où :

$$(f_1 \circ f_2 \circ \cdots \circ f_k)(x) = (f_1 \circ f_2 \circ \cdots \circ f_{k-1})\big(f_k(x)\big) \in (f_1 \circ \cdots \circ f_{k-1})(V_{k-1}) = \{0\}.$$

Cela démontre notre assertion au rang k. Ainsi cette assertion est vraie au rang n. Comme $V_n = K^n$, cela prouve l'égalité $f_1 \circ f_2 \circ \cdots \circ f_n = 0$, c'est-à-dire $f = 0$. La matrice de f dans la base $\mathcal{B}$ est donc nulle, *i.e.* $A = 0$, comme désiré.

II.7.18 Notons r le rang de A, et posons :

$$Z(A) \;:=\; \big\{M \in M_{m,n}(K) \;\big|\; MA = 0\big\}.$$

Si $r = 0$, *i.e.* si $A = 0$, $Z(A)$ est égal à $M_{m,n}(K)$, donc est de dimension mn. Supposons $r \geqslant 1$. Appliquons le théorème 34 de la page 349. Il existe deux matrices $Q \in GL_n(K)$ et $P \in GL_p(K)$ telles que la matrice $A' := Q^{-1}AP$ vaille :

$$A' \;=\; I_r^{(n,p)} \;:=\; \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix} = \sum_{i=1}^{r} E_{i,i}\,.$$

Cela étant, soit $M \in M_{m,n}(K)$. Puisque P est inversible, $MA = 0$ équivaut à $MAP = 0$, ou encore à $MQA' = 0$. On en déduit facilement que $M \mapsto MQ$ est un isomorphisme de $Z(A)$ sur $Z(A')$, d'où $\dim\big(Z(A)\big) = \dim\big(Z(A')\big)$. Soit alors $N \in M_{m,n}(K)$. La définition de la multiplication de deux matrices montre que NA' a les mêmes colonnes d'indices $1, \dots, r$ que N, ses colonnes d'indices $r+1, \dots, p$ étant nulles. Ainsi $Z(A')$ est formé des matrices $N \in M_{m,n}(K)$ dont les r premières colonnes sont nulles. Il en résulte aussitôt que $Z(A')$ est isomorphe à $(K^m)^{n-r}$, d'où :

$$\dim\big(Z(A)\big) \;=\; \dim\big(Z(A')\big) \;=\; m(n-r).$$

Donnons maintenant une solution « géométrique ». Notons $\mathcal{B}, \mathcal{C}, \mathcal{D}$ les bases canoniques de K^m, K^n, K^p respectivement. Soit $f \in \mathcal{L}(K^p, K^n)$ l'application linéaire canoniquement associée à A : $\mathrm{Mat}_{\mathcal{D}}^{\mathcal{C}}(f) = A$. Soient ensuite $M \in M_{m,n}(K)$ une matrice variable et $g \in \mathcal{L}(K^n, K^m)$ l'application linéaire canoniquement associée à M : $\mathrm{Mat}_{\mathcal{C}}^{\mathcal{B}}(g) = M$. Alors $MA = \mathrm{Mat}_{\mathcal{D}}^{\mathcal{B}}(g \circ f)$. Il en résulte aisément que $g \mapsto \mathrm{Mat}_{\mathcal{C}}^{\mathcal{B}}(g)$ est un isomorphisme de $Z(f)$ sur $Z(A)$, en posant :

$$Z(f) \;:=\; \big\{g \in \mathcal{L}(K^n, K^m) \;\big|\; g \circ f = 0\big\}.$$

Nous sommes ramenés à calculer la dimension de $Z(f)$. Notons d'abord que $g \in \mathcal{L}(K^n, K^m)$ appartient à $Z(f)$ si, et seulement si, la restriction de g à $\mathrm{Im}\, f$ est nulle. Soit alors H un supplémentaire de $\mathrm{Im}\, f$ dans K^n : $K^n = \mathrm{Im}\, f \oplus H$. Nous savons qu'une application linéaire $g \in \mathcal{L}(K^n, K^m)$ est entièrement déterminée par ses restrictions à $\mathrm{Im}\, f$ et H. Si donc à g on associe le couple formé par ses deux restrictions à $\mathrm{Im}\, f$ et H respectivement, on obtient un isomorphisme de $\mathcal{L}(K^n, K^m)$ sur $\mathcal{L}(\mathrm{Im}\, f, K^m) \times \mathcal{L}(H, K^m)$. La restriction de cet isomorphisme à $Z(f)$ est alors un isomorphisme de $Z(f)$ sur $\{0\} \times \mathcal{L}(H, K^m)$. D'où :

$$\dim\big(Z(f)\big) \;=\; \dim\big(\mathcal{L}(H, K^m)\big) \;=\; \dim(H) \times \dim(K^m) \;=\; m\dim(H).$$

Enfin $\mathrm{Im}\, f$ est de dimension r, donc $\dim(H) = n - r$ (théorème 12 de la page 335), et nous retrouvons la formule $\dim\big(Z(f)\big) = m(n-r)$.

Supposons enfin que $M \in M_{m,n}(K)$ soit fixée, de rang s. Posons :

$$Z'(M) \;:=\; \big\{A \in M_{n,p}(K) \;\big|\; MA = 0\big\}.$$

Soit $A \in M_{n,p}(K)$. Raisonnons par transposition. L'égalité $MA = 0$ équivaut à ${}^t(MA) = 0$, c'est-à-dire à $({}^tA)({}^tM) = 0$, ou encore à ${}^tA \in Z({}^tM)$. On en déduit aisément que $A \mapsto {}^tA$ est un isomorphisme de $Z'(M)$ sur $Z({}^tM)$. La matrice ${}^tM$ étant aussi de rang s, ce qui précède montre que $\dim\big(Z({}^tM)\big) = p(n-s)$ (en appliquant ce qui précède, il faut échanger m et p). La solution géométrique est ici très simple. Avec les notations introduites ci-dessus, g est fixée, de rang s. L'égalité $g \circ f =$ signifie que f est à valeurs dans $\mathcal{L}(K^p, \mathrm{Ker}\, g)$. Mais le théorème du rang donne $\dim(\mathrm{Ker}\, g) = n - s$. La dimension cherchée est alors celle de $\mathcal{L}(K^p, \mathrm{Ker}\, g)$, c'est-à-dire $p(n-s)$.

II.7.19 Notons A la matrice visée et D son déterminant. La formule (23) donne :

$$D = \big(1\times 4\times 7\big) + \big(3\times 1\times 3\big) + \big((-2)\times(-2)\times 5\big) - \big(3\times(-2)\times 7\big) - \big(5\times 4\times 3\big)$$
$$-\big(1\times 1\times(-2)\big) \;=\; 28 + 9 + 20 - (-42) - (60) - (-2) \;=\; 41.$$

Développons ensuite D par rapport à sa première ligne :

$$D \;=\; 1\times\begin{vmatrix} 4 & 1 \\ -2 & 7 \end{vmatrix} - 3\times\begin{vmatrix} -2 & 1 \\ 3 & 7 \end{vmatrix} + 5\times\begin{vmatrix} -2 & 4 \\ 3 & -2 \end{vmatrix}, \quad \text{soit}$$

$$D \;=\; 1\times(28+2) - 3\times(-14-3) + 5\times(4-12) \;=\; 30+51-40 \;=\; 41.$$

Notons L_1, L_2, L_3 les lignes et C_1, C_2, C_3 les colonnes. Prenons le terme d'indice $(1,1)$ comme pivot. Les transvections $L_2 \leftarrow L_2 + 2L_1$ puis $L_3 \leftarrow L_3 - 3L_1$ donnent :

$$D \;=\; \begin{vmatrix} 1 & 3 & 5 \\ 0 & 10 & 11 \\ 3 & -2 & 7 \end{vmatrix} \;=\; \begin{vmatrix} 1 & 3 & 5 \\ 0 & 10 & 11 \\ 0 & -11 & -8 \end{vmatrix}.$$

Ensuite les transvections $L_2 \leftarrow L_2 + L_3$ puis $L_3 \leftarrow L_3 - 11L_2$ donnent :

$$D \;=\; \begin{vmatrix} 1 & 3 & 5 \\ 0 & -1 & 3 \\ 0 & -11 & -8 \end{vmatrix} \;=\; \begin{vmatrix} 1 & 3 & 5 \\ 0 & -1 & 3 \\ 0 & 0 & -41 \end{vmatrix} \;=\; 1\times(-1)\times(-41) \;=\; 41.$$

En conclusion, par une suite de transvections portant sur les lignes, nous avons transformé A en une matrice triangulaire supérieure, dont le déterminant est produit des termes diagonaux.

II.7.20 Soit D le déterminant à calculer.

Tout d'abord, la transvection $L_4 \leftarrow L_1 + L_2 + L_3 + L_4$ donne :

$$D \;=\; \begin{vmatrix} x & a & b & c \\ a & x & c & b \\ b & c & x & a \\ (x+a+b+c) & (x+a+b+c) & (x+a+b+c) & (x+a+b+c) \end{vmatrix}.$$

Par linéarité par rapport à la dernière ligne, on en déduit :

$$D \;=\; (x+a+b+c)D', \quad \text{où} \quad D' \;:=\; \begin{vmatrix} x & a & b & c \\ a & x & c & b \\ b & c & x & a \\ 1 & 1 & 1 & 1 \end{vmatrix}.$$

La transvection $C_1 \leftarrow C_1 + C_2 - C_3 - C_4$ donne :

$$D' \;=\; (x+a-b-c)D'', \quad \text{où} \quad D'' \;:=\; \begin{vmatrix} 1 & a & b & c \\ 1 & x & c & b \\ -1 & c & x & a \\ 0 & 1 & 1 & 1 \end{vmatrix}.$$

Les transvections $L_1 \leftarrow L_1 + L_3$ et $L_2 \leftarrow L_2 + L_3$ donnent :

$$D'' \;=\; \begin{vmatrix} 0 & a+c & x+b & a+c \\ 0 & x+c & x+c & a+b \\ -1 & c & x & a \\ 0 & 1 & 1 & 1 \end{vmatrix} \;=\; -\begin{vmatrix} a+c & x+b & a+c \\ x+c & x+c & a+b \\ 1 & 1 & 1 \end{vmatrix}.$$

La transvection $C_1 \leftarrow C_1 - C_2$ donne, par linéarité par rapport à la première colonne :

$$D'' \;=\; (x+b-a-c)\begin{vmatrix} 1 & x+b & a+c \\ 0 & x+c & a+b \\ 0 & 1 & 1 \end{vmatrix} \;=\; (x+b-a-c)\begin{vmatrix} x+c & a+b \\ 1 & 1 \end{vmatrix},$$

d'où $D'' = (x+b-a-c)(x+c-a-b)$. On obtient le résultat escompté :

$$D \;=\; (x+a+b+c)(x+a-b-c)(x+b-a-c)(x+c-a-b).$$

II.7.21 Soit D le déterminant en question. Pour tout entier $n \geqslant 2$, notons π_n le morphisme canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$; si n est fixé, π_n sera aussi noté $k \mapsto \bar{k}$. Nous savons que $\pi_n(D)$ est le déterminant obtenu en remplaçant dans D chaque coefficient par son image par π_n. Prenons d'abord $n := 5$. La transvection $C_3 \leftarrow C_1 + C_2 + C_3$ donne :

$$\bar{D} \;=\; \begin{vmatrix} \bar{3} & 0 & \bar{2} \\ \bar{4} & -\bar{1} & \bar{2} \\ -\bar{2} & \bar{2} & 0 \end{vmatrix} \;=\; \begin{vmatrix} \bar{3} & 0 & 0 \\ \bar{4} & -\bar{1} & 0 \\ -\bar{2} & \bar{2} & 0 \end{vmatrix} \;=\; 0.$$

Cela montre que D est multiple de 5. Prenons ensuite $n := 2$:

$$\bar{D} \;=\; \begin{vmatrix} \bar{1} & \bar{1} & \bar{1} \\ 0 & \bar{1} & 0 \\ 0 & 0 & \bar{1} \end{vmatrix} \;=\; \begin{vmatrix} \bar{1} & \bar{1} \\ 0 & \bar{1} \end{vmatrix} \;=\; \bar{1}.$$

Ainsi D est impair, *i.e.* $\pi_2(D) = \bar{1}$. En conclusion, D est congru à 0 modulo 5 et à 0 modulo 2, donc D est congru à 5 modulo 10, ce qui signifie que le chiffre des unités (dans le système décimal) de D est 5.

II.7.22 Soit D le déterminant en question. La formule (23) donne :

$$D \;=\; 1 - \cos^2 a - \cos^2 b - \cos^2 c + 2\cos a \cos b \cos c.$$

Nous savons que $a + b + c = \pi$, d'où :

$$\sin c \;=\; \sin(\pi - a - b) \;=\; \sin(a+b) \;=\; \sin a \cos b + \sin b \cos a.$$

On en déduit :

$$\begin{aligned} 1 - \cos^2 a - \cos^2 b - \cos^2 c &= \sin^2(a+b) - \cos^2 a - \cos^2 b \\ &= (\sin a \cos b + \sin b \cos a)^2 - \cos^2 a - \cos^2 b \\ &= \cos^2 a(\sin^2 b - 1) + \cos^2 b(\sin^2 a - 1) + 2\cos a \cos b \sin a \sin b \\ &= -2\cos^2 a \cos^2 b + 2\cos a \cos b \sin a \sin b \\ &= -2\cos a \cos b(\cos a \cos b - \sin a \sin b) \\ &= -2\cos a \cos b \cos(a+b) \\ &= 2\cos a \cos b \cos(\pi - a - b) \\ &= 2\cos a \cos b \cos c. \end{aligned}$$

D'où $D = 4\cos a \cos b \cos c$, comme annoncé.

II.7.23 Considérons la matrice $B := XI_n - A$, dont les coefficients seront notées $b_{i,j}$. Par définition, $\chi_A = \det B$. Par ailleurs, pour tous $i, j \in [\![1, n]\!]$, $b_{i,j} = \delta_{i,j}X - a_{i,j}$, où $\delta_{i,j}$ est le symbole de Kronecker. Partons de la formule (23) :

$$\det B \;=\; \sum_{s \in \mathfrak{S}_n} \varepsilon(s) P_s\,, \quad \text{où}$$

$$P_s \;:=\; \prod_{j=1}^{n} b_{s(j),j} \;=\; \prod_{j=1}^{n} \bigl(\delta_{s(j),j} X - a_{s(j),j}\bigr).$$

Considérons une permutation $s \in \mathfrak{S}_n$. Appliquons la formule (28) citée pour évaluer P_s :

$$P_s \;=\; \sum_{J} \left(\prod_{j\in J} (-1)^{|J|} a_{s(j),j} \right) \left(\prod_{j\in J'} \delta_{s(j),j} X \right).$$

Dans cette formule, J décrit l'ensemble des parties de $[\![1,n]\!]$ et, pour toute partie J, $|J|$ désigne le cardinal de J et $J' := [\![1,n]\!] \setminus J$. Pour tout entier $k \in [\![1,n]\!]$, notons p_k le coefficient de X^{n-k} dans χ_A. Compte tenu des égalités ci-dessus, il vient :

$$(-1)^k p_k \;=\; \sum_{s\in\mathfrak{S}_n} \varepsilon(s) \left\{ \sum_{|J|=k} \left(\prod_{j\in J} a_{s(j),j} \right) \left(\prod_{j\in J'} \delta_{s(j),j} \right) \right\}, \quad \text{soit}$$

$$(-1)^k p_k \;=\; \sum_{|J|=k} \Delta_J \,,$$

en posant, pour toute partie J de cardinal k de $[\![1,n]\!]$:

$$\Delta_J \;:=\; \sum_{s\in\mathfrak{S}_n} \varepsilon(s) \left(\prod_{j\in J} a_{s(j),j} \right) \left(\prod_{j\in J'} \delta_{s(j),j} \right).$$

Écrivons $J := \{j_1, \ldots, j_k\}$, où $j_1 < j_2 < \cdots < j_k$. Soit $s \in \mathfrak{S}_n$. Le produit des $\delta_{s(j),j}$ pour $j \in J'$ est non nul si, et seulement si, s laisse fixe chaque indice $i \in [\![1,n]\!] \setminus J$, auquel cas ce produit vaut 1. Notons S_J l'ensemble des $s \in \mathfrak{S}_n$ ayant la propriété en question. Nous obtenons :

$$\Delta_J \;=\; \sum_{s\in S_j} \varepsilon(s) \left(\prod_{j\in J} a_{s(j),j} \right).$$

À toute permutation $t \in \mathfrak{S}_k$ associons la permutation s de $[\![1,n]\!]$ définie ainsi : $s(j_h) := j_{t(h)}$ pour tout $h \in [\![1,k]\!]$ et $s(i) := i$ pour tout $i \in [\![1,n]\!] \setminus J$. On définit ainsi un isomorphisme de $\mathfrak{S}_k$ sur S_J, et de plus $\varepsilon(s) = \varepsilon(t)$. D'où :

$$\Delta_J \;=\; \sum_{t\in\mathfrak{S}_k} \varepsilon(t) \left(\prod_{h=1}^{k} a_{j_{t(h)},j_h} \right).$$

cette formule montre que Δ_J est le déterminant de la matrice extraite de A, obtenue à partir des lignes et colonnes de A dont l'indice appartient à J. En d'autres termes, $\Delta_J = D_J$, avec les notations de l'énoncé. D'où la formule annoncée :

$$p_k \;=\; (-1)^k \sum_{|J|=k} D_J.$$

Supposons maintenant que K soit égal à $\mathbb{R}$ et que tous les D_J soient positifs ou nuls. On a donc $(-1)^k p_k \geqslant 0$ pour tout $k \in [\![1,n]\!]$. Considérons un nombre réel $\lambda < 0$, et posons $u := -\lambda$. Alors :

$$\chi_A(\lambda) \;=\; \lambda^n + \sum_{k=1}^{n} (-1)^k p_k \lambda^{n-k} \;=\; (-1)^n \Bigl[u^n + \sum_{k=1}^{n} p_k u^{n-k} \Bigr].$$

Puisque $u > 0$ et $p_k \geqslant 0$ pour tout k, on en déduit : $(-1)^n \chi_A(\lambda) > 0$, en particulier $\chi_A(\lambda) \neq 0$. Cela montre que λ n'est pas valeur propre de A. En conclusion, A ne possède aucune valeur propre réelle strictement négative.

II.7.24 Soit r le rang de A. Si $r := 0$, *i.e.* si $A := 0$, il est clair que $\widetilde{A}$ est aussi nulle, donc de rang 0 et de déterminant 0. Supposons désormais $A \neq 0$. Rappelons que $A \times {}^t\widetilde{A} = \det(A) I_n$. Supposons d'abord A inversible, *i.e.* $r := n$. L'égalité précédente donne, en prenant les déterminants et en se souvenant qu'une matrice carrée et sa transposée ont le même déterminant :

$$\det(A)^n \;=\; \det\big(\det(A) I_n\big) \;=\; \det(A)\det(\widetilde{A}).$$

En simplifiant par $\det A$, il vient : $\det(\widetilde{A}) = \det(A)^{n-1}$. Si A n'est pas inversible, $\det A = 0$. D'un autre côté, $\widetilde{A}$ n'est pas inversible, car, si elle l'était, l'égalité $A \times {}^t\widetilde{A} = \det(A) I_n$ impliquerait $A = 0$. Ainsi $\det(\widetilde{A}) = 0$. L'égalité obtenue est donc vraie quelle que soit A :

$$\det(\widetilde{A}) \;=\; \det(A)^{n-1}.$$

Nous avons vu que, si $r := n$, *i.e.* si A est inversible, $\widetilde{A}$ est inversible, *i.e.* de rang n, puisque son déterminant n'est pas nul. Il nous reste à calculer le rang de $\widetilde{A}$ lorsque $1 \leqslant r \leqslant n-1$. Rappelons que les coefficients de $\widetilde{A}$ sont au signe près des mineurs d'ordre $n-1$ de A. Si $r \leqslant n-2$, tous ces mineurs sont nuls, en vertu du théorème 47 de la page 360 ou de son corollaire. Ainsi $\widetilde{A} = 0$ dans ce cas.

Supposons enfin que $r := n-1$. D'après le théorème 47 de la page 360 ou son corollaire, $\widetilde{A}$ n'est alors pas nulle, car A possède un mineur non nul d'ordre $n-1$. Par ailleurs, soit f (resp. g) l'endomorphisme canoniquement associé à A (resp. $\widetilde{A}$). Comme $\det A = 0$, on a $A \times \widetilde{A} = 0$, d'où $f \circ g = 0$. Ainsi $\operatorname{Im} g \subset \operatorname{Ker} f$. Mais le théorème du rang montre que $\operatorname{Ker} f$ est de dimension 1, donc le rang de g (dimension de $\operatorname{Im} g$) est au plus égal à 1. On en déduit l'inégalité $\operatorname{rang}(\widetilde{A}) = \operatorname{rang}(g) \leqslant 1$, d'où en fait $\operatorname{rang}(\widetilde{A}) = 1$. Voici la conclusion obtenue :

$$\operatorname{rang}(\widetilde{A}) \;=\; \begin{cases} 0 & \text{si } r \leqslant n-2, \\ 1 & \text{si } r := n-1, \\ n & \text{si } r := n. \end{cases}$$

II.7.25 1) Soient donc $\mathcal{B} := (e_1, \ldots, e_n)$ une base de E et A la matrice de u dans cette base. D'après le théorème et définition 49 de la page 362, $\det u = \det A$. Par ailleurs, puisque u est inversible, $\mathcal{C} := \big(u(e_1), \ldots, u(e_n)\big)$ est une base de E, et, par définition, A est la matrice de passage de $\mathcal{B}$ à $\mathcal{C}$. Ainsi, pour que les bases $\mathcal{B}$ et $\mathcal{C}$ soient de même sens, il faut, et il suffit, que le déterminant de A soit strictement positif.

2) Soient donc $\lambda \in \mathbb{R}^*$ et $u := \lambda Id_E$ l'homothétie de rapport λ. Nous savons que $\det u = \lambda^n$. Il en résulte que u conserve l'orientation si, et seulement si, ou bien $\lambda > 0$, ou bien n est pair.

3) Posons $r := \dim(V)$. D'après l'exemple 2 de la page 362, $\det(s) = (-1)^{n-r}$. Il en résulte que s conserve l'orientation si, et seulement si, $n - r$ est pair, *i.e.* si la dimension de W est paire.

II.7.26 La formule explicite (23) donne, pour tout $t \in I$:

$$D(t) \;=\; \det\big(A(t)\big) \;=\; \sum_{s\in\mathfrak{S}_n} \varepsilon(s) P_s(t)\,, \quad \text{où}$$

$$P_s(t) \;:=\; \prod_{j=1}^{n} a_{s(j),j}(t).$$

Comme chacune des fonctions $a_{i,j}$ est dérivable sur I, il en est de même pour les fonctions P_s. Soit $s \in \mathfrak{S}_n$. La règle de dérivation d'un produit donne :

$$P_s'(t) \;=\; \sum_{j=1}^{n} a_{s(1),1}(t) a_{s(2),2}(t) \cdots a'_{s(j),j}(t) \cdots a_{s(n),n}(t).$$

On en déduit ceci : pour tout $t \in I$,

$$D'(t) = \sum_{j=1}^{n} \left(\sum_{s\in\mathfrak{S}_n} \varepsilon(s) a_{s(1),1}(t) a_{s(2),2}(t) \cdots a'_{s(j),j}(t) \cdots a_{s(n),n}(t) \right).$$

Dans le second membre de la dernière égalité, si $j \in [\![1,n]\!]$, le terme d'indice j n'est autre que le déterminant, dans la base canonique de $\mathbb{R}^n$, de la famille $\big(C_1(t), C_2(t), \ldots, C_j'(t), \ldots, C_n(t)\big)$. D'où le résultat annoncé.

II.7.27 1) Pour tout $(a,b) \in \mathbb{C}^2$, posons $M(a,b) := \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$.

Notons f l'application $(a,b) \mapsto M(a,b)$ de $\mathbb{C}^2$ dans $\mathcal{H}$, elle est surjective, par définition de $\mathcal{H}$. La forme de la première ligne d'une matrice $M(a,b)$ montre que f est injective, c'est donc une bijection de $\mathbb{C}^2$ sur $\mathcal{H}$.

Soient $(a,b),(c,d) \in \mathbb{C}^2$ et $\lambda \in \mathbb{R}$. Alors :

$$M(a,b) + M(c,d) = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} + \begin{pmatrix} c & d \\ -\bar{d} & \bar{c} \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -\overline{b+d} & \overline{a+c} \end{pmatrix},$$

soit $M(a,b) + M(c,d) = M(a+c, b+d)$. De même :

$$\lambda M(a,b) \;=\; \lambda \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \;=\; \begin{pmatrix} \lambda a & \lambda b \\ -\overline{\lambda b} & \overline{\lambda a} \end{pmatrix} \;=\; M(\lambda a, \lambda b).$$

Cela montre que f est $\mathbb{R}$-linéaire. Il en résulte que l'image de f, à savoir $\mathcal{H}$, est un sous-$\mathbb{R}$-espace vectoriel de $M_2(\mathbb{C})$. De plus f est un isomorphisme de $\mathbb{R}$-espaces vectoriels. Pour obtenir une base de $\mathcal{H}$ sur $\mathbb{R}$, il suffit de prendre les images par f des vecteurs d'une base de $\mathbb{C}^2$ sur $\mathbb{R}$. Les vecteurs $(1,0)$, $(i,0)$, $(0,1)$ et $(0,i)$ forment une base de $\mathbb{C}^2$ sur $\mathbb{R}$. Avec les notations de la question 3), les images par f des vecteurs précédents sont : $\mathbf{1} := I_2$, $\mathbf{j}$, $-\mathbf{i}$ et $\mathbf{k}$ respectivement. En particulier $(\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k})$ est une base de $\mathcal{H}$ sur $\mathbb{R}$.

Soient $(a,b),(c,d) \in \mathbb{C}^2$. Alors :

$$M(a,b)M(c,d) = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \begin{pmatrix} c & d \\ -\bar{d} & \bar{c} \end{pmatrix} = \begin{pmatrix} ac - b\bar{d} & ad + b\bar{c} \\ -c\bar{b} - \bar{a}\bar{d} & \bar{a}\bar{c} - d\bar{b} \end{pmatrix},$$

soit $M(a,b)M(c,d) = M(ac - b\bar{d}, ad + b\bar{c}) \in \mathcal{H}$. Ainsi $\mathcal{H}$ est une partie multiplicativement stable de $M_2(\mathbb{C})$. Comme $I_2 \in \mathcal{H}$, cela montre que $\mathcal{H}$ est un sous-anneau de $M_2(\mathbb{C})$.

La matrice identité I_2 appartient à $\mathcal{H}$, mais $iI_2 \notin \mathcal{H}$: si $(a,b) \in \mathbb{C}^2$, on ne peut avoir à la fois $a = i$ et $\bar{a} = i$. Ainsi $\mathcal{H}$ n'est pas un sous-$\mathbb{C}$-espace vectoriel de $M_2(\mathbb{C})$, ce qui montre en passant que l'application f n'est pas $\mathbb{C}$-linéaire.

2) Puisque $\mathbf{1} \neq 0$ dans $\mathcal{H}$, l'anneau $\mathcal{H}$ est un corps si, et seulement si, tout élément non nul de $\mathcal{H}$ est inversible dans $\mathcal{H}$. Soient donc $(a,b) \in \mathbb{C}^2$, $(a,b) \neq (0,0)$, et $M := M(a,b)$. Par définition de $M(a,b)$, $\det M = |a|^2 + |b|^2$, d'où $\det M \neq 0$. Ainsi M est inversible dans $M_2(\mathbb{C})$. On peut de plus calculer M^{-1}, par exemple à l'aide du théorème 45 de la page 359 :

$$M^{-1} = \frac{1}{|a|^2+|b|^2}\begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix} = \frac{1}{|a|^2+|b|^2} M(\bar{a}, -b).$$

Puisque $\mathcal{H}$ est un sous-$\mathbb{R}$-espace vectoriel de $M_2(\mathbb{C})$, la formule précédente montre que M^{-1} appartient à $\mathcal{H}$, donc $\mathcal{H}$ est un corps.

Nous avons vu que, si $M \in \mathcal{H}$ n'est pas nulle, $\det(M) \neq 0$. Il en résulte que, si $M, M' \in \mathcal{H}$ sont non nulles, $\det(MM') = \det(M)\det(M') \neq 0$, en particulier $MM' \neq 0$. En d'autres termes, $\mathcal{H}$ est une sous-$\mathbb{R}$-algèbre *intègre* de $M_2(\mathbb{C})$. D'après l'exercice 4 de la page 339, $\mathcal{H}$ est un corps.

3) Soit donc $\mathbf{H}$ le corps des quaternions, *cf.* l'exercice 4 du module II.5. C'est en particulier un $\mathbb{R}$-espace vectoriel de dimension 4, de base $(1, i, j, k)$. Dans cette base, la multiplication de $\mathbf{H}$ obéit à la table de multiplication suivante :

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

La multiplication de $\mathbf{H}$ vérifie en outre la propriété suivante : pour tous $x, y \in \mathbf{H}$ et $a \in \mathbb{R}$, on a : $a \cdot (xy) = x(a \cdot y) = (a \cdot x)y$. Cela étant, il existe un unique isomorphisme de $\mathbb{R}$-espaces vectoriels φ de $\mathcal{H}$ sur $\mathbf{H}$ appliquant $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ sur $1, i, j, k$ respectivement. On vérifie aisément que les éléments $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ de $\mathcal{H}$ obéissent à la même table de multiplication que les éléments $1, i, j, k$ de $\mathbf{H}$. Par exemple :

$$\mathbf{ij} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \mathbf{k}.$$

On en déduit facilement que φ est aussi un isomorphisme d'anneaux de $\mathcal{H}$ sur $\mathbf{H}$. Ainsi les corps $\mathcal{H}$ et $\mathbf{H}$ sont isomorphes.

II.7.28 1) La conclusion est évidente si $n = 1$: la fonction $x \longmapsto t_1 x^{b_1}$ ne s'annule pas sur I. Supposons que la conclusion soit vraie à l'ordre $n-1$, pour un certain entier $n \geqslant 2$. Soient alors $t_1, \ldots, t_n, b_1, \ldots, b_n$ et f comme dans l'énoncé. Considérons la fonction g définie sur I ainsi :

$$g(x) := x^{-b_n} f(x) = t_1 x^{b_1 - b_n} + t_2 x^{b_2 - b_n} + \cdots + t_{n-1} x^{b_{n-1} - b_n} + t_n\,.$$

Pour tout $x \in I$, les égalités $f(x) = 0$ et $g(x) = 0$ sont équivalentes. Raisonnons alors par l'absurde, en supposant qu'il existe n éléments distincts $x_1, \dots, x_n$ de I en lesquels g s'annule. On supposera $x_1 < x_2 < \cdots < x_n$. Les fonctions f et g sont de classe C^1 (et même C^∞) sur I. Nous pouvons donc appliquer le théorème de Rolle sur chacun des intervalles $\big[x_k, x_{k+1}\big]$, pour $k = 1, \dots, n-1$. Pour chaque k, il existe un point $c_k \in \big]x_k, x_{k+1}\big[$ tel que $g'(c_k) = 0$. En outre $c_1 < c_2 < \cdots < c_{n-1}$, de sorte que g' s'annule en au moins $n-1$ points de I. Or, pour tout $x \in I$, $g'(x)$ est la somme :

$$t_1(b_1 - b_n)x^{b_1 - b_n - 1} + t_2(b_2 - b_n)x^{b_2 - b_n - 1} + \cdots + t_{n-1}(b_{n-1} - b_n)x^{b_{n-1} - b_n - 1}.$$

Le fait que g' s'annule en au moins $n-1$ points de I contredit donc l'hypothèse de récurrence. Noter que ce n'est qu'en remplaçant f par g que nous avons pu éliminer, par dérivation, le terme constant t_n.

2) Raisonnons encore par récurrence sur n. Le cas $n = 1$ est évident : alors $D = x_1^{a_1} > 0$. Supposons $n \geqslant 2$, le résultat étant vrai à l'ordre $n-1$. Soient ensuite $x_1, \dots, x_n, a_1, \dots, a_n$ et D, g comme dans l'énoncé. Pour tout $j \in [\![1, n-1]\!]$, $g(x_j)$ est le déterminant d'une matrice ayant deux lignes égales, celles d'indices j et n, donc $g(x_j) = 0$. D'un autre côté, étant donné $x \in I$, développons le déterminant définissant $g(x)$ par rapport à sa dernière ligne :

$$g(x) \;=\; t_1 x^{a_1} + t_2 x^{a_2} + \cdots + t_n x^{a_n}\,, \qquad (*)$$

où $t_1, \dots, t_n \in \mathbb{R}$. En particulier t_n est le déterminant de la matrice de coefficients $x_i^{a_j}$, $(i,j) \in [\![1, n-1]\!]^2$. D'après l'hypothèse de récurrence, t_n est strictement positif, en particulier non nul. Cela étant, si $p \in [\![1, n]\!]$ est le nombre d'indices $i \in [\![1, n]\!]$ tels que $t_i \neq 0$, la question 1) montre que la fonction g s'annule au plus $p-1$ fois sur I. On en déduit l'égalité :

$$\big\{x \in I \;\big|\; g(x) = 0\big\} \;=\; \{x_1, x_2, \dots, x_{n-1}\}.$$

Ainsi, $g(x)$ ne s'annule pas sur l'intervalle $J := \big]x_{n-1}, +\infty\big[$. Comme g est continue sur J, elle garde un signe constant sur J. Or $t_n > 0$, et la suite $(a_1, \dots, a_n)$ est strictement croissante, de sorte que l'égalité $(*)$ montre que $g(x)$ est équivalent, lorsque x tend vers $+\infty$, à $t_n x^{a_n}$. D'où $g(x) > 0$ dès que $x \in J$ est assez grand. Au total, on a donc $g(x) > 0$ pour *tout* $x \in J$, et en particulier $D = g(x_n) > 0$.

II.7.29 1) Soient $n \in \mathbb{N}^*$ et $z_1, \dots, z_n$ des nombres complexes distincts. Il suffit de montrer que la famille $\big(u(z_1), \dots, u(z_n)\big)$ est libre. Soit $(\lambda_1, \dots, \lambda_n) \in \mathbb{C}^n$ une famille de scalaires telle que $\sum_{j=1}^{n} \lambda_j u(z_j) = 0$. Il s'agit là d'une égalité entre suites. Pour tout $k \in \mathbb{N}$, on a donc $\sum_{j=1}^{n} \lambda_j z_j^k = 0$. Considérons le système (S) formé des égalités $\sum_{j=1}^{n} x_j z_j^k = 0$, $k = 0, 1, \dots, n-1$. C'est un système linéaire homogène de n équations à n inconnues $x_1, \dots, x_n$. Le déterminant de ce système est le déterminant de Vandermonde de $z_1, \dots, z_n$ (exercice 8 de la page 358). Comme les z_j sont distincts, ce déterminant n'est pas nul. Or $(\lambda_1, \dots, \lambda_n)$ est une solution de (S). D'après le théorème 66 de la page 376, les λ_j sont tous nuls, d'où la conclusion.

2) Soient $u := (u_n)$ et $v := (v_n)$ deux éléments de F_t et $\lambda \in \mathbb{C}$. Par définition, $u + v := (u_n + v_n)$. Pour tout $n \in \mathbb{N}$, $u_{n+t} = u_n$ et $v_{n+t} = v_n$, donc $(u+v)_{n+t} = (u+v)_n$.

Ainsi $u+v$ est t-périodique, *i.e.* $u+v \in F_t$. On vérifie de même que $\lambda u \in F_t$, donc F_t est un sous-espace vectoriel de E.

Notons f l'application $u \longmapsto (u_0, \dots, u_{t-1})$ de F_t dans $\mathbb{C}^t$, qui est évidemment linéaire. Elle est injective. Soit en effet $u := (u_n) \in \operatorname{Ker} f$: $u_n = 0$ pour $n = 0, \dots, t-1$. Soit $k \in \mathbb{N}$, effectuons la division euclidienne de k par t : $k := qt + r$, où $q \in \mathbb{N}$ et $r \in [\![0, t-1]\!]$. Puisque u est t-périodique, $u_k = u_r = 0$. Ainsi $u_k = 0$ pour tout $k \in \mathbb{N}$, *i.e.* $u = 0$.

Montrons que f est surjective. Soit $(a_0, \dots, a_{t-1}) \in \mathbb{C}^t$. Pour tout $k \in \mathbb{N}$, rappelons que le reste dans la division de k par t est noté $k \bmod t$. Soit $u = (u_n) \in E$ la suite définie par la formule $u_n := a_{n \bmod t}$ pour tout $n \in \mathbb{N}$. Il est clair que d'une part u est t-périodique, *i.e.* $u \in F_t$, et que d'autre part $f(u) = (a_0, \dots, a_{t-1})$. En conclusion, f est un isomorphisme de F_t sur $\mathbb{C}^t$, donc F_t est de dimension t.

3) Partons d'une remarque très simple. Soient $t, p \in \mathbb{N}^*$. Si une suite est t-périodique, elle est aussi tp-périodique. En d'autres termes, $F_t \subset F_{tp}$. Soient alors $u, v \in F$ et $\lambda \in \mathbb{C}$. Il existe $t, p \in \mathbb{N}^*$ tels que $u \in F_t$ et $v \in F_p$. D'après la remarque précédente, u et v appartiennent à F_{tp}, donc $u+v$ et λu appartiennent aussi à F_{tp}, puisque F_{tp} est un sous-espace vectoriel de E. Comme $F_{tp} \subset F$, $u+v$ et λu appartiennent à F, donc F est un sous-espace vectoriel de E ($0 \in F$).

4) Soit d'abord $q \in \mathbb{Q}$, écrivons q sous forme irréductible $q := a/b$, où $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$, a et b étant premiers entre eux. Alors la suite $v(q)$ est b-périodique (elle appartient donc à F). En effet, pour tout $n \in \mathbb{N}$, nous avons :

$$v(q)_n \;=\; u\big(\exp(2\pi i q)\big)_n \;=\; \exp(2\pi i q)^n \;=\; \exp(2\pi i n q) \;=\; \exp(2\pi i n a/b).$$

d'où $v(q)_{n+b} = v(q)_n$ pour tout $n \in \mathbb{N}$, puisque $\exp(2\pi i) = 1$. Remarquons aussi que $v(q+m) = v(q)$ pour tous $q \in \mathbb{Q}$ et $m \in \mathbb{Z}$, à cause de l'égalité $\exp(2\pi i m) = 1$.

Soit maintenant $T = \mathbb{Q} \cap \big[0, 1\big[$. L'application $q \mapsto \exp(2\pi i q)$ de T dans $\mathbb{C}$ est injective : si $q, q' \in T$, l'égalité $\exp(2\pi i q) = \exp(2\pi i q')$ implique $\exp\big(2\pi i (q'-q)\big) = 1$, donc $q' - q \in \mathbb{Z}$ et par suite $q = q'$. La question 1) montre alors que la famille $\big(v(q)\big)_{q \in T}$ est libre. Il reste à montrer que cette famille est une famille génératrice de F. Notons V le sous-espace vectoriel de F engendré par cette famille.

Soit $t \in \mathbb{N}^*$. Pour tout $a \in [\![0, t-1]\!]$, la suite $v(a/t)$ appartient à F_t, nous venons de le voir. Ce qui précède montre de plus que la famille $\big(v(0/t), v(1/t), \dots, v\big((t-1)/t\big)\big)$ est libre. C'est une famille de t vecteurs de l'espace vectoriel F_t, qui est de dimension t, donc cette famille est une base de F_t. Comme $v(a/t) \in V$ pour tout a, cela montre que F_t est inclus dans V. Or, par définition, F est la *réunion* des F_t lorsque t décrit $\mathbb{N}^*$, et par conséquent F est inclus dans V, *i.e.* $V = F$. En conclusion, la famille $\big(v(q)\big)_{q \in T}$ est une base (dénombrable) de F.

II.7.30 1) Pour tous $i, j \in [\![1, n]\!]$, on a, avec des notations évidentes :

$$(J^2)_{i,j} \;=\; \sum_{k=1}^{n} J_{i,k} J_{k,j} \;=\; \sum_{k=1}^{n} 1 \;=\; n \;=\; n J_{i,j}\,,$$

ce qui prouve l'égalité $J^2 = nJ$.

Soient $\mathcal{B} := (e_1, \dots, e_n)$ la base canonique de $\mathbb{R}^n$ et $f \in \mathcal{L}(\mathbb{R}^n)$ l'endomorphisme dont la matrice dans la base $\mathcal{B}$ est J. Posant $u := \sum_{i=1}^{n} e_i$, il vient $f(e_j) = u$ pour tout $j \in [\![1, n]\!]$. On

en déduit évidemment que $f(u) = nu$. D'où, pour tout indice j :

$$f^2(e_j) \;=\; f(u) \;=\; nu \;=\; nf(e_j)\,,$$

ce qui montre que $f^2 = nf$.

En considérant les matrices dans la base $\mathcal{B}$, nous retrouvons l'égalité $J^2 = nJ$.

Les colonnes de J sont toutes égales et non nulles, donc le rang de J vaut 1. Une autre méthode consiste à dire que l'image de f est évidemment la droite $\mathbb{R}u$, de sorte que f est de rang 1. Enfin f et J ont même rang, en vertu du théorème 22 de la page 342.

2) Le théorème du rang montre que $\mathrm{Ker}\, f$ est de dimension $n-1$. Soit $(e'_1, \ldots, e'_{n-1})$ une base de $\mathrm{Ker}\, f$, complétons la en une base $\mathcal{B}' := (e'_1, \ldots, e'_n)$ de $\mathbb{R}^n$. Soit $P \in GL_n(\mathbb{R})$ la matrice de passage de la base $\mathcal{B}$ à la base $\mathcal{B}'$. D'après le théorème 35 de la page 349, $A := P^{-1}JP$ est la matrice de f dans la base $\mathcal{B}'$. Comme $f(e'_j) = 0$ pour $j = 1, \ldots, n-1$, les $n-1$ premières colonnes de A sont nulles. Nous pouvons donc écrire :

$$A \;:=\; \begin{pmatrix} 0 & 0 & \cdots & 0 & t_1 \\ 0 & 0 & \cdots & 0 & t_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & t_{n-1} \\ 0 & 0 & \cdots & 0 & t_n \end{pmatrix}, \quad \text{d'où}$$

$$XI_n - A \;=\; \begin{pmatrix} X & 0 & \cdots & 0 & -t_1 \\ 0 & X & \cdots & 0 & -t_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & X & -t_{n-1} \\ 0 & 0 & \cdots & 0 & X - t_n \end{pmatrix}.$$

La matrice $XI_n - A$ étant triangulaire, son déterminant, à savoir χ_A, est le produit de ses termes diagonaux : $\chi_A = X^{n-1}(X - t_n) = X^n - t_n X^{n-1}$. Il nous faut donc calculer t_n. D'abord, la proposition 59 de la page 371 montre que $\chi_J = \chi_A$. Ensuite, en vertu de la proposition 57 de la page 369, le coefficient de X^{n-1} dans χ_J est l'opposé de la somme des termes diagonaux de J, c'est-à-dire $-n$. Ainsi $t_n = n$, d'où :

$$\chi_J \;=\; X^{n-1}(X - n).$$

II.7.31 Notons $a_{i,j}$ les coefficients de A. Soit $\lambda \in \mathbb{C}$ une valeur propre de A. Il existe un vecteur colonne non nul $X := {}^t(x_1, \ldots, x_n)$ tel que $AX = \lambda X$, soit :

$$\sum_{j=1}^{n} a_{i,j}x_j \;=\; \lambda x_i \;\; (i = 1, \ldots, n). \qquad (*)$$

Posons $t := \max(|x_1|, \ldots, |x_n|)$. D'abord $t > 0$, puisque $X \neq 0$. Considérons un indice i tel que $t := |x_i|$. Dans l'égalité ci-dessus, appliquons l'inégalité triangulaire, en se rappelant que les coefficients de A sont des réels positifs :

$$|\lambda|t \;=\; |\lambda x_i| \;=\; \left|\sum_{j=1}^{n} a_{i,j}x_j\right| \;\leqslant\; \sum_{j=1}^{n} a_{i,j}|x_j| \;\leqslant\; \sum_{j=1}^{n} a_{i,j}t \;=\; t\sum_{j=1}^{n} a_{i,j} \;=\; t.$$

Ainsi $|\lambda|t \leqslant t$, d'où $|\lambda| \leqslant 1$, comme désiré.

II.7.32 Soit $\lambda \in K^*$, supposons que λ soit valeur propre de $g \circ f$. Il existe donc un vecteur non nul $x \in E$ tel que $g\big(f(x)\big) = \lambda x$. Appliquons f aux deux membres de cette égalité. En posant $y := f(x) \in F$, il vient $f\big(g(y)\big) = \lambda y$. De plus $y \neq 0$: dans le cas contraire, $f(x) = 0$, d'où $\lambda x = g\big(f(x)\big) = 0$. Comme $\lambda \neq 0$, cela contredit l'hypothèse $x \neq 0$. Ainsi $y \in F$ est non nul, donc l'égalité $f\big(g(y)\big) = \lambda y$ montre que y est vecteur propre de $f \circ g$, associé à la valeur propre λ.

En conclusion, si $\lambda \in K^*$ est valeur propre de $g \circ f$, c'est aussi une valeur propre de $f \circ g$. La réciproque en résulte, en échangeant les rôles de f et g.

II.7.33 1) Supposons que f possède une valeur propre λ. Par définition, $\lambda \in \mathbb{R}$, et il existe un vecteur non nul $x \in E$ tel que $f(x) = \lambda x$. Alors :

$$-x = (-Id_E)(x) = f^2(x) = f\big(f(x)\big) = f(\lambda x) = \lambda f(x) = \lambda(\lambda x) = \lambda^2 x.$$

Comme x n'est pas nul, $\lambda^2 = -1$, ce qui est absurde puisque λ est réel. Ainsi f ne possède pas de valeur propre, *i.e.* le polynôme caractéristique $\chi_f \in \mathbb{R}[X]$ n'a aucune racine réelle.

Supposons, par l'absurde, que n soit impair. Le polynôme $\chi_f \in \mathbb{R}[X]$ est unitaire de degré n. Puisque n est impair, $\chi_f(x)$ tend vers $+\infty$ (resp. $-\infty$) lorsque x tend vers $+\infty$ (resp. $-\infty$). Ainsi $\chi_f(\mathbb{R})$ est un intervalle de $\mathbb{R}$ $\big($parce que $x \mapsto \chi_f(x)$ est une fonction continue sur $\mathbb{R}\big)$, et cet intervalle n'est ni majoré ni minoré, donc est égal à $\mathbb{R}$. D'où $\chi_f(\mathbb{R}) = \mathbb{R}$. Mais alors $0 \in \chi_f(\mathbb{R})$, *i.e.* il existe $\lambda \in \mathbb{R}$ tel que $\chi_f(\lambda) = 0$. Autrement dit, λ est valeur propre de f, ce qui contredit le début de cette question. En conclusion, n est pair.

2) Parmi les axiomes des espaces vectoriels que nous devons vérifier, le seul qui ne résulte pas trivialement de la linéarité de f ou des axiomes des $\mathbb{R}$-espaces vectoriels est l'associativité mixte : $\lambda \cdot (\mu \cdot x) = (\lambda\mu) \cdot x$ pour tous $x \in E$ et $\lambda, \mu \in \mathbb{C}$. Posons $\lambda := a + ib$ et $\mu := c + id$, où $a, b, c, d \in \mathbb{R}$. Alors $\lambda\mu = (ac - bd) + i(ad + bc)$. Il en résulte que :

$$(\lambda\mu) \cdot x \;=\; (ac - bd)x + (ad + bc)f(x).$$

D'un autre côté $\mu \cdot x = cx + df(x)$, d'où :

$$\lambda \cdot (\mu \cdot x) = (a + ib) \cdot \big(cx + df(x)\big) = a\big(cx + df(x)\big) + bf\big(cx + df(x)\big).$$

La conclusion vient alors de l'égalité $f\big(f(x)\big) = -x$.

Ainsi E est devenu un $\mathbb{C}$-espace vectoriel, et le $\mathbb{R}$-espace vectoriel obtenu en restreignant la loi externe de $\mathbb{C} \times E$ à $\mathbb{R} \times E$ n'est autre que le $\mathbb{R}$-espace vectoriel E donné. Puisque E est de dimension finie n sur $\mathbb{R}$, l'exercice II.7.9 montre que E est de dimension finie m sur $\mathbb{C}$ et que $n = 2m$. Nous retrouvons ainsi le fait que l'entier n soit pair.

II.7.34 Écrivons le système (S) donné sous la forme matricielle habituelle $AX = B$. Soient L_1, L_2, L_3 les lignes de A et $(E_1), (E_2), (E_3)$ les équations constituant (S). Les opérations élémentaires $(E_1) \leftarrow (E_1) - 2(E_3)$ et $(E_2) \leftarrow (E_2) - 3(E_3)$ conduisent aux équations $-y + z = 4$ et $y - 2z = -6$ respectivement. De ces deux nouvelles équations, on déduit aussitôt $y = -2$ et $z = 2$. En reportant dans (E_3), on obtient $x = 3$. Ainsi (S) possède une solution unique, à savoir $(3, -2, 2)$.

Une autre méthode consiste à calculer d'abord $\det A$, en développant par rapport à la troisième ligne :

$$\begin{vmatrix} 2 & 3 & 5 \\ 3 & 7 & 4 \\ 1 & 2 & 2 \end{vmatrix} = 1 \times \begin{vmatrix} 3 & 5 \\ 7 & 4 \end{vmatrix} - 2 \times \begin{vmatrix} 2 & 5 \\ 3 & 4 \end{vmatrix} + 2 \times \begin{vmatrix} 2 & 3 \\ 3 & 7 \end{vmatrix}$$
$$= (12 - 35) - 2(8 - 15) + 2(14 - 9) = -23 + 14 + 10 = 1.$$

Ainsi $\det A = 1$, donc (S) est un système de Cramer, il possède une unique solution (x, y, z). Nous pouvons calculer x, y, z par les formules de Cramer :

$$x = \begin{vmatrix} 10 & 3 & 5 \\ 3 & 7 & 4 \\ 3 & 2 & 2 \end{vmatrix} = 3 \times \begin{vmatrix} 3 & 5 \\ 7 & 4 \end{vmatrix} - 2 \times \begin{vmatrix} 10 & 5 \\ 3 & 4 \end{vmatrix} + 2 \times \begin{vmatrix} 10 & 3 \\ 3 & 7 \end{vmatrix}$$
$$= 3(12 - 35) - 2(40 - 15) + 2(70 - 9) = -69 - 50 + 122 = 3,$$

$$y = \begin{vmatrix} 2 & 10 & 5 \\ 3 & 3 & 4 \\ 1 & 3 & 2 \end{vmatrix} = 1 \times \begin{vmatrix} 10 & 5 \\ 3 & 4 \end{vmatrix} - 3 \times \begin{vmatrix} 2 & 5 \\ 3 & 4 \end{vmatrix} + 2 \times \begin{vmatrix} 2 & 10 \\ 3 & 3 \end{vmatrix}$$
$$= (40 - 15) - 3(8 - 15) + 2(6 - 30) = 25 + 21 - 48 = -2,$$

$$z = \begin{vmatrix} 2 & 3 & 10 \\ 3 & 7 & 3 \\ 1 & 2 & 3 \end{vmatrix} = 1 \times \begin{vmatrix} 3 & 10 \\ 7 & 3 \end{vmatrix} - 2 \times \begin{vmatrix} 2 & 10 \\ 3 & 3 \end{vmatrix} + 3 \times \begin{vmatrix} 2 & 3 \\ 3 & 7 \end{vmatrix}$$
$$= (9 - 70) - 2(6 - 30) + 3(14 - 9) = -61 + 48 + 15 = 2.$$

II.7.35 Pour tout $t \in K$, notons $S(t)$ le système proposé, écrit sous forme matricielle $A(t)X = B(t)$, avec des notations évidentes. Posons $D(t) := \det\big(A(t)\big)$. Commençons par calculer $D(t)$, pour savoir si $S(t)$ est ou n'est pas un système de Cramer.

$$D(t) = \begin{vmatrix} 1 & t & 2 \\ -2 & 1 & t-2 \\ t & 1 & 2 \end{vmatrix}.$$

Les transvections $L_2 \leftarrow L_2 + 2L_1$ et $L_3 \leftarrow L_3 - tL_1$ donnent :

$$D(t) = \begin{vmatrix} 1 & t & 2 \\ 0 & 2t+1 & t+2 \\ 0 & 1-t^2 & 2-2t \end{vmatrix} = \begin{vmatrix} 2t+1 & t+2 \\ 1-t^2 & 2-2t \end{vmatrix}, \quad \text{soit}$$

$D(t) = (2t+1)(2-2t) - (t+2)(1-t^2) = (1-t)\Big[2(2t+1) - (t+2)(1+t)\Big]$, ou encore :

$$D(t) \;=\; (1-t)(-t^2+t) \;=\; t(1-t)^2.$$

Ainsi le système est de Cramer si, et seulement si, $t \neq 0, 1$. Supposons que ce soit le cas. Le système possède alors une solution unique (x, y, z). Calculons x, y, z (en fonction de t) par les formules de Cramer :

$$\begin{vmatrix} t & t & 2 \\ 1 & 1 & t-2 \\ 2t-1 & 1 & 2 \end{vmatrix} = \begin{vmatrix} 0 & t & 2 \\ 0 & 1 & t-2 \\ 2t-2 & 1 & 2 \end{vmatrix} = (2t-2) \begin{vmatrix} t & 2 \\ 1 & t-2 \end{vmatrix}, \quad \text{d'où}$$

$$x \;=\; \frac{2(t-1)(t^2-2t-2)}{t(t-1)^2} \;=\; \frac{2(t^2-2t-2)}{t(t-1)}.$$

Procédons de même pour y. Par linéarité par rapport à la dernière ligne, il vient :

$$\begin{vmatrix} 1 & t & 2 \\ -2 & 1 & t-2 \\ t & 2t-1 & 2 \end{vmatrix} = D(t) + (2t-2)\begin{vmatrix} 1 & t & 2 \\ -2 & 1 & t-2 \\ 0 & 1 & 0 \end{vmatrix}, \quad \text{d'où}$$

$$y = \frac{t(t-1)^2-(2t-2)(t+2)}{t(t-1)^2} = \frac{t(t-1)-2(t+2)}{t(t-1)} = \frac{t^2-3t-4}{t(t-1)}.$$

Pour calculer z, il est aussi simple de reprendre la première équation :

$$2z \;=\; t-x-ty \;=\; \frac{t^2(t-1)-2(t^2-2t-2)-t(t^2-3t-4)}{t(t-1)},$$

ce qui donne :

$$z \;=\; \frac{4t+2}{t(t-1)}.$$

Il reste à étudier les cas $t := 0$ et $t := 1$. Si $t := 0$, on obtient le système suivant :

$$\begin{cases} x + 0y + 2z = 0 \\ -2x + y - 2z = 1 \\ 0x + y + 2z = -1\,. \end{cases}$$

En ajoutant deux fois la première égalité à la seconde, on obtient $y + 2z = 1$, ce qui est incompatible avec la dernière équation. Le système $S(0)$ n'est donc pas compatible.

Si $t := 1$, on obtient le système suivant :

$$\begin{cases} x + y + 2z = 1 \\ -2x + y - z = 1 \\ x + y + 2z = 1 \end{cases}, \quad \text{et} \quad A(1) \;=\; \begin{pmatrix} 1 & 1 & 2 \\ -2 & 1 & -1 \\ 1 & 1 & 2 \end{pmatrix}.$$

La matrice $A(1)$ est de rang 2 : ses deux premières lignes sont indépendantes, et sa troisième ligne est égale à la première. Le système $S(1)$ est compatible : les deux premières équations sont indépendantes, et la troisième est égale à la première. On en déduit que les solutions de $S(1)$ forment une droite affine D.

Prenons comme équations principales les deux premières et comme inconnues principales x et y. D'après le théorème 70 de la page 380, nous pouvons choisir arbitrairement l'inconnue non principale z, les inconnues principales x, y étant alors données par le système de Cramer suivant :

$$\begin{cases} x + y = 1 - 2z \\ -2x + y = 1 + z. \end{cases}$$

On trouve facilement :

$$x \;=\; -z \quad \text{et} \quad y \;=\; 1 - z.$$

Nous avons ainsi obtenu une représentation paramétrique de la droite D.

II.7.36 Appliquons le théorème 47 de la page 360 ou son corollaire. Puisque A est de rang $n-1$, $\det A = 0$, mais A possède un mineur non nul d'ordre $n-1$. Il existe donc deux indices

$k, i \in [\![1, n]\!]$ tels que $D_{k,i} \neq 0$. L'indice k étant ainsi fixé, définissons les y_j comme dans l'énoncé. D'abord $y_i \neq 0$. Montrons ensuite que $Y := {}^t(y_1, \dots, y_n)$ est solution du système $AX = 0$. Notons $\widetilde{A}$ la comatrice de A. Puisque $\det A = 0$, le théorème 44 de la page 359 montre que $A \times {}^t\widetilde{A} = 0$. Pour tout $h \in [\![1, n]\!]$, on a donc :

$$0 = (A \times {}^t\widetilde{A})_{h,k} = \sum_{j=1}^{n} (-1)^{k+j} a_{h,j} D_{k,j} = \sum_{j=1}^{n} a_{h,j} y_j = (AY)_h \,,$$

ce qui montre que $AY = 0$. Puisque A est de rang $n-1$, le théorème 65 de la page 376 montre que les solutions du système homogène $AX = 0$ forment une droite vectorielle. Vu ce qui précède, cette droite est engendrée par Y.

II.7.37 Posons donc :

$$A := \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{et} \quad B := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

$$\chi_A = \begin{vmatrix} X & -1 & -1 \\ -1 & X & -1 \\ 0 & 0 & X-1 \end{vmatrix} = (X-1) \begin{vmatrix} X & -1 \\ -1 & X \end{vmatrix} = (X-1)(X^2-1)\,,$$

c'est-à-dire $\chi_A = (X-1)^2(X+1)$. Les valeurs propres de A sont les racines de χ_A, ce sont donc 1 et -1.

Déterminons l'espace propre de A relatif à la valeur propre 1. Il s'agit de résoudre le système suivant :

$$\begin{cases} y + z = x \\ x + z = y \\ z = z. \end{cases}$$

Les deux premières équations donnent $x = y$ et $z = 0$. L'espace propre cherché est donc la droite vectorielle engendrée par le vecteur ${}^t(1, 1, 0)$.

Déterminons de même l'espace propre de A relatif à la valeur propre -1. Il s'agit de résoudre le système suivant :

$$\begin{cases} y + z = -x \\ x + z = -y \\ z = -z. \end{cases}$$

Ce système équivaut évidemment à $z = 0$ et $x + y = 0$. L'espace propre cherché est donc la droite vectorielle engendrée par le vecteur ${}^t(1, -1, 0)$.

$$\chi_B = \begin{vmatrix} X & -1 & 0 \\ -1 & X & -1 \\ 0 & -1 & X \end{vmatrix} = X \begin{vmatrix} X & -1 \\ -1 & X \end{vmatrix} + \begin{vmatrix} X & 0 \\ -1 & -1 \end{vmatrix} = X(X^2-1) - X\,,$$

d'où $\chi_B = X(X^2-2)$. Ainsi B a trois valeurs propres : 0, $\sqrt{2}$ et $-\sqrt{2}$.

Déterminons l'espace propre de B relatif à la valeur propre 0. Il est défini par les égalités $y = 0$ et $x + z = 0$, c'est donc la droite vectorielle engendrée par ${}^t(1, 0, -1)$.

Déterminons de même l'espace propre de B relatif à la valeur propre $\sqrt{2}$. Il s'agit de résoudre le système suivant :

$$\begin{cases} y = x\sqrt{2} \\ x + z = y\sqrt{2} \\ y = z\sqrt{2}. \end{cases}$$

Ce système est équivalent au système formé des équations $x = z$ et $y = x\sqrt{2}$. On en déduit aussitôt que l'espace propre cherché est la droite vectorielle engendrée par le vecteur ${}^t(1, \sqrt{2}, 1)$.

Pour l'espace propre de B relatif à la valeur propre $-\sqrt{2}$, il suffit de remplacer $\sqrt{2}$ par $-\sqrt{2}$: l'espace propre cherché est la droite vectorielle engendrée par le vecteur ${}^t(1, -\sqrt{2}, 1)$.

II.7.38 Notons A la matrice de l'énoncé. Puisque nous devons déterminer non seulement les valeurs propres, mais aussi les vecteurs propres de A, le calcul de χ_A n'est pas la meilleure méthode : il faudra de toutes façons résoudre certains systèmes linéaires.

Observons que la matrice $B := A - I_n$ est plus simple que A :

$$B = \begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Pour tout $\lambda \in \mathbb{R}$, $\lambda I_n - A = (\lambda - 1)I_n - B$. Il en résulte que λ est valeur propre de A si, et seulement si, $\lambda - 1$ est valeur propre de B. Lorsque c'est le cas, l'espace propre de A relatif à la valeur propre λ est égal à l'espace propre de B relatif à la valeur propre $\lambda - 1$. Nous allons donc déterminer les *éléments propres* (valeurs et vecteurs propres) de B, et nous en déduirons ceux de A.

Soit $t \in \mathbb{R}$. Le système $BX = tX$ s'écrit ainsi, si $X := {}^t(x_1, \dots, x_n)$:

$$\begin{cases} x_2 + x_3 + \cdots + x_n = tx_1 \\ x_1 = tx_2 \\ \quad \vdots \\ x_1 = tx_n. \end{cases}$$

Si $t := 0$, ce système équivaut auxdeux équations $x_1 = x_2 + \cdots + x_n = 0$. Ainsi 0 est valeur propre de B. L'espace propre V de B relatif à la valeur propre 0 est de dimension $n - 2$ (il est défini par les deux équations linéairement indépendantes ci-dessus). Si l'on veut, une base de V est donnée par les vecteurs $E_2 - E_i$, $i = 3, \dots, n$, en notant $(E_1, \dots, E_n)$ la base canonique de $M_{n,1}(\mathbb{R})$.

Supposons $t \neq 0$. Dans le système ci-dessus, les $n - 1$ dernières équations donnent : $x_i = t^{-1}x_1$, pour $i = 2, \dots, n$. La première équation s'écrit alors : $(n-1)t^{-1}x_1 = tx_1$. Bien entendu, nous ne nous intéressons qu'aux solutions *non triviales* dudit système. Pour une telle solution, $x_1 \neq 0$, car sinon tous les x_i seraient nuls. D'où l'égalité $t^2 = n - 1$. Ainsi $t \in \mathbb{R}^*$ est valeur propre de B si, et seulement si, $t^2 = n - 1$. En conclusion, $t := \sqrt{n-1}$ est valeur propre de B, l'espace propre correspondant étant la droite vectorielle D engendrée

par ${}^t(t,1,\dots,1)$. De même $t' := -\sqrt{n-1}$ est valeur propre de B, l'espace propre correspondant étant la droite vectorielle D' engendrée par ${}^t(t',1,\dots,1)$.
Revenons à A. Nous savons maintenant que A possède trois valeurs propres, à savoir $1, 1+t$ et $1+t'$, les espaces propres correspondants étant V, D et D' respectivement.

II.7.39 Notons D le déterminant en question. L'idée est la même que dans l'exercice 14 de la page 376. On recherche un plan affine P, d'équation $ax+by+cz+d=0$, où $(a,b,c,d) \in \mathbb{R}^4$ et $(a,b,c) \neq (0,0,0)$, passant par les quatre points M_i. Dire que P passe par ces points revient à dire que (a,b,c,d) est solution du système homogène suivant :

$$(S) : \begin{cases} ax_1 + by_1 + cz_1 + d = 0 \\ ax_2 + by_2 + cz_2 + d = 0 \\ ax_3 + by_3 + cz_3 + d = 0 \\ ax_4 + by_4 + cz_4 + d = 0\,. \end{cases}$$

Si les points M_i sont coplanaires (appartiennent à un même plan), le système (S) possède une solution non triviale, donc $D = 0$. Supposons inversement que $D = 0$. Le système (S) possède donc une solution $(a,b,c,d) \neq (0,0,0,0)$. En fait, la première équation de (S) donne $(a,b,c) \neq (0,0,0)$, et par suite le plan d'équation $ax+by+cz+d=0$ passe par les points M_i.

II.7.40 Notons Δ le déterminant en question. La nullité de Δ est équivalente à l'existence d'une solution non triviale (x,y,z) du système homogène suivant :

$$(S) : \begin{cases} a_1x + b_1y + c_1z = 0 \\ a_2x + b_2y + c_2z = 0 \\ a_3x + b_3y + c_3z = 0\,. \end{cases}$$

Notons A la matrice de ce système :

$$A := \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \\ & & \end{pmatrix}.$$

Supposons d'abord que les trois droites soient concourantes : elles passent par un même point $M = (x,y)$. Alors $(x,y,1)$ est une solution non triviale de (S), donc $\Delta = 0$. Supposons ensuite que ces droites soient parallèles. Le fait que D_1 et D_2 soient parallèles se traduit par la nullité du déterminant $D_{3,3} = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}$. De même $D_{1,3} = 0$ et $D_{2,3} = 0$. En développant Δ par rapport à sa troisième colonne, on en déduit que $\Delta = 0$.
Supposons inversement que Δ soit nul. Le système (S) possède donc une solution non triviale (x,y,z). Si $z \neq 0$, on peut supposer que $z := 1$, car $(x/z, y/z, 1)$ est encore solution de (S). Supposant donc que $z := 1$, on voit que le point $M = (x,y)$ appartient aux trois droites, qui sont ainsi concourantes. Supposons enfin que z soit nul, et donc $(x,y) \neq (0,0)$. Considérons le système homogène (S') formé par les deux premières équations de (S), dans lesquelles on remplace z par 0. Puisque (x,y) est une solution non triviale de (S'), le déterminant de (S') est nul, *i.e.* $D_{3,3} = 0$. Cela signifie que les droites D_1 et D_2 sont parallèles. On montre de même que D_1 et D_3 sont parallèles. Les trois droites sont donc toutes parallèles.

II.7.41 Écrivons le système (S) en question ainsi :

$$\begin{cases} 2ax_1 + 2by_1 - c = x_1^2 + y_1^2 \\ 2ax_2 + 2by_2 - c = x_2^2 + y_2^2 \\ 2ax_3 + 2by_3 - c = x_3^2 + y_3^2 \,. \end{cases}$$

Notons A la matrice de ce système et D son déterminant :

$$D \;=\; \begin{vmatrix} 2x_1 & 2y_1 & -1 \\ 2x_2 & 2y_2 & -1 \\ 2x_3 & 2y_3 & -1 \end{vmatrix} \;=\; -4 \begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix} \;:=\; -4\Delta \,.$$

D'après l'exercice 14 de la page 376, D n'est donc pas nul, autrement dit le système (S) est un système de Cramer. Ainsi (S) possède une unique solution (a, b, c). Pour $i = 1, 2, 3$, la $i^{ème}$ équation de (S) peut être écrite ainsi :

$$(x_i - a)^2 + (y_i - b)^2 \;=\; a^2 + b^2 - c.$$

On en déduit l'inégalité $a^2+b^2-c \geqslant 0$. En fait, cette inégalité est stricte. En effet, si a^2+b^2-c était nul, on aurait $x_i = a$ et $y_i = b$ pour tout i, *i.e.* les trois points donnés seraient égaux. Posons alors $R := \sqrt{a^2 + b^2 - c}$. Les égalités ci-dessus signifient que les trois points M_i appartiennent au cercle C de centre $\Omega := (a, b)$ et de rayon R. Nous avons ainsi prouvé que les trois points appartenaient à un unique cercle.

Les formules de Cramer permettent de plus de calculer a, b, c en fonction des x_i, y_i :

$$a \;=\; \frac{\begin{vmatrix} x_1^2 + y_1^2 & y_1 & 1 \\ x_2^2 + y_2^2 & y_2 & 1 \\ x_3^2 + y_3^2 & y_3 & 1 \end{vmatrix}}{2\Delta} \;,\quad b \;=\; \frac{\begin{vmatrix} x_1 & x_1^2 + y_1^2 & 1 \\ x_2 & x_2^2 + y_2^2 & 1 \\ x_3 & x_3^2 + y_3^2 & 1 \end{vmatrix}}{2\Delta} \,,$$

$$c \;=\; \frac{-\begin{vmatrix} x_1 & y_1 & x_1^2 + y_1^2 \\ x_2 & y_2 & x_2^2 + y_2^2 \\ x_3 & y_3 & x_3^2 + y_3^2 \end{vmatrix}}{\Delta}.$$

Passons à l'application numérique. Calculons d'abord Δ :

$$\Delta \;=\; \begin{vmatrix} -7 & 5 & 1 \\ 1 & 1 & 1 \\ 7 & -3 & 1 \end{vmatrix} \;=\; \begin{vmatrix} -8 & 4 & 1 \\ 0 & 0 & 1 \\ 6 & -4 & 1 \end{vmatrix} \;=\; -\begin{vmatrix} -8 & 4 \\ 6 & -4 \end{vmatrix} \;=\; -8.$$

Calculons ensuite a, b, c :

$$-16a \;=\; \begin{vmatrix} 74 & 5 & 1 \\ 2 & 1 & 1 \\ 58 & -3 & 1 \end{vmatrix} \;=\; \begin{vmatrix} 72 & 4 & 0 \\ 2 & 1 & 1 \\ 56 & -4 & 0 \end{vmatrix} \;=\; -\begin{vmatrix} 72 & 4 \\ 56 & -4 \end{vmatrix} \;=\; 512 \,,$$

d'où $a = -32$.

$$-16b \;=\; \begin{vmatrix} -7 & 74 & 1 \\ 1 & 2 & 1 \\ 7 & 58 & 1 \end{vmatrix} \;=\; \begin{vmatrix} -8 & 72 & 0 \\ 1 & 2 & 1 \\ 6 & 56 & 0 \end{vmatrix} \;=\; -\begin{vmatrix} -8 & 72 \\ 6 & 56 \end{vmatrix} \;=\; 880 \,,$$

d'où $b \;=\; -55$. Le centre du cercle C circonscrit au triangle $M_1M_2M_3$ est donc $\Omega = (-32, -55)$, donc C a pour équation : $(x + 32)^2 + (y + 55)^2 = R^2$.

Pour calculer R, exprimons que C passe par M_2 :

$$R^2 \;=\; 33^2 + 56^2 \;=\; 1089 + 3136 \;=\; 4225 \;=\; 65^2.$$

Ainsi C est le cercle de centre $\Omega := (-32, -55)$ et de rayon $R := 65$.

II.7.42 Notons (S) le système (53), écrit sous forme matricielle : $AX = B$. Par hypothèse, $A \in M_{n,p}(K)$ et $B \in M_{n,1}(K)$. Écartons le cas trivial $A := 0$. Dans ce cas, que l'on se place sur K ou sur L, la condition nécessaire et suffisante de compatibilité de (S) est la même, à savoir $B = 0$.

Soit $r \geqslant 1$ le rang de la matrice A, considérée comme élément de $M_{n,p}(K)$. L'idée essentielle est que r est aussi le rang de la matrice A, considérée comme élément de $M_{n,p}(L)$. En effet, nous savons qu'il existe une matrice carrée A' d'ordre r extraite de A et inversible dans $M_r(K)$, et que r est le plus grand entier possédant cette propriété (théorème 47 de la page 360 et son corollaire). Or A' est inversible dans $M_r(K)$ si, et seulement si, $\det(A') \neq 0$, et $\det(A')$ est le même, que l'on calcule ce déterminant dans K ou dans L $\big($*cf.* la formule (23)$\big)$. D'où l'égalité des rangs de A sur K et sur L.

Appliquons ce qui précède à la matrice $[A; B] \in M_{n,p+1}(K)$. D'après la proposition 67 de la page 377, le système (S) est compatible sur K (resp. L) si et seulement si le rang de $[A; B]$ considérée comme élément de $M_{n,p+1}(K)$ $\big($resp. $M_{n,p+1}(L)\big)$ est égal à r. D'où la conclusion voulue : (S) est compatible sur K si, et seulement s'il est compatible sur L.

II.7.43 Reprenons les notations de l'exercice en question. Notons d'abord D le pgcd (unitaire) de A et B, et posons $d := \deg(D)$. Écrivons $A := DA_1$ et $B := DB_1$, où A_1 et B_1 sont deux polynômes premiers entre eux, de degrés $n - d$ et $p - d$ respectivement.

Considérons maintenant les espaces vectoriels $E := \mathbb{C}_{p-1}[X] \times \mathbb{C}_{n-1}[X]$ et $F := \mathbb{C}_{n+p-1}[X]$. Ils sont de même dimension finie, à savoir $n + p$. L'application f de E dans F définie par la formule $f(P, Q) := AP + BQ$ est évidemment linéaire. Munissons E de la base suivante :

$$\mathcal{B} \;:=\; \big((1,0),(X,0),\dots,(X^{p-1},0),(0,1),(0,X),\dots,(0,X^{n-1})\big)$$

et F de sa base canonique $\mathcal{C} := (1, X, \dots, X^{n+p-1})$. On vérifie que la matrice de f dans les bases $\mathcal{B}$ et $\mathcal{C}$ n'est autre que la transposée de la matrice $S(A, B)$ de l'exercice précité. D'après le théorème du rang, on a donc :

$$\operatorname{rang}\big(S(A,B)\big) = \operatorname{rang}\big({}^tS(A,B)\big) = \operatorname{rang}(f) = n + p - \dim(\operatorname{Ker} f).$$

Il nous faut donc déterminer le noyau de f. Par définition de f, ce noyau est formé des couples $(P, Q) \in E$ tels que $AP + BQ = 0$.

Soit $(P, Q) \in \operatorname{Ker} f$, supposons $(P, Q) \neq (0, 0)$. On a donc $P \neq 0$ et $Q \neq 0$. L'égalité $AP + BQ = 0$ implique $D(A_1P + B_1Q) = 0$, soit $PA_1 = (-Q)B_1$. Comme $A_1 \wedge B_1 = 1$, le théorème de Gauß montre que B_1 divise P (parce que B_1 divise PA_1). Il existe donc un unique polynôme $T \in \mathbb{C}[X]$ tel que $P = TB_1$. Alors $TB_1A_1 = (-Q)B_1$, d'où $Q = -TA_1$. De plus :

$$\deg(P) \;=\; \deg(T) + \deg(B_1) \;=\; \deg(T) + p - d \;\leqslant\; p - 1\,,$$

c'est-à-dire $\deg(T) \leqslant d-1$, et bien sûr $T \neq 0$. Si $d = 0$, *i.e.* si $A \wedge B = 1$, les conditions précédentes ne peuvent être vérifiées, *i.e.* $\operatorname{Ker} f = \{0\}$. Dans ce cas, le rang de $S(A, B)$ est $n+p$,

comme annoncé. Supposons $d \geqslant 1$. Nous venons de montrer que tout élément de $\mathrm{Ker}\, f$ est de la forme $(TB_1, -TA_1)$, où $T \in \mathbb{C}_{d-1}[X]$. La réciproque est évidente : si $T \in \mathbb{C}_{d-1}[X]$ et si l'on pose $P := TB_1$ et $Q := -TA_1$, on a $\deg(P) \leqslant (d-1) + (p-d) = p-1$, de même $\deg(Q) \leqslant n-1$, et $PA + QB = D(PA_1 + QB_1) = DT(B_1A_1 - A_1B_1) = 0$. D'où :

$$\mathrm{Ker}\, f \;=\; \big\{(TB_1, -TA_1) \;\big|\; T \in \mathbb{C}_{d-1}[X]\big\}.$$

Il est alors clair que $T \mapsto (TB_1, -TA_1)$ est un isomorphisme de $\mathbb{C}_{d-1}[X]$ sur $\mathrm{Ker}\, f$, ce qui montre que $\mathrm{Ker}\, f$ est de dimension d. Il en résulte que le rang de $S(A,B)$ est $n+p-d$, là encore. D'où la formule générale annoncée :

$$\mathrm{rang}\big(S(A,B)\big) \;= n + p - \deg(A \wedge B).$$

Intéressons-nous maintenant aux éventuelles racines communes à A et B. Si $z \in \mathbb{C}$ est une telle racine commune, $X - z$ divise A et B, donc aussi leur pgcd D. Dans ce cas, $d = \deg(D) \geqslant 1$. Inversement, supposons $d \geqslant 1$. D'après le théorème de d'Alembert-Gauß, le polynôme non constant $D \in \mathbb{C}[X]$ possède au moins une racine z : $D(z) = 0$. Alors $A(z) = (DA_1)(z) = D(z)A_1(z) = 0$, et de même $B(z) = 0$. En d'autres termes, z est une racine commune à A et B. La conclusion obtenue est la suivante : A et B possèdent une racine commune si, et seulement si, $d \geqslant 1$. Compte tenu des résultats précédents, on en déduit les équivalences :

$$\det\big(S(A,B)\big) = 0 \iff \mathrm{rang}\big(S(A,B)\big) \leqslant n+p-1 \iff \deg(A \wedge B) \geqslant 1,$$

et chacune de ces conditions est équivalente à l'existence d'une racine commune à A et B.

Module II.8 : Initiation à l'algorithmique et au calcul formel

II.8.1 Soient $m := \sum_{i=0}^{k} c_i b^i$ et $n := \sum_{j=0}^{l} d_j b^j$ les nombres à multiplier, avec $c_i, d_j \in [\![0, b-1]\!]$ et $c_k, d_l \neq 0$. On peut calculer le produit par la formule :

$$mn = (d_0 m) + (d_1 m)b + \cdots + (d_l m)b^l.$$

Algorithme correspondant (abrégé) :

```
produit := d[0] * m ;
pour j de 1 a l faire
   produit := produit + d[j] * m * b^j ;;
```

Nous écrirons $|m|$ pour $|m|_b$, etc. Nous supposerons de plus que $|n| \leqslant |m|$ (quitte à permuter m et n). Chaque multiplication $d_j m$ se fait en temps $\Theta(|m|)$, car c'est une multiplication par un nombre à un chiffre (succession de $(k+1)$ multiplications de deux nombres à un chiffre et de propagations de retenues). Chaque multiplication par b^j se fait en temps constant $\Theta(1)$, car c'est un simple décalage sur les chiffres. Enfin, on additionne successivement des nombres de tailles $|m|+1$, $|m|+2, \ldots$, jusqu'à $|m|+|n|$. De la formule $\sum_{i=1}^{|n|}(|m|+i) = |m||n| + \dfrac{|n|(|n|+1)}{2}$, on déduit que le coût est bien $\Theta(|m||n|)$.

II.8.2 Cet exercice concerne le théorème de Lamé, son corollaire, et la remarque qui les précède.
Notons $r := x \mod y$ le reste de la division euclidienne $x = qy + r$. Tout diviseur commun à x et y divise y et $x - qy = r$, donc $x \wedge y | y \wedge r$. Tout diviseur commun à y et r divise y et $qy + r = x$, donc $y \wedge r | x \wedge y$. On a donc bien $y \wedge (x \mod y) = x \wedge y$.
Rappelons que $F_0 = 0$, $F_1 = 1$, $F_2 = 1$ et $F_3 = 2$. On voit d'abord par récurrence que tous les F_i $(i \geqslant 1)$ sont strictement positifs : c'est vrai pour $i = 1, 2$ et l'on utilise la relation $F_{i+2} = F_{i+1} + F_i$ pour une récurrence à deux pas. Ainsi, pour $i \geqslant 1$, on a $0 < F_i = F_{i+2} - F_{i+1}$ et la suite est strictement croissante à partir du rang 2.
On a, par construction, $x_{k-1} > x_k > x_{k+1} = 0$, d'où l'on déduit que $x_k \geqslant 1$ et $x_{k-1} \geqslant 2$. L'assertion $x_{k-i} \geqslant F_{i+2}$ est donc vraie pour $i = 0, 1$. On la prouve par récurrence à deux pas. Si $x_{k-(i-1)} \geqslant F_{i+1}$ et $x_{k-i} \geqslant F_{i+2}$, alors, d'après l'inégalité $x_{i-1} \geqslant x_i + x_{i+1}$ de la preuve du théorème de Lamé, en remplaçant i par $k - i$, on trouve :

$$x_{k-i-1} \geqslant x_{k-i} + x_{k-i+1} \geqslant F_{i+1} + F_{i+2} = F_{i+3},$$

qui est l'inégalité voulue au rang $i+1$, achevant la récurrence.
Selon la méthode de l'exercice II.5.6 de la page 276, on est conduit à rechercher les racines du trinôme $X^2 - X - 1$; ce sont $\rho := \dfrac{1+\sqrt{5}}{2}$ et $\rho' := \dfrac{1-\sqrt{5}}{2}$, et l'on sait que $F_k = \alpha\rho^k + \alpha'\rho'^k$ pour des coefficients α, α' convenables. Ces coefficients sont obtenus en prenant $k = 0, 1$, ce qui donne $\alpha + \alpha' = 0$ et $\alpha\rho + \alpha'\rho' = 1$, d'où $\alpha = \dfrac{1}{\rho - \rho'}$ et $\alpha' = \dfrac{1}{\rho' - \rho}$, d'où la formule $F_k = \dfrac{\rho^k - \rho'^k}{\rho - \rho'}$.

Ainsi, $\log F_k = k\log\rho + \log\big(1-\left(\dfrac{\rho'}{\rho}\right)^k\big) - \log(\rho-\rho') = k\log\rho + O(1)$, puisque $\left|\dfrac{\rho'}{\rho}\right| < 1$.

Comme $k\log\rho \to +\infty$, on a bien $\log F_k \sim k\log\rho$ et $k \sim \dfrac{\log F_k}{\log\rho}$.

II.8.3 La taille de a^k est égale à $k|a| + \Theta(1)$; dans les calculs qui suivent, nous l'assimilerons à $k|a|$, ce qui ne modifie pas l'ordre de grandeur des résultats.

Le coût de la multiplication $a^k \times a$ est, d'après le modèle des coûts bilinéaires, $\Theta(k|a|^2)$. Le coût cumulé des multiplications successives de a jusqu'à a^n est donc $|a|^2 \sum_{k=1}^{n-1} k = \dfrac{n(n-1)}{2}|a|^2$, donc $\Theta(n^2|a|^2)$.

Dans l'exponentiation dichotomique, on passe de a^k à a^{2k} par une élévation au carré de coût $k^2|a|^2$; pour passer de a^k à a^{2k+1}, il faut encore une multiplication par a, de coût $2k|a|^2$. Le coût total est donc de la forme $C(n) = c(n)|a|^2$, où le facteur $c(n)$ vérifie les règles suivantes : $c(1) = 0$; $c(2k) = c(k) + k^2$; enfin, $c(2k+1) = c(k) + k^2 + 2k$. Ces relations suffisent à déterminer toutes les valeurs de $c(n)$ (donc de $C(n)$). Quelques essais permettent de se convaincre que $c(n)$ est de l'ordre de grandeur de n^2. En fait, on a l'encadrement :

$$\forall n \in \mathbb{N}^*,\ \frac{n^2}{4} \leqslant c(n) \leqslant \frac{n^2+2n}{3}.$$

La minoration est évidente, au vu des formules précédentes. La majoration se prouve par récurrence forte : un calcul montre que, si elle est vraie pour $n = k$, elle est encore vraie pour $n = 2k$ et pour $n = 2k+1$ (grâce aux relations ci-dessus). Pour un $n \geqslant 2$ donné, elle se déduit donc de l'inégalité correspondante pour $\left\lfloor \dfrac{n}{2} \right\rfloor < n$.

II.8.4 On a $C(1) = 0$, $C(2n) = C(n) + 1$ et $C(2n+1) = C(n) + 2$.

On en tire l'encadrement $1 \leqslant C(n) - C\left(\dfrac{n}{2}\right) \leqslant 2$, d'où il est facile de conclure que $C(n) = \Theta(\log n)$. On peut cependant préciser cette estimation : notons, pour des bits $b_0, \dots, b_k \in \{0,1\}$, $K(b_0,\dots,b_k) := C(b_0 + \cdots + b_k 2^k) - k$. Alors $K(1) = 0$ et $K(b_0,\dots,b_k) = b_0 + K(b_1,\dots,b_k)$ (on n'a fait que traduire les relations ci-dessus), et l'estimation donnée dans le cours en découle immédiatement.

II.8.5 Selon les six cas possibles, et dans l'ordre d'écriture de l'algorithme, le nombre d'échanges est 0, 1, 2, 1, 2 ou 1. La moyenne est $\dfrac{0+1+2+1+2+1}{6} = \dfrac{7}{6}$, et c'est aussi l'espérance si les six cas sont équiprobables.

II.8.6 Sur $[k, k+1]$, l'inégalité $\ln k \leqslant \ln t \leqslant \ln(k+1)$ entraîne $\ln k \leqslant \displaystyle\int_k^{k+1} \ln t\, dt \leqslant \ln(k+1)$, donc $\displaystyle\sum_{k=1}^{n-1} \ln k \leqslant \int_1^n \ln t\ dt \leqslant \sum_{k=1}^{n} \ln k$. On en déduit d'abord l'encadrement : $\displaystyle\int_1^n \ln t\, dt \leqslant \sum_{k=1}^{n} \ln k \leqslant \int_1^n \ln t\, dt + \ln n$, puis (compte tenu de la primitive $t\ln t - t$

de $\ln t$) l'estimation : $\sum_{k=1}^{n} \ln k = n\ln n - n + O(\ln n)$.
A fortiori, $\ln n! \sim n\ln n$.

II.8.7 (i) Si l'on suppose $i < j$, la formule correcte est, bien sûr, $N(\tau_{i,j}) = 2(j-i)-1$. Les inversions qui interviennent dans $\tau_{i,j}$ sont les couples (i,k) avec $i<k<j$, les couples (k,j) avec $i<k<j$, et le couple (i,j). Il y en a donc $2(j-i-1)+1 = 2(j-i)-1$.
Soit $\sigma \in \mathfrak{S}_n$; nous voulons établir les formules :

$$N(\sigma\circ\tau_{k,k+1}) = \begin{cases} N(\sigma)-1 \text{ si } \sigma_k > \sigma_{k+1} \\ N(\sigma)+1 \text{ si } \sigma_k < \sigma_{k+1}. \end{cases}$$

Pour comprendre l'argumentation qui suit, on peut adopter un langage intuitif pour décrire la permutation $\sigma = \begin{pmatrix} 1 & \dots & i & \dots & n \\ x & \dots & a & \dots & y \end{pmatrix}$: nous dirons que la valeur $a \in [\![1,n]\!]$ est en position $i \in [\![1,n]\!]$ pour exprimer l'égalité $a = \sigma(i)$. Ainsi, les inversions où intervient la valeur a correspondent d'une part aux valeurs $\sigma(i') = a' < a$ dont la position i' est à droite de a, *i.e.* $i' > i$, d'autre part aux valeurs $\sigma(i'') = a'' > a$ dont la position i'' est à gauche de a, *i.e.* $i'' < i$.
L'effet de la composition de σ par $\tau_{k,k+1}$ *à droite* est de permuter des *valeurs quelconques* en *positions consécutives*. Ainsi :

$$\sigma = \begin{pmatrix} 1 & \dots & k & k+1 & \dots & n \\ x & \dots & a & b & \dots & y \end{pmatrix} \Longrightarrow \sigma\circ\tau_{k,k+1} = \begin{pmatrix} 1 & \dots & k & k+1 & \dots & n \\ x & \dots & b & a & \dots & y \end{pmatrix}.$$

Les valeurs autres que a et b à gauche de $k, k+1$ sont les mêmes que pour σ, et il en est de même à droite. Aucune inversion mettant en cause d'autres indices que $k, k+1$ n'a donc été affectée. Par ailleurs, si $a < b$, il n'y avait pas d'inversion en ces positions et il y en a maintenant une ; si $a > b$, c'est le contraire : on retrouve la formule indiquée.
(ii) Nous devons démontrer que le nombre moyen $\overline{N}_n$ d'inversions d'une permutation de $\mathfrak{S}_n$, naturellement défini comme : $\overline{N}_n := \dfrac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} N(\sigma)$, vérifie la relation de récurrence : $\overline{N}_{n+1} = \overline{N}_n + \dfrac{n}{2}$ Comme on a construit une bijection $(\sigma,k) \mapsto \langle\sigma,k\rangle$ de $\mathfrak{S}_n \times \{0,\dots,n\}$ dans $\mathfrak{S}_{n+1}$, et que l'on a démontré l'égalité : $N\big(\langle\sigma,k\rangle\big) = N(\sigma)+k$, le calcul se déroule comme suit :

$$\begin{aligned}
\overline{N}_{n+1} &= \frac{1}{(n+1)!}\sum_{\sigma\in\mathfrak{S}_n}\sum_{k=0}^{n}\big(N(\sigma)+k\big) \\
&= \frac{1}{(n+1)!}\sum_{\sigma\in\mathfrak{S}_n}\sum_{k=0}^{n} N(\sigma) + \frac{1}{(n+1)!}\sum_{\sigma\in\mathfrak{S}_n}\sum_{k=0}^{n} k \\
&= \frac{1}{(n+1)!}\sum_{\sigma\in\mathfrak{S}_n}(n+1)N(\sigma) + \frac{1}{(n+1)!}\sum_{\sigma\in\mathfrak{S}_n}\frac{n(n+1)}{2} \\
&= \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} N(\sigma) + \frac{1}{(n+1)!}n!\frac{n(n+1)}{2} \\
&= \overline{N}_n + \frac{n}{2}\,.
\end{aligned}$$

II.8.8 (i) De l'inclusion :

$$\{j \in [\![1,n]\!] \mid j < \sigma^{-1}(i) \text{ et } \sigma(j) > i\} \subset \{j \in [\![1,n]\!] \mid \sigma(j) > i\} = \sigma^{-1}[\![i+1,n]\!],$$

on déduit que $0 \leqslant b_i(\sigma) \leqslant n-i$. De plus, $\sum_{i=1}^{n} b_i(\sigma)$ est le cardinal de l'ensemble :

$$\{(i,j) \in [\![1,n]\!]^2 \mid j < \sigma^{-1}(i) \text{ et } \sigma(j) > i\};$$

par changement bijectif d'indice de i en $\sigma(i)$, cet ensemble est en bijection avec l'ensemble :

$$\{(i,j) \in [\![1,n]\!]^2 \mid j < i \text{ et } \sigma(j) > \sigma(i)\},$$

qui a, par définition, $N(\sigma)$ éléments.

(ii) On se donne des $\beta_i \in [\![0, n-i]\!]$ pout $i = 1, \ldots, n$, et l'on veut reconstituer la permutation σ telle que $\beta_i = b_i(\sigma)$. Pour cela, on va successivement placer les valeurs $n, \ldots, 1$ (voir l'exercice précédent pour la distinction entre valeur et position). L'idée est que $b_i(\sigma)$ est le nombre de valeurs $b = \sigma(j)$ plus grandes que la valeur i et dont la position j est plus petite que la position $\sigma^{-1}(i)$ de la valeur i, donc le nombre de valeurs plus grandes que i et situées à gauche de i. La méthode suivie procède par insertions successives :

1. On place d'abord la valeur n arbitrairement.
2. Si $\beta_{n-1} = 0$, il n'y a à gauche de $n-1$ aucune valeur plus grande : on place donc $n-1$ à gauche de n. Si $\beta_{n-1} = 1$, il y a à gauche de $n-1$ une valeur plus grande, qui ne peut être que n : on place donc $n-1$ à droite de n.
3. Supposons les valeurs $n, n-1, \ldots, i+1$ placées les unes par rapport aux autres. On insère parmi elles la valeur i de manière à laisser exactement $b_i(\sigma)$ éléments à sa gauche parmi ces $n-i$ éléments. Les $(n-i+1)$ valeurs possibles de $b_i(\sigma)$ dans $[\![0, n-i]\!]$ correspondent aux $(n-i+1)$ positions d'insertion possibles parmi ces $n-i$ éléments (de tout à gauche à tout à droite).

Il est clair que ce processus reconstitue l'unique ordre possible des valeurs de σ, et l'on a ainsi explicité une réciproque à l'application $\sigma \mapsto \big(b_n(\sigma), \ldots, b_1(\sigma)\big)$. Cette dernière est donc une bijection $\mathfrak{S}_n$ sur $\{0\} \times \{0,1\} \times \cdots \times \{0, \ldots, n-1\}$.

À titre d'exemple, partant de $(0,1,1,2,0,1)$, on obtient, par insertions successives, les listes : (6), puis $(6,5)$, puis $(6,4,5)$, puis $(6,4,3,5)$, puis $(2,6,4,3,5)$, et enfin $(2,1,6,4,3,5)$. Le lecteur vérifiera que le tableau d'inversions de la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 4 & 3 & 5 \end{pmatrix}$ est bien (à l'envers) $(0,1,1,2,0,1)$.

II.8.9 Chaque passe qui a un effet diminue de 1 chacun des $b_i(\sigma)$ qui n'est pas nul. La dernière passe, sans effet, ne modifie rien parce que les $b_i(\sigma)$ sont déjà tous nuls. Le nombre total de passes est donc $1 + \max\big(b_1(\sigma), \ldots, b_n(\sigma)\big)$. (Attention, c'est bien un $\max$ et non un $\min$.)

II.8.10 Si $P = a_0 + \cdots + a_d X^d$ et $Q = b_0 + \cdots + b_d X^d$, notons $P + Q = c_0 + \cdots + c_d X^d$; les coefficients sont rangés dans des tableaux et l'algorithme s'écrit :

```
pour i de 0 a d faire
   c[i] := a[i] + b[i] ;;
```

L'algorithme est simple parce qu'il n'y a pas de propagation des retenues ! Le coût est $(n+1)C$, où C est le coût de l'addition des scalaires.

II.8.11 Soient d, e les degrés de P, Q, et $f = d + e$ le degré de PQ. Le nombre de termes intervenant dans le coefficient de degré k de PQ, à savoir $c_k = \sum_{i+j=k} a_i b_j$, est l'entier :

$$\begin{aligned} N_k &:= \{(i,j) \in [\![0,d]\!] \times [\![0,e]\!] \mid i+j=k\} \\ &= \{i \in [\![0,d]\!] \mid 0 \leqslant k-i \leqslant e\} \\ &= \operatorname{card}\left([\![0,d]\!] \cap [\![k-e,k]\!]\right). \end{aligned}$$

Si $k > f = e + d$, ou si $k < 0$, ce dernier ensemble est vide et $N_k = 0$. Pour analyser les autres cas, nous supposerons que $d \leqslant e$, donc $\min(d,e) = d$ et $\max(d,e) = e$.

1. Si $0 \leqslant k \leqslant d$, alors $[\![0,d]\!] \cap [\![k-e,k]\!] = [\![0,k]\!]$ et $N_k = k+1$.
2. Si $d \leqslant k \leqslant e$, alors $[\![0,d]\!] \cap [\![k-e,k]\!] = [\![0,d]\!]$ et $N_k = d+1$.
3. Si $e \leqslant k \leqslant f$, alors $[\![0,d]\!] \cap [\![k-e,k]\!] = [\![k-e,d]\!]$ et $N_k = f-k+1$.

Remarquez que, dans chaque cas limite $k = d$ et $k = e$, les deux formules applicables donnent le même résultat. Voici le calcul final :

$$\begin{aligned} \sum_{k=0}^{f} N_k &= \sum_{k=0}^{d-1}(k+1) + \sum_{k=d}^{e}(d+1) + \sum_{k=e+1}^{f}(f-k+1) \\ &= \frac{d(d+1)}{2} + (e-d+1)(d+1) + \frac{d(d+1)}{2} \\ &= (d+1)(e+1), \end{aligned}$$

comme prévu.

II.8.12 Appliquons l'algorithme aux polynômes A de degré d et B de degré $\deg B < d$. On pose $A_0 := A$, $A_1 := B$, puis l'on effectue les divisions euclidiennes $A_{i-1} = Q_i A_i + A_{i+1}$. L'algorithme s'arrête avec $A_k \neq 0$, $A_{k+1} = 0$. Si l'on note $x_i := \deg A_i - \deg A_{i+1}$, le coût de la division euclidienne $A_{i-1} = Q_i A_i + A_{i+1}$ est $\deg Q_i \deg A_i$, c'est-à-dire $x_{i-1}(x_i + \cdots + x_k)$. Le coût total est donc $\sum_{0 \leqslant i < j \leqslant k} x_i x_j$, et l'on a la contrainte : $\sum_{i=0}^{k} x_i = d$.

Il découlera du cours de L2 sur les fonctions de plusieurs variables que le maximum est atteint lorsque les x_i sont égaux, et qu'il vaut donc $\dfrac{kd^2}{2(k+1)}$ (en admettant des valeurs non entières pour les x_i ! ! !) On a donc certainement une majoration par $\dfrac{d^2}{2}$, ce que nous pouvons montrer « à la main » ; en effet, on a de toutes façons :

$$d^2 = \left(\sum_{i=0}^{k} x_i\right)^2 = \sum_{i=0}^{k} x_i^2 + 2 \sum_{0 \leqslant i < j \leqslant k} x_i x_j \geqslant 2 \sum_{0 \leqslant i < j \leqslant k} x_i x_j,$$

d'où la majoration voulue. S'il y a beaucoup d'étapes (k grand), on approche donc le majorant $\dfrac{kd^2}{2(k+1)}$; mais si, par exemple, B est de degré e et divise A, le coût total est $e(d-e)$ qui varie entre $d-1$ et $\dfrac{d^2}{4}$.

II.8.13 (i) L'addition et la multiplication comportent chacune n^2 calculs de coefficients. Pour l'addition de matrices, il y a donc n^2 additions de scalaires. Pour la multiplication, chaque $\sum a_{i,k}b_{k,j}$ comporte n multiplications et $(n-1)$ additions ; il y a donc au total $n^2(n-1)$ additions et n^3 multiplications de scalaires.

(ii) Le terme $7C(n)$ provient des 7 multiplications de matrices de taille moitié plus petites et le terme an^2 des 18 additions de matrices (a est donc le coût de 18 additions de scalaires, d'après la première question). Le raisonnement qui conduit à l'estimation $C(n) = \Theta(n^\beta)$, où $\beta = \log_2 7 \approx 2{,}81 < 3$, est alors exactement le même que celui du théorème qui fournit l'estimation de l'algorithme de Karatsuba.

Module III.1 : Géométrie dans les espaces affines

III.1.1 Toute application continue $f : \mathbb{R} \to \mathbb{R}$ admet des primitives. L'ensemble X des primitives de f est donc non vide. Deux primitives diffèrent d'une constante. Nous allons montrer que X est un espace affine dirigé par $\mathbb{R}$, l'application $X \times X \to \mathbb{R}$ étant l'application $(F_1, F_2) \mapsto \overrightarrow{F_1F_2} := F_2(0) - F_1(0)$ (on aurait pu considérer la différence en n'importe quel point étant donné que $F_2 - F_1$ est une fonction constante).

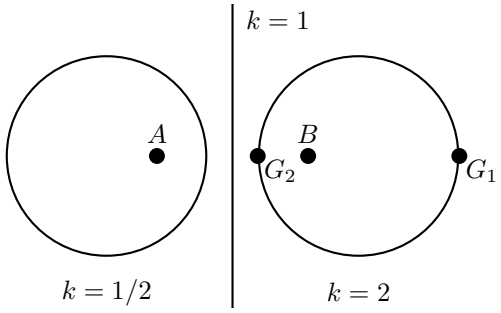
La relation de Chasles est vérifiée puisque

$$\overrightarrow{F_1F_2} + \overrightarrow{F_2F_3} = \big(F_2(0) - F_1(0)\big) + \big(F_3(0) - F_2(0)\big) = F_3(0) - F_1(0) = \overrightarrow{F_1F_3}.$$

Pour toute primitive F et tout réel C, il existe une unique primitive G de f telle que $\overrightarrow{FG} = G(0) - F(0) = C$: c'est l'application $G : x \mapsto F(x) + C$.

L'ensemble des primitives de f est donc un espace affine de dimension 1.

III.1.2



Si $k = 1$, l'ensemble des points M tels que $AM = BM$ est la médiatrice du segment $[AB]$.

Supposons maintenant que $k \neq 1$. On a $AM = k \cdot BM$ si, et seulement si :

$$AM^2 - k^2BM^2 = 0,$$

donc si, et seulement si :

$$\big(\overrightarrow{AM} - k\overrightarrow{BM} \;\big|\; \overrightarrow{AM} + k\overrightarrow{BM}\big) = 0.$$

Considérons le barycentre G_1 de $\{(A, 1), (B, -k)\}$ et le barycentre G_2 de $\{(A, 1), (B, k)\}$. Alors :

$$\overrightarrow{AM} - k\overrightarrow{BM} = \overrightarrow{AG_1} + \overrightarrow{G_1M} - k\overrightarrow{BG_1} - k\overrightarrow{G_1M} = (1 - k)\overrightarrow{G_1M}$$

et

$$\overrightarrow{AM} + k\overrightarrow{BM} = \overrightarrow{AG_2} + \overrightarrow{G_2M} + k\overrightarrow{BG_2} + k\overrightarrow{G_2M} = (1 + k)\overrightarrow{G_2M}.$$

Par conséquent, $AM = k \cdot BM$ si, et seulement si, $\big(\overrightarrow{G_1M} \;\big|\; \overrightarrow{G_2M}\big) = 0$, donc si, et seulement si, M appartient au cercle de diamètre $[G_1G_2]$. Donc, le lieu des points M tels que $AM = k \cdot BM$ est le cercle de diamètre $[G_1G_2]$.

III.1.3 Si M est le barycentre de $\{(A, \alpha), (B, \beta)\}$ avec $\alpha \geqslant 0$ et $\beta \geqslant 0$, alors :

$$\alpha\overrightarrow{AM} + \beta\overrightarrow{BM} = \vec{0}$$

et donc $\overrightarrow{AM}$ et $\overrightarrow{BM}$ sont colinéaires de sens opposés. Par conséquent, le point M appartient au segment $[AB]$.

Réciproquement, si le point M appartient au segment $[AB]$, alors les vecteurs $\overrightarrow{AM}$ et $\overrightarrow{BM}$ sont colinéaires, donc il existe $\alpha \in \mathbb{R}$ et $\beta \in \mathbb{R}$ tels que $(\alpha, \beta) \neq (0, 0)$ et :

$$\alpha\overrightarrow{AM} + \beta\overrightarrow{BM} = \vec{0}.$$

Si α et β étaient de signes opposés, les vecteurs $\overrightarrow{AM}$ et $\overrightarrow{BM}$ seraient de même sens et donc M n'appartiendrait pas au segment $[AB]$. Par conséquent, α et β sont de même signes, et quitte à remplacer (α, β) par $(-\alpha, -\beta)$, on peut supposer qu'ils sont tous deux positifs. Cela montre que $\alpha + \beta \neq 0$ et que M est le barycentre de $\{(A, \alpha), (B, \beta)\}$.

III.1.4 Soit G le barycentre de la famille $\{(A, 1), (B, 1), (C, 1), (D, 1)\}$. Comme A_1 est le barycentre de la famille $\{(B, 1), (C, 1), (D, 1)\}$, la propriété d'associativité du barycentre montre que G est le barycentre de $\{(A, 1), (A_1, 3)\}$. En particulier, G appartient à la médiane AA_1. On montre de même que G est le barycentre de $\{(B, 1), (B_1, 3)\}$ et qu'il appartient donc à la médiane BB_1. De même, G appartient aux médianes CC_1 et DD_1 et les quatre médianes sont donc concourantes en G.

III.1.5 Soit f la rotation de centre A et d'angle α. Soit L la rotation vectorielle d'angle α. Alors, pour tout point M de $\mathbb{R}^2$, on a :

$$\overrightarrow{Af(M)} = L\big(\overrightarrow{AM}\big).$$

Par conséquent, si M_1 et M_2 sont deux points de $\mathbb{R}^2$, on a :

$$\overrightarrow{f(M_1)f(M_2)} = \overrightarrow{Af(M_2)} - \overrightarrow{Af(M_1)} = L\big(\overrightarrow{AM_2}\big) - L\big(\overrightarrow{AM_1}\big) = L\big(\overrightarrow{M_1M_2}\big).$$

L'application f est donc une application affine et l'application linéaire associée est la rotation vectorielle d'angle α.

III.1.6 Soit E et F les espaces vectoriels qui dirigent respectivement X et Y, soit L l'application linéaire associée à f, soit $Y' := f(X')$, soit E' l'espace vectoriel qui dirige X' et soit $F' := L(E')$. Alors, F' est sous-espace vectoriel de F (l'image d'un espace vectoriel par une application linéaire est un espace vectoriel).

Soient B_1 et B_2 deux points de Y'. Alors, $B_1 = f(A_1)$ avec $A_1 \in X'$ et $B_2 = f(A_2)$ avec $A_2 \in X'$. On a donc :

$$\overrightarrow{A_1A_2} \in E' \quad \text{et} \quad \overrightarrow{B_1B_2} = \overrightarrow{f(A_1)f(A_2)} = L\big(\overrightarrow{A_1A_2}\big) \in F'.$$

Enfin, si $B \in Y'$ et $\vec{v} \in F'$, alors $B = f(A)$ avec $A \in X'$ et $\vec{v} = L(\vec{u})$ avec $\vec{u} \in E'$. Puisque X' est un sous-espace vectoriel dirigé par E', on a $A + \vec{u} \in X'$, et donc :

$$B + \vec{v} = f(A) + L(\vec{u}) = f(A + \vec{u}) \in Y'.$$

III.1.7 Les matrices de X sont exactement les matrices de la forme :

$$M = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + a\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \quad \text{avec} \quad (a, b) \in \mathbb{R}^2.$$

Les deux matrices $A := \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$ et $B := \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ ne sont pas proportionnelles. Elles forment donc une famille libre de $M_2(\mathbb{R})$. Par conséquent, X est un plan de $M_2(\mathbb{R})$ donné par une équation paramétrique. Ce plan passe par le point $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ est il est dirigé par le plan vectoriel engendré par les deux matrices A et B.

III.1.8 L'espace affine $X := \mathcal{F}(\mathbb{R}, \mathbb{R})$ est dirigé par l'espace vectoriel $E := \mathcal{F}(\mathbb{R}, \mathbb{R})$. Soit F le sous-espace vectoriel des fonctions impaires, c'est-à-dire les fonctions telles que :

$$f(x) + f(-x) = 0$$

(on voit que F est un sous-espace vectoriel de E car il contient la fonction nulle, que la somme de deux fonctions impaires est impaire et que le produit d'une fonction impaire par un scalaire est une fonction impaire).

Soit $Y \subset X$ l'ensemble des fonctions $f \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ telles que $f(x) + f(-x) = 1$. Cet ensemble contient la fonction constante égale à $1/2$ et n'est donc pas vide.

Si f et g sont deux fonctions de Y, alors :

$$(g - f)(x) + (g - f)(-x) = \big(g(x) + g(-x)\big) - \big(f(x) - f(-x)\big) = 0.$$

Par conséquent, $g - f \in F$.

Si $f \in Y$ et si $g \in F$, alors :

$$(f + g)(x) + (f + g)(-x) = \big(f(x) + f(-x)\big) + \big(g(x) + g(-x)\big) = 1 + 0 = 1.$$

Par conséquent, $f + g \in Y$.

Cela montre que Y est un sous-espace affine de X.

III.1.9 Soit $X := \mathcal{F}(\mathbb{R}, \mathbb{R})$ l'espace affine dirigé par l'espace vectoriel $E := \mathcal{F}(\mathbb{R}, \mathbb{R})$.

Il est facile de vérifier que l'application :

$$\begin{array}{rccc} L: & E & \longrightarrow & \mathbb{R} \\ & h & \longmapsto & h(1) - h(0) \end{array}$$

est une forme linéaire non nulle, car $L(\lambda h_1 + h_2) = \lambda L(h_1) + L(h_2)$ et $L(\mathrm{Id}) = 1$.

Soit $\varphi : X \to \mathbb{R}$ l'application $f \mapsto f(1) - f(0)$. Cette application est une application affine, l'application linéaire associée étant L. En effet, si f et g sont des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, alors :

$$\varphi(g) - \varphi(f) = \big(g(1) - g(0)\big) - \big(f(1) - f(0)\big) = (g - f)(1) - (g - f)(0) = L(g - f).$$

Comme l'application linéaire associée est une forme linéaire non nulle, on en déduit que :

$$Y := \big\{ f \in X \;\big|\; \varphi(f) = 1 \big\}$$

est un hyperplan affine de X.

III.1.10 La trace d'une matrice carrée est la somme des éléments de la diagonale. L'application $f : M_n(\mathbb{R}) \to \mathbb{R}$ qui à une matrice M associe sa trace est une application linéaire. C'est une forme linéaire non nulle. C'est donc également une forme affine non constante. Par conséquent, l'ensemble :

$$X := \big\{ M \in M_n(\mathbb{R}) \;\big|\; f(M) = 2 \big\}$$

est un hyperplan affine de $M_n(\mathbb{R})$.

III.1.11 Une équation de la droite est donnée par :

$$\det\begin{pmatrix} x & 1 & -2 \\ y & 2 & 1 \\ 1 & 1 & 1 \end{pmatrix} = 0,$$

c'est-à-dire, $x \cdot (2-1) - y \cdot (1+2) + 1 \cdot (1+4) = 0$. Une équation de la droite est donc :

$$x - 3y + 5 = 0.$$

On vérifie d'ailleurs facilement que les points A et B appartiennent bien à cette droite en substituant leurs coordonnées dans l'équation.

III.1.12 Une équation du plan est donnée par :

$$\det\begin{pmatrix} x & 0 & 0 & 1 \\ y & 0 & 0 & 0 \\ z & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} = 0,$$

c'est-à-dire :

$$x \cdot \det\begin{pmatrix} 0 & 0 & 0 \\ 1 & 2 & 1 \\ 1 & 1 & 1 \end{pmatrix} - y \cdot \det\begin{pmatrix} 0 & 0 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$
$$+ z \cdot \det\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix} + 1 \cdot \det\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{pmatrix} = 0.$$

Une équation du plan est donc $y = 0$, ce qui a posteriori se devine immédiatement puisque les trois points A, B et C ont leur coordonnée y qui est nulle.

III.1.13 Pour déterminer l'équation paramétrique d'une droite de $\mathbb{R}^2$, il suffit d'exprimer les variables x et y comme fonctions affines d'une même variable. Il est possible d'exprimer y en fonction de x :

$$y = \frac{1}{2} - \frac{3}{2}x$$

Une équation paramétrique de la droite est donc :

$$\begin{cases} x = \lambda \\ y = \dfrac{1}{2} - \dfrac{3}{2}\lambda \end{cases} \quad \text{avec} \quad \lambda \in \mathbb{R}.$$

III.1.14 Pour déterminer l'équation paramétrique d'une droite de $\mathbb{R}^3$, il suffit d'exprimer les variables x, y et z comme fonctions affines d'une même variable. Il est possible d'exprimer y et z en fonction de x :

$$\begin{cases} y = -x \\ z = -2 + 2x \end{cases} \quad \text{avec} \quad x \in \mathbb{R}.$$

Une équation paramétrique de la droite est donc :

$$\begin{cases} x = \lambda \\ y = -\lambda \\ z = -2 + 2\lambda \end{cases} \quad \text{avec} \quad \lambda \in \mathbb{R}.$$

III.1.15 Pour déterminer l'équation paramétrique d'un plan de $\mathbb{R}^3$, il suffit d'exprimer les variables x, y et z comme fonctions affines de deux variables. Ici, on peut exprimer z comme fonction de x et de y :

$$z = 3x + 2y.$$

Une équation paramétrique du plan est donc :

$$\begin{cases} x = \lambda \\ y = \mu \\ z = 3\lambda + 2\mu \end{cases} \quad \text{avec} \quad (\lambda, \mu) \in \mathbb{R}^2.$$

III.1.16 Les trois points A_1, A_2 et A_3 appartiennent à la même droite d'équation :

$$ax + by + c = 0$$

si, et seulement si, le système suivant de trois équations à trois inconnues (a, b, c) admet une solution non triviale :

$$\begin{cases} x_1 \cdot a + y_1 \cdot b + 1 \cdot c = 0 \\ x_2 \cdot a + y_2 \cdot b + 1 \cdot c = 0 \\ x_3 \cdot a + y_3 \cdot b + 1 \cdot c = 0. \end{cases}$$

Donc, les trois points A_1, A_2 et A_3 sont alignés si, et seulement si, le déterminant du système est nul, donc si, et seulement si :

$$\det \begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{pmatrix} = 0.$$

Enfin, Le déterminant d'une matrice est égal au déterminant de la matrice transposée.

III.1.17 L'intersection $P_1 \cap P_2 \cap P_3$ est un singleton si, et seulement si, le système suivant de trois équations à trois inconnues (x, y, z) admet une unique solution :

$$\begin{cases} a_1 x + b_1 y + c_1 z + d_1 = 0 \\ a_2 x + b_2 y + c_2 z + d_2 = 0 \\ a_3 x + b_3 y + c_3 z + d_3 = 0. \end{cases}$$

L'intersection est donc un singleton si, et seulement si :

$$\det \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix} \neq 0.$$

III.1.18 Les quatre points A_1, A_2, A_3 et A_4 appartiennent à un même plan d'équation $ax + by + cz + d = 0$ si, et seulement si, le système suivant de quatre équations à quatre inconnues (a, b, c, d) admet une solution non triviale :

$$\begin{cases} x_1 \cdot a + y_1 \cdot b + z_1 \cdot c + 1 \cdot d = 0 \\ x_2 \cdot a + y_2 \cdot b + z_2 \cdot c + 1 \cdot d = 0 \\ x_3 \cdot a + y_3 \cdot b + z_3 \cdot c + 1 \cdot d = 0 \\ x_4 \cdot a + y_4 \cdot b + z_4 \cdot c + 1 \cdot d = 0. \end{cases}$$

Donc, les quatre points A_1, A_2, A_3 et A_4 sont coplanaires si, et seulement si, le déterminant du système est nul, donc si, et seulement si :

$$\det\begin{pmatrix} x_1 & y_1 & z_1 & 1\\ x_2 & y_2 & z_2 & 1\\ x_3 & y_3 & z_3 & 1\\ x_4 & y_4 & z_4 & 1 \end{pmatrix} = 0.$$

III.1.19 1. Posons $F := F_1 + F_2$. Puisque D_1 et D_2 ne sont pas parallèles, $F_1 \neq F_2$ et donc, la dimension de F est égale à 2.

Soit A un point de D_2 et soit X le sous-espace affine de $\mathbb{R}^3$ passant par A et dirigé par F. C'est l'espace :

$$X := A + F = \left\{M \in \mathbb{R}^3 \;\middle|\; \overrightarrow{AM} \in F_1 + F_2\right\}.$$

Notons que X est un plan et que :

$$D_2 = A + F_2 \subset X.$$

2. Soit A' un point de D_1 et soit L la partie linéaire de f (c'est la projection vectorielle sur F parallèlement à $F^\perp$). Comme $F_1 \subset F$, on a $L(F_1) = F_1$. Par conséquent :

$$f(D_1) = f(A') + L(F_1) = f(A') + F_1.$$

Donc, $f(D_1)$ est une droite contenue dans le plan X et les droites $f(D_1)$ (dirigée par F_1) et D_2 (dirigée par $F_2 \neq F_1$) ne sont pas parallèles. On en déduit que ces deux droites s'intersectent en un unique point A_2.

3. D'une part, comme $A_2 \in f(D_1)$, il existe un point $A_1 \in D_1$ tel que $f(A_1) = A_2$.

D'autre part, si $M \in D_1$, alors $\overrightarrow{A_1M} \in F_1 \subset F$ et si $f(M) = A_2$, alors $\overrightarrow{A_2M} \in F^\perp$, donc

$$\overrightarrow{A_1M} = \underbrace{\overrightarrow{A_1A_2}}_{\in F^\perp} + \underbrace{\overrightarrow{A_2M}}_{\in F^\perp} \in F^\perp.$$

Comme F et $F^\perp$ sont supplémentaires et comme $\overrightarrow{A_1M} \in F \cap F^\perp$, on a $\overrightarrow{A_1M} = \vec{0}$ et $A_1 = M$.

4. Si $B_1 \in D_1$ et si $B_2 \in D_2$, on a :

$$\overrightarrow{B_1B_2} = \underbrace{\overrightarrow{B_1A_1}}_{\in F} + \underbrace{\overrightarrow{A_1A_2}}_{\in F^\perp} + \underbrace{\overrightarrow{A_2B_2}}_{\in F}.$$

D'après le théorème de Pythagore, on a donc :

$$\left\|\overrightarrow{B_1B_2}\right\|^2 = \left\|\overrightarrow{A_1A_2}\right\|^2 + \left\|\overrightarrow{B_1A_1} + \overrightarrow{A_2B_2}\right\|^2 \geqslant \left\|\overrightarrow{A_1A_2}\right\|^2$$

avec égalité si, et seulement si, $\overrightarrow{B_1A_1} + \overrightarrow{A_2B_2} = \vec{0}$. Les deux vecteurs $\overrightarrow{B_1A_1} \in F_1$ et $\overrightarrow{B_2A_2} \in F_2$ ne sont colinéaires que si $\overrightarrow{B_1A_1} = \overrightarrow{B_2A_2} = \vec{0}$, c'est-à-dire, si $A_1 = B_1$ et $A_2 = B_2$.

III.1.20 Il nous suffit de déterminer le projeté orthogonal de B sur la droite D et de calculer $\left\|\overrightarrow{BC}\right\|$. Soient (x, y, z) les coordonnées du point C. Puisque C appartient à la droite D, on

a :

$$\begin{cases} x = 2\lambda \\ y = 1 - \lambda \\ z = 1. \end{cases}$$

Tout plan orthogonal à la droite D a une équation de la forme $2x - y = d$. Le plan orthogonal à D passant par B a donc pour équation $2x - y = 1$. Par conséquent $4\lambda - 1 + \lambda = 1$, donc :

$$\lambda = \frac{2}{5}, \quad x = \frac{4}{5}, \quad y = \frac{3}{5} \quad \text{et} \quad z = 1.$$

On en tire :

$$\left\|\overrightarrow{BC}\right\|^2 = \left(1 - \frac{4}{5}\right)^2 + \left(1 - \frac{3}{5}\right)^2 + (-2 - 1)^2 = \frac{46}{5}.$$

Par conséquent :

$$d(B, D) = \sqrt{46/5}.$$

III.1.21 Soient D et D' les deux directrices associées respectivement aux foyers F et F' et soit $e \in]0, 1[$ l'excentricité de l'ellipse. Un point $M \in \mathbb{R}^2$ appartient à l'ellipse si, et seulement si, $d(M, F) = e \cdot d(M, D)$ si, et seulement si, $d(M, F') = e \cdot d(M, D')$. Par conséquent, pour tout $M \in \mathcal{E}$:

$$d(M, F) + d(M, F') = e \cdot \big(d(M, D) + d(M, D')\big).$$

Comme tous les points de l'ellipse se trouvent entre les deux directrices et comme $\overrightarrow{MD}$ et $\overrightarrow{MD'}$ sont tous deux perpendiculaires à D et D', on a :

$$d(M, D) + d(M, D') = \left\|\overrightarrow{AA'}\right\|$$

avec A le projeté orthogonal de M sur D et A' le projeté orthogonal de M sur D'. En effet, $\overrightarrow{AA'} = \overrightarrow{AM} + \overrightarrow{MA'}$ avec $\overrightarrow{AM}$ et $\overrightarrow{MA'}$ colinéaires et de même sens.

Le vecteur $\overrightarrow{AA'}$ ne dépend pas de M. En effet, $A \in D$, A' est le projeté orthogonal de A sur D'. Si B est un autre point de D et B' son projeté orthogonal sur D', alors $\overrightarrow{BB'} = \overrightarrow{BA} + \overrightarrow{AA'} + \overrightarrow{A'B'}$ et donc :

$$\overrightarrow{BB'} - \overrightarrow{AA'} = \overrightarrow{BA} + \overrightarrow{A'B'}.$$

Le terme de gauche dirige l'orthogonal de D et le terme de droite dirige D. Par conséquent, les deux termes sont nuls. Donc $\overrightarrow{BB'} = \overrightarrow{AA'}$.

III.1.22 Soient D et D' les deux directrices associées respectivement aux foyers F et F' et soit $e > 1$ l'excentricité de l'hyperbole. Un point $M \in \mathbb{R}^2$ appartient à l'hyperbole si, et seulement si, $d(M, F) = e \cdot d(M, D)$ si, et seulement si, $d(M, F') = e \cdot d(M, D')$. Par conséquent, pour tout $M \in \mathcal{E}$:

$$\big|d(M, F) - d(M, F')\big| = e \cdot \big|d(M, D) - d(M, D')\big|.$$

Comme aucun point de l'hyperbole ne se trouve entre les deux directrices et comme $\overrightarrow{MD}$ et $\overrightarrow{MD'}$ sont tous deux perpendiculaires à D et D', on a :

$$\big|d(M, D) - d(M, D')\big| = \left\|\overrightarrow{AA'}\right\|$$

avec A le projeté orthogonal de M sur D et A' le projeté orthogonal de M sur D'.

Comme dans l'exercice précédent, la norme de $\overrightarrow{AA'}$ ne dépend pas de M.

Module III.2 : Courbes paramétrées

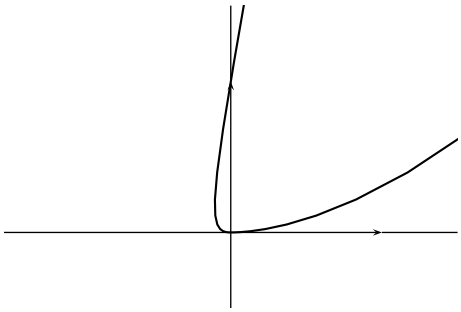
III.2.1 Au temps $t = 0$, les trois courbes passent par l'origine $(0,0)$. De plus, les trois courbes sont de classe $\mathcal{C}^\infty$ au voisinage de $t = 0$. Nous allons donc rechercher s'il existe deux vecteurs non colinéaires u_0 et v_0 et deux entiers p et q tels que

$$\gamma(t) = (0,0) + t^p\lambda(t)u_0 + t^q v_0 + t^q\varepsilon(t) \quad \text{avec} \quad \lambda(t) \underset{t\to 0}{\longrightarrow} 1 \quad \text{et} \quad \varepsilon(t) \underset{t\to 0}{\longrightarrow} (0,0).$$

On a :

$$\gamma_1(t) = \begin{pmatrix} 0 \\ 0 \end{pmatrix} + t^3(1+t)\begin{pmatrix} 1 \\ 0 \end{pmatrix} + t^6\begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

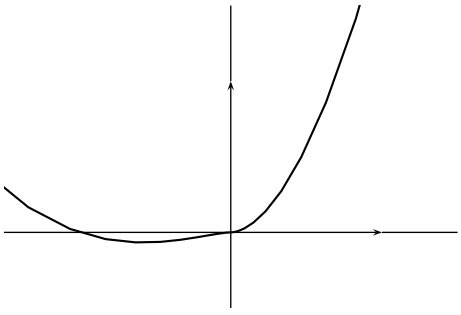
On peut donc considérer $u_0 := (1,0)$, $p = 3$, $v_0 := (0,1)$ et $q = 6$. Comme p est impair et q est pair, le point est un point ordinaire. La tangente est la droite qui passe par l'origine et est dirigée par le vecteur u_0, c'est-à-dire l'axe des abscisses.



On a

$$\gamma_2(t) = \begin{pmatrix} 0 \\ 0 \end{pmatrix} + t^3\begin{pmatrix} 1 \\ 0 \end{pmatrix} + t^5\begin{pmatrix} 0 \\ 1 \end{pmatrix} + t^5\begin{pmatrix} 0 \\ t \end{pmatrix}.$$

On peut donc considérer $u_0 := (1,0)$, $p = 3$, $v_0 := (0,1)$ et $q = 5$. Comme p et q sont impairs, le point est un point d'inflexion. La tangente est la droite qui passe par l'origine et est dirigée par le vecteur u_0, c'est-à-dire l'axe des abscisses.



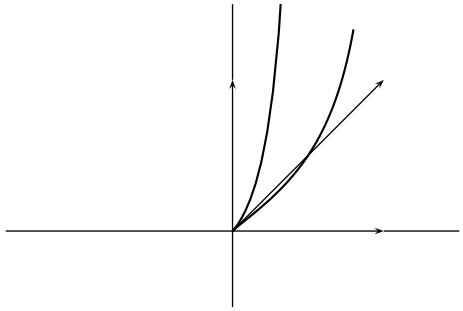
Notons que

$$\frac{t^2}{1+t^2} = t^2 + t^3\varepsilon(t) \quad \text{et} \quad \frac{t^2}{1+t} = t^2 - t^3 + t^3\varepsilon(t).$$

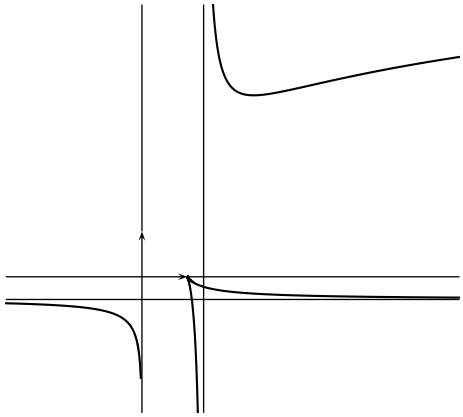
Par conséquent,

$$\gamma_3(t) = \begin{pmatrix} 0 \\ 0 \end{pmatrix} + t^2\begin{pmatrix} 1 \\ 1 \end{pmatrix} + t^3\begin{pmatrix} 0 \\ -1 \end{pmatrix} + t^3\varepsilon(t) \quad \text{avec} \quad \varepsilon(t) \underset{t\to 0}{\longrightarrow} (0,0).$$

On peut donc considérer $u_0 := (1,1)$, $p = 2$, $v_0 := (0,-1)$ et $q = 3$. Comme p est pair et q est impair, le point est un point de rebroussement de première espèce. La tangente est la droite qui passe par l'origine et est dirigée par le vecteur u_0, c'est-à-dire la première bissectrice.



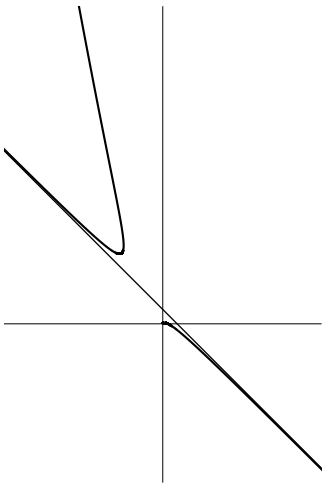
III.2.2



Nous devons d'abord déterminer pour quelles valeurs t_0 on a $\big\|\gamma(t)\big\| \underset{t\to t_0}{\longrightarrow} +\infty$. En ce qui concerne γ_1, cela se produit pour $t_0 = \pm 1$ et $t_0 = \pm\infty$. Lorsque $t \to 1$, on a $x(t) \to e/2$. La droite d'équation $x = -e/2$ est donc asymptote à la courbe. Lorsque $t \to -1$, on a $y(t) \to -1/2$. La droite d'équation $y = -1/2$ est donc asymptote à la courbe. Lorsque $t \to -\infty$, on a $x(t) \to 0$. L'axe des ordonnées est donc asymptote à la courbe. Enfin, lorsque $t \to +\infty$, $x(t)$ et $y(t)$ tendent tous deux vers $+\infty$. Il nous faut donc étudier le rapport $y(t)/x(t)$. Notons que :

$$\frac{y(t)}{x(t)} \sim \frac{t}{e^t} \underset{t\to+\infty}{\longrightarrow} 0.$$

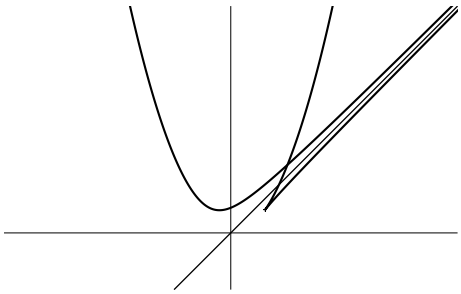
Par conséquent, la courbe admet une branche parabolique horizontale.



En ce qui concerne γ_2, il y a des branches infinies quand $t \to -1$ et $t \to -\infty$. Lorsque $t \to +\infty$, il y a un point d'arrêt puisque $\gamma_2(t) \to (0,0)$. Quand $t \to -1$, $x(t)$ et $y(t)$ tendent tous deux vers $\pm\infty$, mais $y(t)/x(t) = t \to -1$. Par conséquent, il y a une direction asymptotique $y = -x$. Pour déterminer s'il y a une asymptote, étudions la quantité :

$$y(t) + x(t) = \frac{te^{-t}}{t+1} + \frac{e^{-t}}{t+1} = e^{-t} \underset{t\to -1}{\longrightarrow} e.$$

La droite d'équation $y = -x + e$ est donc asymptote à la courbe. Quand $t \to -\infty$, $x(t) \to -\infty$ et $y(t) \to +\infty$. De plus, $y(t)/x(t) = t \to -\infty$. Il y a donc une branche parabolique verticale.



En ce qui concerne γ_3, il y a des branches infinies quand $t \to 0$ et quand $t \to \pm\infty$. Lorsque $t \to 0$, $x(t) \to \pm\infty$ et $y(t) \to +\infty$. De plus :

$$\frac{y(t)}{x(t)} = \frac{t^4+1}{t(t^3+2)} \to \pm\infty.$$

Par conséquent, il y a deux branches paraboliques verticales. De plus, lorsque $t \to \pm\infty$, $x(t)$ et $y(t)$ sont tous deux équivalents à t^2. Il tendent donc vers $+\infty$ et le rapport $y(t)/x(t)$ tend vers 1. Enfin, $y(t) - x(t)$ tend vers 0 ce qui montre que la droite d'équation $y = x$ est asymptote à la courbe.

III.2.3 L'ensemble de définition de x est $\mathbb{R} \setminus \{1, -2\}$ et celui de y est $\mathbb{R} \setminus \{1\}$. On doit donc étudier trois courbes définies sur les trois intervalles $]-\infty, -2[$, $]-2, 1[$ et $]1, +\infty[$.

Il n'y a pas de symétrie particulière qui permette de réduire l'ensemble d'étude.

Étudions les variations de x et de y. On a :

$$x'(t) = \frac{3t^2(t^2+t-2) - t^3(2t+1)}{(t^2+t-2)^2}$$

qui est du même signe que $3(t^2+t-2) - t(2t+1) = t^2+2t-6$. La dérivée de x s'annule donc en $-1+\sqrt{7}$ et $-1-\sqrt{7}$, elle est positive en dehors des racines, négative entre les racines. On a :

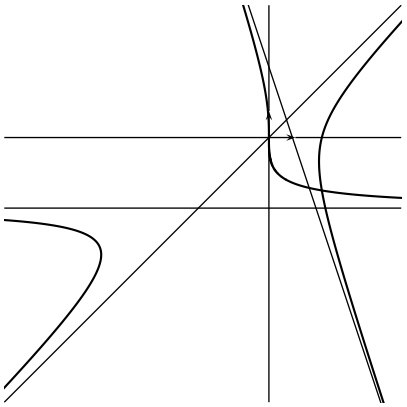
$$y'(t) = \frac{(2t-2)(t-1) - (t^2-2t)}{(t-1)^2}$$

qui est du même signe que $2t^2-4t+2-t^2+2t = t^2-2t+2$. La dérivée de y est donc toujours strictement positive. On obtient donc le tableau de variations suivant.

t	$-\infty$		$-1-\sqrt{7}$		-2		1		$-1+\sqrt{7}$		$+\infty$
$x'(t)$		$+$	0	$-$	‖	$-$	‖	$-$	0	$+$	
$x(t)$	$-\infty$	↗	$\frac{-2(10+7\sqrt{7})}{9}$	↘	$-\infty$ ‖ $+\infty$	↘	$-\infty$ ‖ $+\infty$	↘	$\frac{2(7\sqrt{7}-10)}{9}$	↗	$+\infty$
$y'(t)$		$+$		$+$		$+$	‖	$+$		$+$	
$y(t)$	$-\infty$	↗	$\frac{-2(4+\sqrt{7})}{3}$	↗	$-\frac{8}{3}$ ‖ $+\infty$	↗	$-\infty$ ‖ $+\infty$	↗	$\frac{-2(4-\sqrt{7})}{3}$	↗	$+\infty$

Il y a une asymptote horizontale quand $t \to -2$ puisque $x \to \pm\infty$ et $y \to -8/3$. Cette asymptote est la droite d'équation $y = -8/3$. Lorsque $t \to 1$, x et y tendent tous deux vers $\pm\infty$ et :

$$\frac{y}{x} = \frac{(t^2-2t)(t+2)}{t^3} \underset{t\to 1}{\longrightarrow} -3.$$



Il y a donc une direction asymptotique $y = -3x$. De plus :

$$y+3x = \frac{t^2-2t}{t-1} + 3\frac{t^3}{(t-1)(t+2)}$$
$$= \frac{t^3-4t+3t^3}{(t-1)(t+2)} = \frac{4t(t+1)}{t+2} \underset{t\to 1}{\longrightarrow} \frac{8}{3}.$$

Par conséquent, la droite d'équation $y = -3x + 8/3$ est asymptote à la courbe. Enfin, quand $t \to \pm\infty$, $x \sim t$ et $y \sim t$. Par conséquent, tous deux tendent vers $\pm\infty$ et comme $y/x \to 1$, il y a une direction asymptotique $y = x$. Comme :

$$y - x = \frac{t^2 - 2t}{t-1} - \frac{t^3}{(t-1)(t+2)} = \frac{t^3 - 4t - t^3}{(t-1)(t+2)} = \frac{-4t}{(t-1)(t+2)} \underset{t\to\pm\infty}{\longrightarrow} 0,$$

la première bissectrice $y = x$ est asymptote à la courbe.

III.2.4 Le domaine de définition de x et de y est $\mathbb{R}$. Les fonctions sont périodiques de période 2π. La fonction x est impaire et la fonction y est paire. On peut donc étudier la courbe sur l'intervalle $[0, \pi]$. On obtiendra alors toute la courbe par symétrie par rapport à l'axe des ordonnées.

On a $x'(t) = \cos(t)$ et on calcule :

$$\frac{-2\cos(t)\sin(t)\big(2 - \cos(t)\big) - \cos^2(t)\sin(t)}{\big(2 - \cos(t)\big)^2} = -\cos(t)\sin(t)\frac{4 - \cos(t)}{\big(2 - \cos(t)\big)^2}.$$

On a donc le tableau de variations suivant.

t	0		$\pi/2$		π
$x'(t)$		$+$	0	$-$	
$x(t)$	0	↗	1	↘	0
$y'(t)$	0	$-$	0	$+$	0
$y(t)$	1	↘	0	↗	1

Il y a un point stationnaire en $t = \pi/2$. Si l'on pose $t = \pi/2 + u$, on a :

$$x = \cos(u) \quad \text{et} \quad y = \frac{\sin^2(u)}{2 + \sin(u)}.$$

Par conséquent,

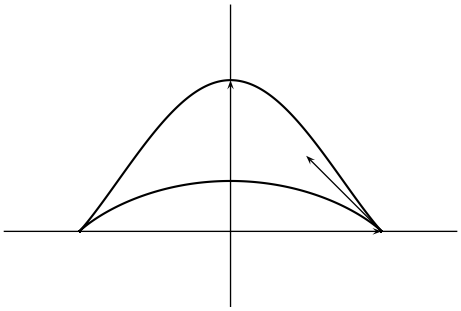
$$x = 1 - \frac{1}{2}u^2 + u^3\varepsilon(u) \quad \text{et} \quad y = \frac{u^2}{2+u} + u^3\varepsilon(u) = \frac{1}{2}u^2 - \frac{1}{4}u^3 + u^3\varepsilon(u).$$

Par conséquent,

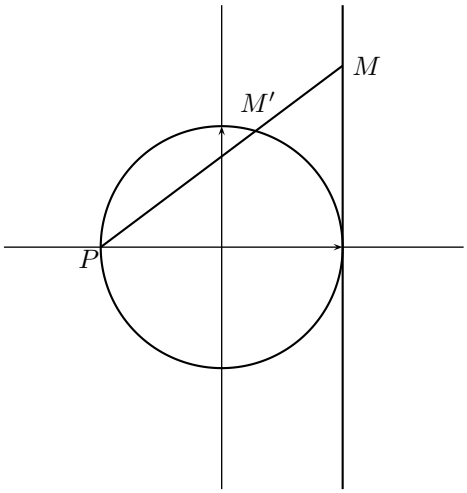
$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} + u^2 \begin{pmatrix} -1/2 \\ 1/2 \end{pmatrix} + u^3 \begin{pmatrix} 0 \\ -1/4 \end{pmatrix} + u^3\varepsilon(u) \quad \text{avec} \quad \varepsilon(u) \underset{u\to 0}{\longrightarrow} (0,0).$$

Il y a une tangente dirigée par le vecteur $(-1/2, 1/2)$. Le point est un point de rebroussement

de première espèce.



III.2.5



1. Une équation de la droite (PM) est :

$$\det\begin{pmatrix} x & -1 & 1 \\ y & 0 & 2t \\ 1 & 1 & 1 \end{pmatrix} = 0,$$

c'est-à-dire, $-2tx+2y-2t=0$. Par conséquent, si $t \neq 0$, on a $x = y/t-1$. Puisque M' appartient au cercle C, on a $x^2+y^2=1$, donc :

$$\Big(\frac{y}{t}-1\Big)^2 + y^2 = 1 \iff \frac{y^2}{t^2} - 2\frac{y}{t} + y^2 = 0$$
$$\iff \frac{y}{t^2}\big((1+t^2)y - 2t\big) = 0.$$

2. Comme $M' \neq P$, on a $y \neq 0$ et donc, $(1+t^2)y - 2t$. Par conséquent, si $t \neq 0$:

$$y = \frac{2t}{1+t^2} \quad \text{et} \quad x = \frac{2}{1+t^2} - 1 = \frac{1-t^2}{1+t^2}\cdot$$

Si $t=0$, le point $M := (1,0)$ appartient à C et donc, $M' = M = (1,0)$.

3. Lorsque t parcourt $\mathbb{R}$ en croissant, le point $M := (1, 2t)$ parcourt la droite d'équation $x = 1$ en montant. Le point M' parcourt $C \setminus P$ dans le sens trigonométrique.

III.2.6 1. La fonction $\rho : \theta \mapsto 1 + \cos(\theta)$ est périodique de période 2π et paire. On peut donc l'étudier sur l'intervalle $[0, 2\pi]$. On obtiendra alors toute la courbe par symétrie par rapport à l'axe des abscisses. En effet, le point M de coordonnées $x := \rho(\theta)\cos(\theta)$ et $y := \rho(\theta)\sin(\theta)$ appartient à la courbe si, et seulement si, le point M' de coordonnées $\rho(-\theta)\cos(-\theta) = x$ et $\rho(-\theta)\sin(-\theta) = -y$ appartient à la courbe.
Si $\theta \in [0, \pi[$, $\rho(\theta) > 0$. La courbe admet donc des points réguliers pour $\theta \in [0, \pi[$. De plus, en $\theta = \pi$, ρ ne change pas de signe. La courbe admet donc une tangente dirigée par le vecteur $u_\pi = \big(\cos(\pi), \sin(\pi)\big) = (-1, 0)$ (cette tangente est l'axe des abscisses) et un point de rebroussement de première espèce.
Comme la fonction ρ est bornée, il n'y a pas de branche infinie.
La fonction ρ est décroissante sur l'intervalle $[0, \pi]$ car sa dérivée, $\rho'(\theta) = -\sin(\theta)$ y est négative. Par conséquent, ρ admet un maximum pour $\theta = 0$. Comme $\rho(0) = 2$, on voit que la courbe est contenue dans le disque centré en 0 de rayon 2. Au temps $\theta = 0$, la courbe admet une tangente dirigée par le vecteur $v_0 = \big(-\sin(0), \cos(0)\big) = (0, 1)$. Elle admet donc une tangente verticale au point $(0, 2)$.

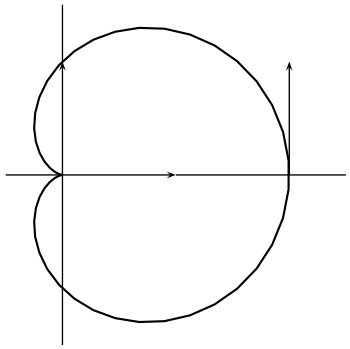


FIGURE V.3.4 – La courbe définie en coordonnées polaires par $\rho(\theta) = 1 + \cos(\theta)$ est une cardioïde.

2. La fonction $\rho : \theta \mapsto \sqrt{2\cos(2\theta)}$ n'est définie que lorsque $\cos(2\theta) \geqslant 0$, c'est-à-dire lorsque θ appartient à un intervalle de la forme $[-\pi/4 + k\pi, \pi/4 + k\pi]$ avec $k \in \mathbb{Z}$. Comme la fonction ρ est périodique de période π et paire, nous ramenons l'étude à l'intervalle $[0, \pi/4]$ et nous compléterons la courbe par symétrie par rapport à l'axe des abscisses (ce qui permet de tracer la courbe sur l'intervalle $[-\pi/4, 0]$) puis par symétrie centrale (ce qui permet de tracer la courbe sur l'intervalle $[3\pi/4, 5\pi/4]$). En effet, le point M de coordonnées $x := \rho(\theta)\cos(\theta)$ et $y := \rho(\theta)\sin(\theta)$ appartient à la courbe si, et seulement si, le point M' de coordonnées $\rho(\theta + \pi)\cos(\theta + \pi) = -x$ et $\rho(\theta + \pi)\sin(\theta + \pi) = -y$ appartient à la courbe.
Si $\theta \in [0, \pi/4[$, $\rho(\theta) > 0$. La courbe admet donc des points réguliers pour $\theta \in [0, \pi/4[$. Comme $\rho(\pi/4) = 0$, la courbe admet une tangente passant par l'origine et dirigée par le vecteur $u_{\pi/4}$. Cette tangente est la première bissectrice.

La fonction ρ est décroissante sur l'intervalle $[0, \pi/4]$; la courbe admet donc une tangente verticale passant par le point $(0, \sqrt{2})$.

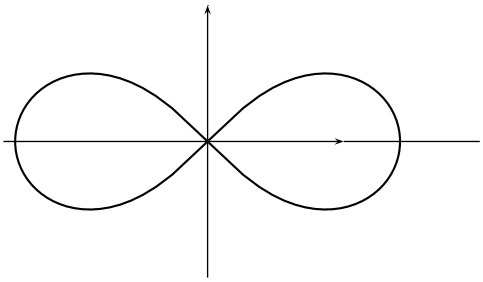
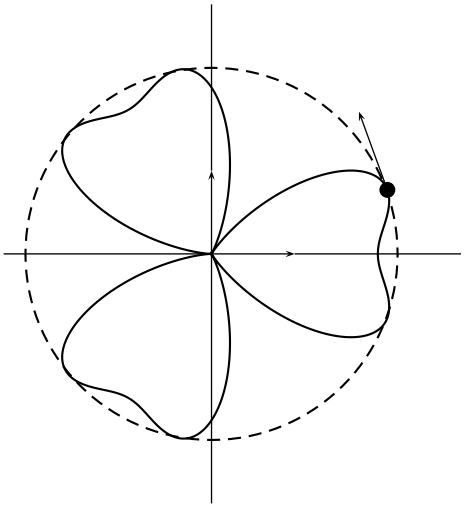


FIGURE V.3.5 – La courbe définie en coordonnées polaires par $\rho(\theta) = \sqrt{2\cos(2\theta)}$ est une lemniscate.

3. La fonction $\rho : \theta \mapsto 1 + \cos(3\theta) + \sin^2(3\theta)$ est périodique de période $2\pi/3$ et c'est une fonction paire. Nous pouvons donc ramener l'étude à l'intervalle $[0, \pi/3]$. Nous obtiendrons la courbe sur l'intervalle $[-\pi/3, 0]$ par symétrie par rapport à l'axe des abscisses, puis sur les intervalles $[\pi/3, 4\pi/3]$ et $[4\pi/3, 2\pi]$ en réalisant deux rotations centrées à l'origine d'angles respectifs $2\pi/3$ et $4\pi/3$.



De nouveau, la fonction ρ est positive sur $[0, \pi/3[$ et admet donc des points réguliers sur cet intervalle. En $\pi/3$ la fonction ρ s'annule sans changer de signe. Elle y admet donc un point de rebroussement de première espèce.
Comme :

$$\begin{aligned}\rho'(\theta) &= -3\sin(3\theta) + 6\sin(3\theta)\cos(3\theta)\\ &= -3\sin(3\theta)\big(1 - 2\cos(3\theta)\big),\end{aligned}$$

on voit que la fonction ρ est croissante sur l'intervalle $[0, \pi/9]$ puis décroissante sur l'intervalle $[\pi/9, \pi/3]$. Elle admet donc une tangente verticale au point $(2, 0)$ (quand $\theta = 0$) et une tangente passant par le point $\frac{9}{4}u_{\pi/9}$ et dirigée par le vecteur $v_{\pi/9}$ (quand $\theta = \pi/9$).

III.2.7 La fonction :

$$\rho : \theta \mapsto \frac{1}{\alpha\cos(\theta) + \beta\sin(\theta)}$$

est définie si $\alpha\cos(\theta) + \beta\sin(\theta) \neq 0$.

Si $\beta = 0$, la fonction ρ est donc définie pour $\theta \neq \pi/2 + k\pi$, $k \in \mathbb{Z}$. Si $\beta \neq 0$, la fonction ρ est donc définie pour $\tan(\theta) \neq -\alpha/\beta$, c'est-à-dire pour $\theta \neq \arctan(-\alpha/\beta) + k\pi$, $k \in \mathbb{Z}$.

On suppose dorénavant que θ appartient à l'ensemble de définition de ρ. Notons que le point $M(\theta)$ a pour coordonnées cartésiennes :

$$x := \frac{\cos(\theta)}{\alpha\cos(\theta) + \beta\sin(\theta)} \quad \text{et} \quad y := \frac{\sin(\theta)}{\alpha\cos(\theta) + \beta\sin(\theta)}.$$

On voit donc que $\alpha x + \beta y = 1$ et le point $M(\theta)$ appartient à la droite d'équation $\alpha x + \beta y = 1$.

Réciproquement, soit M un point de la droite de coordonnées cartésiennes (x, y). Soit $\theta \in [0, 2\pi[$ son argument et $\rho \in [0, +\infty[$ son module. Alors, $x = \rho\cos(\theta)$ et $y = \rho\sin(\theta)$. Par conséquent, $\alpha\rho\cos(\theta) + \beta\rho\sin(\theta) = 1$ et :

$$\rho = \frac{1}{\alpha\cos(\theta) + \beta\sin(\theta)}.$$

III.2.8 Le point $M(\theta)$ admet pour coordonnées cartésiennes :

$$x := \rho(\theta)\cos(\theta) \quad \text{et} \quad y := \rho(\theta)\sin(\theta).$$

On a alors :

$$\begin{aligned}(x-\alpha)^2 + (y-\beta)^2 &= \big(\rho(\theta)\cos(\theta) - \alpha\big)^2 + \big(\rho(\theta)\sin(\theta) - \beta\big)^2 \\ &= \rho(\theta)^2 - \rho(\theta)\big(2\alpha\cos(\theta) + 2\beta\sin(\theta)\big) + \alpha^2 + \beta^2 \\ &= \alpha^2 + \beta^2.\end{aligned}$$

Par conséquent, le point $M(\theta)$ appartient au cercle de centre (α, β) passant par $(0, 0)$.

Réciproquement, si M est un point de ce cercle, on note $\theta \in [0, 2\pi[$ son argument et $\rho \in [0, +\infty[$ son module. Alors, le calcul précédent montre que :

$$\rho^2 - \rho\big(2\alpha\cos(\theta) + 2\beta\sin(\theta)\big) = 0.$$

Par conséquent, ou bien $\rho = 0$, ou bien

$$\rho = 2\alpha\cos(\theta) + 2\beta\sin(\theta).$$

Pour voir que tout point du cercle admet des coordonnées polaires de la forme :

$$\rho(\theta) = 2\alpha\cos(\theta) + 2\beta\sin(\theta),$$

il suffit donc de montrer qu'il existe θ tel que $2\alpha\cos(\theta) + 2\beta\sin(\theta) = 0$. Il suffit de considérer pour cela θ', l'argument de (α, β) et de poser $\theta = \theta' + \pi/2$. Alors, le vecteur $\big(\cos(\theta), \sin(\theta)\big)$ est orthogonal au vecteur (α, β) et donc le produit scalaire $\alpha\cos(\theta) + \beta\sin(\theta)$ est nul.

III.2.9 D'après l'exercice III.2.7, la courbe d'équation :

$$\rho(\theta) = \frac{p}{e\cos(\theta)}$$

est la droite D d'équation $x = \rho(\theta)\cos(\theta) = p/e$. La conique de foyer $(0,0)$, de directrice D et d'excentricité e est l'ensemble des points M tels que $OM = e \cdot d(M,D)$.
Considérons maintenant la courbe d'équation :

$$\rho(\theta) = \frac{p}{1 + e\cos(\theta)}.$$

Si $e > 1$, l'ensemble de définition de cette courbe est $\mathbb{R}$. Si $e = 1$, la fonction ρ n'est pas définie pour $\theta = \pi + 2k\pi$, $k \in \mathbb{Z}$. Si $e < 1$, la fonction ρ n'est pas définie quand $\cos(\theta) = -1/e$, c'est-à-dire si $\theta = \arccos(-1/e) + 2k\pi$ ou si $\theta = -\arccos(-1/e) + 2k\pi$, $k \in \mathbb{Z}$. On suppose dorénavant que θ appartient à l'ensemble de définition de ρ.
Si $M(\theta)$ est le point de coordonnées polaires θ et $\rho(\theta)$, alors :

$$OM = \big|\rho(\theta)\big| = \left|\frac{p}{1 + e\cos(\theta)}\right|$$

et

$$\cdot d(M,D) = e\left|\rho(\theta)\cos(\theta) - \frac{p}{e}\right| = \left|\frac{p\cos(\theta)}{1 + e\cos(\theta)} - \frac{p}{e}\right| = \left|\frac{-p}{e\big(1 + e\cos(\theta)\big)}\right|.$$

Par conséquent, le point $M(\theta)$ appartient à la conique de foyer $(0,0)$, de directrice D et d'excentricité e.
Réciproquement, soit M un point de cette conique. Considérons d'abord le cas où M se trouve du même côté de D que l'origine. Soit $\theta \in [0, 2\pi[$ l'argument de M et $\rho \in [0, +\infty[$ son module. Alors :

$$\rho = OM = e \cdot d(M,D) = e\left(\frac{p}{e} - \rho\cos(\theta)\right).$$

D'où :

$$\rho = \frac{p}{1 + e\cos(\theta)}.$$

Considérons maintenant le cas où M se trouve à droite de D (ce qui ne peut se produire que si $e < 1$, c'est-à-dire si la conique est une hyperbole). Dans ce cas, soit θ l'argument de M augmenté de π et soit ρ l'opposé du module de M. Alors :

$$\rho = -OM = -e \cdot d(M,D) = -e\left(-\rho\cos(\theta - \pi) - \frac{p}{e}\right) = e\left(\frac{p}{e} - \rho\cos(\theta)\right).$$

On retrouve la même équation que précédemment :

$$\rho = \frac{p}{1 + e\cos(\theta)}.$$

III.2.10 1. Posons $\gamma(t) := (3t, 3t^2)$. Alors, $\gamma'(t) = (3, 6t)$ et :

$$\big\|\gamma'(t)\big\| = 3\sqrt{1 + 4t^2}.$$

Par conséquent, la longueur de la courbe paramétrée par $t \in [0,1] \mapsto (3t, 3t^2)$ est :

$$\int_0^1 \big\|\gamma'(t)\big\|\,\mathrm{d}t = 3\int_0^1 \sqrt{1 + 4t^2}\,\mathrm{d}t.$$

Le calcul de la primitive est un peu compliqué. On peut par exemple observer que :

$$\sqrt{1 + 4t^2} = \frac{1 + 4t^2}{\sqrt{1 + 4t^2}} = \frac{1}{2}\frac{2}{\sqrt{1 + (2t)^2}} + t \cdot \frac{4t}{\sqrt{1 + 4t^2}}.$$

De plus, notons que :

$$\Big(\sqrt{1+4t^2}\Big)' = \frac{4t}{\sqrt{1+4t^2}}\cdot$$

Par conséquent, une intégration par partie donne :

$$\int_0^1 \sqrt{1+4t^2}\,\mathrm{d}t = \frac{1}{2}\big[\operatorname{argsh}(2t)\big]_0^1 + \big[t\sqrt{1+4t^2}\big]_0^1 - \int_0^1 \sqrt{1+4t^2}\,\mathrm{d}t.$$

La longueur de la courbe est donc égale à :

$$\frac{3}{4}\operatorname{argsh}2 + \frac{3\sqrt{5}}{2}\cdot$$

2. Posons maintenant $\gamma(t) := (\cos t + \cos^2 t, \sin t + \sin t\cos t)$. Alors :

$$\begin{aligned}\gamma'(t) &= (-\sin t - 2\sin t\cos t, \cos t + \cos^2 t - \sin^2 t)\\ &= \big(-\sin(t) - \sin(2t), \cos(t) + \cos(2t)\big).\end{aligned}$$

Par conséquent :

$$\big\|\gamma'(t)\big\|^2 = 2\big(1 + \sin(t)\sin(2t) + \cos(t)\cos(2t)\big) = 2(1+\cos t).$$

On voit donc que la longueur de la courbe est égale à :

$$\sqrt{2}\int_0^\pi \sqrt{1+\cos(t)}\,\mathrm{d}t.$$

On fait le changement de variable $u = \cos t$ de sorte que

$$\mathrm{d}u = -\sin t\,\mathrm{d}t = -\sqrt{1-u^2}\,\mathrm{d}t.$$

Alors :

$$\begin{aligned}\int_0^\pi \sqrt{1+\cos(t)}\,\mathrm{d}t &= \int_1^{-1} \sqrt{1+u}\,\frac{-\,\mathrm{d}u}{\sqrt{1-u^2}}\\ &= \int_{-1}^1 \frac{\mathrm{d}u}{\sqrt{1-u}}\\ &= \left[-\frac{\sqrt{1-u}}{2}\right]_{-1}^1 = \frac{\sqrt{2}}{2}\cdot\end{aligned}$$

La longueur de la courbe est donc égale à 1.

III.2.11 Tout d'abord, on a :

$$\gamma' = (x', y'), \quad \overrightarrow{T} = \frac{\gamma'}{\|\gamma'\|} = \frac{1}{\sqrt{x'^2+y'^2}}\begin{pmatrix} x'\\ y'\end{pmatrix} \quad \text{et} \quad \overrightarrow{N} = \frac{1}{\sqrt{x'^2+y'^2}}\begin{pmatrix} -y'\\ x'\end{pmatrix}.$$

Par conséquent :

$$\begin{aligned}\overrightarrow{T}' &= -\frac{1}{2}(x'^2+y'^2)^{-3/2}(2x'x''+2y'y'')\begin{pmatrix} x'\\ y'\end{pmatrix} + (x'^2+y'^2)^{-1/2}\begin{pmatrix} x''\\ y''\end{pmatrix}\\ &= \frac{1}{(x'^2+y'^2)^{3/2}}\begin{pmatrix} -x'(x'x''+y'y'') + x''(x'^2+y'^2)\\ -y'(x'x''+y'y'') + y''(x'^2+y'^2)\end{pmatrix}\\ &= \frac{x'y''-y'x''}{(x'^2+y'^2)^{3/2}}\begin{pmatrix} -y'\\ x'\end{pmatrix}.\end{aligned}$$

Si s désigne une abscisse curviligne paramétrant la même courbe géométrique orientée que γ, on a :

$$s' = \sqrt{x'^2 + y'^2}.$$

Par conséquent :

$$\frac{\mathrm{d}\overrightarrow{T}}{\mathrm{d}s} = \frac{\overrightarrow{T}'}{s'} = \frac{x'y'' - y'x''}{(x'^2 + y'^2)^{3/2}}\overrightarrow{N}.$$

On a donc :

$$\kappa = \frac{x'y'' - y'x''}{(x'^2 + y'^2)^{3/2}}.$$

III.2.12 Il suffit de reprendre le résultat de l'exercice précédent avec $x(t) = t$ et $y(t) = f(t)$. On a $x' = 1$, $y' = f'$, $x'' = 0$ et $y'' = f''$, d'où :

$$\kappa = \frac{x'y'' - y'x''}{(x'^2 + y'^2)^{3/2}} = \frac{f''}{(1 + f'^2)^{3/2}}.$$

III.2.13 1. Tout d'abord :

$$\overrightarrow{T} = \frac{\gamma'}{\|\gamma'\|}.$$

Par conséquent :

$$\begin{aligned}\overrightarrow{T}' &= \frac{\gamma''}{\|\gamma'\|} + \left(-\frac{1}{2}(\,\gamma' \mid \gamma'\,)^{-3/2}2(\gamma' \mid \gamma'')\right)\gamma' \\ &= \frac{\gamma''}{\|\gamma'\|} - \frac{(\gamma' \mid \gamma'')\gamma'}{\|\gamma'\|^3}.\end{aligned}$$

On a donc :

$$\begin{aligned}\|\overrightarrow{T}'\|^2 &= \frac{\|\gamma''\|^2}{\|\gamma'\|^2} + \frac{\|\gamma'\|^2(\gamma' \mid \gamma'')^2}{\|\gamma'\|^6} - \frac{2(\gamma' \mid \gamma'')^2}{\|\gamma'\|^4} \\ &= \frac{\|\gamma''\|^2\|\gamma'\|^2 - (\gamma' \mid \gamma'')^2}{\|\gamma'\|^4}.\end{aligned}$$

D'autre part, si α désigne l'angle que font les vecteurs γ' et γ'', on a :

$$\begin{aligned}\|\gamma' \wedge \gamma'\|^2 &= \|\gamma'\|^2\|\gamma''\|^2 \sin^2\alpha \\ &= \|\gamma'\|^2\|\gamma''\|^2(1 - \cos^2\alpha) \\ &= \|\gamma'\|^2\|\gamma''\|^2\left(1 - \frac{(\gamma' \mid \gamma'')^2}{\|\gamma'\|^2\|\gamma''\|^2}\right) \\ &= \|\gamma'\|^2\|\gamma''\|^2 - (\gamma' \mid \gamma'')^2.\end{aligned}$$

Par conséquent :

$$\|\overrightarrow{T}'\| = \frac{\|\gamma' \wedge \gamma''\|}{\|\gamma'\|^2}.$$

Si s est une abscisse curviligne paramétrant la même courbe géométrique que γ, on a $s' = \|\gamma'\|$. D'où :

$$\kappa = \left\|\frac{\mathrm{d}\overrightarrow{T}}{\mathrm{d}s}\right\| = \frac{\|\overrightarrow{T}'\|}{\|\gamma'\|} = \frac{\|\gamma' \wedge \gamma''\|}{\|\gamma'\|^3}.$$

2. Pour déterminer la torsion κ, nous allons utiliser la formule :

$$\frac{\mathrm{d}\overrightarrow{N}}{\mathrm{d}s} = -\kappa\overrightarrow{T} - \tau\overrightarrow{B}$$

qui implique :

$$\tau = -\left(\frac{\mathrm{d}\overrightarrow{N}}{\mathrm{d}s}\,\middle|\,\overrightarrow{B}\right) = -\frac{1}{\|\gamma'\|}(\,\overrightarrow{N}'\mid\overrightarrow{B}\,).$$

Notons que

$$\overrightarrow{T} = \frac{\gamma'}{\|\gamma'\|} \quad \text{et} \quad \overrightarrow{N} = \frac{\overrightarrow{T}'}{\|\overrightarrow{T}'\|} = A\gamma'' + B\gamma'$$

avec

$$A := \frac{\|\gamma'\|}{\|\gamma'\wedge\gamma''\|} \quad \text{et} \quad B := -\frac{(\,\gamma'\mid\gamma''\,)}{\|\gamma'\|\cdot\|\gamma'\wedge\gamma''\|}.$$

Par conséquent :

$$\overrightarrow{B} = \overrightarrow{T}\wedge\overrightarrow{N} = \frac{A}{\|\gamma'\|}\gamma'\wedge\gamma''$$

est orthogonal au plan engendré par γ' et γ''. De plus :

$$\overrightarrow{N}' = A'\gamma'' + A\gamma''' + B'\gamma' + B\gamma''.$$

Donc :

$$(\,\overrightarrow{N}'\mid\overrightarrow{B}\,) = \left(A\gamma'''\,\middle|\,\frac{A}{\|\gamma'\|}\gamma'\wedge\gamma''\right) = \frac{\|\gamma'\|\cdot(\,\gamma'\wedge\gamma''\mid\gamma'''\,)}{\|\gamma'\wedge\gamma''\|^2}.$$

Finalement :

$$\tau = -\frac{1}{\|\gamma'\|}(\,\overrightarrow{N}'\mid\overrightarrow{B}\,) = -\frac{(\,\gamma'\wedge\gamma''\mid\gamma'''\,)}{\|\gamma'\wedge\gamma''\|^2}.$$

III.2.14 On va utiliser les résultats de l'exercice précédent. On a :

$$\gamma'(t) = \begin{pmatrix} 1 \\ 2t \\ 3t^2 \end{pmatrix}, \quad \gamma''(t) = \begin{pmatrix} 0 \\ 2 \\ 6t \end{pmatrix} \quad \text{et} \quad \gamma'''(t) = \begin{pmatrix} 0 \\ 0 \\ 6 \end{pmatrix}.$$

Par conséquent :

$$\gamma'\wedge\gamma''(t) = \begin{pmatrix} 6t^2 \\ -6t \\ 2 \end{pmatrix} \quad \text{et} \quad \kappa(t) = \frac{2\sqrt{1+9t^2+9t^4}}{(1+4t^2+9t^4)^{3/2}}.$$

De plus :

$$(\,\gamma'\wedge\gamma''\mid\gamma'''\,) = 12 \quad \text{et} \quad \tau(t) = -\frac{3}{1+9t^2+9t^4}.$$

III.2.15 1. (a) Comme $\overrightarrow{T}$, $\overrightarrow{N}$ et $\overrightarrow{B}$ sont des fonctions dérivables, la fonction G est elle-même dérivable. On a :

$$G' = \begin{pmatrix} 2(\overrightarrow{T} \mid \overrightarrow{T}') \\ (\overrightarrow{T} \mid \overrightarrow{N}') + (\overrightarrow{T}' \mid \overrightarrow{N}) \\ (\overrightarrow{T} \mid \overrightarrow{B}') + (\overrightarrow{T}' \mid \overrightarrow{B}) \\ 2(\overrightarrow{N} \mid \overrightarrow{N}') \\ (\overrightarrow{N} \mid \overrightarrow{B}') + (\overrightarrow{N}' \mid \overrightarrow{B}) \\ 2(\overrightarrow{B} \mid \overrightarrow{B}') \end{pmatrix}.$$

En utilisant :

$$\overrightarrow{T}' = \kappa\overrightarrow{N}, \quad \overrightarrow{N}' = -\kappa\overrightarrow{T} - \tau\overrightarrow{B} \quad \text{et} \quad \overrightarrow{B}' = \tau\overrightarrow{N},$$

on voit que :

$$G' = \begin{pmatrix} 0 & 2\kappa & 0 & 0 & 0 & 0 \\ -\kappa & 0 & -\tau & \kappa & 0 & 0 \\ 0 & \tau & 0 & 0 & \kappa & 0 \\ 0 & -2\kappa & 0 & 0 & -2\tau & 0 \\ 0 & 0 & -\kappa & \tau & 0 & -\tau \\ 0 & 0 & 0 & 0 & 2\tau & 0 \end{pmatrix} \cdot G.$$

(b) Il suffit de vérifier que :

$$\begin{pmatrix} 0 & 2\kappa & 0 & 0 & 0 & 0 \\ -\kappa & 0 & -\tau & \kappa & 0 & 0 \\ 0 & \tau & 0 & 0 & \kappa & 0 \\ 0 & -2\kappa & 0 & 0 & -2\tau & 0 \\ 0 & 0 & -\kappa & \tau & 0 & -\tau \\ 0 & 0 & 0 & 0 & 2\tau & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

(c) La fonction constante égale à $(1,0,0,1,0,1)$ et la fonction $\left(\overrightarrow{T}, \overrightarrow{N}, \overrightarrow{B}\right)$ coïncident en s_0 car (u_0, v_0, w_0) est une base orthonormée. Ce sont deux solutions de la même équation différentielle linéaire à coefficients constants. Puisqu'il y a unicité de la solution maximale qui prend la valeur $(1,0,0,1,0,1)$ au temps s_0, les deux fonctions coïncident. Ainsi, pour tout $s \in J$:

$$\begin{pmatrix} (\overrightarrow{T} \mid \overrightarrow{T}) \\ (\overrightarrow{T} \mid \overrightarrow{N}) \\ (\overrightarrow{T} \mid \overrightarrow{B}) \\ (\overrightarrow{N} \mid \overrightarrow{N}) \\ (\overrightarrow{N} \mid \overrightarrow{B}) \\ (\overrightarrow{B} \mid \overrightarrow{B}) \end{pmatrix}(s) = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}.$$

Pour tout $s \in J$, $\left(\overrightarrow{T}(s), \overrightarrow{N}(s), \overrightarrow{B}(s)\right)$ est une base orthonormée de $\mathbb{R}^3$.

(d) Comme les fonctions $\overrightarrow{T}$, $\overrightarrow{N}$ et $\overrightarrow{B}$ sont continues, le déterminant de la matrice $\begin{pmatrix} \overrightarrow{T} & \overrightarrow{N} & \overrightarrow{B} \end{pmatrix}$ est continu. Comme la base $\left(\overrightarrow{T}(s), \overrightarrow{N}(s), \overrightarrow{B}(s)\right)$ est une base orthonormée pour tout $s \in J$, ce déterminant vaut $+1$ ou -1.

(e) Comme la base $\big(\overrightarrow{T}(s_0), \overrightarrow{N}(s_0), \overrightarrow{B}(s_0)\big)$ est orthonormée directe, le déterminant de la matrice $\begin{pmatrix} \overrightarrow{T} & \overrightarrow{N} & \overrightarrow{B} \end{pmatrix}$ vaut $+1$ en s_0.

(f) La fonction $\det \begin{pmatrix} \overrightarrow{T} & \overrightarrow{N} & \overrightarrow{B} \end{pmatrix}$ est donc constante égale à $+1$. La base $\big(\overrightarrow{T}(s), \overrightarrow{N}(s), \overrightarrow{B}(s)\big)$ est donc orthonormée directe.

(g) Comme la longueur du vecteur $\big(\overrightarrow{T}(s), \overrightarrow{N}(s), \overrightarrow{B}(s)\big)$ est bornée sur J (en fait constante égale à $\sqrt{3}$), la solution maximale est définie sur I, *i.e.* $J = I$. La courbe $\gamma : I \to \mathbb{R}^3$ définie par :

$$\gamma(s) := \gamma_0 + \int_{s_0}^{s} \overrightarrow{T}(t)\,\mathrm{d}t$$

est un paramétrage normal car $\big\|\overrightarrow{T}\big\| = 1$. Comme $\overrightarrow{N}' = -\kappa\overrightarrow{T} - \tau\overrightarrow{B}$ et comme $\overrightarrow{B}' = \tau \cdot \overrightarrow{N}$, les fonctions $\overrightarrow{N}$ et $\overrightarrow{B}$ sont de classe $\mathcal{C}^1$. Comme $\overrightarrow{T}' = \kappa\overrightarrow{N}$, la fonction $\overrightarrow{T}$ est de classe $\mathcal{C}^2$. Sa primitive γ est donc de classe $\mathcal{C}^3$. De plus, comme $\overrightarrow{T}(s) = \gamma'(s)$, comme $\kappa > 0$, comme $\overrightarrow{T}' = \kappa\overrightarrow{N}$ et comme $\big(\overrightarrow{T}, \overrightarrow{N}, \overrightarrow{B}\big)$ est une base orthonormée directe, le repère de Serret-Frenet de γ au temps s est $\big(\gamma(s); \overrightarrow{T}(s), \overrightarrow{N}(s), \overrightarrow{B}(s)\big)$ et la courbure de γ est κ. Enfin, comme $\overrightarrow{B}' = \tau\overrightarrow{N}$, la torsion est τ.

2. (a) Au temps s_0, $\overrightarrow{T}_1 = \overrightarrow{T}_2 = u_0$, $\overrightarrow{N}_1 = \overrightarrow{N}_2 = v_0$ et $\overrightarrow{B}_1 = \overrightarrow{B}_2 = w_0 := u_0 \wedge v_0$. La base (u_0, v_0, w_0) est orthonormée directe, et donc :

$$f(s_0) = (\,u_0 \mid u_0\,) + (\,v_0 \mid v_0\,) + (\,w_0 \mid w_0\,) = 1.$$

De plus :

$$\begin{aligned} f' &= \big(\,\overrightarrow{T}_1' \mid \overrightarrow{T}_2\,\big) + \big(\,\overrightarrow{T}_1 \mid \overrightarrow{T}_2'\,\big) + \big(\,\overrightarrow{N}_1' \mid \overrightarrow{N}_2\,\big) \\ &\quad + \big(\,\overrightarrow{N}_1 \mid \overrightarrow{N}_2'\,\big) + \big(\,\overrightarrow{B}_1' \mid \overrightarrow{B}_2\,\big) + \big(\,\overrightarrow{B}_1 \mid \overrightarrow{B}_2'\,\big) \\ &= \kappa\big(\,\overrightarrow{N}_1 \mid \overrightarrow{T}_2\,\big) + \kappa\big(\,\overrightarrow{T}_1 \mid \overrightarrow{N}_2\,\big) - \kappa\big(\,\overrightarrow{T}_1 \mid \overrightarrow{N}_2\,\big) - \tau\big(\,\overrightarrow{B}_1 \mid \overrightarrow{N}_2\,\big) \\ &\quad - \kappa\big(\,\overrightarrow{N}_1 \mid \overrightarrow{T}_2\,\big) - \tau\big(\,\overrightarrow{N}_1 \mid \overrightarrow{B}_2\,\big) + \tau\big(\,\overrightarrow{N}_1 \mid \overrightarrow{B}_2\,\big) + \tau\big(\,\overrightarrow{B}_1 \mid \overrightarrow{N}_2\,\big) \\ &= 0. \end{aligned}$$

Puisque la dérivée de f est identiquement nulle, la fonction f est constante égale à $f(s_0)$.

(b) Comme tous les vecteurs sont de norme 1, les trois produits scalaires sont inférieurs ou égaux à 1, avec égalité si, et seulement si, $\overrightarrow{T}_1 = \overrightarrow{T}_2$ et $\overrightarrow{N}_1 = \overrightarrow{N}_2$ et $\overrightarrow{B}_1 = \overrightarrow{B}_2$. Comme la somme des trois produits scalaires est égale à 3, ils sont tous trois égaux à 1. Par conséquent, $\overrightarrow{T}_1(s) = \overrightarrow{T}_2(s)$ pour tout $s \in I$ et les courbes γ_1 et γ_2 coïncident.

Module IV.1 : Nombres réels suites numériques

IV.1.1 1. La partie A est non vide et majorée par n'importe quel élément de B (et il en existe puisque B est non vide). Donc A admet une borne supérieure α. Comme tout élément b de B majore A, on a $\alpha \leqslant b$ puisque α est le plus petit des majorants de A. Ainsi α est un minorant de B et un majorant de A, ce qui donne :

$$\forall a \in A\,,\ \forall b \in B\,,\ a \leqslant \alpha \leqslant b.$$

2. Soient K un corps vérifiant cette propriété et A une partie de K non vide majorée. Alors l'ensemble B des majorants de A est non vide et tout élément de B est supérieur ou égal à tout élément de A. Par hypothèse, il existe donc un élément x de K tel que $\forall a \in A\,,\ \forall b \in B\,,\ a \leqslant x \leqslant b$. Donc x est un majorant de A et tout majorant de A, c'est-à-dire tout élément de B, est supérieur ou égal à x. Ainsi, x est le plus petit des majorants de A, c'est-à-dire la borne supérieure de A.
Donc K vérifie la propriété de la borne supérieure.

3. Soit A une partie non vide majorée d'un tel corps K. On peut donc prendre un élément de A, que l'on note a_0 et un majorant de A que l'on note b_0. Supposons construits $a_0 \leqslant a_1 \leqslant \cdots \leqslant a_n$ dans A et $b_0 \geqslant b_1 \geqslant \cdots \geqslant b_n$ des majorants de A. Considérons $x := (a_n + b_n)/2$.
   - Si x est un majorant de A, on pose $a_{n+1} := a_n$ et $b_{n+1} := x$.
   - Sinon, il existe un élément de A supérieur à x ; notons-le a_{n+1}.
     Alors $b_{n+1} := a_{n+1} + (b_n - a_n)/2 \geqslant x + (b_n - a_n)/2 = b_n$, donc b_{n+1} est un majorant de A.

   Dans les deux cas, on a construit a_{n+1} dans A et b_{n+1} majorant de A tels que $a_n \leqslant a_{n+1} \leqslant b_{n+1} \leqslant a_n$ et $b_{n+1} - a_{n+1} = (b_n - a_n)/2$.
   Par hypothèse sur K, il existe $c \in K$ tel que $\forall n \in \mathbb{N}\,,\ a_n \leqslant c \leqslant b_n$. Montrons que c est la borne supérieure de A.
   Tout d'abord, puisque K est archimédien, pour tout $\varepsilon > 0$ dans $\mathbb{K}$, il existe un entier n tel que $b_n - a_n = (b_0 - a_0)/2^n \leqslant \varepsilon$.
   - Soit $x < c$. Prenons n tel que $b_n - a_n \leqslant (c-x)/2$. Alors $c - a_n \leqslant b_n - a_n < c - x$, donc $a_n > x$. Cela prouve que x n'est pas un majorant de A. Comme K est totalement ordonné, on en déduit que tous les majorants de A sont supérieurs ou égaux à c.
   - Soit $x > c$. Prenons n tel que $b_n - a_n \leqslant (x-c)/2$. Alors $b_n - c \leqslant b_n - a_n < x - c$, donc $b_n < x$. Cela prouve que x n'est pas dans A et donc, de la même façon que précédemment, que tout élément de A est inférieur ou égal à c.

   Ainsi, c est bien le plus petit des majorants de A et K vérifie la propriété de la borne supérieure.

IV.1.2 1. On suppose que $\sqrt{p} + \sqrt{q} = a/b$, avec $a, b \in \mathbb{N}^*$. On en déduit $\sqrt{q} = \frac{a}{b} - \sqrt{p}$, puis $q = \frac{a^2}{b^2} - 2\frac{a}{b}\sqrt{p} + p$ et $\sqrt{p} = \frac{a}{2b} + (p-q)\frac{b}{2a} \in \mathbb{Q}$, d'où une contradiction.

2. Notons $a := \sqrt{2} + \sqrt{3} + \sqrt{5}$. On a $(a - \sqrt{2})^2 = (\sqrt{3} + \sqrt{5})^2 = 8 + 2\sqrt{15}$, puis $a^2 - 2\sqrt{2}a - 6 = 2\sqrt{15}$ et $(a^2 - 2\sqrt{2}a - 6)^2 = 60$. On en déduit :

$$a^4 - 4a^2 - 24 = 4\sqrt{2}a(a^2 - 6).$$

On raisonne par l'absurde. On suppose a rationnel. Alors $a^2 - 6 = 0$, sinon $\sqrt{2}$ serait rationnel. On en déduit $-12 = 0$, donc une contradiction.

3. On suppose $\sqrt[m]{n} = p/q$, avec $p \in \mathbb{N}$ et $q \in \mathbb{N}^*$ premiers entre eux. Alors $p^m = nq^m$, donc n divise p : $p = np'$ et $n^{m-1}p'^m = q^m$. Oa a $m-1 \geqslant 1$, donc n divise q et l'on a une contradiction.

IV.1.3 Soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ la décomposition en facteurs premiers de n (unique à l'ordre près). Si les entiers $\alpha_1, \alpha_2, \dots, \alpha_m$ sont *tous pairs*, $\sqrt{n} = p_1^{\alpha_1/2} p_2^{\alpha_2} \dots p_m^{\alpha_m/2}$ est entier. Sinon, il existe *au moins un* α_i *impair*. Nous allons montrer *qu'alors* $\sqrt{n}$ *est irrationnel*.

On a $\sqrt{p^{2\gamma+1}} = p^\gamma \sqrt{p}$, on en déduit qu'il suffit de traiter le cas où la décomposition en facteurs premiers de n est de la forme $n = p_1 p_2 \dots p_k$.

On raisonne par l'absurde en supposant que $n = a/b$, où a et b sont des entiers strictement positifs premiers entre eux. On a $b^2 p_1 p_2 \dots p_k = a^2$. Soit p un diviseur premier de a. Il ne divise pas b, c'est donc l'un des p_i ($\text{ß} \in [\![1, k]\!]$). Supposons par exemple que $p = p_1$. On écrit $a = pa'$, d'où $b^2 p_2 \dots p_k = pa'^2$. Ainsi p divise $b^2 p_2 \dots p_k$, ce qui est impossible (il ne divise pas b, ni les $p_2, \dots, p_k$).

Inversement, il résulte immédiatement de ce qui précède que si $\sqrt{n}$ est irrationnel, il existe au moins un α_i impair.

IV.1.4 Supposons que $\ln 3/\ln 2 = a/b$, avec a et b entiers strictement positifs.

Alors $b \ln 3 = a \ln 2$, relation équivalente à $3^b = 2^a$. Cette dernière égalité est impossible : elle entraînerait que 2 divise 3.

IV.1.5 1. On note $\tau := e^{2i\pi/5}$. On a, en utilisant $\tau^5 = 1$ et $\tau \neq 1$: $\tau + \tau^2 + \tau^3 + \tau^4 = -1$. En utilisant les formules d'Euler, on obtient :

$$\cos\frac{2\pi}{5} = \frac{\tau + \tau^{-1}}{2} = \frac{\tau + \tau^4}{2} \quad \text{et} \quad \cos\frac{4\pi}{5} = \frac{\tau^2 + \tau^{-2}}{2} = \frac{\tau^2 + \tau^4}{2}$$

$$\cos\frac{2\pi}{5} + \cos\frac{4\pi}{5} = \frac{1}{2}(\tau + \tau^4 + \tau^2 + \tau^3) = -\frac{1}{2}$$

$$\cos\frac{2\pi}{5}\cos\frac{4\pi}{5} = \frac{1}{4}(\tau^3 + \tau^4 + \tau + \tau^2) = -\frac{1}{4}.$$

Par suite $\cos 2\pi/5$ est une racine de l'équation du second degré $4X^2 + 2X - 1 = 0$ et, puisque $\cos 2\pi/5 > 0$, on a $\cos 2\pi/5 = \frac{\sqrt{5}-1}{4}$ (la moitié de l'inverse du nombre d'or). Le réel $\sqrt{5}$ est irrationnel, donc $\cos 2\pi/5$ l'est aussi.

Variante. Posons $a := \cos\frac{2\pi}{5}$. On a $\cos\frac{4\pi}{5} = 2a^2 - 1$.

À partir de $-1/2 = \cos\frac{2\pi}{5} + \cos\frac{4\pi}{5} = a + 2a^2 - 1$, on obtient $4a^2 + 2a - 1 = 0$.

2. Nous allons montrer que $\cos 2\pi/7$, $\cos 4\pi/7$ et $\cos 6\pi/7$ sont solutions d'une équation du troisième degré à coefficients entiers en calculant leurs fonctions symétriques élémentaires. On note $\omega := e^{2i\pi/7}$. On a $\omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6 = -1$. En utilisant les formules d'Euler, on obtient

$$\cos\frac{2\pi}{7} + \cos\frac{4\pi}{7} + \cos\frac{6\pi}{7} = \frac{1}{2}(\omega + \omega^6 + \omega^2 + \omega^5 + \omega^3 + \omega^4) = -1/2,$$

$$\cos\frac{2\pi}{7}\cos\frac{4\pi}{7}+\cos\frac{2\pi}{7}\cos\frac{6\pi}{7}+\cos\frac{4\pi}{7}\cos\frac{6\pi}{7}$$
$$=\frac{1}{4}\left((\omega^3+\omega^6+\omega+\omega^4)+(\omega^4+\omega^5+\omega^2+\omega^3)+(\omega^5+\omega^6+\omega+\omega^2)\right)$$
$$=\frac{2}{4}(\omega+\omega^2+\omega^3+\omega^4+\omega^5+\omega^6)=-\frac{1}{2},$$

$$\cos\frac{2\pi}{7}\cos\frac{4\pi}{7}\cos\frac{6\pi}{7}=\frac{1}{8}(\omega+\omega^6)(\omega^2+\omega^5)(\omega^3+\omega^4)$$
$$=\frac{1}{8}(\omega^6+1+\omega^2+\omega^3+\omega^4+\omega^5+1+\omega)=\frac{1}{8}(2-1)=\frac{1}{8}\cdot$$

Ainsi $\cos 2\pi/7$, $\cos 4\pi/7$ et $\cos 6\pi/7$ sont solutions de $X^3+\frac{1}{2}X^2-\frac{1}{2}X-\frac{1}{8}=0$, ou de façon équivalente de $8X^3+4X^2-4X-1=0$. Posons $2X=Y$. On a $8X^3+4X^2-4X-1=Y^3+Y^2-2Y-1$ et $2\cos 2\pi/7$ est solution de $Y^3+Y^2-2Y-1=0$.

Variante. Posons $a:=\cos\frac{2\pi}{7}\cdot$ On a $\cos\frac{4\pi}{7}=2a^2-1$ et $\cos\frac{6\pi}{7}=4a^3-3a$.

À partir de $-1/2=\cos\frac{2\pi}{7}+\cos\frac{4\pi}{7}+\cos\frac{6\pi}{7}=a+2a^2-1+4a^3-3a$, on obtient $8a^3+4a^2-4a-1=0$.

Montrons que $Y^3+Y^2-2Y-1=0$ n'admet pas de solution rationnelle. On raisonne par l'absurde. Supposons qu'il existe $p\in\mathbb{Z}$ et $q\in\mathbb{N}^*$ *premiers entre eux* tels que p/q soit solution de $Y^3+Y^2-2Y-1=0$. On a $\frac{p^3}{q^3}+\frac{p^2}{q^2}-2\frac{p}{q}-1=0$, donc $p^3=q(-p^2+2pq+q^2)$. Par suite q divise p^3 et, puisqu'il est premier avec p, on a nécessairement $q=1$ et $p/q=p$. Donc $2\cos 2\pi/7$ est entier. Puisque $0<2\cos 2\pi/7<2$, la seule valeur possible est $2\cos 2\pi/7=1$. Mais 1 n'est pas racine de $Y^3+Y^2-2Y-1=0$. On aboutit donc à une contradiction. Par suite $2\cos 2\pi/7\notin\mathbb{Q}$ et $\cos 2\pi/7\notin\mathbb{Q}$.

IV.1.6 1. Notons $K:=\{a+b\sqrt{2}\in\mathbb{Q}\mid a,b\in\mathbb{Q}\}$. On vérifie facilement que c'est un sous-anneau de $\mathbb{R}$. On a $(a+b\sqrt{2})(a-b\sqrt{2})=a^2-2b^2$ et $a^2-2b^2=0$ si, et seulement si, $(a,b)=(0,0)$ (car $\sqrt{2}\notin\mathbb{Q}$). Par suite, si $(a,b)\neq(0,0)$, $a+b\sqrt{2}$ est inversible dans $\mathbb{R}$ et son inverse est $\frac{1}{a^2-2b^2}(a-b\sqrt{2})\in\mathbb{K}$. Donc $a+b\sqrt{2}$ est inversible dans K et K est un sous-corps de $\mathbb{R}$; muni de la relation d'ordre induite par celle de $\mathbb{R}$ c'est un corps totalement ordonné. On a $\sqrt{2}\notin\mathbb{Q}$, donc $K\neq\mathbb{Q}$. Par ailleurs K est dénombrable et $\mathbb{R}$ ne l'est pas, donc $K\neq\mathbb{R}$.

2. Soit L un corps tel que $\mathbb{R}\subset L\subset\mathbb{C}$, l'inclusion $\mathbb{R}\subset L$ étant *stricte*. Il existe $a,b\in\mathbb{R}$, avec $b\neq 0$, tels que $a+bi\in L$. On en déduit que $i\in L$.

Supposons qu'il existe une structure de corps totalement ordonné sur L.

On a $-1=i^2\geqslant 0$ et $1>0$, donc $0=-1+1>0$ et une contradiction.

IV.1.7 Si $x\in\mathbb{R}$ est positif, il existe $y\in\mathbb{R}$ tel que $y^2=x$. On a $f(x)=f(y^2)=f(y)^2\geqslant 0$. Ainsi $f(\mathbb{R}_+)\subset\mathbb{R}_+$.

Si $x\leqslant x'$, $x'-x\geqslant 0$, donc $f(x')-f(x)=f(x'-x)\geqslant 0$ et $f(x)\leqslant f(x')$. Par suite f est *croissante*.

On a $f(1) = 1$, donc, pour tout $n \in \mathbb{N}^*$, $f(n) = f(1) + \cdots + f(1) = n$. On a $f(0) = 0$ et $0 = f(n-n) = f(n) + f(-n) = n + f(-n)$, donc $f(-n) = -n$. Ainsi f induit l'identité sur $\mathbb{Z}$. On a, pour tout $q \in \mathbb{N}^*$, $1 = f(qq^{-1}) = f(q)f(q^{-1}) = qf(q^{-1})$, donc $f(q^{-1}) = q^{-1}$. Pour tout $p \in \mathbb{N}$, on a $f(pq^{-1}) = f(p)f(q^{-1}) = pq^{-1}$. Ainsi f induit l'identité sur $\mathbb{Q}$.

Soit $\alpha \in \mathbb{R}$. En utilisant la remarque de la page 518, on a, en notant $A_\alpha := \{r \in \mathbb{Q} \mid r < \alpha\}$, $\sup A_\alpha = \alpha$. Puisque $A_\alpha \subset \mathbb{Q}$, on a $f(A_\alpha) = A_\alpha$.

Puisque f est croissante, $f(\alpha)$ est un majorant de A_α. Montrons que c'est le plus petit. Sinon, il existerait un majorant β de A_α tel que $\beta < \alpha$ et, par suite un rationnel r tel que $\beta < r < \alpha$. On aurait $r \in A_\alpha$ et une contradiction. Ainsi $f(\alpha)$ est la borne supérieure de A_α et $f(\alpha) = \alpha$. Donc $K = \mathbb{R}$ et f est l'identité.

Soient $g_1, g_2 : \mathbb{R} \to L$ deux isomorphismes du corps K sur le corps L. Alors $g_1^{-1} : L \to \mathbb{R}$ est un isomorphisme de corps et $g_1^{-1} \circ g_2$ est un automorphisme du corps $\mathbb{R}$. Donc $g_1^{-1} \circ g_2$ est l'identité et $g_1 = g_2$.

IV.1.8 Le lecteur pourra se persuader des encadrements ci-dessous en considérant le pavé rectangulaire décrit par le couple (x, y) et les différentes courbes de niveau définies par les expressions $x \pm y$, xy et x/y.

1. On a $-1 \leqslant x + y \leqslant 4$, les bornes étant atteintes pour $(3, -4)$ et $(6, -2)$.
2. On a $5 \leqslant x - y \leqslant 10$, les bornes étant atteintes pour $(3, -2)$ et $(6, -4)$.
3. Comme $x \geqslant 0$ et $-y \geqslant 0$, on peut multiplier les inégalités $3 \leqslant x \leqslant 6$ et $2 \leqslant -y \leqslant 4$ terme à terme, ce qui donne $6 \leqslant x(-y) \leqslant 24$ et donc $-24 \leqslant xy \leqslant -6$, les bornes étant atteintes pour $(6, -4)$ et $(3, -2)$.
4. On peut commencer par encadrer $-\frac{1}{y}$: $\frac{1}{4} \leqslant -\frac{1}{y} \leqslant \frac{1}{2}$ et de la même façon que ci-dessus, on obtient $-3 = -\frac{6}{2} \leqslant \frac{x}{y} \leqslant -\frac{3}{4}$.

IV.1.9 1. On a :

$$\sqrt{n+1} - \sqrt{n} = \frac{(\sqrt{n+1} - \sqrt{n})(\sqrt{n+1} + \sqrt{n})}{\sqrt{n+1} + \sqrt{n}} = \frac{1}{\sqrt{n+1} + \sqrt{n}} < \frac{1}{2\sqrt{n}}$$

et

$$\sqrt{n} - \sqrt{n-1} = \frac{(\sqrt{n} - \sqrt{n-1})(\sqrt{n} + \sqrt{n-1})}{\sqrt{n} + \sqrt{n-1}} = \frac{1}{\sqrt{n} + \sqrt{n-1}} > \frac{1}{2\sqrt{n}}.$$

2. En additionnant les doubles inégalités de la question 1 pour n variant de 1 à 10000, on obtient :

$$\sum_{n=1}^{10000} \left(\sqrt{n+1} - \sqrt{n}\right) < \sum_{n=1}^{10000} \frac{1}{2\sqrt{n}} < \sum_{n=1}^{10000} \left(\sqrt{n} - \sqrt{n-1}\right),$$

c'est-à-dire $\sqrt{10001} - 1 < a < \sqrt{10000}$, d'où $99 < a < 100$. Par suite la partie entière de a est 99.

IV.1.10 1. On vérifie que A est un sous-anneau de $\mathbb{R}$. On en déduit $\alpha^n \in A$.

2. On a $1 < \sqrt{2} < 3/2$, donc $0 < \alpha < 1/2$. On montre par récurrence que, pour tout $n \in \mathbb{N}^*$, $2^n > n$. Par suite $\alpha < 1/n$.

   Pour tous $x, y \in \mathbb{R}$ tels que $0 < x < y$, il existe $n \in \mathbb{N}^*$ tel que $1/n < y - x$ et l'on a $\alpha^n < y - x$.

3. On peut supposer $0 \leqslant x$. (Si $x < 0$, on s'y ramène en considérant $0 \leqslant \min(-y, 0) < -x$.) D'après la question précédente, il existe $n \in \mathbb{N}^*$ tel que $0 < \alpha^n < y - x$. D'après la propriété d'Archimède, il existe $m \in \mathbb{N}^*$ tel que $x < m\alpha^n$. On peut supposer m minimal et l'on a alors $(m-1)\alpha^n \leqslant x < m\alpha^n$. Posons $a := m\alpha^n$. On a $a \in A$ et, en utilisant 2, $a = (m-1)\alpha^n + \alpha^n < x + y - x = y$, donc $x < a < y$.

IV.1.11 1. Si $G = \{0\}$, alors $G = a\,\mathbb{Z}$ avec $a := 0$.

2. Comme on suppose $G \neq \{0\}$, il existe un élément $x \in G$ non nul et alors $-x$ est aussi dans G. Ainsi, $|x| \in G$ et $|x| > 0$. L'ensemble $A := \{x \in G \mid x > 0\}$ est donc une partie non vide de $\mathbb{R}$ minorée par 0, ce qui donne l'existence de $a := \inf A \geqslant 0$.

3. a) Puisque $a > 0$, on a $2a > a$. D'après la proposition 3 de la page 513, il existe donc $x \in A$ tel que $a \leqslant x < 2a$.

   Montrons que $x = a$. On raisonne par l'absurde. Supposons $a < x$. Alors, il existe $y \in A$ tel que $a \leqslant y < x$ et l'on a $0 < x - y < 2a - a = a$ et $x - y \in A$. On aboutit à une contradiction.

   b) Supposons toujours $a > 0$. Alors $a \in G$ d'après la question précédente. Comme G est un groupe, $a\,\mathbb{Z} \subset G$ ($a\,\mathbb{Z}$ est le sous-groupe de $\mathbb{R}$ engendré par a d'après la proposition 16 de la page 122).

   Inversement, soit $x \in G$. Posons $n := E(x/a)$. D'après la définition de la partie entière, on a $0 \leqslant x - n\,a < a$. Or, $x - n\,a \in G$ puisque x et $n\,a$ sont dans G. Par définition de a on ne peut pas avoir $0 < x - n\,a < a$, donc $x = n\,a \in a\,\mathbb{Z}$.

   Finalement, $G = a\,\mathbb{Z}$.

4. Supposons $a = 0$ et montrons que G est dense dans $\mathbb{R}$. Soient x et y dans $\mathbb{R}$ tels que $x < y$. Comme $\inf A = 0 < y - x$, il existe $z \in A$ tel que $z < y - x$. Prenons alors le plus grand multiple de z strictement inférieur à y, c'est-à-dire $n\,z$ avec $n := E(y/z) - 1$. Comme n est le plus grand, on a $(n+1)\,z \geqslant y$, ce qui donne $n\,z \geqslant y - z > y - (y - x) = x$ et donc $n\,z$ est un élément de A strictement compris entre x et y.

   Donc A est dense dans $\mathbb{R}$.

IV.1.12 1. On a évidemment $0 \in B$ ($k := 0$). Soient $b_1 := \dfrac{k_1\pi}{3.2^{n_1}}$ et $b_2 := \dfrac{k_2\pi}{3.2^{n_2}}$, avec $k_1, k_2 \in \mathbb{Z}$ et $n_1, n_2 \in \mathbb{N}$. On peut supposer $n_2 \geqslant n_1$, on a alors :

$$b_1 - b_2 = \frac{k_1\pi}{3.2^{n_1}} - \frac{k_2\pi}{3.2^{n_2}} = \frac{(2^{n_2-n_1}k_1 - k_2)\pi}{3.2^{n_2}} = \frac{k\pi}{3.2^n},$$

avec $k := 2^{n_2-n_1}k_1 - k_2 \in \mathbb{Z}$ et $n := n_2$. Par suite $b_1 - b_2 \in A$. Ainsi B est un sous-groupe de $\mathbb{R}$.

On choisit $k := 1$ et $n \in \mathbb{N}$. On obtient ainsi une suite (x_n) d'éléments de B, en posant $x_n := \frac{\pi}{3.2^n}$. Les x_n sont strictement positifs et la suite (x_n) tend vers 0. On

pose $A := B \cap]0, +\infty[$. La borne inférieure de A est 0. En utilisant l'exercice IV.1.11, on en déduit que B est dense dans $\mathbb{R}$.

L'ensemble B est dénombrable. Montrons que $\mathbb{R} \setminus B$ est dense dans $\mathbb{R}$. On raisonne par l'absurde. On suppose que $\mathbb{R} \setminus B$ n'est pas dense dans R. Il existe donc $a, b \in \mathbb{R}$, $a < b$ tels que $]a, b[\cap (\mathbb{R} \setminus B) = \varnothing$. Alors $]a, b[\subset B$. Mais $]a, b[$n'est pas dénombrable et a fortiori B ne l'est pas non plus. On aboutit à une contradiction. Ainsi $\mathbb{R} \setminus B$ est dense dans $\mathbb{R}$

2. L'application f est continue. On vérifie qu'elle est surjective. On en déduit que $f(B)$ et $f(\mathbb{R} \setminus B)$ sont denses dans $[0, 1]$ en utilisant la proposition 35 de la page 545.

IV.1.13 Il suffit de résoudre la seconde question. Si $\varepsilon \geqslant 1$, il est clair que $n \geqslant 2$ suffit, puisqu'alors $2n^2 - 3n - 1 > 0$. Soit donc $0 < \varepsilon < 1$. Dans ce cas $n > 3/\varepsilon$ suffit, puisqu'alors $3n > \varepsilon$ d'où :

$$2n^2 - 1 > \frac{6n}{\varepsilon} - 1 > \frac{3n}{\varepsilon}.$$

IV.1.14 On suppose $n \in \mathbb{N}^*$. La stricte croissance de la suite découle, au choix, des relations :

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{x^2-2}{x^2+x}\right) = \frac{x^2+4x+2}{(x^2+x)^2} > 0, \quad \frac{n^2+2n-1}{(n+1)(n+2)} - \frac{n^2-2}{n(n+1)} = \frac{n+4}{n(n+1)(n+2)} > 0.$$

La limite est 1 puisque :

$$1 - \frac{n^2-2}{n^2+n} = \frac{n+2}{n^2+n} = \frac{\frac{1}{n} + \frac{2}{n^2}}{1+\frac{1}{n}} \to 0.$$

IV.1.15 La décroissance large de la suite découle de la relation :

$$\frac{2+(-1)^n}{3^n} - \frac{2-(-1)^n}{3^{n+1}} = \frac{4(1+(-1)^n)}{3^{n+1}} \geqslant 0.$$

La limite est 0 car $|u_n| \leqslant \frac{3}{3^n} \underset{n\to+\infty}{\longrightarrow} 0$.

IV.1.16 On a aussitôt, par identification, les égalités :

$$u_n = \frac{2}{9n^2+15n+4} = \frac{2/3}{3n+1} - \frac{2/3}{3n+4}.$$

Par suite, $S_n = \dfrac{2}{3} - \dfrac{2/3}{3n+4}$ par télescopage. La limite de S_n est clairement $2/3$.

IV.1.17 Les limites respectives sont :

1. 0, car $|\sin n| \leqslant 1$.
2. $1/2$, car $\dfrac{n^3+2n-1}{2n^3-3n+2} = \dfrac{1+\frac{2}{n^3}-\frac{1}{n^3}}{2-\frac{3}{n^2}+\frac{2}{n^3}}$.

3. 0, car $\dfrac{n!}{n^n} = \displaystyle\prod_{k=1}^{n} \frac{k}{n} \leqslant \frac{1}{n}$.

4. 0, car $\sqrt{n+1} - \sqrt{n} = \dfrac{1}{\sqrt{n+1} + \sqrt{n}} \leqslant \dfrac{1}{2\sqrt{n}}$.

5. 1, car $\dfrac{n - (-1)^n}{n + (-1)^n} = \dfrac{1 - (-1)^n/n}{1 + (-1)^n/n}$.

6. 1, par application du lemme des gendarmes, puisque :

$$\frac{1}{1+\frac{1}{n}} = \frac{n^2}{n^2+n} \leqslant \sum_{k=1}^{n} \frac{n}{n^2+k} \leqslant \frac{n^2}{n^2+1} = \frac{1}{1+\frac{1}{n^2}}.$$

7. Il n'y a pas de limite si $b = -a$ puisqu'alors la suite n'est pas définie pour $n = 1$; il y a une limite évidemment nulle si $b = a$.
   Si $|b| < |a|$, la limite est 1, car $a \neq 0$ et $\dfrac{a^n - b^n}{a^n + b^n} = \dfrac{1 - (b/a)^n}{1 + (b/a)^n}$.
   Si $|b| > |a|$, la limite est -1 pour une raison analogue.

IV.1.18 1. On raisonne par l'absurde. On suppose que la suite (u_n) converge vers ℓ. On a : $\sin a - \sin b = 2\sin\frac{a-b}{2}\cos\frac{a+b}{2}$. Pour $a := n+1$ et $b := n-1$, on obtient $u_{n+1} - u_{n-1} = 2\sin 1 \cos n$. On a : $\lim\limits_{n\to+\infty}(u_{n+1} - u_{n-1}) = 0$, donc, puisque $\sin 1 \neq 0$, $\lim\limits_{n\to+\infty} \cos n = 0$. On en déduit $\lim\limits_{n\to+\infty} \cos 2n = 0$. Mais $\cos 2n = 2\cos^2 n - 1$, donc $0 = \lim\limits_{n\to+\infty} \cos 2n = 2 \lim\limits_{n\to+\infty} \cos^2 n - 1 = -1$, ce qui est absurde.

Remarque. On peut montrer que l'image de la suite (u_n) est dense dans $[-1, 1]$, mais c'est plus difficile… (*cf.* l'exercice IV.1.51).

2. On suppose $n \in \mathbb{N}^*$. Pour tout $k \in \mathbb{N}$, $k \geqslant 2$, on note $x_k := \mathrm{e}^{\frac{\pi}{2}+2k\pi}$ et $n_k := E(x_k) + 1$. On a $\sin(\ln x_k) = \sin(\pi/2 + 2k\pi) = 1$, donc la suite $(\sin(\ln x_k))$ tend vers 1. Montrons que la suite $(\sin(\ln n_k))$ tend aussi vers 1.
   On a $n_k > x_k$. D'après l'inégalité des accroissements finis, pour les fonctions sin et ln, on a :

$$|\sin(\ln n_k) - \sin(\ln x_k)| \leqslant |\ln n_k - \ln x_k| \leqslant \frac{n_k - x_k}{x_k} \leqslant e^{-\pi/2} e^{-2k\pi} < e^{-2k\pi}.$$

   On a $\lim\limits_{k\to+\infty} e^{-2k\pi} = 0$, donc $\lim\limits_{k\to+\infty} \sin(\ln n_k) = \lim\limits_{k\to+\infty} \sin(\ln x_k) = 1$. On vérifie par ailleurs que la suite (n_k) est strictement croissante. Ainsi $(\sin(\ln n_k))$ est une suite extraite de (v_n) qui converge vers 1. On construit de même une suite extraite qui converge vers -1 en utilisant $y_k := \mathrm{e}^{-\frac{\pi}{2}+2k\pi}$ et $m_k := E(y_k) + 1$. On en déduit la divergence de (v_n).

IV.1.19 On définit u par $u_n = 1$ si n est un nombre premier et $u_n = 0$ sinon. Cette suite est évidemment divergente. Si $k \geqslant 2$ et $n \in \mathbb{N}$, kn n'est pas premier, donc $u_{kn} = 0$.

IV.1.20 1. Il existe des suites convergentes non monotones (ex : $u_n := (-1)^n/n$).

2. Il existe des suites divergentes non monotones (ex : $u_n := (-1)^n$).
3. Il existe des suites divergentes bornées (même exemple).
4. Toute suite décroissante non minorée diverge vers $-\infty$ puisqu'aucun réel a n'en étant minorant, il existe un N tel que $u_N < a$, puis $u_n < a$ pour tout $n \geqslant N$.

IV.1.21 1. Toute suite dont les valeurs absolues tendent vers 0 tend vers 0.

2. La suite définie par $u_n = (-1)^n$ diverge, mais $|u_n|$ tend vers 1.
3. Toute suite convergeant vers ℓ est telle que sa valeur absolue converge vers $|\ell|$.
4. Il existe des suites à valeurs strictement positives qui convergent vers 0 (ex : $u_n := 1/n$).
5. Il existe des suites (u_n) telles qu'il existe une suite (v_n) convergeant vers 0 telle que $u_n v_n$ ne tende pas vers 0 (ex : $u_n := n^2$, $v_n = 1/n$).

IV.1.22 Soit q la raison cherchée, telle que $u_n = 90\,q^n$. La somme $\displaystyle\sum_{k=0}^{n} u_k$ ne converge que si, et seulement si, $|q| < 1$, et alors sa limite est $\dfrac{u_0}{1-q}\cdot$ Par suite, $q = 1 - \dfrac{90}{150} = \dfrac{2}{5}$ qui est bien strictement inférieur à 1 en module.

IV.1.23 On a $v_0 = -\ln 2$ et $v_{n+1} = \ln(u_{n+1}) - \ln 2 = \dfrac{v_n}{2}\cdot$

La suite (v_n) est donc géométrique, de premier terme $v_0 = -\ln 2$ et de raison $q = 1/2$. Par suite $v_n \to 0$, et $u_n = 2e^{v_n} \to 2$.

IV.1.24 1. En développant $(i-1)^3$ par la formule classique, on obtient :

$$i^3 - (i-1)^3 = 3i^2 - 3i + 1.$$

On a une *somme télescopique* :

$$\sum_{i=1}^{n} \left(i^3 - (i-1)^3\right) = n^3 - (n-1)^3 + (n-1)^3 - (n-2)^3 + \cdots + 1^3 - 0^3 = n^3.$$

D'où, en sommant, pour i de 1 à n, chacun des membres de l'égalité $i^3 - (i-1)^3 = 3i^2 - 3i + 1$: $n^3 = 3S_2(n) - 3S_1(n) + S_0(n)$. On en déduit $S_2(n) = \frac{1}{3}n^3 + S_1(n) - \frac{1}{3}S_0(n)$. On a évidemment $S_0(n) = 1$ et on sait que $S_1(n) = \frac{1}{2}n(n+1)$. Donc $S_2(n) = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n = \frac{n(n+1)(2n+1)}{6}$.

2. Pour tout $k \in \mathbb{N}$ et tout $i \in \mathbb{N}^*$, en utilisant la formule du binôme pour développer $(i-1)^k$, on obtient :

$$i^{k+1} - (i-1)^{k+1} = \binom{k+1}{1} i^k - \binom{k+1}{2} i^{k-1} + \cdots + (-1)^k \qquad (39)$$

On a une *somme télescopique* :

$$\sum_{i=1}^{n}\left(i^{k+1}-(i-1)^{k+1}\right)=n^{k+1}-(n-1)^{k+1}+(n-1)^{k+1}-(n-2)^{k+1}+\cdots$$
$$\cdots+2^{k+1}-1^{k+1}+1^{k+1}-0^{k+1}$$
$$=n^{k+1}.$$

D'où, en sommant, pour i de 1 à n, chacun des membres de l'égalité (39) :

$$n^{k+1}=\binom{k+1}{1}S_k(n)-\binom{k+1}{2}S_{k-1}(n)+\cdots+(-1)^kS_0(n).$$

On en déduit (14).

3. La formule (14) permet de calculer $S_k(n)$ par récurrence sous forme de polynôme de degré $k+1$ en n en utilisant $S_0(n)=n$[1]. Si, pour $k\in\mathbb{N}$ fixé, $P,Q\in\mathbb{Q}[X]$ vérifient $P(n)=Q(n)=S_k(n)$, pour tout $n\in\mathbb{N}^*$, le polynôme $P-Q$ a une infinité de racines donc $P-Q=0$. On a donc l'unicité.
Pour $k=3$ on obtient :
$$4S_3(n)=n^4+6(n^3/3+n^2/2+n/6))-4(n^2/2+n/2)+n=n^4+2n^3+n^2,$$
d'où l'on déduit[2] : $S_3(n)=\frac{1}{4}(n^4+2n^3+n^2)=\left(\frac{n(n+1)}{2}\right)^2=S_1^2(n)$.
Pour $k=4$, on obtient :
$$5S_4(n)=n^5+10(n^4/4+n^3/2+n^2/4)-10(n^3/3+n^2/2+n/6))+5(n^2/2+n/2)-n$$
$$=n^5+\frac{5}{2}n^4+\frac{5}{3}n^3-\frac{1}{6}n=\frac{n}{6}(n^4+15n^3+10n^2-n),$$
d'où l'on déduit $S_4(n)=\frac{n}{30}(6n^4+15n^3+10n^2-n)$.

IV.1.25 1. Soit $r\in\mathbb{N}^*$. On a $\Delta(x^r)=x^r-(x-1)^r=\sum_{i=1}^{r}(-1)^{i+1}\binom{r}{i}x^{r-i}$ et $\binom{r}{1}=r\neq 0$, donc $\deg\Delta(x^r)=r-1$.
L'application Δ est évidemment linéaire et, d'après $\deg\Delta(x^r)=r-1$, on a, pour tout $P\in\mathbb{Q}[X]$, $P\neq 0$: $\deg\Delta(P)<\deg(P)$. On en déduit que, pour tout $r>0$, l'image $\Delta\left(\mathbb{Q}[X]_r\right)$ de $\mathbb{Q}[X]_r$ par Δ est contenue dans $\mathbb{Q}[X]_{r-1}$.
Supposons $P\neq 0$ et $\deg P=r>0$. On a $P=a_rx^r+Q$, avec $a_r\neq 0$ et $\deg Q<r$. Alors $\Delta(P)=a_r\Delta(x^r)+\Delta(Q)$ et $\deg\Delta(Q)<r-1$, donc $\deg\Delta(P)=r-1$. Si P est constant, c'est-à-dire $P\in\mathbb{Q}$, $\Delta(P)=0$ et, d'après ce qui précède, si $P\notin\mathbb{Q}$, $\Delta(P)\neq 0$, donc $\operatorname{Ker}\Delta=\mathbb{Q}$. Notons, pour tout $r\in\mathbb{N}^*$, Δ_r la restriction de Δ au sous-espace vectoriel $\mathbb{Q}[X]_r$ de $\mathbb{Q}[X]$. On a $\operatorname{Ker}\Delta_r=\mathbb{Q}$ et $\dim\mathbb{Q}[X]_r=r+1$, donc, d'après le théorème du rang, $\dim\Delta\left(\mathbb{Q}[X]_r\right)=\dim\Delta_r\left(\mathbb{Q}[X]_r\right)=r$.
Puisque $\Delta\left(\mathbb{Q}[X]_r\right)\subset\mathbb{Q}[X]_{r-1}$ et $\dim\mathbb{Q}[X]_{r-1}=r$, on a $\Delta\left(\mathbb{Q}[X]_r\right)=\mathbb{Q}[X]_{r-1}$.

[1] L'idée d'une formule polynomiale en n pour $S_k(n)$ est dûe à Johann Faulhaber dans son *Academia Algebrae* publiée en 1631. Il donne les calculs pour $k\in[\![0,23]\!]$.
[2] Cette formule a été obtenue au XI$^{\text{e}}$ siécle par le mathématicien persan al-Karaji.

Soient $k \in \mathbb{N}$ et $Q \in \mathbb{Q}[X]$, $Q \neq 0$, de degré k. On a $Q \in \mathbb{Q}[X]_k$ et, d'après ce qui précède, il existe $R \in \mathbb{Q}[X]_{k+1} \subset \mathbb{Q}[X]$ tel que $\Delta(R) = Q$. Si l'on pose $P := R - R(0)$, on a $\Delta(P) = Q$ et $P(0) = 0$. Montrons l'unicité. Si $S \in \mathbb{Q}[X]$ vérifie $\Delta(S) = Q$ et $S(0) = 0$, on a $S - P \in \operatorname{Ker} \Delta = \mathbb{Q}$, donc $S - P = S(0) - P(0) = 0$ et $S = P$. On a $\deg P = k + 1$.

2. On a, par un calcul *télescopique* :

$$\begin{aligned} S_k(n) &= 1^k + 2^k + \cdots + n^k \\ &= P_k(1) - P_k(0) + P_k(2) - P_k(1) + \cdots + P_k(n) - P_k(n-1) \\ &= P_k(n) - P_k(0) = P_k(n). \end{aligned}$$

Calculons P_0, P_1 et P_2.

- On a évidemment $P_0 = x$ et l'on retrouve $S_0(n) = n$.
- Soit $P := ax^2 + bx$. On a $\Delta(P)(x) = P(x) - P(x-1) = 2ax - a + b$. Ainsi, on a $\Delta(P)(x) = x^2$ si, et seulement si, $2ax - a + b = x$, c'est-à-dire si, et seulement si, $a = 1/2$ et $b = 1/2$. Donc $P_1(x) = \frac{1}{2}x^2 + \frac{1}{2}x$ et l'on retrouve $S_1(n) = \frac{n(n+1)}{2}$.
- Soit $P := ax^3 + bx^2 + cx$. On a :

$$\Delta(P)(x) = P(x) - P(x-1) = 3ax^2 + (2b - 3a)x + a - b + c.$$

Ainsi, on a $\Delta(P)(x) = x^2$ si, et seulement si, $3ax^2 + (2b-3a)x + a - b + c = x^2$, c'est-à-dire si, et seulement si, (a, b, c) est solution du système :

$$\begin{aligned} 3a &= 1 \\ -3a + 2b &= 0 \\ a - b + c &= 0. \end{aligned}$$

On obtient $a = 1/3$, $b = 1/2$, $c = 1/6$, donc $P_2(x) = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x$ et :

$$S_2(n) = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n = \frac{1}{6}n(n+1)(2n+1).$$

3. Soit $k \in \mathbb{N}$. Nous avons vu dans 2 qu'il existe un unique polynôme $P_k \in \mathbb{Q}[X]$ tel que $\Delta(P_k) = x^k$ et $P_k(0) = 0$. On a $\deg P_k = k + 1$.

Soit $P := a_{k+1}x^{k+1} + a_k x^k + \cdots + a_1 x$. Montrons comment calculer les $k+1$ coefficients $a_{k+1}, a_k, \ldots, a_1$ de P_k.

L'équation $\Delta(P_k) = x^k$ est équivalente à un système linéaire d'ordre $k+1$, dont les inconnues sont $a_{k+1}, a_k, \ldots, a_1$. Ce système est de Cramer d'après l'unicité de P_k. Il existe donc une solution unique, ce qui permet de calculer P_k.

Supposons $k = 3$. Soit $P := ax^4 + bx^3 + cx^2 + dx$. On a :

$$\Delta(P)(x) = P(x) - P(x-1) = 4ax^3 + (3b - 6a)x^2 + (4a - 3b + 2c)x - a + b - c + d.$$

Ainsi, on a $\Delta(P)(x) = x^3$ si, et seulement si, :

$$4ax^3 + (3b - 6a)x^2 + (4a - 3b + 2c)x - a + b - c + d = x^3,$$

c'est-à-dire si, et seulement si, (a,b,c,d) est solution du système :

$$\begin{aligned} 4a &= 1\\ -6a+3b &= 0\\ 4a-3b+2c &= 0\\ -a+b-c+d &= 0. \end{aligned}$$

On obtient $a=1/4$, $b=1/2$, $c=1/4$, $d=0$, donc $P_3=\frac{1}{4}x^4+\frac{1}{2}x^3+\frac{1}{4}x^2$ et $S_3(n)=\frac{1}{4}n^4+\frac{1}{2}n^3+\frac{1}{4}n^2=\frac{1}{4}n^2(n+1)^2$.

IV.1.26 1. On a $f(0)=1/2$ et $f(1)=1$. On a, pour tout $x\in\mathbb{R}\setminus\{-4\}$, $f'(x)=\frac{10}{(x+4)^2}>0$. On en déduit $f(I)=[1/2,1]\subset I$.

On a $f(x)-x=\frac{(1-x)(x+2)}{x+4}$. Les points fixes de f sont donc 1 et -2. L'unique point fixe dans I est 1.

2. On a $u_{n+1}-u_n=f(u_n)-u_n=\frac{(1-u_n)(u_n+2)}{u_n+4}$ et, puisque $u_n\in I$, $u_{n+1}-u_n\geqslant 0$. Ainsi la suite u_n est croissante. Elle est bornée par 1, elle converge donc vers $\ell\in I$ qui est un point fixe de f. On a nécessairement $\ell=1$.
3. On pose $v_n=\frac{u_n-1}{u_n+2}$. On a $v_{n+1}=\frac{2}{5}v_n=f'(1)$. La suite (v_n) est une suite géométrique de limite 0, donc la suite (u_n) converge vers 1.

IV.1.27 Supposons quil existe $\tau\in\mathbb{N}$ tel que les τ suites : $(u_{p\tau+q})_{p\in\mathbb{N}^*}$, $q\in[\![0,\tau-1]\!]$, extraites de (u_n), convergent respectivement vers ℓ_0, $\ell_1,\dots,\ell_{\tau-1}$. Soit $q\in[\![0,\tau-1]\!]$. On a, pour tout $p\in\mathbb{N}$, $f^{\circ\tau}(u_{p\tau+q}))=u_{(p+1)\tau+q}$, donc la suite récurrente définie par $f^{\circ\tau}$ et u_q est $(u_{p\tau+q})_{p\in\mathbb{N}^*}$. Elle converge vers ℓ_q, donc ℓ_q est un point fixe de $f^{\circ\tau}$.

Soit $q\in[\![0,\tau-1]\!]$. La suite $\left(f\left(f^{\circ p\tau}(u_q)\right)\right)_{p\in\mathbb{N}}$ converge vers $f(\ell_q)$. Mais :

$$\left(f\left(f^{\circ p\tau}(u_q)\right)=f^{\circ p\tau}\left(f(u_q)\right)=f^{\circ p\tau}(u_{q+1}).\right.$$

La suite $\left(f^{\circ p\tau}(u_{q+1})\right)_{p\in\mathbb{N}}$ converge vers ℓ_{q+1} si $q\in[\![0,q-2]\!]$ et vers ℓ_0 si $q=q-1$. Donc $f(\ell_q)=\ell_{q+1}$ si $q\in[\![0,q-2]\!]$ et $f(\ell_{q-1})=\ell_0$. Les suites définies par f et les conditions initales ℓ_q ($q\in[\![0,\tau-1]\!]$) sont donc périodiques de période τ.

Les τ suites extraites sont bornées, donc la suite (u_n) est bornée. Si la suite (u_n) converge vers ℓ, toutes les suites extraites convergent vers ℓ, donc, en particulier, $\ell_q=\ell$ pour tout $q\in[\![1,\tau-1]\!]$.

Inversement, supposons que τ les suites extraites $(u_{p\tau+q})_{p\in\mathbb{N}^*}$, $q\in[\![0,\tau-1]\!]$, convergent vers ℓ. Soit $\varepsilon>0$. Il existe alors P_0 tel que, pour tout $p\geqslant P_0$ et tout $q\in[\![0,\tau-1]\!]$, $|u_{p\tau+q}-\ell|<\varepsilon$. Posons $N_0:=P_0\tau$. Soit $n\geqslant N_0$. Par division euclidienne $n=p\tau+q$ avec $q\in[\![0,\tau-1]\!]$. On a nécessairement $p\geqslant P_0$, donc $|u_n-\ell|=|u_{p\tau+q}-\ell|<\varepsilon$. Ainsi la suite (u_n) tend vers ℓ.

IV.1.28 1. Le nombre de points fixes de $T^{\circ 4}$ est $2^4=16$. Chacun de ces points est un point fixe de T ou il appartient à un d-cycle de T avec $d=2$ ou 4. Il y a deux points fixes

et un 2-cycle. Il reste $16-4=12$ points qui appartiennent chacun à un 4-cycle. Il y a donc trois 4-cycles.

Le nombre de points fixes de $T^{\circ 5}$ est $2^5=32$. Il y a $32-2=30$ points qui appartiennent chacun à un 5-cycle. Il y a donc six 5-cycles.

Le nombre de points fixes de $T^{\circ 6}$ est $2^6=64$. Chacun de ces points est un point fixe de T ou il appartient à un d-cycle de T avec $d=2$, 3 ou 6. Une fois enlevés les 2 points fixes, le 2-cycle et les deux 3-cycles, il reste $64-2-2-6=54$ points qui appartiennent chacun à un 6-cycle. Il y a donc neuf 6-cycles.

2. On généralise la méthode utilisée dans la question 1. Le nombre de points fixes de $T^{\circ\tau}$ est 2^τ. En utilisant les remarques de la page 526, on obtient $\sum_{\tau'|\tau}\omega(\tau')=2^\tau$.

3. D'après la question 2, on a $\omega(1)+\omega(p)=2^p$, donc $\frac{2^p-2}{p}$ est entier et $\omega(p)=\frac{2^p-2}{p}$.

   D'après le petit théorème de Fermat (*cf.* le théorème 51 de la page 146) $2^{p-1}-1$ est divisible par p et l'on retrouve que $\frac{2^p-2}{p}=2\frac{2^{p-1}-1}{p}$ est entier. On a $\omega(17)=7710$.

IV.1.29 1. La suite définie par $u_0:=0$ est constante : 0 est un point fixe. Si $u_0:=1$, $u_1=4$, $u_2=2$ et $u_4=u_0$: $(1,4,2)$ est un 3-cycle de f. Si $u_0:=-1$, $u_1=-2$ et $u_3=-1$: $(-1,-2)$ est un 2-cycle de f. La valeur initiale $u_0:=-5$ donne un 5-cycle de f : $(-5,-14,-7,-20,-10)$. La valeur initiale $u_0:=-17$ donne un 18-cycle de f :

$$(-17,-50,-25,-74,-37,-110,-55,-164,-82,-41,-122,-61,$$
$$-182,-91,-272,-136,-68,-34)$$

2. Asinitrottant[3]… Le lecteur courageux pourra traiter « à la main » le cas $u_0:=27$: il faut 111 itérations.

   Voici un programme en *Maple* pour écrire les termes de la suite ($a:=u_0$ et p est le nombre d'itérations) :

```
syracuse := proc(a,p)
    local n, i;
    n:=a;
    for i to p do
        if n mod 2=0 then n:=n/2 else n:=3*n+1 fi
        end do
    end proc;
```

   On trouve par exemple :
   syracuse$(12345,50)=1$, syracuse$(99999,226)=1$, syracuse$(837799,525)=1$, syracuse$(100759293214567,1820)=1$ et syracuse$(279731455495736617,2258)=1$.
   Dans tous les cas la valeur de p est minimale : on le vérifie facilement « par quelques essais ». Les trois derniers cas ne sont pas faciles à découvrir…

3. On utilise le résultat de l'exercice 11 de la page 526. Si l'image de f est bornée, alors elle est *finie* (c'est un sous-ensemble de $\mathbb{Z}$). L'application f admet un point fixe unique 0. Si $f(n)=0$, on a $n=0$ donc l'unique suite récurrente dont l'image contient 0 est la suite constante nulle. Si $u_0\neq 0$, alors l'image de la suite contient un cycle.

[3] Néologisme : « qui marche au pas de l'âne ».

4. a) On a $a > 0$ (sinon $\operatorname{card} A = 1$ et A n'est pas un cycle). Notons $a' := f(a)$. On a $a' \in A$ et $a < a'$. Si a était pair, on aurait $a' = a/2 < a$ et une contradiction, donc a est impair.

   b) On a $a_1 \neq 1$ et $a_1 \neq 2$, donc $a_1 \geqslant 3$. Puisque a_1 est impair, $a_2 = 3a_1 + 1$ est pair et $a_3 = \frac{3a_1+1}{2}$. L'entier a_3 est impair. Sinon l'on aurait $a_4 = \frac{3a_1+1}{4} < a_1$, ce qui contredirait la minimalité de a_1. Puisque a_3 est impair, $a_4 = 3a_3 + 1$ est pair. On a $a_1 = f(a_5)$. Si a_5 était impair, on aurait $a_5 < a_1$, ce qui est impossible, donc a_5 est pair.
   On a $a_1 = f(a_5) = \frac{a_5}{2}$, $a_2 = f(a_1) = 3a_1 + 1$, $a_3 = f(a_2) = \frac{a_2}{2}$, $a_4 = f(a_3) = 3a_3 + 1$ et $a_5 = f(a_4) = \frac{a_4}{2}$.
   On a :

$$P = a_1a_2a_3a_4a_5 = f(a_5)f(a_1)f(a_2)f(a_3)f(a_4) = \frac{a_5}{2}(3a_1+1)\frac{a_2}{2}(3a_3+1)\frac{a_4}{2},$$

   donc $a_1a_3 = \frac{1}{8}(3a_1 + 1)(3a_3 + 1)$, c'est-à-dire $8 = \left(3 + \frac{1}{a_1}\right)\left(3 + \frac{1}{a_3}\right)$. Mais cette équation est impossible car le second membre est supérieur à 9. On en conclut que f ne possède pas de 5 cycle *positif*. (Nous avons vu plus haut que f possède un 5-cycle.)

IV.1.30 Montrons (i) $\Rightarrow$ (ii). Soit $(x_{n_k})_{k\in\mathbb{N}}$ une suite extraite convergeant vers a. Soit $\varepsilon > 0$, il existe $k_0 \in \mathbb{N}$, tel que, pour tout $k \geqslant k_0$, l'on ait $|x_{n_k} - a| < \varepsilon$. Soit $N \in \mathbb{N}$, il existe $k_1 \geqslant k_0$ tel que $n_{k_1} \geqslant N$. On a $|x_{n_{k_1}} - a| < \varepsilon$.

Montrons (ii) $\Rightarrow$ (i). On suppose que la condition (ii) est satisfaite. Nous allons construire, par récurrence, une suite extraite $(x_{n_k})_{k\in\mathbb{N}}$ satisfaisant la condition suivante : pour tout $k \in \mathbb{N}^*$, $|x_{n_k} - a| < 1/k$. Une telle suite converge vers a. On choisit arbitrairement $n_0 \in \mathbb{N}$. D'après (ii), avec $\varepsilon := 1$ et $N := n_0 + 1$, il existe $n_1 \geqslant N$ tel que $|x_{n_1} - a| < 1$. Par hypothèse de récurrence, supposons connus $x_{n_0}, x_{n_1}, \ldots, x_{n_k}$ satisfaisant la condition. On utilise (ii), avec $\varepsilon := \frac{1}{k+1}$ et $N := n_k+1$; il existe donc $n_{k+1} \geqslant N$ tel que $|x_{n_{k+1}} - a| < \frac{1}{k+1}$.

Montrons (ii) $\Rightarrow$ (iii). En utilisant (ii) avec $N := 0$, on obtient n_0 tel que $|u_{n_0} - a| < \varepsilon$. En utilisant à nouveau (ii) avec $N := n_0 + 1$, on obtient $n_1 \geqslant N > n_0$ tel que $|u_{n_1} - a| < \varepsilon$. En poursuivant par récurrence, on obtient (iii).

Montrons (iii) $\Rightarrow$ (ii). Supposons que (iii) est vrai et (ii) faux. alors, il existe $\varepsilon > 0$ et $N \in \mathbb{N}$, tel que, pour tout $n \geqslant N$, $|u_n - \varepsilon| \geqslant \varepsilon$. Par suite l'ensemble $\{n \in \mathbb{N} \mid |u_n - \varepsilon| < \varepsilon\}$ est fini et l'on a une contradiction.

IV.1.31 1. Le résultat est évident si l'ensemble des valeurs d'adhérence $\mathcal{V}$ est vide ou s'il est réduit à un point. On suppose donc qu'il contient au moins deux éléments.

On va montrer que si $a,\ b \in \mathbb{R}$ sont des valeurs d'adhérence, tout $c \in]a, b[$ est valeur d'adhérence, autrement dit que $\mathcal{V}$ est *convexe*, ce qui entraînera le résultat (en utilisant la proposition 15 de la page 519).

On raisonne par l'absurde. Supposons qu'il existe $c \in]a, b[$ qui ne soit pas valeur d'adhérence. Alors (en niant l'assertion (ii) de IV.1.30), il existe $\varepsilon > 0$ et $N \in \mathbb{N}^*$, tel que, pour tout $n \geqslant N$, $u_n \notin [c - \varepsilon, c + \varepsilon]$. Le résultat reste vrai si l'on diminue ε ; on peut donc supposer $\varepsilon < c - a$ et $\varepsilon < b - c$, c'est-à-dire $a < c - \varepsilon < c + \varepsilon < b$.

Puisque $u_{n+1}-u_n \to 0$, il existe $N' \in \mathbb{N}$ tel que, pour tout $n \geqslant N'$, $|u_{n+1}-u_n| \leqslant \varepsilon$. Soit $N'' := \max(N, N')$. On va montrer que les hypothèses $u_{N''} < c-\varepsilon$ et $u_{N''} > c+\varepsilon$ sont impossibles. Par suite, puisque l'on ne peut pas non plus avoir $u_{N''} \in [c-\varepsilon, c+\varepsilon]$ (car $N'' \geqslant N$), on aboutira à une contradiction.

- Montrons que $u_{N''} < c-\varepsilon$ est impossible. On raisonne par l'absurde. On suppose $u_{N''} < c-\varepsilon$. On prouve, d'abord, en raisonnant à nouveau par l'absurde, que, pour tout $n \geqslant N''$, $u_n \leqslant c-\varepsilon$. L'idée de la preuve est la suivante : le saut d'un terme au suivant est inférieur à ε et les termes ne peuvent pas entrer dans le segment $[c-\varepsilon, c+\varepsilon]$, ils ne peuvent donc pas passer de l'autre côté. Plus précisément, s'il existait $n > N''$ tel que $u_n > c-\varepsilon$, alors il existerait n' tel que $N'' \leqslant n' < n$ et $u_{n'} \leqslant c-\varepsilon$ et $u_{n'+1} > c-\varepsilon$. Mais l'on ne peut pas avoir $u_{n'+1} \in [c-\varepsilon, c+\varepsilon]$, donc $u_{n'+1} > c+\varepsilon$ et $u_{n'+1} - u_{n'} \geqslant 2\varepsilon$ et l'on obtiendrait une contradiction.
  Ainsi, pour tout $n \geqslant N''$, $u_n \leqslant c-\varepsilon$. Puisque b est valeur d'adhérence, on a $b \leqslant c-\varepsilon$, ce qui contredit $b > c+\varepsilon$.
- On montre, de façon similaire, que $u_{N''} > c+\varepsilon$ est impossible, ce qui termine la preuve.

2. On a :
$$\left|\sin\left(\ln(n+1)\right) - \sin(\ln n)\right| \leqslant \ln(n+1) - \ln n = \ln(1+1/n),$$
donc $\lim\limits_{n\to+\infty}(v_{n+1}-v_n) = 0$.

Notons A l'ensemble des valeurs d'adhérence de v. On a évidemment $A \subset [-1,1]$. D'après l'exercice IV.1.18 de la page 597, 1 et -1 appartiennent à A, donc, d'après la question 1, $[-1,1] \subset A$. Par suite $A = [-1,1]$.

IV.1.32 On raisonne par l'absurde en considérant la fonction $h := g - f$. Supposons que h ne s'annule pas sur I. On traite le cas $h \geqslant 0$ (le cas $h \leqslant 0$ est similaire). La fonction h est continue sur I, elle est donc minorée sur I par $\alpha > 0$ et l'on a, pour tout $x \in I$:
$$g\left(g(x)\right) - f\left(g(x)\right) = h\left(g(x)\right) \geqslant \alpha$$
$$g\left(f(x)\right) - f\left(f(x)\right) = h\left(f(x)\right) \geqslant \alpha.$$

En utilisant $f \circ g(x) = g \circ f(x)$, on en déduit $g^{\circ 2}(x) \geqslant f^{\circ 2}(x) + 2\alpha$, puis, par récurrence sur $n \in \mathbb{N}^*$, $g^{\circ n}(x) \geqslant f^{\circ n}(x) + n\alpha$, pour tous $n \in \mathbb{N}^*$ et tout $x \in I$. On obtient une contradiction car les suites $(f^{\circ n}(x))_{n\in\mathbb{N}}$ et $(g^{\circ n}(x))_{n\in\mathbb{N}}$ sont, par hypothèse, bornées.

IV.1.33 Montrons d'abord que $\lim q_n = +\infty$. On raisonne par l'absurde. Supposons que (q_n) ne tende pas vers $+\infty$. Alors il existe une suite extraite *bornée* $(q_{n(k)})$. Un ensemble borné d'entiers est fini, donc l'image A de cette suite extraite est un sous-ensemble fini de $\mathbb{N}^*$. Notons $r \in \mathbb{N}^*$ le PGCD des éléments de A. Pour tout $k \in \mathbb{N}$, on a $\frac{r}{q_{n(k)}} \in \mathbb{N}$, donc $r\frac{p_{n(k)}}{q_{n(k}} \in \mathbb{N}$. La suite $\left(r\frac{p_{n(k)}}{q_{n(k}}\right)$ converge vers $r\alpha$. Mais cette suite est à valeurs entières, donc sa limite est entière et l'on a $r\alpha \in \mathbb{N}$, donc $\alpha \in \mathbb{Q}$ et une contradiction. Ainsi $\lim q_n = +\infty$.
Montrons que $\lim p_n = +\infty$. Sinon l'on aurait une suite extraite bornée $(p_{n(h)}$ et la suite $\left(\frac{p_{n(k)}}{q_{n(k}}\right)$ tendrait vers 0. Comme elle tend vers α, l'on aurait $\alpha = 0$ et une contradiction puisque α est irrationnel.

IV.1.34 On peut supposer que, pour tout $n \in \mathbb{N}$, $q_n > 0$. On raisonne par l'absurde. On suppose que $\alpha = p/q$, avec $p \in \mathbb{Z}$ et $q \in N^*$. On note $\Delta_n := \left|\alpha - p_n/q_n\right|$; c'est un nombre rationnel *strictement positif* s'écrivant r_n/qq_n. On a donc $\Delta_n \geqslant 1/qq_n$. Par suite $1/qq_n \leqslant \Delta_n < \varepsilon_n/q_n$ et, $\forall n \in \mathbb{N}$, $1/q < \varepsilon_n$, ce qui est impossible puisque $\lim \varepsilon_n = 0$.
Cet exercice généralise la méthode utilisée pour prouver l'irrationalité de e (*cf.* l'exercice 33 de la page 557 : pour tout $n \in N^*$, $p_n/q_n := 1/n!$ et $\varepsilon_n := 1/n$).

IV.1.35 1. On suppose $\alpha \notin \mathbb{Q}$. Soient $m_1, m_2 \in \mathbb{N}$. Supposons $\langle m_1\alpha\rangle = \langle m_2\alpha\rangle$, alors $(m_1 - m_2)\alpha = E(m_1\alpha) - E(m_2\alpha)$. Si $m_1 \neq m_2$, alors $\alpha \in \mathbb{Q}$ et l'on a une contradiction.
On note $J := [0, 1[$. Soit $Q \in \mathbb{N}^*$. On a, pour tout $x \in \mathbb{R}$, $\langle x\rangle \in J$, donc, pour tout $m \in \mathbb{N}^*$, $\langle m\alpha\rangle \in J$. On veut montrer qu'il existe m_1 et m_2 distincts tels que $\langle m_1\alpha\rangle$ et $\langle m_2\alpha\rangle$ soient « suffisamment proches ». Pour cela, on va utiliser le principe des tiroirs en divisant J en Q « tiroirs » puis en observant comment $Q + 1$ valeurs particulières de $\langle m\alpha\rangle$ sont rangées dans ces tiroirs.

On partage J en Q intervalles semi-ouverts disjoints $J_k := \left[\frac{k}{Q}, \frac{k+1}{Q}\right[$, $k \in [\![0, Q-1]\!]$, de longueur $1/Q$. Les $Q+1$ points $\alpha_m := \langle m\alpha\rangle$, $m \in [\![0, Q]\!]$ sont deux à deux distincts et appartiennent à J. Les J_k, $k \in [\![0, Q-1]\!]$, forment une *partition* de J, donc, d'après le principe des tiroirs, *l'un* des J_k contient (au moins) *deux* de ces points. Il existe donc $m_1, m_2 \in [\![0, Q]\!]$, $m_1 \neq m_2$, tels que $|\alpha_{m_1} - \alpha_{m_2}| < 1/Q$. Ceci s'écrit :

$$\left|\langle m_1\alpha\rangle - \langle m_2\alpha\rangle\right| = \left|(m_1 - m_2)\alpha - (E(m_1) - E(m_2))\right| < 1/Q.$$

On peut supposer $m_1 > m_2$. En posant $q := m_1 - m_2$ et $p := E(m_1) - E(m_2)$, on obtient $|q\alpha - p| < 1/Q$, c'est-à-dire $|\alpha - p/q| < 1/qQ \leqslant 1/q^2$ (en utilisant $q \leqslant m_1 \leqslant Q$).

2. On suppose $\alpha \notin \mathbb{Q}$. On note A l'ensemble des rationnels s'écrivant p/q, avec $|p/q - \alpha| < 1/q^2$. Cet ensemble n'est pas vide : on a $|E(\alpha) - \alpha| < 1$, donc $p := E(\alpha)$, $q := 1$ répond à la question. (On peut aussi utiliser 1). Pour montrer que A est infini, on raisonne par l'absurde. Supposons A fini : $A := \{p_1/q_1, \ldots, p_r/q_r\}$. Puisque $\alpha \notin \mathbb{Q}$, $\min\limits_{i\in[\![1,r]\!]} |p_i/q_i - \alpha| > 0$. Il existe donc $Q \in \mathbb{N}^*$ tel que $|p_i/q_i - \alpha| > 1/Q$, pour tout $i \in [\![1, r]\!]$. En utilisant la question 1, on peut trouver $p/q \in A$ tel que $|p/q - \alpha| < 1/qQ \leqslant 1/Q$. On a, pour tout $i \in [\![1, r]\!]$, $|p/q - \alpha| < |p_i/q_i - \alpha|$, donc p/q n'est pas l'un des p_i/q_i et l'on a une contradiction.

3. Supposons $\alpha \in \mathbb{Q}$. alors $\alpha = a/b$, avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Si $p/q \neq \alpha$, on a $\left|\dfrac{p}{q} - \dfrac{a}{b}\right| = \dfrac{|bp - aq|}{qb} \geqslant \dfrac{1}{qb}$. La condition $|p/q - \alpha| < 1/q^2$ implique alors $q < b$. D'où le résultat.

IV.1.36 1. On a :

$$\begin{aligned}(1-q)w_n &= (1-q)(1+q)(1+q^2)(1+q^4)\ldots(1+q^{2^n})\\ &= (1-q^2)(1+q^2)(1+q^4)\ldots(1+q^{2^n})\\ &= (1-q^4)(1+q^4)\ldots(1+q^{2^n}) = \ldots = (1-q^{2^{n+1}}).\end{aligned}$$

On a $\lim\limits_{n\to\infty}(1-q^{2^{n+1}})=1$ et $(1-q)\neq 0$, donc (w_n) converge et $\lim\limits_{n\to\infty} w_n=\frac{1}{1-q}$.

2. On peut supposer $a\geqslant b$. Les suites sont évidemment bien définies et à termes strictement positifs. On remarque, pour tout $n\in\mathbb{N}$: $u_{n+1}-v_{n+1}=\dfrac{u_n^2-v_n^2}{u_n+v_n}=u_n-v_n$. On en déduit par récurrence $u_n-v_n=u_0-v_0=a-b$.
Par ailleurs $u_{n+1}-u_n=-v_n\frac{u_n}{u_n+v_n}<0$, donc la suite (u_n) est strictement décroissante. On montre de même que la suite (v_n) est strictement décroissante. De plus les suites (u_n) et (v_n) sont minorées par 0. Elles sont donc convergentes. On note α et β leurs limites respectives. On a $\alpha-\beta=a-b\geqslant 0$.
Montrons que $\beta=0$. On raisonne par l'absurde. Supposons $\beta>0$. Alors, on peut passer à la limite dans les relations de récurrence. On obtient $\alpha=\frac{\alpha^2}{\alpha+\beta}$, donc $\alpha=\alpha+\beta$, c'est-à-dire $\beta=0$ et une contradiction.
Ainsi $\beta=0$ et $\alpha=a-b$.

3. Explicitons u_n. On a :

$$u_1=\frac{a^2}{a+b},\quad u_2=\frac{\frac{a^4}{(a+b)^2}}{\frac{a^2+b^2}{a+b}}=\frac{a^4}{(a+b)(a^2+b^2)},\quad u_3=\frac{a^8}{(a+b)(a^2+b^2)(a^4+b^4)}.$$

On montre par récurrence : $u_n=\dfrac{a^{2^n}}{(a+b)(a^2+b^2)\dots(a^{2^{n-1}}+b^{2^{n-1}})}$. Pour $a:=1$ et $b:=q$, on obtient, pour tout $n\in\mathbb{N}^*$ $u_n=\dfrac{1}{(1+q)(1+q^2)\dots(1+q^{2^{n-1}})}=\dfrac{1}{w_{n-1}}$.
De $\lim u_n=1-q$, l'on déduit $\lim w_n=\frac{1}{1-q}$.
Inversement, supposons connues la convergence de (w_n) et sa limite. On peut en déduire la convergence des suites (u_n) et (v_n) et leurs limites. On observe que, pour tout $\lambda>0$ si l'on remplace a et b par λa et b par λb, les suites (u_n) et (v_n) ont remplacées par (λu_n) et (λv_n). Il suffit donc de traiter le cas où $a:=1$ et $b:=q$ qui se déduit de 1.

4. Si $x\geqslant c$, $f(x)=\frac{x^2}{2x-c}\geqslant\frac{c^2}{c}=c$.
Si $x\geqslant c$, on a $f(x)=x$ si, et seulement si, $x=c$.
Par ailleurs $f(x)=x\frac{x}{2x-c}$ et, si $x\geqslant c$, $\frac{x}{2x-c}\leqslant 1$. Par suite la suite récurrente définie par f et $u_0:=a\geqslant c$ est décroissante. Elle est minorée par c, elle est donc convergente. Sa limite est nécessairement c.
Le problème est équivalent à celui traité en 2 en posant $v_n=u_n-c$, $c:=b-a$ et $v_0:=b$.

IV.1.37 1. Les suites sont définies par leur condition initiale u_0. On prouve par récurrence $u_n=u_0^{2^n}=u_1^{2^{n-1}}$. Si $|u_0|<1$, alors $\lim\limits_{n\to+\infty}u_n=0$. Si $|u_0|=1$, alors $u_1=1$ et la suite est constante à partir du premier terme. Si $|u_0|>1$, alors $u_1>1$ et la suite tend vers $+\infty$.

2. On a $u_{n+1}-u_n=u_n^2-u_n+1\geqslant 0$ (car le discriminant du trinôme x^2-x+1 est $\Delta=-3$, donc négatif). Donc la suite est croissante. Montrons qu'elle n'est pas majorée. On raisonne par l'absurde. Supposons la suite majorée. puisqu'elle est croissante, elle converge vers $\ell\in\mathbb{R}$ et l'on a $\ell^2+1=\ell$, ce qui est impossible puisque l'équation $x^2-x+1=0$ n'a pas de racine réelle. Par suite la suite tend vers $+\infty$.

3. Le segment $X := [-2, 2]$ est invariant par f ($f(X) \subset [0, 2]$). L'équation aux points fixes est $x = \sqrt{2-x}$. On doit avoir $x^2 + x - 2 = 0$, c'est-à-dire $x = 1$ ou $x = -2$ et, puisque $x \geqslant 0$, il y a un unique point fixe $\ell := 1$.
   On a $|u_{n+1} - 1| = \left|\sqrt{2-u_n} - 1\right| = \frac{|u_n - 1|}{\sqrt{2-u_n}+1} \leqslant |u_n - 1|$. La suite $(v_n := |u_n - 1|)$ est positive et décroissante, elle est donc convergente. Notons ℓ_1 sa limite. Montrons que l'on ne peut pas avoir $\ell_1 > 0$. On raisonne par l'absurde. On suppose $\ell_1 > 0$. On a, pour n assez grand, $|u_{n+1} - 1| > 0$ et $\sqrt{2-u_n} + 1 = \frac{|u_n - 1|}{|u_{n+1} - 1|}$. Par suite $\lim\limits_{n\to+\infty} \sqrt{2-u_n} + 1 = \ell_1/\ell_1 = 1$ et $\lim\limits_{n\to+\infty} \sqrt{2-u_n} = 0$, donc $\lim\limits_{n\to+\infty} u_n = 2$, ce qui est impossible ($2 \neq 1$). Par suite $\ell_1 = 0$ et $\lim\limits_{n\to+\infty} u_n = 1$.

4. On a, pour tout $n \in \mathbb{N}$, $u_n > 0$. Montrons, par récurrence, que, pour tout $n \in \mathbb{N}^*$, $u_n < u_{n+1}$. On a $u_1 = \sqrt{a}$ et $u_2 = \sqrt{a + \sqrt{a}}$, donc $u_1 < u_2$. Supposons $u_n < u_{n+1}$. On a $u_{n+2} = \sqrt{a + u_{n+1}}$ et $u_{n+1} = \sqrt{a + u_n}$, donc $u_{n+1} < u_{n+2}$.
   Montrons, par récurrence, que, pour tout $n \in \mathbb{N}$, $u_n < a + 1$. On a $u_0 = a < a + 1$. Supposons $u_n < a + 1$. On a $u_{n+1} = \sqrt{a + u_n} < \sqrt{2a + 1} < a + 1$. La suite (u_n) est croissante et majorée, elle est donc convergente. Notons ℓ sa limite. On a $\ell^2 = a + \ell$, donc $\ell = \frac{1 \pm \sqrt{1+4a}}{2}$. Puisque $\ell > 0$, on a $\ell = \frac{1+\sqrt{1+4a}}{2}$. Pour $a := 1$, ℓ est le nombre d'or.

5. Notons $g : x \to g(x) := f(x) - x$. On a $g'(x) = x^2 - 1$, $g(-1) = 1$ et $g(1) = -1/3$. La fonction g est strictement croissante sur $]-\infty, -1[$, strictement décroissante sur $]-1, 1[$ et strictement croissante sur $]1, +\infty[$. De plus $\lim\limits_{x\to\pm\infty} g = \pm\infty$. On en déduit que l'équation $g(x) = 0$ admet trois racines réelles distinctes a, b, c telles que $a < -1 < b < 1 < c$.
   La fonction f est croissante, donc (par récurrence) :
   - si $u_0 \leqslant a$ (resp. b, c), alors, pour tout $n \in \mathbb{N}$, $u_n \leqslant \alpha$ (resp. b, c) ;
   - Si $u_0 \geqslant a$ (resp. b, c) alors, pour tout $n \in \mathbb{N}$, $u_n \geqslant a$ (resp. b, c).

   En utilisant la croissance de f et le signe de g, on montre que la suite est décroissante si $u_0 \in]-\infty, a[$ ou $u_0 \in]b, c[$ et croissante si $u_0 \in]a, b[$ ou $u_0 \in]c, +\infty[$. Les seules limites possibles sont a, b, c. On en déduit que :
   - si $u_0 = a$, b, ou c, la suite est constante ;
   - si $u_0 \in]-\infty, a[$ la suite tend vers $-\infty$;
   - si $u_0 \in]c, +\infty[$ la suite tend vers $+\infty$;
   - si $u_0 \in]a, c[$ la suite tend vers b.

   On peut retrouver ces résultats en précisant la nature des points fixes (*cf.* la proposition 50 de la page 561). On a $g'(a) > 1$, $g'(c) > 1$ et $\left|g'(b)\right| < 1$, donc les points fixes a et c sont répulsifs tandis que b est attractif.

IV.1.38 On montre par récurrence que la suite est bien définie et que $u_n > 0$. On a $\frac{u_{n+2}}{u_{n+1}} = \frac{u_{n+1}}{u_n}$, donc la suite $(v_n := \frac{u_{n+1}}{u_n})$ est constante et égale à $v_0 = \frac{u_1}{u_0} = \frac{b}{a}$. On a :

$$u_n = u_{n-1}v_{n-1} = u_{n-1}\frac{b}{a} = u_{n-2}\left(\frac{b}{a}\right)^2 = u_0\left(\frac{b}{a}\right)^n = a\left(\frac{b}{a}\right)^n.$$

La suite (u_n) est donc une suite géométrique de raison b/a. Elle converge si, et seulement si, $b \leqslant a$.

IV.1.39 1. On vérifie par récurrence que la suite (u_n) est bien définie et que ses termes sont strictement positifs. Pour tout $n \in \mathbb{N}^*$, on a :

$$u_{n+1} - u_n = \sqrt{\sum_{k=0}^{n} u_k} - \sqrt{\sum_{k=0}^{n-1} u_k} = \frac{u_n}{\sqrt{\sum_{k=0}^{n} u_k} + \sqrt{\sum_{k=0}^{n-1} u_k}} = \frac{u_n}{u_{n+1} + u_n}\cdot \quad (40)$$

Donc la suite (u_n) est strictement croissante. Montrons qu'elle n'est pas convergente. On raisonne par l'absurde. Supposons que $\lim\limits_{n\to+\infty} u_n = \ell$. En passant à la limite dans (40), on obtient $0 = \frac{\ell}{\ell+\ell} = \frac{1}{2}$, ce qui est absurde. Par suite la suite (u_n) tend vers $+\infty$.

2. On a montré $u_{n+1} - u_n = \frac{u_n}{u_{n+1}+u_n}$, donc $\frac{u_{n+1}}{u_n} - 1 = \frac{1}{u_{n+1}+u_n}\cdot$
Puisque $\frac{1}{u_{n+1}+u_n}$ tend vers 0, $\lim\limits_{n\to+\infty} \frac{u_{n+1}}{u_n} = 1$.
On peut écrire $v_n = u_{n+1} - u_n = \frac{1}{\frac{u_{n+1}}{u_n}+1}$, donc $\lim\limits_{n\to+\infty} v_n = 1/2$.

IV.1.40 On vérifie par récurrence que la suite (u_n) est croissante.

- On suppose que la suite (v_n) est constante : pour tout $n \in \mathbb{N}$, $v_n = a$. Si $a = 0$, (u_n) est la suite nulle. Supposons $a > 0$. Nous avons vu dans l'exercice IV.1.37 qu'alors la suite (u_n) est convergente.
- On suppose que $(v_n := ab^{2^n})$, avec $a, b > 0$. On a :

$$u_0 = v_0 = ba,\ \ u_1 = \sqrt{v_1} = \sqrt{ab^2} = b\sqrt{a},\ \ u_2 = \sqrt{ab^2 + \sqrt{ab^4}} = b\sqrt{a + \sqrt{a}}.$$

On vérifie par récurrence que la suite (u_n) est obtenue à partir de celle étudiée ci-dessus en multipliant cette dernière par b : $u_n := b\sqrt{a + \sqrt{a + \cdots + \sqrt{a}}}$. Elle est donc convergente.

- Nous allons montrer que la suite $u := (u_n)$ converge si, et seulement si, la suite $(v_n^{2^{-n}})$ est majorée.
Supposons que (u_n) converge vers ℓ. On a :

$$u_n^2 = v_1 + \sqrt{v_2 + \sqrt{v_3 + \cdots + \sqrt{v_n}}},$$

donc $v_1 \leqslant u_n^2$ et $\sqrt{v_2 + \sqrt{v_3 + \cdots + \sqrt{v_n}}} \leqslant u_n^2$.
On en déduit $v_2 \leqslant u_n^4$ et $\sqrt{v_3 + \sqrt{v_4 + \cdots + \sqrt{v_n}}} \leqslant u_n^4$. On montre par récurrence que $v_n \leqslant u_n^{2^n}$, donc $v_n^{2^{-n}} \leqslant u_n \leqslant \ell$. Ainsi la suite $(v_n^{2^{-n}})$ est bornée.
Inversement, supposons que la suite $(v_n^{2^{-n}})$ est bornée par b. Alors $v_n \leqslant b^{2^n}$ et la suite (u_n) est majorée par la suite $(\tilde{u}_n)$ définie par $\left(\tilde{u}_n := b^{2^n}\right)$. Nous avons vu que $(\tilde{u}_n)$ converge, donc la suite croissante (u_n) converge.

IV.1.41 1. On vérifie par récurrence que la suite (w_n) est bien définie et que $w_n > 0$. Considérons l'équation aux points fixes $x = \frac{1}{x+\ell+1}\cdot$ On l'écrit $x^2+(\ell+1)x-1 = 0$. Cette équation admet une unique racine strictement positive notée ℓ_1. Montrons que (w_n) converge vers ℓ_1

On a :

$$|w_{n+1}-\ell_1| = \left|\frac{1}{w_n+\ell+1} - \frac{1}{\ell_1+\ell+1}\right| \leqslant \frac{|w_n-\ell_1|}{\ell_1+1}.$$

Donc $\lim\limits_{n\to+\infty} w_n = \ell_1$.

2. La suite (u_n) est une suite récurrente si, et seulement si, la suite (v_n) est constante. Sinon elle satisfait une formule de récurrence *non autonome*. On note $M = \sup\limits_{n\in\mathbb{N}} v_n$. On vérifie par récurrence que la suite (u_n) est bien définie et que $\frac{1}{M+2} \leqslant u_n \leqslant 1$.
   - Supposons que la suite (u_n) converge. Sa limite est strictement positive. On a $v_n = \frac{1}{u_{n+1}} - u_n - 1$, donc la suite (v_n) converge.
   - Inversement supposons que la suite (v_n) converge vers ℓ. On définit une suite (w_n) comme en 2. a). Elle converge et l'on note ℓ_1 sa limite. Notons $s_n := u_n - w_n$. On a :

$$s_{n+1} = \frac{1}{u_n+v_n+1} - \frac{1}{w_n+\ell+1} = \frac{-s_n+\ell-v_n}{(u_n+v_n+1)(w_n+\ell+1)}.$$

   La suite (w_n) est à termes strictement positifs et elle converge vers $\ell_1 > 0$, elle est donc minorée par $m > 0$. Notons $\lambda := \frac{1}{m+1} \in]0,1[$. On a $|s_{n+1}| \leqslant \lambda\,(|s_n| + |v_n-\ell|)$ et l'on en déduit par récurrence

$$|s_n| \leqslant \lambda^n|s_0| + \sum_{k=0}^{n-1} \lambda^{n-k}|v_k-\ell|.$$

   Soit $\varepsilon > 0$. Il existe $k_0 \in \mathbb{N}$ tel que, pour tout $k \geqslant k_0$, l'on ait $|v_k-\ell| \leqslant \varepsilon$. On a $\sum\limits_{k=0}^{k_0-1} \lambda^{n-k}|v_k-\ell| = \lambda^n \sum\limits_{k=0}^{k_0-1} \lambda^{-k}|v_k-\ell| = C\lambda^n$, où C est une constante indépendante de n. Par ailleurs, il existe $n_0 \in \mathbb{N}$ tel que, pour tout $n \geqslant n_0$, l'on ait $C\lambda^n \leqslant \varepsilon$ et $\lambda^n|s_0| \leqslant \varepsilon$. Pour $n > k_0$, on a :

$$\sum_{k=k_0}^{n-1} \lambda^{n-k}|v_k-\ell| \leqslant \varepsilon \sum_{h\geqslant 1} \lambda^h = \frac{\lambda\varepsilon}{1-\lambda}.$$

   Alors, pour $n \geqslant \max(k_0,n_0)$, $|s_n| \leqslant 2\varepsilon + \frac{\lambda\varepsilon}{1-\lambda}$.
   On en déduit $\lim\limits_{n\to+\infty} s_n = 0$, puis $\lim\limits_{n\to+\infty} u_n = \ell_1$.

IV.1.42 On a :

$$z_1 = \frac{re^{i\theta}+r}{2} = r\cos\frac{\theta}{2}e^{\frac{i\theta}{2}}.$$

On montre par récurrence : $z_n = r\cos\dfrac{\theta}{2}\cos\dfrac{\theta}{4}\ldots\cos\dfrac{\theta}{2^n}e^{\frac{i\theta}{2^n}}$.

On a, pour tout $k \in [\![1,n]\!]$, $\cos\dfrac{\theta}{2^k} = \dfrac{\sin\frac{\theta}{2^{k-1}}}{2\sin\frac{\theta}{2^k}}$. On en déduit $z_n = r\dfrac{\sin\theta}{2^n\sin\frac{\theta}{2^n}}e^{\frac{i\theta}{2^n}}$.

On a $\lim\limits_{n\to+\infty} 2^n\sin\frac{\theta}{2^n} = \theta$ et $\lim\limits_{n\to+\infty} e^{\frac{i\theta}{2^n}} = 1$, donc $\lim\limits_{n\to+\infty} z_n = r\frac{\sin\theta}{\theta}$.

IV.1.43 1. a) On a, pour tous $\lambda \in [0,1]$ et $n \in \mathbb{N}$, $\lambda 5^n + (1-\lambda)6^n \geqslant 5^n > 0$.
On suppose d'abord $\lambda \neq 1$. On a :

$$u_n := \frac{\lambda 5^{n+1} + (1-\lambda)6^{n+1}}{\lambda 5^n + (1-\lambda)6^n} = 6\frac{\lambda(5/6)^{n+1} + (1-\lambda)}{\lambda(5/6)^n + (1-\lambda)}.$$

On a $\lim(5/6)^{n+1} = \lim(5/6)^n = 0$, donc $\lim u_n = 6$.
Si $\lambda = 1$, on a $u_n = 5$, la suite est constante et sa limite est 5.

b) Compte tenu de l'études des suites homographiques (*cf.* le point méthode de la page 536) et de la question précédente, il est « naturel » de calculer : $\frac{u_n-5}{u_n-6}$. On a :

$$u_n - 5 = (1-\lambda)\frac{6^n}{\lambda 5^n + (1-\lambda)6^n} \quad \text{et} \quad u_n - 6 = -\lambda\frac{5^n}{\lambda 5^n + (1-\lambda)6^n},$$

donc, si $\lambda \neq 0$ (et par suite $u_n \neq 6$) :

$$\frac{u_n - 5}{u_n - 6} = \frac{\lambda - 1}{\lambda}\left(\frac{6}{5}\right)^n \quad \text{et, par suite :} \quad \frac{u_{n+1} - 5}{u_{n+1} - 6} = \frac{6}{5}\,\frac{u_n - 5}{u_n - 6}.$$

On en déduit la relation : $5(u_{n+1} - 5)(u_n - 6) = 6(u_{n+1} - 6)(u_n - 5)$ (qui reste vraie pour $u_n = u_{n+1} = 6$). On a donc $u_n u_{n+1} = 11u_n - 30$ et, puisque $u_n > 0$, $u_{n+1} = \frac{11u_n - 30}{u_n}$. Ainsi u vérifie une récurrence homographique. La condition initiale est $u_0 := 6 - \lambda$.

2. On vérifie facilement que l'ensemble E des suites solutions de la récurrence (15) est un sous-espace vectoriel de l'espace des suites réelles et que l'application $(w_0, w_1) \in \mathbb{R}^2 \mapsto (w_n) \in E$ est linéaire, injective et surjective. Par suite E est *de dimension* 2.
La suite (ρ^n) appartient à E si, et seulement si :

$$\forall n \in \mathbb{N},\ \rho^{n+2} = 11\rho^{n+1} - 30\rho^n,$$

c'est-à-dire si, et seulement si, $\rho^2 - 11\rho + 30 = 0$. Par suite $\rho = 5$ ou $\rho = 6$.
Montrons que les deux suites (5^n) et (6^n) forment un système *libre* de E. Il suffit de montrer que les deux vecteurs $(1,5)$ et $(1,6)$ forment un système libre de $\mathbb{R}^2$ et ceci résulte de $\begin{vmatrix} 1 & 1 \\ 5 & 6 \end{vmatrix} = 1 \neq 0$.
Par suite les deux suites (5^n) et (6^n) forment une base de E et tout élément de E s'écrit de façon unique $(w_n) = \lambda_1(5^n) + \lambda_2(6^n)$, avec $\lambda_1, \lambda_2 \in \mathbb{R}$.

3. Soit (w_n) une suite réelle dont tous les termes sont non nuls. On suppose que la suite définie par $(v_n := w_{n+1}/w_n)$ pour $n \in \mathbb{N}$ vérifie la récurrence (16). Alors :

$$\frac{w_{n+2}}{w_{n+1}} = \frac{11w_{n+1} - 30w_n}{w_{n+1}},$$

donc :

$$w_{n+2} = 11w_{n+1} - 30w_n.$$

Inversement, si la suite (w_n), dont tous les termes sont non nuls, vérifie la récurrence linéaire (15), on obtient, en divisant par w_{n+1} :

$$\frac{w_{n+2}}{w_{n+1}} = 11 - \frac{30w_n}{w_{n+1}},$$

et, en posant, pour $n \geqslant 1$, $v_n := w_{n+1}/w_n$:

$$v_{n+1} = \frac{11v_n - 30}{v_n}.$$

par suite, quand la récurrence (16) est bien définie, on a : $v_n := \frac{\lambda_1 5^{n+1} + \lambda_2 6^{n+1}}{\lambda_1 5^n + \lambda_2 6^n}$ (avec $\lambda_1 + \lambda_2 \neq 0$). On peut imposer $\lambda_1 + \lambda_2 = 0$ et l'on trouve $v_n := \frac{\lambda 5^{n+1} + (1-\lambda)6^{n+1}}{\lambda 5^n + (1-\lambda)6^n}$.

4. Montrons par récurrence que $t_{n+1} = \frac{11t_n - 30}{t_n}$ et que, par suite $t_n = u_n$ et $t_n > 0$. Le résultat est vrai pour $n = 0$. Supposons le vrai pour $n \geqslant 0$. On a $t_n = \frac{30}{11 - t_{n+1}}$, donc :

$$t_{n+2} = 111 - \frac{1130}{t_{n+1}} + \frac{3000}{t_n t_{n+1}} = 111 - \frac{1130}{t_{n+1}} + \frac{100(11 - t_{n+1})}{t_{n+1}} = \frac{11t_{n+1} - 30}{t_{n+1}}.$$

IV.1.44 On note $\rho_1 := \frac{1+\sqrt{5}}{2}$ et $\rho_2 := \frac{1-\sqrt{5}}{2}$ les solutions de $\rho^2 - \rho - 1 = 0$. On cherche w_n sous la forme $w_n = \lambda_1 \rho_1^n + \lambda_2 \rho_2^n$. On a nécessairement $\lambda_1 + \lambda_2 = 1$ et $\lambda_1 \rho_1 + \lambda_2 \rho_2 = \rho_2$, ce qui équivaut à $\lambda_1 = \frac{\varepsilon}{\sqrt{5}}$ et $\lambda_1 = 1 - \frac{\varepsilon}{\sqrt{5}}$. On vérifie par récurrence que, pour tout $n \in \mathbb{N}$, $w_n = \frac{\varepsilon}{\sqrt{5}} \rho_1^n + \left(1 - \frac{\varepsilon}{\sqrt{5}}\right) \rho_2^n$.

On a $\rho_1 > 1$ $|\rho_2| < 1$ et, si $\varepsilon \neq 0$, la suite (w_n) tend vers l'infini. Par contre, si $\varepsilon = 0$, la suite tend vers 0.

Supposons ε « très petit » (mais non nul), et considérons le comportement de la suite (w_n). Si n « n'est pas trop grand », $\frac{\varepsilon}{\sqrt{5}} \rho_1^n$ est numériquement négligeable devant $\left(1 - \frac{\varepsilon}{\sqrt{5}}\right) \rho_2^n$ et w_n est pratiquement égal à $\left(1 - \frac{\varepsilon}{\sqrt{5}}\right) \rho_2^n$ qui tend vers 0 ; on a donc l'impression que la suite tend vers 0. Par contre, quand n devient « suffisamment grand », $\left(1 - \frac{\varepsilon}{\sqrt{5}}\right) \rho_2^n$ devient numériquement négligeable devant $\frac{\varepsilon}{\sqrt{5}} \rho_1^n$, qui tend vers l'infini et l'on observe numériquement la convergence vers l'infini de w_n.

Revenons au calcul numérique de la suite (v_n) de l'exercice 27. Quand on calcule sur un ordinateur et que l'on entre $v_1 := \rho_2$, la machine remplace le nombre irrationnel ρ_2 par une valeur décimale arrondie par défaut ; par exemple $v_1 := -0{,}6180339887 = \rho_2 + \varepsilon$, avec $\varepsilon < 0$ et $0 < -\varepsilon < 5.10^{-11}$. Ainsi, croyant calculer la suite (v_n), on calcule en fait la suite (w_n) (définie par $w_0 := 1$ et $w_1 := \rho_2 + \varepsilon = -0{,}6180339887$), ce qui explique le comportement observé (compte tenu du fait que le calcul numérique de (w_n) et le calcul *exact* de w_n en rationnels, en utilisant $w_1 := -\frac{6180339887}{10^10}$, donnent des résultats très voisins). Si l'on change l'arrondi de ρ_2, les valeurs numériques changent, mais le comportement reste similaire.

Voici un exemple des calculs en utilisant *Maple* sur un *MacBook Pro*.

On définit **`f:=(x,y) -> x+y`**, puis une procédure :

```
sfib :=proc(a,b,n)
local u0, u1, t, k, r;
    u0:=a; u1:=b;
    for k to n-1 do
        t:=u1; u1:=f(u0,u1); u0:=t; od;
    r:=u1;
    r
end proc
```

On vérifie que $f_n = \text{sfib}(0,1,n)$: on retrouve la suite de Fibonacci.

On a $v_n = \text{sfib}(1, 1/2 - \frac{\sqrt{5}}{2}, n)$ et l'on obtient une valeur arrondie $\tilde{v}_n$ de v_n en utilisant $evalf\left(\text{sfib}(1, 1/2 - \frac{\sqrt{5}}{2}, n)\right)$.

Le calcul *numérique* de de w_n donne les valeurs $\tilde{w}_n := \text{sfib}(1, -0{,}6180339887, n)$.
Voici un tableau de comparaison de quelques valeurs de $\tilde{v}_n$ et $\tilde{w}_n$.

n	10	15	20	50	80	100
$\tilde{v}_n$	-0,0081	-0,0073	0,000068	0,00000	0,00000	0,00000
$\tilde{w}_n$	-0,0081	-0,0073	0,000068	0,62799	$1{,}168\ 10^7$	$1{,}767\ 10^{10}$

IV.1.45 1. a) On a $u_1 = \frac{\cos\alpha+1}{2} = \cos^2\frac{\alpha}{2}$ et $v_1 = \cos\frac{\alpha}{2}$. On montre par récurrence que, pour $n \in \mathbb{N}^*$, $u_n = \cos^2\frac{\alpha}{2^n}\prod_{k=1}^{n-1}\cos\frac{\alpha}{2^k}$ et $v_n = \prod_{k=1}^{n}\cos\frac{\alpha}{2^k}$, donc $u_n = v_n\cos\frac{\alpha}{2^n}$.

b) On a, pour $n \in \mathbb{N}^*$:

$$\sin\frac{\alpha}{2^n}\,v_n = \sin\frac{\alpha}{2^n}\cos\frac{\alpha}{2^n}\,v_{n-1} = \frac{1}{2}\sin\frac{\alpha}{2^{n-1}}\,v_{n-1}.$$

On en déduit $\sin\frac{\alpha}{2^n}\,v_n = \frac{1}{2^n}\sin\alpha$ et $v_n = \frac{\sin\alpha}{2^n\sin\frac{\alpha}{2^n}}$. On a $\lim_{n\to+\infty} 2^n\sin\frac{\alpha}{2^n} = \alpha$, donc $\lim_{n\to+\infty} v_n = \frac{\sin\alpha}{\alpha}$. Par ailleurs $\lim_{n\to+\infty}\cos\frac{\alpha}{2^n} = 1$, donc $\lim_{n\to+\infty} u_n = \frac{\sin\alpha}{\alpha}$.

2. a) On a :

$$u'_1 = \frac{u'_0+v'_0}{2} = \lambda\frac{u_0+v_0}{2} = \lambda u_1 \quad \text{et} \quad v'_1 = \sqrt{u'_1v'_0} = \lambda\sqrt{u_1v_0} = \lambda v_1.$$

On montre par récurrence que, pour tout $n \in \mathbb{N}$, $u'_n = \lambda u_n$ et $v'_n = \lambda v_n$. Par suite (u_n) (resp. (v_n)) converge si, et seulement si, (u'_n) (resp. (v'_n)) converge et l'on a alors $\lim u'_n = \lambda\lim u_n$ et $\lim v'_n = \lambda\lim v_n$.

b) Si $a = b$, les deux suites u et v sont constantes. On peut donc supposer $a \neq b$.

∗ Supposons d'abord $a < b$. On note $\tilde{u}$ et $\tilde{v}$ les suites définies par la relation de récurrence (R) et $(\tilde{u}_0, \tilde{v}_0) := (a/b, 1)$. On note $\tilde{\alpha} = \arccos(a/b)$. On a $\tilde{\alpha} \in]0, \pi/2[$ et $\cos\tilde{\alpha} = a/b$. D'après 1. b), les deux suites $\tilde{u}$ et $\tilde{v}$ convergent vers une limite commune $\tilde{\ell} = \frac{\sin\tilde{\alpha}}{\tilde{\alpha}}$. D'après 2. a) on a $u = b\tilde{u}$ et $v = b\tilde{v}$. Donc les deux suites u et v convergent vers la limite commune :

$$\ell := b\frac{\sin\tilde{\alpha}}{\tilde{\alpha}} = \frac{\sqrt{b^2-a^2}}{\arccos(a/b)}.$$

∗ On suppose $b = 1$ et $a > 1$. On note $\beta := \text{argcosh}\,a$. On a $\beta \in]0, +\infty[$ et $\cosh\beta = a$.
On a $u_1 = \frac{\cosh\beta+1}{2} = \cosh^2\frac{\beta}{2}$ et $v_1 = \cosh\frac{\beta}{2}$. On montre par récurrence que, pour $n \in \mathbb{N}^*$, $u_n = \cosh^2\frac{\beta}{2^n}\prod_{k=1}^{n-1}\cosh\frac{\beta}{2^k}$ et $v_n = \prod_{k=1}^{n}\cosh\frac{\beta}{2^k}$, donc $u_n = v_n\cosh\frac{\beta}{2^n}$. Par une méthode similaire à celle utilisée en 1. b), on montre $v_n = \frac{\sinh\beta}{2^n\sin\frac{\beta}{2^n}}$. On en déduit $\lim_{n\to+\infty} v_n = \lim_{n\to+\infty} u_n = \frac{\sinh\beta}{\beta}$.

∗ Supposons maintenant $a > b$. On note $\tilde{u}$ et $\tilde{v}$ les suites définies par la relation de récurrence et $(\tilde{u}_0, \tilde{v}_0) := (a/b, 1)$. On note $\tilde{\beta} = \operatorname{argcosh}(a/b)$. On a $\tilde{\beta} \in]0, +\infty[$ et $\cosh\tilde{\beta} = a/b$. D'après 1. b), les deux suites $\tilde{u}$ et $\tilde{v}$ convergent vers une limite commune $\tilde{\ell} = \frac{\sinh\tilde{\beta}}{\tilde{\beta}}$.
D'après 2. a), on a $u = b\tilde{u}$ et $v = b\tilde{v}$. Donc les deux suites u et v convergent vers la limite commune $\ell := b\frac{\sinh\tilde{\beta}}{\tilde{\beta}} = \frac{\sqrt{a^2-b^2}}{\operatorname{argcosh}(a/b)}$.

IV.1.46 1. On montre par récurrence que les deux suites (a_n) et (b_n) sont à termes strictement positifs. On a, pour tout $n \in \mathbb{N}$:

$$a_{n+1}^2 - b_{n+1}^2 = \left(\frac{a_n + b_n}{2}\right)^2 - a_n b_n = \frac{1}{4}(a_n - b_n)^2 \geqslant 0. \tag{41}$$

On en déduit $b_n \leqslant a_n$. Puis, en utilisant la définition des suites, $a_{n+1} \leqslant a_n$ et $b_{n+1} \geqslant b_n$.
Les deux suites sont monotones et bornées, elles convergent donc, respectivement vers α et β. En passant à la limite dans la relation $a_{n+1} = \frac{a_n+b_n}{2}$, on obtient $\alpha = \frac{\alpha+\beta}{2}$, donc $\alpha = \beta$.

2. En utilisant (41), on obtient $c_{n+1} = \frac{1}{2}(a_n - b_n)$. Puisque $a_{n+1} - b_{n+1} \leqslant a_n - b_n$, la suite (c_n) décroît vers 0. Par ailleurs, $c_n^2 = (a_n - b_n)(a_n + b_n) = 4c_{n+1}a_{n+1}$. On en déduit $c_{n+1} \leqslant \frac{c_n^2}{4M(a,b)}$.
Notons $M := M(a, b)$. On a $c_{n+1}/4M \leqslant (c_n/4M)^2$, par suite la convergence vers 0 de la suite $(c_n/4M)$ est *quadratique* (c'est-à-dire que la précision double à chaque étape), donc « très rapide ».
Il existe $n_0 \in \mathbb{N}$ tel que $c_{n_0}/4M < 1/10$. On a alors :

$$a_n - b_n = 2c_{n+1} \leqslant 8M \times 10^{-2^{n+1-n_0}}.$$

On a $a_n - \alpha \leqslant a_n - b_n$, $\beta - b_n \leqslant a_n - b_n$, donc la convergence des suites (a_n) et (b_n) est aussi « très rapide ».

3. On a $a_1 = \frac{1}{2}(1+1/\sqrt{2})$, $b_1 = 1/\sqrt[4]{2}$, $c_1 = \frac{1}{2}(1-1/\sqrt{2})$ et $c_1/4M \leqslant c_1/4b_1 = \sqrt[4]{2}\frac{c_1}{4}$.
On a $c_1/4 \leqslant 0{,}037$ et $\sqrt[4]{2} \leqslant 0{,}190$, donc $c_1/4M \leqslant c_1/4b_1 \leqslant 0{,}044 < 0,1$.
En utilisant la question 2 ($n_0 := 1$), on obtient $c_n \leqslant 4M \times 10^{-2^{n-1}} \leqslant 4 \times 10^{-2^{n-1}}$. On en déduit $a_n - M \leqslant 2c_{n+1} \leqslant 8 \times 10^{-2^n}$. On a $2^{30} = 1073741824$, par suite a_{30} donne une approximation de M avec plus *d'un milliard* de décimales.

IV.1.47 1. Si $x(0) = 0$ ou $x(0) = 1$, la fonction $x : t \in \mathbb{R} \mapsto x(t) := 0$ est solution.
Cherchons des solutions x ne s'annulant pas. On a $\frac{1}{x^2}\mathrm{d}x/\mathrm{d}t = \rho(1/x - 1)$, ce qui s'écrit $dy/dt = \rho(1 - y)$. Les solutions de cette équation différentielle à coefficients constants sont de la forme $y : t \mapsto 1 - Ce^{-\rho t}$. On a $y(0) = 1 - C$, donc $C = 1 - y(0) = \frac{x(0)-1}{x(0)}$ et $x(t) = \dfrac{1}{1 - Ce^{-\rho t}} = \dfrac{x(0)}{x(0) + (1 - x(0))\, e^{-\rho t}}$.

On vérifie que si $x(0) := 0$, alors $x : t \in \mathbb{R} \mapsto x(t) := \frac{x(0)}{x(0)+(1-x(0))e^{-\rho t}} = 0$ est solution.

Si $\rho > 0$, quand $t \to +\infty$, $x(t)$ tend vers 1. Si $\rho < 0$, quand $t \to +\infty$, $x(t)$ tend vers 0.

2. Notons $p : t \mapsto p(t)$ la fonction *population en fonction du temps*. On convient dans la modélisation de la supposer continue et dérivable.

Si la population peut croître sans limites, il est « naturel » de prendre pour modèle de croissance l'équation différentielle $dp/dt = \lambda p$, donc les solutions sont de la forme $t \mapsto p(t) = Ce^{\lambda t}$. En effet, on a alors, pour $n \in \mathbb{N}$, $p(n+1) = e^{\lambda} p(n)$ et l'on retrouve le modèle d'Euler et Malthus en posant $\Lambda := e^{\lambda}$.

S'il y a des facteurs limitatifs et si la population admet une valeur maximale P, on peut supposer que λ est variable et proportionnel à $P - p$. On obtient alors l'équation différentielle $dp/dt = \nu p(P-p)$. En posant $x := p/P$, elle s'écrit $dx/dt = \frac{\nu}{P} x(1-x)$ et l'on peut poser $\rho := \nu P$ et obtenir $dx/dt = \rho x(1-x)$.

On a, par hypothèse, $0 \leqslant p(0) \leqslant P$. Si $\rho > 0$, la population croît avec le temps et tend vers la population maximum P quand t tend vers $+\infty$. Si $\rho < 0$, la population décroît avec le temps et tend vers 0 quand t tend vers $+\infty$. Si $\rho = 0$ la population reste constante.

IV.1.48 On reprend les notations de la page 567.

(i) (a) On suppose $0 < \mu \leqslant 1$. On a $\alpha_1 \leqslant 0$. On a $f_\mu(0) = f_\mu(1) = 0$.

On a $f_\mu(x) - x = \mu x(\alpha_1 - x))$ et $\alpha_1 \leqslant 0$, donc $f_\mu(x) \leqslant x$.

Si $u_0 \in [0,1]$, la suite est décroissante et converge vers un point fixe ℓ. On a nécessairement $\ell = 0$.

(b) On suppose $1 < \mu \leqslant 2$. On a $0 < \alpha_1 \leqslant 1/2 \leqslant 1/\mu < 1$.

On a $f_\mu(0) = f_\mu(1) = 0$, $f_\mu(\alpha_1) = \alpha_1$ et $f_\mu(1/\mu) = \alpha_1$, donc, pour tout $n \in \mathbb{N}^*$, $f_\mu^{\circ n}(1/\mu) = \alpha_1$.

Si $u_0 \in]0, \alpha_1]$ (resp. $u_0 \in]\alpha_1, 1/2]$) on a $\alpha_1 - x \geqslant 0$ (resp. $\alpha_1 - x \leqslant 0$), donc la suite définie par f_μ et u_0 est croissante (resp. décroissante) et converge vers un point fixe $\ell > 0$ (resp. $\ell \leqslant 1/2$). On a nécessairement $\ell = \alpha_1$.

Supposons $u_0 \in]1/2, 1[$. Si $u_0 \in [1/\mu, 1[$ (resp. $u_0 \in]1/2, 1/\mu[$), alors $u_1 = f_\mu(u_0) \in]0, \alpha_1]$ (resp. $u_1 \in]\alpha_1, 1/2[$). On est donc ramené au cas précédent.

(ii) On suppose $2 < \mu < 3$. On a $1/3 < \gamma < 1/2 < \alpha_1 < 2/3$.

(a) Montrons que $f \circ f(J) \subset [1/2, \alpha_1] \subset J$.

La fonction f_μ atteint son maximum en $1/2$, donc $\alpha_1 \leqslant \mu/4$ et $f_\mu(J) = [\alpha_1, \mu/4]$.

La fonction f est décroissante sur $[1/2, 1]$, donc $f(\mu/4) \leqslant \alpha_1$. On en déduit $f \circ f(J) = f([\alpha_1, \mu/4]) = [f(\mu/4), \alpha_1]$. Montrons que $f(\mu/4) \geqslant 1/2$. Cette inégalité s'écrit $g(\mu) := \mu^2(4-\mu) \geqslant 8$. On a $g(2) = 8$ $g(3) = 9 > 8$, $g'(\mu) = \mu^2(8-3\mu)$. On en déduit que, pour $\mu \in [2,3]$, $g(\mu) \geqslant 8$. Ainsi $f \circ f(J) \subset [1/2, \alpha_1]$.

On a $[1/2, \alpha_1] \subset [\gamma, \alpha_1] = J$, donc l'intervalle $[1/2, \alpha_1]$ est stable par $f \circ f$.

Si $u \in [1/2, \alpha_1]$, on a $f'(u) \geqslant 0$ et $f(u) \in [1/2, \alpha_1]$, donc $f'(f(u)) \geqslant 0$. Par suite la fonction $f \circ f$ est croissante sur l'intervalle $[1/2, \alpha_1]$. On en déduit que la suite u_{2n} est monotone et elle converge vers un point fixe $\ell \in [1/2, \alpha_1]$ de $f \circ f$.

Les points fixes de $f \circ f$ autres que 0 et α_1 sont racines de l'équation $\mu^2 x^2 - \mu(\mu+1)x + \mu + 1 = 0$. Il n'y en a pas si $\mu < 3$, donc $\ell = \alpha_1$. En ap-

pliquant f, on en déduit que la suite (u_{2n+1}) converge aussi vers α_1. Par suite la suite (u_n) converge vers α_1.

(b) On suppose $0 < u_0 < \gamma < \alpha_1$. Pour $x < \alpha_1$, on a $f(x) > x$, donc $u_0 < u_1$. La suite croît tant qu'elle reste inférieure à γ. Si elle le restait, elle serait convergente vers $\ell \leqslant \gamma$, ce qui est impossible puisque $\gamma < \alpha_1$. Soit $k-1$ le dernier indice tel que $u_{k-1} < \gamma$. Alors $\gamma \leqslant u_k = f(u_{k-1}) < f(\gamma) = \alpha_1$, donc $u_k \in J$ et l'on est ramené au cas de (a). Par suite la suite converge vers α_1.

(c) On a déjà traité le cas $\gamma \leqslant u_0 \leqslant \alpha_1$. On peut donc supposer $\alpha_1 < u_0 < 1$. La fonction f est décroissante sur l'intervalle $[\alpha_1, 1]$, donc $u_1 \in f\,(]\alpha_1, 1[) =]0, \alpha_1[$ et l'on est ramené à l'un des cas de (a) ou (b). Par suite la suite converge vers α_1.

IV.1.49 1. L'inverse de $h_{\alpha,\beta}$ est aussi une transformation affine ; on a :

$$h_{\alpha^{-1},-\alpha^{-1}\beta}(\xi) = \alpha^{-1}\xi - \alpha^{-1}\beta = x,$$

donc $h_{\alpha^{-1},-\alpha^{-1}\beta} = h_{\alpha,\beta}^{-1}$.

2. a) Pour conjuguer f à un g_γ, on résout l'équation $g_\gamma \circ h_{\alpha,\beta} = h_{\alpha,\beta} \circ f$ aux inconnues $\alpha,\ \beta,\ \gamma$, c'est-à-dire $(\alpha x + \beta)^2 + \gamma = \alpha(ax^2 + bx + c) + \beta$, pour tout $x \in \mathbb{K}$. On obtient une unique solution : $\alpha = a,\ \beta = \frac{b}{2},\ \gamma = -ac - \frac{b}{2} + \frac{b^2}{4}$.

b) On a $f_\mu(x) = -\mu x^2 + \mu x$, donc $a = -\mu,\ b = \mu,\ c = 0$. Par suite :

$$\alpha = -\mu,\ \beta = \frac{\mu}{2},\ \gamma = -\frac{\mu}{2} + \frac{\mu^2}{4}.$$

Si $\mu = 4$, on obtient $\gamma = 2$. Les applications f_μ et $f_{\mu'}$ sont conjuguées si, et seulement si, $\mu(2 - mu) = \mu'(2 - mu')$. Par suite f_μ et $f_{2-\mu}$ sont conjuguées.

IV.1.50 Soit $x \in [0,1]$, il existe $a \in \mathbb{R}$ tel que $x = \sin^2(\pi a/2)$. Alors :

$$f_4(x) = 4x(1-x) = \left(2\sin(\pi a/2)\cos(\pi a/2)\right)^2 = \sin^2(\pi a).$$

Par récurrence, pour tout $n \in \mathbb{N}^*$, $f_4^{\circ n}(x) = \sin^2(2^{n-1}\pi a)$.

Il est clair que $\sin(\pi a/2)$ ne dépend que de la *partie fractionnaire* $\langle a \rangle := a - E(a) \in [0,1[$ de a. Passer de x à $f_4(x)$ revient à passer de $\langle a/2 \rangle$ à $\langle a \rangle$. En écriture binaire pour $\langle a/2 \rangle$, ceci revient à supprimer la première décimale et à décaler d'un cran vers la gauche les décimales restantes : ce que l'on appelle le *décalage de Bernoulli* (*cf.* l'exercice IV.1.65). Ceci permet d'étudier l'itération de f_4 à partir de celle du décalage de Bernoulli.

IV.1.51 1. D'après l'exercice IV.1.11, le sous-groupe $B \subset \mathbb{R}$ est dense dans $\mathbb{R}$ ou de la forme $B = \mathbb{Z}a$, avec $a > 0$. Si l'on est dans le second cas, on a $1 \in \mathbb{Z}a$ et $\xi \in \mathbb{Z}a$. Il existe donc $p \in \mathbb{Z}^*,\ q \in \mathbb{N}^*$ tels que $\xi = pa$ et $1 = qa$ et l'on a $\xi = \frac{p}{q} \in \mathbb{Q}$. Ce second cas est donc impossible et B est dense dans $\mathbb{R}$.

Il existe donc une suite (b_n) de B tendant vers 0 et telle que, pour tout $n \in \mathbb{N}$, l'on ait $b_n \neq 0$. Il existe donc deux suites d'entiers relatifs (u_n) et (v_n) telles que, pour tout $n \in \mathbb{N}$, $b_n = u_n + v_n\xi \neq 0$ et $\lim\limits_{n\to+\infty}(u_n + v_n\xi) = 0$.

On définit deux suites d'entiers relatifs (x_n) et (y_n) de la façon suivante : $x_n := u_n$, $y_n := v_n$ si $v_n \geqslant 0$ et $x_n := -u_n$, $y_n := -v_n$ sinon. La suite (y_n) est *positive* et l'on a, pour tout $n \in \mathbb{N}$, $x_n + y_n\xi \neq 0$ et $\lim\limits_{n\to+\infty}(x_n + y_n\xi) = 0$.

Supposons (y_n) bornée. On peut alors en extraire une suite convergente $(y_{n(k)})$ (*cf.* le théorème 47 de la page 558) : $\lim\limits_{k\to\infty} y_{n(k)} = \ell$. Les $y_{n(k)}$ étant entiers positifs, la suite $(y_{n(k)})$ est stationnaire et $\ell \in \mathbb{N}$.

La suite $(x_{n(k)})_{k\in\mathbb{N}^*}$ est convergente de limite $-\xi\ell$. Les $(x_{n(k)}$ étant entiers, elle est nécessairement stationnaire et égale à $-\xi\ell$ à partir d'un certain rang. On a donc $\ell \neq 0$ (sinon $x_n + y_n\xi$ serait nul à partir d'un certain rang). Par ailleurs, la limite de la suite d'entiers $(x_{n(k)})$ est un entier ℓ', donc $\xi = -\ell'/\ell$ est rationnel, et l'on a une contradiction. Ainsi (y_n) n'est pas bornée.

On en déduit qu'il existe deux suites extraites $(x_{n(h)})_{h\in\mathbb{N}^*}$ et $(y_{n(h)})_{h\in\mathbb{N}^*}$ telles que :

$$\lim_{h\to+\infty}(x_{n(h)} + y_{n(h)}\xi) = 0 \quad \text{et} \quad \lim_{n\to+\infty} y_{n(h)} = +\infty \tag{42}$$

2. Soit $\alpha \in A$. Soit $\varepsilon > 0$. Par densité de B, il existe des entiers a et b tels que $|a + b\xi - \alpha| < \varepsilon/2$. Si $b \geqslant 0$, $a + b\xi \in A$. Sinon, d'après ce qui précède (*cf.* (42)), il existe des entiers c et d tels que $|c + d\xi| < \varepsilon/2$ et $d > -b$. On en déduit $|a + c + (b + d)\xi - \alpha| < \varepsilon$, avec $a + c + (b + d)\xi \in A$. Par suite A est dense dans $\mathbb{R}$.
3. On note : $\Phi : t \in [0, 1[\to \Phi(t) := e^{2i\pi t} \in U$. On a :
$$\Phi(A) = \{e^{2mi\pi\xi}\}_{m\in\mathbb{N}} = \{k^m\}_{m\in\mathbb{N}} = \mathcal{X}.$$
L'application Φ est continue et bijective, donc, d'après la proposition 35 de la page 545, $\Phi(A) = \mathcal{X}$ est dense dans $\Phi([0, 1[) = U$. Le cas de $\mathcal{X}'$ est similaire : on remplace ξ par $-\xi$.
4. On prouve facilement a) et b) en utilisant 3.
5. D'après la question 3., pour $\xi := \frac{1}{2\pi} \notin \mathbb{Q}$, l'image de la suite (e^{in}) est dense dans U. Par ailleurs l'application $U \to [-1, 1]$ définie par $z \mapsto \operatorname{Im} z$ est continue et surjective. On en déduit que l'image de la suite $(\sin n)$ est dense dans $[-1, 1]$.

IV.1.52 1. (i) On choisit $\xi \in \mathbb{R} \setminus \mathbb{Z}$ tel que $k := e^{2i\pi\xi}$.
On a nécessairement $c \neq 0$. Par homogénéité on peut supposer $c := 1$. Puisque i et $-i$ sont solutions de l'équation aux points fixes $x^2 + (d - a)x - b = 0$, on doit avoir $0 = i - i = a - d$ et $b = -i^2 = 1$
Alors a, b, d doivent vérifier :
$$\frac{d - i}{d + i} = k, \quad a = d, \quad b = -1,$$
c'est-à-dire :
$$a = d = -i\frac{k + 1}{k - 1} = -i\frac{e^{2i\pi\xi+1}}{e^{2i\pi\xi} - 1} = -\operatorname{cotan}\pi\xi, \quad c = 1 \quad \text{et} \quad b = -1.$$
On vérifie que a, b, c, $d \in \mathbb{R}$.
On peut multiplier a, b, c, d par $-\sin\pi\xi$, on obtient l'homographie réelle
$$f : x \mapsto f(x) := \frac{(\cos\pi\xi)\,x + \sin\pi\xi}{-(\sin\pi\xi)\,x + \cos\pi\xi}.$$

qui répond à la question.

(ii) On applique (i) en choisissant pour k une racine primitive $p^{ème}$ de l'unité. L'homographie réelle obtenue est conjuguée par une homographie (complexe) à $g : t \mapsto kt$. Le résultat s'en déduit.

2. Notons :
$$v = g(u) = \frac{u-\alpha}{u-\bar{\alpha}} \quad \text{et} \quad u = h(v) := \frac{\bar{\alpha}v-\alpha}{v-1}\cdot$$
On a : $g \circ f \circ h(v) = kv$.
L'homographie g réalise un homéomorphisme entre $\mathbb{C} \setminus \{\bar{\alpha}\}$ et $\mathbb{C} \setminus \{1\}$. On vérifie qu'elle induit un homéomorphisme entre $\mathbb{R}$ et $U \setminus \{1\}$. La densité, dans $\mathbb{R}$, de l'image de la suite (u_n) se déduit donc de la densité, dans U, de la suite (v_n) qui a été prouvée dans l'exercice IV.1.51.
Considérons l'ensemble $X \subset \mathbb{R}$ tel que, pour tout $u_0 \in X$, la suite soit définie. On a $u_0 \in X$ si, et seulement si, $v_0 \notin Y := \{k^{-n} \mid n \in \mathbb{N}^*\}$.
Si l'on note Z l'image de $Y \setminus \{1\}$ par l'application $v \mapsto u = h(v) := \frac{\beta v-\alpha}{v-1}$, on obtient $X = \mathbb{R} \setminus Z$.
Le résultat de densité prouvé ci-dessus reste vrai si l'on remplace k par k^{-1}, donc Y est *dense* dans U. Par suite $Y - \setminus\{1\}$ est dense dans $U \setminus \{1\}$ et son image Z par l'application *continue* h est dense dans $h(U \setminus \{1\}) = \mathbb{R}$.

3. On a nécessairement $c \neq 0$. Par homogénéité on peut supposer $c := 1$. Puisque i et $-i$ sont solutions de l'équation aux points fixes $x^2 + (d-a)x - b = 0$, on doit avoir $a - d = \alpha + \bar{\alpha}$ et $b = -\alpha\bar{\alpha}$.
Alors $a,\ b,\ d$ doivent vérifier :
$$\frac{d-i}{d+i} = k, \quad a = d, \quad b = -\alpha\bar{\alpha},$$
c'est-à-dire :
$$d = -i\frac{k+1}{k-1} = -i\frac{e^{2i\pi\xi+1}}{e^{2i\pi\xi}-1} = -\operatorname{cotan}\pi\xi, \quad a = d+\alpha+\bar{\alpha}, \quad c = 1 \quad \text{et} \quad b = -\alpha\bar{\alpha}.$$
On vérifie que $a,\ b,\ c,\ d \in \mathbb{R}$.
On peut multiplier $a,\ b,\ c,\ d$ par $-\sin\pi\xi$, on obtient l'homographie réelle
$$f : x \mapsto f(x) := \frac{(\cos\pi\xi - (\alpha+\bar{\alpha})\sin\pi\xi)\,x + \alpha\bar{\alpha}\sin\pi\xi}{-(\sin\pi\xi)\,x + \cos\pi\xi}\cdot$$
qui répond à la question.

IV.1.53 Montrons qu'un nombre décimal est inversible dans $\mathbb{D}$ si, et seulement s'il est de la forme $\pm 2^m 5^n$, avec $m, n \in \mathbb{Z}$.
Un rationnel $\frac{p}{10^a}$ ($p \in \mathbb{Z},\ a \in \mathbb{N}$) est inversible dans $\mathbb{D}$ si, et seulement s'il existe un rationnel $\frac{p'}{10^{a'}}$ ($p' \in \mathbb{Z},\ a' \in \mathbb{N}$) tel que $\frac{p}{10^a}\frac{p'}{10^{a'}} = 1$, ce qui revient à dire que $pp' = 10^{a+a'}$, ou encore que 2 et 5 sont les seuls diviseurs premiers de p et p'. Le résultat s'en déduit.

IV.1.54 On note $[.]$ la partie entière.

1. Soit $n \in \mathbb{N}^*$. On a $\sqrt{n^2+n} = n_0, \alpha_1\alpha_2\ldots$,
$$n_0 = [\sqrt{n^2+n}] \quad \text{et} \quad \alpha_1 = [10\sqrt{n^2+n}] - 10[\sqrt{n^2+n}].$$

De $n < \sqrt{n^2+n} < n+1$, l'on déduit $n_0 = [\sqrt{n^2+n}] = n$.

On vérifie, par ailleurs, en comparant les carrés, que : $10n+4 < 10\sqrt{n^2+n} < 10n+5$, donc $[10\sqrt{n^2+n}] = 10n+4$ et $\alpha_1 = 4$.

2. Soit $n \in \mathbb{N}^*$, $n \geqslant 5$. On a $\sqrt{n^2+2n} = m_0, \beta_1\beta_2\ldots$,

$$m_0 = [\sqrt{n^2+2n}] \quad \text{et} \quad \beta_1 = [10\sqrt{n^2+2n}] - 10[\sqrt{n^2+2n}].$$

De $n < \sqrt{n^2+2n} < n+1$, l'on déduit $m_0 = [\sqrt{n^2+2n}] = n$. On vérifie, par ailleurs, en comparant les carrés, que, si $n \geqslant 5$: $10n+9 < 10\sqrt{n^2+2n} < 10n+10$, donc :

$$[10\sqrt{n^2+2n}] = 10n+9 \qquad \text{et} \qquad \beta_1 = 9.$$

IV.1.55 1. On utilise la proposition 73 de la page 592.

2. On reprend la méthode de la solution de l'exercice 39 en utilisant l'exercice 38 de la page 581. Nous laissons les détails au lecteur.

3. Notons $L \subset \mathbb{R}$ l'ensemble des nombres de Liouville. L'application qui à une écriture décimale $u \in \mathcal{U}$ associe l'écriture décimale $x(u) \in L$ est *bijective*. L'ensemble $\mathcal{U}$ est en bijection avec $\mathbb{R}$ donc il est non-dénombrable et il en est de même de L.

IV.1.56 Rectification de l'énoncé : lire α_n au lieu de α_k.

On a, pour tout $n \geqslant k$:

$$\begin{aligned}\binom{n+10\times k!}{k} &= \frac{(n+10\times k!)(n+10\times k!-1)\ldots(n+10\times k!-k-1)}{k!}\\ &= \frac{(n+10\times k!)(n-1+10\times k!)\ldots(n-k-1+10\times k!)}{k!}\\ &= \frac{n(n-1)\ldots(n-k+1)+m\times 10\times k!}{k!}\\ &= \frac{n(n-1)\ldots(n-k+1)}{k!} + m\times 10 = \binom{n}{k} + m\times 10,\end{aligned}$$

pour un *entier* $m \in \mathbb{N}$ convenable. On en déduit, pour $n \geqslant k$, $\alpha_{n+10\times k!} = \alpha_n$. Ainsi la suite (α_n) est périodique de période $10\times k!$ à partir du rang k. Le résultat s'en déduit.

IV.1.57 L'application f est évidemment injective, donc $\operatorname{card} \mathcal{P}(\mathbb{N}^*) \leqslant \operatorname{card} J$.

On sait que $\mathcal{P}(\mathbb{N}^*)$ n'est pas dénombrable (*cf.* le théorème 1 de la page 14). Par suite J et *a fortiori* $\mathbb{R}$ ne le sont pas non plus.

IV.1.58 1. a) On a $S_2 = X^2-2$, $S_3 = X^3-3X$, $S_4 = X^4-4X^2+2$, $S_5 = X^5-5X^3+5X$, $S_6 = X^6-6X^4+9X^2-2$, $S_7 = X^7-7X^5+14X^3-7X$.

On montre par récurrence que S_n est un polynôme unitaire de degré n à coefficients entiers.

Montrons par récurrence que, pour tout $n \in \mathbb{N}$, $S_n\left(X+\frac{1}{X}\right) = X^n + \frac{1}{X^n}$. On a $S_0\left(X+\frac{1}{X}\right) = 2 = X^0 + \frac{1}{X^0}$ et $S_0\left(X+\frac{1}{X}\right) = X + \frac{1}{X} = X^1 + \frac{1}{X^1}$. Soit $n \geqslant 1$, supposons $S_n\left(X+\frac{1}{X}\right) = X^n + \frac{1}{X^n}$. On a :

$$\begin{aligned} S_{n+1}\left(X+\frac{1}{X}\right) &= \left(X+\frac{1}{X}\right) S_n\left(X+\frac{1}{X}\right) - S_{n-1}\left(X+\frac{1}{X}\right) \\ &= \left(X+\frac{1}{X}\right)\left(X^n+\frac{1}{X^n}\right) - \left(X^{n-1}+\frac{1}{X^{n-1}}\right) \\ &= X^{n+1} + \frac{1}{X^{n+1}}. \end{aligned}$$

b) La relation $S_n\left(X+\frac{1}{X}\right) = X^n + \frac{1}{X^n}$ reste vraie pour $X \in \mathbb{C}^*$.
Si $X := e^{i\theta}$, $X + \frac{1}{X} = 2\cos\theta$ et $X^n + \frac{1}{X^n} = e^{in\theta} + e^{-in\theta} = \cos n\theta$, donc :

$$S_n(2\cos\theta) = 2\cos n\theta.$$

2. Soit $P := x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$, avec $a_0, \ldots, a_{n-2}, a_{n-1} \in \mathbb{Z}$.
Soient $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ *premiers entre eux* tels que $P(p/q) = 0$. On a :

$$p^n = -q(a_{n-1}p^{n-1} + a_{n-2}qp^{n-2} + \cdots + a_0 q^n),$$

donc q divise p^n, donc p et, puisqu'il est premier avec p, $q = 1$. Ainsi $p/q = p \in \mathbb{Z}$.

3. On a $\sin\lambda\pi = \cos(\pi/2 - \lambda\pi)$. Il suffit donc de traiter le cas de $\cos\lambda\pi$. On peut supposer $\lambda \neq 0$.
Supposons que $\cos\lambda\pi \in \mathbb{Q}$. Alors $2\cos\lambda\pi \in \mathbb{Q}$ et il existe $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ *premiers entre eux* tels que $2\cos\lambda\pi \in \mathbb{Q} = p/q$. On peut écrire le rationnel λ sous la forme $2k/n$, avec $k \in \mathbb{Z}^*$ et $n \in \mathbb{N}^*$. Alors $2\cos n\lambda\pi = 2$ et l'on a $S_n(p/q) = S_n(2\cos\lambda\pi) = 2$. Par suite p/q est une racine de $P := S_n - 2$. Ce polynôme est unitaire et à coefficients entiers. Donc d'après 2, $q = 1$ et $2\cos\lambda\pi = p \in \mathbb{Z}$. Puisque $2|\cos\lambda\pi| \leqslant 2$. Les seules possibilités sont $p = 0$, $p = 1$, $p = 2$, c'est-à-dire $\cos\lambda\pi = 0$, $1/2$ ou 1.
Ainisi $\cos\lambda\pi$ est irrationnel sauf si $\lambda = 0 \mod \pi$ ou $\pm 1/3 \mod \pi$ ou $\pm 1/2 \mod \pi$.

4. Soit :

$$P := a_d x^d + a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_1 x + a_0.$$

On a $x^d P(1/x) = a_0 x^d + a_1 x^{d-1} + a_2 x^{d-2} + \cdots + a_{d-1}x + a_d$. Par suite, le polynôme P est réciproque si, et seulement si,pour tout $k \in [\![0, n]\!]$, $a_{d-k} = a_k$. Autrement dit si, en lisant à l'envers (en verlan…) le « mot » $a_d a_{d-1} \ldots a_0$ on retrouve le mot initial. Un mot possédant cette propriété est appelé un *palindrome*. Par exemple : radar, kayak, ara, ressasser, rotor ou «νίψον ανομήματα μη μόναν όψιν » (en grec ancien : *lave tes péchés et pas seulement ton visage*). Pour cette raison les polynômes réciproques sont aussi appelés *palindromiques*.
Supposons d pair : $d = 2\delta$. Pour tout $Q \in \mathbb{K}[Z]$, le polynôme $Z^\delta Q\left(Z+\frac{1}{Z}\right)$ est évidemment réciproque.
Inversement soit :

$$P := a_d x^d + a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_1 x + a_0.$$

un polynôme réciproque. On a, en utilisant $a_{d-k} = a_k$:

$$Z^{-\delta}P(Z) = a_0\left(Z^\delta + \frac{1}{Z^\delta}\right) + a_1\left(Z^{\delta-1} + \frac{1}{Z^{\delta-1}}\right) + \cdots + a_{\delta-1}\left(Z+\frac{1}{Z}\right) + a_\delta.$$

Par suite, en utilisant 1. a), on obtient :

$$Z^{-\delta}P(Z) = a_0 S_\delta \left(Z + \frac{1}{Z}\right) + a_1 S_{\delta-1}\left(Z + \frac{1}{Z}\right) + a_{\delta-1} S_1 \left(Z + \frac{1}{Z}\right) + a_\delta$$

$$= (a_0 S_\delta + a_1 S_{\delta-1} + \cdots + a_{\delta-1} S_1)\left(Z + \frac{1}{Z}\right) + a_\delta,$$

donc $P(Z) = Z^\delta Q\left(Z + \frac{1}{Z}\right)$, avec $Q = a_0 S_\delta + a_1 S_{\delta-1} + \cdots + a_{\delta-1} S_1 + a_\delta$.

Si $P := Z^4 + Z^3 + Z^2 + Z + 1$, on a $Q = S_2 + S_1 + 1 = X^2 + X - 1$.

Si $P := Z^6 + Z^5 + \cdots + Z + 1$, on a $Q = S_3 + S_2 + S_1 + 1 = X^3 + X^2 - 2X - 1$.

5. Soit $n \in \mathbb{N}^*$ impair : $n = 2\nu + 1$. Considérons $P_{2\nu} := Z^{2\nu} + Z^{2\nu-1} + \cdots + Z + 1$. On a $(Z-1)P_{2\nu} = Z^n - 1$.

Il existe un polynôme Q_ν de degré ν tel que $Z^{-\nu}P_{2\nu}(Z) = Q_\nu\left(Z + \frac{1}{Z}\right)$ et Q_ν est unitaire. Pour tout $k \in [\![1, \nu]\!]$, $\mathrm{e}^{2i\pi k/n}$ est racine de $P_{2\nu}$, donc $2\cos 2k\pi/n$ est racine de Q_ν. Les ν réels $\{2\cos 2k\pi/n\}_{k\in[\![1,\nu]\!]}$ sont deux à deux distincts, donc :

$$Q_\nu = (X - 2\cos 2\pi/n)(X - 2\cos 4\pi/n)\ldots(X - 2\cos 2\nu\pi/n).$$

C'est un polynôme à coefficients entiers. Ainsi $V_n = Q_\nu$ est un polynôme à coefficients entiers. On a donc une variante de la preuve de l'irrationalité de $\cos 2\pi/n$ faite ci-dessus en utilisant 2 et en généralisant la méthode de l'exercice IV.1.5 de la page 596 (on a $V_5(2Y) = 4Y^2 + 2Y - 1$ et $V_7(2Y) = 8Y^3 + 4Y^2 - 4Y_1$).

Soit $n \in \mathbb{N}^*$ impair : $n := 2\nu + 1$. Soit 2ξ une racine de $S_n - 2$. Considérons l'équation du second degré $x^2 - 2\xi x + 1 = 0$. Elle a toujours deux racines distinctes (si $\xi \neq 1$) ou confondues (si $\xi = 1$) dans $\mathbb{C}$. Soit $a \in \mathbb{C}$ tel que $2\xi = a + 1/a$, on a $a^n + 1/a^n = 2$, donc $a^n = 1$. Ainsi $2\xi = \omega + 1/\omega$, où ω est une racine $n^{ème}$ de l'unité. Ainsi $S_n - 2$ a exactement $\nu + 1$ racines dans $\mathbb{C}$. Elles sont réelles et égales à : 2 ou $2\cos 2k\pi/n$, avec $k \in [\![1, \nu]\!]$.

Les polynômes V_n et $\frac{S_{2\nu+1}-2}{X-2}$ ont les mêmes racines (les multiplicités pouvant différer). On vérifie : $S_5 - 2 = (X-2)V_5^2$ et $S_7 - 2 = (X-2)V_7^2$.

6. Les polynômes de Tchebychef de première espèce $\{T_n\}$ sont définis par $T_0 := 1$, $T_1 := x$ et la relation de récurrence $T_{n+1} = 2xT_n - T_{n-1}$. En comparant S_n et T_n pour $n \in [\![0, 7]\!]$, on devine la relation $S_n(X) = 2T_n(X/2)$. On la prouve facilement par récurrence.

Montrons, en utilisant les polynômes de Tchebychef de deuxième espèce $\{U_n\}$, que les ν nombres $2\cos 2k\pi/n$, avec $k \in [\![1, \nu]\!]$ sont des racines *doubles* de $S_n - 2$. Il suffit de montrer que les nombres $\cos 2k\pi/n$, avec $k \in [\![1, \nu]\!]$ sont des racines simples de $(T_n - 1)' = T_n'$. Ceci résulte de $T_n' = nU_{n-1}$ et de la factorisation des U_{n-1} (*cf.* le corollaire 48 et le théorème 49 de la page 309. On en déduit : $S_n - 2 = (X-2)V_n^2$.

7. a) Le réel $2\cos 2\pi/15$ est racine du polynôme V_{15} qui est de degré 7. Le but de la question est de chercher un polynôme à coefficients entiers *de degré plus petit* annulant $2\cos 2\pi/15$. L'idée est de remplacer $Z^{14} + Z^{13} + \cdots + Z + 1$ par le polynôme cyclotomique Φ_{15}.

On utilise la formule : $\Phi_n(X) = \prod_{d|n}(X^d - 1)^{\mu(n/d)}$, où μ est la fonction de Möbius (*cf.* page 307). Les diviseurs de 15 sont 1, 3, 5 et 15. On a $\mu(1) = 1$, $\mu(3) = -1$, $\mu(5) = -1$ et $\mu(15) = 1$, donc $\Phi_{15}(X) = \frac{(X^{15}-1)(X-1)}{(X^3-1)(X^5-1)}$.

On en déduit « facilement » $\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$ (à la main, en utilisant la division euclidienne et un peu de courage, ou avec un système de calcul formel, en utilisant une fonction de simplification des fractions rationnelles, comme **`simplify`** en *Maple*). Le polynôme Φ_{15} est réciproque et de degré 8. Il existe donc un polynôme V, de degré 4 tel que $X^{-4}\Phi_{15}(X) = V\left(X + \frac{1}{X}\right)$. En utilisant la question 4, on obtient : $V = S_4 - S_3 + S_1 - 1 = X^4 - X^3 - 4X^2 + 4X + 1$. On définit $P(Y) := V(2Y) = 16Y^4 - 8Y^3 - 16Y^2 + 8Y + 1$. C'est un polynôme de degré 4 à coefficients entiers. Le réel $2\cos 2\pi/15$ est une racine de V, donc $\cos 2\pi/15$ est une racine de P. (Les trois autres racines sont $\cos 4\pi/15$, $\cos 8\pi/15$ et $\cos 14\pi/15$.)

b) On a $\Phi_1(X) = X - 1$ qui n'est pas réciproque et $\Phi_2(X) = X + 1$ qui l'est. On utilise la définition des polynômes cyclotomiques. Pour tout $n \in \mathbb{N}^*$, on note $E_n = \{k \in [\![0, n-1]\!] \mid k \wedge n = 1\}$. On a $\operatorname{card} E_n = \varphi(n)$ (où φ est la fonction indicatrice d'Euler). On a $\Phi_n = \prod_{k \in E_n} (X - \mathrm{e}^{2ik\pi/n})$. Supposons $n > 2$.

L'application $\begin{array}{ccc} E_n & \longrightarrow & E_n \\ k & \longmapsto & n-k \end{array}$ est une bijection et $n - k \neq k$ (puisque $k \wedge n = 1$). On en déduit que $\operatorname{card} E_n = \varphi(n)$ est pair puis, en regroupant les racines en $\frac{\varphi(n)}{2}$ paires $\left(\mathrm{e}^{2ik\pi/n}, \mathrm{e}^{2i(n-k)\pi/n}\right)$ et en utilisant $\mathrm{e}^{-2ik\pi/n} = \mathrm{e}^{2i(n-k)\pi/n}$, que $\prod_{k \in E_n} \mathrm{e}^{2ik\pi/n} = 1$ (ce qui équivaut à $\Phi_n(0) = 1$). On a, pour tout $X \in \mathbb{C}^*$:

$$\begin{aligned} X^{\varphi(n)}\Phi_n\left(\frac{1}{X}\right) &= \prod_{k \in E_n} X\left(\frac{1}{X} - \mathrm{e}^{2ik\pi/n}\right) = \prod_{k \in E_n} \left(1 - \mathrm{e}^{2ik\pi/n} X\right) \\ &= (-1)^{\varphi(n)} \prod_{k \in E_n} \left(1 - \mathrm{e}^{2ik\pi/n} X\right) = \prod_{k \in E_n} \left(\mathrm{e}^{2ik\pi/n} X - 1\right) \\ &= \prod_{k \in E_n} \mathrm{e}^{2i\pi k/n} \prod_{k \in E_n} \left(X - \mathrm{e}^{-2i\pi k/n}\right) = \prod_{k \in E_n} \left(X - \mathrm{e}^{-2i\pi k/n}\right) \\ &= \prod_{k \in E_n} \left(X - \mathrm{e}^{2i\pi(n-k)/n}\right) = \prod_{k \in E_n} \left(X - \mathrm{e}^{2i\pi k/n}\right) = \Phi_n(X). \end{aligned}$$

Ainsi, pour $n \in \mathbb{N}$, $n \geqslant 2$, le polynôme Φ_n est réciproque.

Variante On peut aussi montrer que les polynômes Φ_n et $X^{\varphi(n)}\Phi_n(1/X)$ ont les mêmes racines dans $\mathbb{C}$ (elles sont toutes simples) et qu'ils sont tous les deux unitaires ($\Phi_n(0) = 1$). Ils sont donc égaux.

IV.1.59 La preuve de l'irrationalité de π^2 proposée dans l'exercice est inspirée par un article de Ivan Niven (1947).

1. Pour $m \in [\![1, 10]\!]$, on calcule $\int_0^\pi x^m \sin x \, \mathrm{d}x$ par récurrence en utilisant des intégrations par parties. On obtient :

   $I_2 = 12 - \pi^2$, $I_3 = 120 - \pi^2$, $I_4 = 1680 - 180\pi^2 + \pi^4$, $I_5 = 30240 - 3360\pi^2 + 30\pi^4$.

   La fonction intégrée est *strictement* positive sur $]0, \pi[$ donc $I_n > 0$. Par ailleurs, pour $0 \leqslant x \leqslant \pi$, $0 \leqslant x^n(\pi - x)^n \sin x \leqslant \pi^{2n}$, donc $I_n \leqslant \frac{\pi^{2n+1}}{2n!} < \frac{\pi^{2n+1}}{n!}$.

2. On obtient (pour tout polynôme f) par deux intégrations par parties :

$$\begin{aligned}\int_0^\pi f(x)\sin x\,\mathrm{d}x &= [-f(x)\cos x]_0^\pi + \int_0^\pi f'(x)\cos x\,\mathrm{d}x\\ &= f(\pi)+f(0)+[f'(x)\sin x]_0^\pi - \int_0^\pi f''(x)\sin x\,\mathrm{d}x\\ &= f(\pi)+f(0)-\int_0^\pi f''(x)\sin x\,\mathrm{d}x,\end{aligned}$$

En remplaçant f par $-f''$, on obtient :

$$-\int_0^\pi f''(x)\sin x\,\mathrm{d}x = -f''(\pi)-f''(0)+\int_0^\pi f^{(4)}(x)\sin x\,\mathrm{d}x$$

et l'on poursuit par récurrence. On obtient, en utilisant $\deg f = 2n$:

$$\begin{aligned}\int_0^\pi f(x)\sin x\,\mathrm{d}x = f(\pi)+f(0)-f''(\pi)-f''(0)+f^{(4)}(\pi)+f^{(4)}(0)-\cdots\\ \cdots+(-1)^n\left(f^{2n}(\pi)+f^{2n}(0)\right).\end{aligned}$$

La fonction f est invariante par $x\mapsto \pi-x$. On en déduit $f^{2k}(\pi)=f^{2k}(0)$, pour tout $k\in\mathbb{N}$. Donc

$$\int_0^\pi f(x)\sin x\,\mathrm{d}x = 2f(0)-2f''(0)+2f^{(4)}(0)-\cdots+(-1)^n 2f^{2n}(0). \tag{43}$$

Le polynôme f est de degré $2n$, donc, pour tout $k>2n$, $f^{(k)}(0)=0$.

C'est aussi un multiple de x^n, donc, pour tout $k<n$, $f^{(k)}(0)=0$. Pour $n\leqslant k\leqslant 2n$, on développe $(\pi-x)^n$ en utilisant la formule du binôme et l'on obtient :

$$f(x)=x^n(\pi-x)^n=\sum_{h=0}^{n}\binom{n}{h}(-1)^{n-h}\pi^h x^{2n-h}. \tag{44}$$

D'après la formule de Taylor pour les polynômes :

$$f(x)=\sum_{k=0}^{2n}\frac{f^{(k)}(0)}{k!}x^k.$$

Supposons $n\leqslant k\leqslant 2n$. Dans (44) le monôme en x^k apparaît pour $h=2n-k$. Ainsi, en égalant les coefficients de x^k dans les deux écritures, on obtient :

$$\frac{f^{(k)}(0)}{k!}=\binom{n}{h}(-1)^{n-h}\pi^h=\binom{n}{2n-k}(-1)^{k-n}\pi^{2n-k}=\binom{n}{k-n}(-1)^{k-n}\pi^{2n-k}.$$

Ainsi :

$$f^{(k)}(0)=k!\binom{n}{k-n}(-1)^{k-n}\pi^{2n-k}=k!a_{n,k}\pi^{2n-k},$$

avec $a_{n,k}:=(-1)^{k-n}\binom{n}{k-n}\in\mathbb{N}$.

Par suite $\frac{1}{n!}f^{(k)}(0)=\frac{k!}{n!}a_{n,k}\pi^{2n-k}$, avec $\frac{k!}{n!}a_{n,k}\in\mathbb{Z}$. Dans (43) n'interviennent que les dérivées *d'ordre pair* en 0 de f. On en déduit $I_n\in\mathbb{Z}[\pi^2]$ et que son « degré » est au plus $\frac{n}{2}$ si n est pair et au plus $\frac{n-1}{2}$ si n est impair, c'est-à-dire au plus $E[n/2]$ dans les deux cas.

3. Montrons que π^2 est irrationnel (on en déduira immédiatement que π est irrationnel). On raisonne par l'absurde. On suppose que $\pi^2 = p/q$, où p et q sont des entiers strictement positifs. Puisque $I_n \in \mathbb{Z}[\pi^2]$ et est de « degré » au plus $n' := E[n/2] \leqslant n$, pour tout $n \in \mathbb{N}$, $I_n \in \mathbb{Q}$ et est de la forme $m/q^{n'}$, avec $m \in \mathbb{Z}$. De $I_n > 0$, on déduit $m \in \mathbb{N}^*$ et $I_n = m/q^{n'} \geqslant 1/q^{n'} \geqslant 1/q^n$. En utilisant $I_n \leqslant \frac{\pi^{2n+1}}{n!}$, on obtient $\frac{1}{q^n} \leqslant \frac{\pi^{2n+1}}{n!}$, pour tout $n \in \mathbb{N}^*$. En d'autres termes $n! \leqslant q^n \pi^{2n+1} = \pi(q\pi^2)^n$. Cette égalité est fausse pour n assez grand ($\lim\limits_{n\to\infty} n!\,(q\pi^2)^{-n} = 0$) et l'on aboutit à une contradiction.
4. Soit $a = r/s \in \mathbb{Q}^*$ fixé ($r \in \mathbb{Z}$ et $s \in \mathbb{N}^*$). On peut supposer $a > 0$ (c'est-à-dire $r > 0$). En effet $\mathrm{e}^{-a} = 1/e^a$ est irrationnel si, et seulement si, e^a l'est.

   Pour tout $n \in \mathbb{N}^*$, on définit $J_n := \frac{1}{n!} \displaystyle\int_0^a x^n (a-x)^n \mathrm{e}^x \,\mathrm{d}x$.

   On note $g(x) := x^n(a-x)^n$. On obtient (pour tout polynôme g) par intégration par parties :

$$\int_0^a g(x)\mathrm{e}^x \,\mathrm{d}x = [g(x)e^x]_0^a - \int_0^\pi f'(x)\mathrm{e}^x \,\mathrm{d}x = g(a)e^a - g(0) - \int_0^\pi f'(x)\mathrm{e}^x \,\mathrm{d}x.$$

   En remplaçant g par $-g'$, on obtient :

$$\int_0^a g(x)\mathrm{e}^x \,\mathrm{d}x = g(a)e^a - g(0) - (g'(a)e^a - g'(0)) + \int_0^\pi f''(x)\mathrm{e}^x \,\mathrm{d}x,$$

   puis, par récurrence :

$$\int_0^a g(x)\mathrm{e}^x \,\mathrm{d}x = \sum_{k=0}^{2n} (-1)^k \left(g^{(k)}(a)e^a - g^{(k)}(0)\right).$$

   On a $g(a-x) = g(x)$, donc, pour tout $k \in \mathbb{N}$, $g^{(k)}(a) = (-1)^k g^{(k)}(0)$. On en déduit :

$$\int_0^a g(x)\mathrm{e}^x \,\mathrm{d}x = \sum_{k=0}^{2n} (-1)^k \left(g^{(k)}(a)e^a - g^{(k)}(0)\right) = \sum_{k=0}^{2n} g^{(k)}(0)\left(\mathrm{e}^a + (-1)^{k+1}\right).$$

   On a, pour tout $k > 2n$ et tout $k < n$, $g^{(k)}(0) = 0$ et, en raisonnant comme plus haut en remplaçant π par a, pour tout $k \in [\![n, 2n]\!]$:

$$g^{(k)}(0) = k! \binom{n}{k-n} (-1)^{k-n} a^{2n-k},$$

   Donc, puisque $\frac{k!}{n!} s^n a^{2n-k} \in \mathbb{N}$, $\frac{s^n}{n!} g^{(k)}(0) \in \mathbb{Z}$. On en déduit que, pour tout $n \in \mathbb{N}$, $s^n J_n \in \mathbb{Z}\mathrm{e}^a + \mathbb{Z}$; autrement dit qu'il existe $\alpha_n, \beta_n \in \mathbb{Z}$ tels que $s^n J_n = \alpha_n \mathrm{e}^a + \beta_n$.

   On a, pour tout $n \in \mathbb{N}$, $s^n J_n \leqslant \frac{1}{n!} s^n a^{2n+1} \mathrm{e}^a = a\mathrm{e}^a \frac{(sa^2)^n}{n!}$, donc $s^n J_n$ tend vers 0 quand n tend vers $+\infty$.

   On a, par ailleurs $J_n > 0$.

   Montrons que e^a est irrationnel. On raisonne par l'absurde. On suppose que $e^a = p/q$, avec $p \in \mathbb{N}$ et $q \in \mathbb{N}^*$. On a, pour tout $n \in \mathbb{N}$, $qs^n J_n \in \mathbb{Z}$ et, puisque $qs^n J_n > 0$, on a $qs^n J_n \geqslant 1$, ce qui contredit $\lim\limits_{n\to+\infty} qs^n J_n = 0$.

   Soit $b \in \mathbb{Q}_+^* \setminus \{1\}$. Pour montrer que $\ln b$ est irrationnel, on raisonne par l'absurde. On suppose que $a := \ln b \in \mathbb{Q}$, alors, d'après ce qui précède, $\mathrm{e}^a = e^{\ln b} = b$ est irrationnel, ce qui contredit l'hypothèse.

Remarque. On peut montrer que π est transcendant (Lindemann 1882). On en déduit que, pour tout $n \in \mathbb{N}$, π^n est transcendant. *A fortiori* π^n est irrationnel.

IV.1.60 L'exercice reprend la méthode originale utilisée par Johann Faulhaber (dans *Academia Algebrae* 1631[4]) et Jakob Bernoulli (dans *Ars conjectandi* 1713).

1. a) On écrit les onze premières lignes du triangle de Pascal :

1										
1	1									
1	2	1								
1	3	3	1							
1	4	6	4	1						
1	5	10	10	5	1					
1	6	15	20	15	6	1				
1	7	21	35	35	21	7	1			
1	8	28	56	70	56	28	8	1		
1	9	36	84	126	126	84	36	9	1	
1	10	45	120	210	252	210	120	45	10	1

Pour $p \in \mathbb{N}^*$, dans la $p^{ème}$ colonne figurent les $\binom{m}{p-1}$ $(m < p,\ m \in [\![1, 11]\!])$.

b) Nous avons déjà fait les calculs jusqu'à $k = 4$. On poursuit sans difficulté (moyennant un peu de courage comme les anciens ou un calculateur formel) et l'on obtient :

$$2S_1(n) = n^2 + n$$
$$3S_2(n) = n^3 + \frac{3}{2}n^2 + \frac{1}{2}n$$
$$4S_3(n) = n^4 + 2n^3 + n^2$$
$$5S_4(n) = n^5 + \frac{5}{2}n^4 + \frac{5}{3}n^3 - \frac{1}{6}n$$
$$6S_5(n) = n^6 + 3n^5 + \frac{5}{2}n^4 - \frac{1}{12}n^2$$
$$7S_6(n) = n^7 + \frac{7}{2}n^6 + \frac{7}{2}n^5 - \frac{7}{6}n^3 + \frac{1}{6}n$$
$$8S_7(n) = n^8 + 4n^7 + \frac{14}{3}n^6 - \frac{7}{3}n^4 + \frac{2}{3}n^2$$
$$9S_8(n) = n^9 + \frac{9}{2}n^8 + 6n^7 - \frac{21}{5}n^5 + 2n^3 - \frac{3}{10}n$$
$$10S_9(n) = n^{10} + 5n^9 + \frac{15}{2}n^8 - 7n^6 + 5n^4 - \frac{3}{2}n^2$$
$$11S_{10}(n) = n^{11} + \frac{11}{2}n^{10} + \frac{55}{6}n^9 - 11n^7 + 11n^5 - \frac{11}{2}n^3 + \frac{5}{6}n.$$

On constate que, pour $k \in [\![0, 10]\!]$, le coefficient de n^{k+1} est 1 et que celui de n^k est $\frac{k+1}{2}$, c'est-à-dire que : $(k+1)S_k(n) = n^{k+1} + \frac{k+1}{2}n^k + \cdots$.

[4] *Darinnen die miraculosische Inventiones...*

c) Pour $k \in [\![2, 10]\!]$, la liste des coefficients de n^{k-1} est :

$$\frac{1}{2},\ 1,\ \frac{5}{3},\ \frac{5}{2},\ \frac{7}{2},\ \frac{14}{3},\ 6,\ \frac{15}{2},\ \frac{55}{6}.$$

Le plus petit dénominateur commun de ces fractions est 6. En multipliant par 6 on obtient :

$$3,\ 6,\ 10,\ 15,\ 21,\ 28,\ 36,\ 45.$$

Ces nombres figurent dans la *troisième* colonne du triangle de Pascal, par suite, pour $k \in [\![2, 10]\!]$:

$$(k+1)S_k(n) = n^{k+1} + \frac{k+1}{2}n^k + \frac{1}{6}\binom{k+1}{2}n^{k-1} + \cdots$$

d) Pour $k \in [\![3, 10]\!]$, le coefficient de n^{k-2} dans $(k+1)S_k(n)$ est nul.

Pour $k \in [\![5, 10]\!]$, le coefficient de n^{k-4} dans $(k+1)S_k(n)$ est également nul.

Pour $k \in [\![4, 10]\!]$, la liste des coefficients de n^{k-3} est :

$$-\frac{1}{6},\ -\frac{1}{2},\ -\frac{7}{6},\ -\frac{7}{3},\ -\frac{21}{5},\ -7.$$

Le plus petit dénominateur commun de ces fractions est 30. En multipliant par -30 on obtient :

$$5,\ 15,\ 35,\ 70,\ 126,\ 210.$$

Ces nombres figurent dans la *cinquième* colonne du triangle de Pascal, par suite, pour $k \in [\![4, 10]\!]$:

$$(k+1)S_k(n) = n^{k+1} + \frac{1}{2}\binom{k+1}{1}n^k + \frac{1}{6}\binom{k+1}{2}n^{k-1} - \frac{1}{30}\binom{k+1}{4}n^{k-3} + \cdots$$

Pour $k \in [\![6, 10]\!]$, la liste des coefficients de n^{k-5} est :

$$\frac{1}{6},\ \frac{2}{3},\ 2,\ 5.$$

Le plus petit dénominateur commun de ces fractions est 42. En multipliant par 42 on obtient :

$$7,\ 28,\ 84,\ 210.$$

Ces nombres figurent dans la *septième* colonne du triangle de Pascal, par suite, pour $k \in [\![6, 10]\!]$:

$$(k+1)S_k(n) = n^{k+1} + \frac{1}{2}\binom{k+1}{1}n^k + \frac{1}{6}\binom{k+1}{2}n^{k-1} - \frac{1}{30}\binom{k+1}{4}n^{k-3} + \frac{1}{42}\binom{k+1}{6}n^{k-5} + \cdots$$

On complète les résultats précédents en vérifiant que :

$$\forall k \in [\![0, 10]\!], \quad (k+1)S_k(n) = \sum_{p=0}^{k}\binom{k+1}{p}f_p n^{k-p+1},$$

On a, pour tout $k \in [\![0, 10]\!]$, $S_k(1) = 1$, donc, en faisant $n = 1$ dans la formule ci-dessus, on obtient :

$$\forall k \in [\![0, 10]\!], \quad k+1 = \sum_{p=0}^{k}\binom{k+1}{p}f_p.$$

Ces formules permettent, pour $k \in [\![1, 10]\!]$, de retrouver les f_k par récurrence à partir de $f_0 = 1$.

2. L'égalité (18) a déjà été écrite dans la question précédente pour $k \in [\![0, 10]\!]$. Elle permet de déterminer les $\{f_n\}_{n\in\mathbb{N}}$ par récurrence à partir de $f_0 := 1$.

   On a $k+1 = \binom{k+1}{1}$ et $f_1 = 1/2$, par suite l'égalité :

$$k+1 = f_0\binom{k+1}{0} + f_1\binom{k+1}{1} + f_2\binom{k+1}{2} + \cdots + f_k\binom{k+1}{k}$$

   est équivalente à la suivante :

$$0 = f_0\binom{k+1}{0} - f_1\binom{k+1}{1} + f_2\binom{k+1}{2} + \cdots f_k\binom{k+1}{k}$$

   Notons $a_n := f_n$ pour tout $n \neq 1$, et $a_1 := -f_1$. On a :

$$a_0 = 1 \quad \text{et} \quad \forall m \geqslant 2, \quad \sum_{p=0}^{m-1} \binom{m}{p} a_p = 0,$$

   En comparant avec la formule de récurrence pour les nombres $(b_n)_{n\in\mathbb{N}}$ de l'exercice 11 de la page 878 (*cf.* (28)) :

$$b_0 := 1 \quad \text{et} \quad \forall m \geqslant 2, \quad \sum_{p=0}^{m-1} \binom{m}{p} b_p = 0, \tag{45}$$

   on en déduit que, pour tout $n \in \mathbb{N}$, $a_n = b_n$. Par suite, on a :

   - pour tout $p \geqslant 1$, $f_{2p+1} = b_{2p+1} = 0$;
   - pour tout $p \geqslant 1$, $f_{2p} = b_{2p} = (-1)^{p+1} B_p$;
   - $f_1 = -b_1$.

   On a, par suite, pour tout $n \in \mathbb{N}$, $f_n = (-1)^n b_n$. Ainsi la seconde égalité de (45) peut s'écrire :

$$\sum_{p=0}^{m-1} (-1)^p \binom{m}{p} f_p = 0. \tag{46}$$

3. On a : $\binom{n}{a}\binom{n-a}{b} = \frac{n!}{(n-a)!a!}\frac{(n-a)!}{(n-a-b)!b!} = \frac{n!}{(n-a-b)!a!b!} = \frac{n!}{(n-b)!b!}\frac{(n-b)!}{(n-a-b)!a!} = \binom{n}{b}\binom{n-b}{a}$.

4. b) a) On, pour tout $k \in [\![0, 10]\!]$, $(k+1)S_k(n) = \Phi_k(n)$, ce qui justifie l'introduction de $\Phi_k(x)$.
   D'après la question 2 de l'exercice IV.1.25, on en déduit $\Delta(\Phi_k(x)) = (k+1)x^k$, pour tout $k \in [\![0, 10]\!]$.
   b) Calculons $\Delta(\Phi_k(x))$, pour tout $k \in \mathbb{N}$. Il faut du courage et un peu d'ingénio-

sité ! On a :

$$\begin{aligned}
\Delta\left(\Phi_k(n)\right) = \Phi_k(n) - \Phi_k(n-1) &= \sum_{p=0}^{k} \binom{k+1}{p} f_p \left(n^{k-p+1} - (n-1)^{k-p+1}\right) \\
&= \sum_{p=0}^{k} \binom{k+1}{p} f_p \left(n^{k-p+1} - \sum_{i=0}^{k-p+1} \binom{k-p+1}{i} n^i (-1)^{k-p+1-i}\right) \\
&= \sum_{p=0}^{k} \binom{k+1}{p} f_p \sum_{i=0}^{k-p} \binom{k-p+1}{i} n^i (-1)^{k-p-i} \\
&= \sum_{0 \leqslant p,i;i+p \leqslant k} (-1)^{k-p-i} \binom{k+1}{p} \binom{k-p+1}{i} f_p n^i \\
&= \sum_{0 \leqslant p,i;i+p \leqslant k} (-1)^{k-p-i} \binom{k+1}{i} \binom{k-i+1}{p} f_p n^i \\
&= \sum_{i=0}^{k} (-1)^{k-i} \binom{k+1}{i} \left(\sum_{p=0}^{k-i} (-1)^p \binom{k-i+1}{p} f_p\right) n^i \\
&= \binom{k+1}{k} n^k = (k+1) n^k.
\end{aligned}$$

Pour passer de la première à la deuxième ligne, on utilise la formule du binôme. Pour passer de la quatrième à la cinquième ligne, on utilise la question 3. Pour passer de la sixième à la septième ligne, on utilise (46) avec $m := k - i + 1$, $i < k$:

$$\sum_{p=0}^{k-i} (-1)^p \binom{k-i+1}{p} f_p = 0.$$

On a $\Delta\left(\frac{\Phi_k}{k+1}\right) = x^k$ et $\Phi_k(0) = 0$, donc, en utilisant l'exercice IV.1.25 :

$$S_k(n) = \frac{\Phi_k(n)}{k+1}.$$

Remarque. Si l'on connaît les polynômes de Bernoulli (et leurs principales propriétés), on peut les utiliser pour prouver la formule de Faulhaber.

IV.1.61 1. a) On a $u_0, u_1 \in \mathbb{Q}$ et l'on montre par récurrence que $u_n \in \mathbb{Q}$ pour tout $n \in \mathbb{N}$. La suite (u_n) ne peut pas tendre vers 0. Si elle tend vers $\ell \in \mathbb{R}^*$, on a :

$$\ell = 111 - \frac{1130}{\ell} + \frac{3000}{\ell^2} \qquad \text{c'est-à-dire} \qquad \ell^3 - 111\ell^2 + 1130\ell - 3000 = 0.$$

On « trouve » que cette équation du troisième degré admet les racines $\ell = 5$, $\ell = 6$ et $\ell = 100$. Par exemple, avec *Maple*, on peut utiliser

```
solve(111x^2-1130x+3000=x^3,x)
```

qui retourne `[100,6,5]` et vérifier que ces valeurs conviennent.

b) On peut, pour faciliter les comparaisons, faire tous les calculs avec un même programme et, selon les cas, entrer les conditions initiales en valeurs flottantes (calcul numérique) ou fractionnaires (calcul exact). Dans le premier cas le programme est exécuté en flottants et dans le second exactement.

Voici un programme en *Maple*. On définit :

```
f:(x,y) -> 111-1130/x+3000/x*y
```

puis une procédure :

```
suite :=proc(a,b,n)
    local u0, u1, t, k, r;
    u0:=a; v1:=b;
    for k to n-1 do
        t:=u1; u1:=f(u0,u1);u0:=t
        od;
    r:=u1; r
    end~proc
```

Ce programme donne, pour $n \in \mathbb{N}^*$, $u_n = suite(a, b, n)$ en fonction de $u_0 := a$, $u_1 := b$ et de n. Le lecteur pourra facilement l'adapter à son système préféré de calcul formel. Les exemples numériques donnés plus loin ont été obtenus avec ce programme sur un MacBook Pro. Pour des conditions initiales en flottants, on utilise une notation avec une virgule ou **a:=evalf(.)** et **b:=evalf(.)**. Pour évaluer des résultats exacts obtenus sous forme fractionnaire, on utilise **evalf(suite(a,b,n))**.

- Quand on calcule *numériquement* une vingtaine de termes de la suite (u_n) on observe un comportement assez similaire *quelle que soit la machine utilisée* : la suite croit d'abord lentement, puis elle « se promène un peu erratiquement » et ensuite elle semble converger *rapidement* vers 100 (à partir du $10^{ème}$ terme sur notre machine).
  Dans le détail les résultats dépendent du nombre de chiffres (ou de bits) utilisés par la calculette ou la machine.
  Nous avons obtenu pour le $15^{ème}$ terme u_{15} :
  $$\texttt{suite(evalf(11/2),evalf(61/11),15)} = 100{,}0000084.$$
- Si l'on calcule *formellement*, les résultats sont *indépendants de la machine utilisée*. Apparemment la suite est croissante et converge *assez lentement* vers 6. Les valeurs sont d'abord très proches des valeurs numériques obtenues ci-dessus numériquement, puis elles s'en écartent (à partir du $7^{ème}$ terme sur notre machine).
  Nous avons obtenu pour *l'évaluation en flottant* du $23^{ème}$ terme u_{23} calculé *exactement* :
  $$\texttt{evalf(suite(11/2,61/11,23)} = 5{,}985129531,$$
  et, pour le $30^{ème}$ terme : $5{,}995804952$.
- On calcule *formellement* la suite, mais avec un « très petit » changement de la valeur initiale : u_0 est inchangé, mais $u_1 := 61/11$ est remplacé par une valeur décimale approchée (à 6×10^{-21} près). Les résultats sont *indépendants de la machine utilisée* et la suite semble converger vers 100.
  Nous avons obtenu pour le $23^{ème}$ terme u_{23} :
  $$\texttt{evalf(suite(11/2,5545454545454545454/10\^{}20,23)} = 100{,}0011217.$$

c) Si $u_0 := 6$ et $u_1 := 6$, la suite u_n est *constante* : pour tout $n \in \mathbb{N}$, $u_n = 6$.
- Quand on calcule *numériquement* une vingtaine termes de la nouvelle suite (u_n)

ainsi définie, le résultat est *fort surprenant* : quelle que soit la machine ou la calculette utilisée, la suite semble tendre vers 100.

Nous avons obtenu pour le $12^{ème}$ terme u_{12} :

suite(6.,6.,12)=suite(evalf(6),evalf(6),12) $= 100{,}0868871.$

On comparera avec **suite(6,6,12)** $= 6\ldots$

- Quand on calcule *formellement* les termes (u_n), on trouve toujours (sans surprise !) $u_n = 6$.
- Quand on calcule *formellement* la suite $(\tilde{u}_n)$ définie par les conditions initiales $\tilde{u}_0 = 6$ et $\tilde{u}_1 := 6000000000003 \times 10^{-12}$, la suite semble converger vers 100.

  Nous avons obtenu pour le $19^{ème}$ terme $\tilde{u}_{19}$:

  evalf(suite(6,6000000000003/10^12,20) $= 99{,}99999998.$

  Notons que, si l'on commence par $u_0 = u_1 = 6$ et si, en calculant avec 14 chiffres significatifs, on arrondit u_2, on obtient $6{,}000000000003$, ce qui nous ramène au cas ci-dessus, avec un décalage d'indices de 1.
- Si $u_0 := 5$ et $u_1 := 5$, la suite u_n est *constante*. Quand on calcule à partir de ces valeurs initiales, les résultats numériques et formels *coïncident* :

  suite(5.,5.,n) $=$ **suite(5,5,n)** $= 5.$

d) On peut faire quelques hypothèses pour expliquer les résultats observés ci-dessus. Elles seront confirmées par les réponses aux questions suivantes qui permettront une approche *rigoureuse*.

On peut penser que la limite de la suite (u_n) est 6. Si l'on considère les résultats purement numériques, on peut penser qu'il y a une accumulation des erreurs d'arrondi conduisant à un résultat aberrant. En fait ce n'est pas le cas. Le troisième calcul effectué de façon exacte, pour $n \geqslant 2$, à partir de la première erreur d'arrondi pour u_1, c'est-à-dire en remplaçant la fraction $61/11$ par la fraction décimale $5545454545454545454/10^{20}$, permet de penser que l'on est en fait dans un cas de *grande sensibilité aux conditions initiales* : si $u_0 := 11/2$ et $u_1 := 61/11$ la suite converge vers 6, mais si, sans changer u_0, on remplace u_1 par une valeur très voisine, mais différente (par exemple de 10^{-20}), la suite converge vers 100. Ceci est confirmé si l'on considère le cas $u_0 = u_1 = 6$, puis si l'on remplace $u_1 := 6$ par $\tilde{u}_1 := 6000000000003/10^{12}$.

Par contre, si $u_0 = u_1 = 5$, on a :

$$u_2 = 111 - \frac{1130}{u_1} + \frac{3000}{u_0 u_1} = 111 - \frac{1130}{5} + \frac{3000}{25} = 111 - 226 + 120 = 5.$$

Dans ce cas, les calculs formels et numériques coïncident car, contrairement à ce qui se passe dans le cas précédent, les divisions « tombent juste ». Dans les deux cas, on trouve donc une suite constante.

e) Montrons que, pour tout $n \in \mathbb{N}$, $u_n = \frac{5^{n+1}+6^{n+1}}{5^n+6^n}$. On procède par récurrence. On a $u_0 = \frac{11}{2} = \frac{5+6}{1+1}$ et $u_1 = \frac{61}{11} = \frac{5^2+6^2}{5+6}$. Supposons la formule vraie pour $n \geqslant 1$ et montrons la pour $n+1$.

On a :

$$\begin{aligned} u_{n+1} &= 111 - 1130\frac{5^n+6^n}{5^{n+1}+6^{n+1}} + 3000\frac{5^{n-1}+6^{n-1}}{5^{n+1}+6^{n+1}} \\ &= \frac{111(5^{n+1}+6^{n+1}) - 1130(5^n+6^n) + 3000(5^{n-1}+6^{n-1})}{5^{n+1}+6^{n+1}}. \end{aligned}$$

On a vu que :

$5^3 - 111 \times 5^2 + 1130 \times 5 - 3000 = 0 \quad$ et $\quad 6^3 - 111 \times 6^2 + 1130 \times 6 - 3000 = 0,$

donc :

$$5^{n+2} = 111 \times 5^{n+1} + 1130 \times 5^n - 3000 \times 5^{n-1}$$
$$6^{n+2} = 111 \times 6^{n+1} + 1130 \times 6^n - 3000 \times 6^{n-1}.$$

On en déduit $u_{n+1} = \dfrac{5^{n+2} + 6^{n+2}}{5^{n+1} + 6^{n+1}}$.

Le lecteur peut légitimement se demander comment l'on a pu deviner la formule que nous venons d'établir. Il le comprendra un peu plus loin… (on peut aussi utiliser la question 4 de l'exercice IV.1.43, en remarquant : $\frac{61}{11} = 11 - \frac{30}{11/2}$).

Puisque, pour tout $n \in \mathbb{N}$, $5^n + 6^n > 0$, la suite u_n est bien définie.

On peut écrire $u_n = \dfrac{5^{n+1} + 6^{n+1}}{5^n + 6^n} = 6\,\dfrac{(5/6)^{n+1} + 1}{(5/6)^n + 1}$.

Quand n tend vers $+\infty$, $(5/6)^n$ tend vers 0, donc u_n tend vers 6.

2. a) Soit (w_n) une suite réelle dont tous les termes sont non nuls. On suppose que la suite définie par $(v_n := w_{n+1}/w_n)$, pour $n \in \mathbb{N}$, vérifie la récurrence (19). Alors :

$$\frac{w_{n+3}}{w_{n+2}} = 111 - \frac{1130 w_{n+1}}{w_{n+2}} + \frac{3000 w_n}{w_{n+2}},$$

donc :

$$w_{n+3} = 111 w_{n+2} - 1130 w_{n+1} + 3000 w_n.$$

Inversement, si une suite (w_n), dont tous les termes sont non nuls, vérifie la récurrence linéaire $w_{n+3} = 111 w_{n+2} - 1130 w_{n+1} + 3000 w_n$, on obtient, en divisant par w_{n+2} :

$$\frac{w_{n+3}}{w_{n+2}} = 111 - \frac{1130 w_{n+1}}{w_{n+2}} + \frac{3000 w_n}{w_{n+2}},$$

et, en posant, pour $n \geqslant 1$, $v_n := w_{n+1}/w_n$:

$$v_{n+2} = 111 - \frac{1130}{v_{n+1}} + \frac{3000}{v_n v_{n+1}}.$$

b) On vérifie facilement que l'ensemble E des suites solutions de la récurrence (20) est un sous-espace vectoriel de l'espace des suites réelles et que l'application

$$\begin{array}{ccc} \mathbb{R}^3 & \longrightarrow & E \\ (w_0, w_1, w_2) & \longmapsto & (w_n) \end{array}$$

est injective et surjective. Par suite E est *de dimension* 3.

La suite (ρ^n) appartient à E si, et seulement si, pour tout $n \in \mathbb{N}$:

$$\rho^{n+3} = 111 \rho^{n+2} - 1130 \rho^{n+1} + 3000 \rho^n,$$

c'est-à-dire si, et seulement si, $\rho^3 = 111\rho^2 - 1130\rho + 3000$.

Par suite $\rho = 5$ ou $\rho = 6$ ou $\rho = 100$.

Montrons que les trois suites (5^n), (6^n) et (100^n) forment un système *libre* de E. Il suffit de montrer que les trois vecteurs $(1, 5, 5^2)$, $(1, 6, 6^2)$ et $(1, 100, 100^2)$ forment un système libre de $\mathbb{R}^3$. Un calcul simple, laissé au lecteur (qui peut aussi utiliser les

déterminants de Vandermonde) montre que $\begin{vmatrix} 1 & 1 & 1 \\ 5 & 6 & 100 \\ 5^2 & 6^2 & 100^2 \end{vmatrix} = 8930 \neq 0$, d'où le résultat.

Par conséquent, les 3 suites (5^n), (6^n) et (100^n) forment une base de E et tout élément de E s'écrit de façon unique $(w_n) = \lambda_1(5^n) + \lambda_2(6^n) + \lambda_3(100^n)$, avec $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$.

c) Soient $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$. D'après la question précédente, si, pour tout $n \in \mathbb{N}$, $\lambda_1(5^n) + \lambda_2(6^n) + \lambda_3(100^n) \neq 0$, alors $v_n := \dfrac{\lambda_1 5^{n+1} + \lambda_2 6^{n+1} + \lambda_3 100^{n+1}}{\lambda_1 5^n + \lambda_2 6^n + \lambda_3 100^n}$ ne s'annule jamais et la suite (v_n) vérifie la récurrence (19). Notons que v_n ne change pas si l'on multiplie $(\lambda_1, \lambda_2, \lambda_3)$ par un même réel non nul. On peut donc choisir $w_0 := \lambda_1 + \lambda_2 + \lambda_3 = 1$. Alors $w_1 = v_0$ et $w_2 = v_1 w_1 = v_1 v_0$.

Inversement, supposons que la suite (v_n) vérifie la récurrence (19) (ce qui sous-entend, en particulier, que, pour tout $n \in \mathbb{N}$, $v_n \neq 0$). On cherche $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ tels que :

$$5\lambda_1 + 6\lambda_2 + 10\lambda_3 = v_0 \quad \text{et} \quad 5^2\lambda_1 + 6^2\lambda_2 + 100^2\lambda_3 = v_1.$$

Les λ_i ne sont pas tous nuls ($v_0 \neq 0$). À un coefficient de proportionnalité près, on peut supposer de plus $\lambda_1 + \lambda_2 + \lambda_3 = 1$ et l'on trouve une solution unique.

En utilisant $v_n \neq 0$, on montre par récurrence que :

$$\lambda_1 5^n + \lambda_2 6^n + \lambda_3 100^n \neq 0 \quad \text{et} \quad v_n = \frac{\lambda_1 5^{n+1} + \lambda_2 6^{n+1} + \lambda_3 100^{n+1}}{\lambda_1 5^n + \lambda_2 6^n + \lambda_3 100^n}.$$

Si $\lambda_3 \neq 0$, on écrit :

$$v_n = 100\,\frac{\lambda_1(5/100)^{n+1} + \lambda_2(6/100)^{n+1} + \lambda_3}{\lambda_1(5/100)^n + \lambda_2(6/100)^n + \lambda_3}.$$

On a $\lim(5/100)^n = \lim(6/100)^n = 0$. On en déduit que $\lim v_n = 100$.

Si $\lambda_3 = 0$ et $\lambda_2 \neq 0$, on écrit :

$$v_n = 6\,\frac{\lambda_1(5/6)^{n+1} + \lambda_2}{\lambda_1(5/6)^n + \lambda_2}.$$

On en déduit que la suite v_n tend vers 6.

Si $\lambda_3 = 0$ et $\lambda_2 = 0$, $\lambda_1 \neq 0$ et $v_n = 5$. La suite (v_n) est constante et égale à 5.

d) Si $v_0 = 6$ et $v_1 = 6$, alors $\lambda_1 = \lambda_3 = 0$.

Si $v_0 = 6$ et $v_1 = 6 + \varepsilon$, avec $\varepsilon \neq 0$ (on a vu ci-dessus le cas où $\varepsilon := 3 \times 10^{-12}$), on ne peut pas avoir $\lambda_3 = 0$. Si c'était le cas, on aurait :

$$\lambda_1 + \lambda_2 = 1, \quad 5\lambda_1 + 6\lambda_2 = 6 \quad \text{et} \quad 5^2\lambda_1 + 6^2\lambda_2 = 6(6 + \varepsilon),$$

donc $\lambda_1 = 0$, $\lambda_2 = 1$, $\varepsilon = 0$ et une contradiction (on peut aussi calculer $\lambda_3 = \frac{6\varepsilon}{8930}$)· On en déduit que la suite converge vers 100, ce qui est en accord avec les calculs évoqués plus haut.

3. Soient $0 < p_1 < p_2 < p_3$ des entiers. On note $\sigma_1 := p_1 + p_2 + p_3$, $\sigma_2 := p_1p_2 + p_2p_3 + p_3p_1$, $\sigma_3 := p_1p_2p_3$ et l'on considère la suite « définie » par la relation de récurrence :

$$u_{n+2} = \sigma_1 - \frac{\sigma_2}{u_{n+1}} + \frac{\sigma_3}{u_n u_{n+1}}.$$

et les conditions initiales :

$$u_0 := \frac{p_1 + p_2}{2} \quad \text{et} \quad u_1 := \frac{p_1^2 + p_2^2}{p_1 + p_2}.$$

Nous laissons au lecteur l'étude de cette suite et de celles obtenues en prenant des valeurs initiales arbitraires.

IV.1.62 On conjecture que l'application de Collatz f n'a pas d'autre cycle positif que le cycle trivial $(1, 4, 2)$. Le but de l'exercice est de mettre en évidence des propriétés que devrait avoir un tel cycle A s'il existait. En particulier $\operatorname{card} A = 18$ est impossible et, en admettant un résultat vérifié en utilisant un ordinateur, on doit avoir $\operatorname{card} A > 10^{10}$.

1. a) Notons $b_1, \dots, b_p$ les éléments *pairs* du cycle A.
Notons P le produit des éléments de A. On a $P = b_1 \dots b_p c_1 \dots c_q$ et, puisque A est invariant par f : $P = \frac{b_1}{2} \dots \frac{b_p}{2}(3c_1 + 1) \dots (3c_q + 1)$. On en déduit :

$$b_1 \dots b_p c_1 \dots c_q = \frac{b_1}{2} \dots \frac{b_p}{2}(3c_1 + 1) \dots (3c_q + 1),$$

d'où : $2^p = \left(3 + \dfrac{1}{c_1}\right)\left(3 + \dfrac{1}{c_2}\right) \dots \left(3 + \dfrac{1}{c_q}\right)$.

On en déduit : $3^q < 2^p \leqslant \left(3 + \dfrac{1}{a}\right)^q$, puis, en utilisant les logarithmes à base 10 :

$$\frac{\log_{10} 3}{\log_{10} 2} < \frac{p}{q} < \frac{\log_{10}\left(3 + \frac{1}{a}\right)}{\log_{10} 2}. \tag{47}$$

b) On suppose que $\operatorname{card} A = 18$. On a $p + q = 18$, donc $p = 18 - q$.
Par suite $3^q < 2^{18-q} \leqslant \left(3 + \frac{1}{a}\right)^q$ et, en utilisant $a \geqslant 1$, $3^q < 2^{18-q} < 4^q$.
Supposons $q \geqslant 7$. On a $3^7 = 2187 > 2048 = 2^{11}$, donc $3^q > 2^{18-q}$, ce qui contredit $3^q < 2^{18-q}$ et l'on a une contradiction.
Supposons $q \leqslant 5$. On a $2^{13} > 2^{10} = 4^5$, donc $2^{18-q} > 4^q$, ce qui contredit $2^{18-q} < 4^q$ et l'on a une contradiction.
Supposons $q = 6$. On a $2^{18-6} = 2^1 2 = 4^6$, ce qui contredit $2^{12} < 4^6$ et l'on a encore une contradiction.
Ainsi $\operatorname{card} A = 18$ est impossible : *il n'existe pas de* 18*-cycle positif.*

c) On suppose que l'on sait que toute suite récurrente définie par f et $u_0 \in \mathbb{N}^*$ tel que $u_0 \leqslant 5 \times 10^{18}$ prend la valeur 1. On a donc $a > 5 \times 10^{18}$, $1/a < 2 \times 10^{-19}$ et :

$$\frac{\ln 3}{\ln 2} = \frac{\log_{10} 3}{\log_{10} 2} < \frac{p}{q} < \frac{\log_{10}\left(3 + 2 \times 10^{-19}\right)}{\log_{10} 2}.$$

On en déduit en utilisant un logiciel de calcul numérique ou formel que :

$$p/q \in J :=]1{,}584962500721156181\,45,\ 1{,}584962500721156181\,55[.$$

On vérifie aussi que $\frac{\log_{10} 3}{\log_{10} 2} \in J$. Ainsi p/q appartient à un « tout petit intervalle » (de longueur 10^{-19}) qui contient aussi $\log_2 3$. La question suivante, qui porte sur l'approximation rationnelle, nous permettra d'en déduire que p et q sont nécessairement « grands » et par suite que $\operatorname{card} A = p + q$ est « grand ».

2. a) On a $\operatorname{pgcd}(r_1, s_1) = \operatorname{pgcd}(r_2, s_2) = 1$.

b) Montrons (i)$\Rightarrow$ (ii). Supposons $r_1/s_1 < r/s < r_2/s_2$ et notons $\lambda := r_2 s - r s_2 > 0$ et $\mu := r s_1 - r_1 s > 0$. Alors et $\lambda := r_2 s - r s_2 > 0$. En utilisant $s_1 r_2 - s_2 r_1 = 1$, on obtient $r = \lambda r_1 + \mu r_2$ et $s = \lambda s_1 + \mu s_2$. Si l'on suppose r/s irréductible, λ et μ sont nécessairement premiers entre eux.
Montrons (ii)$\Rightarrow$ (i). Soient λ et μ des entiers strictement positifs premiers entre eux. On pose $r = \lambda r_1 + \mu r_2$ et $s = \lambda s_1 + \mu s_2$. Alors, en utilisant $s_1 r_2 - s_2 r_1 = 1$, on obtient $\lambda := r_2 s - r s_2 > 0$ et $\mu := r s_1 - r_1 s > 0$. Tout diviseur commun à r et s divise λ et μ et est donc égal à 1. Ainsi la fraction r/s est irréductible. De $\lambda > 0$ et $\mu > 0$ on déduit $r_1/s_1 < r/s < r_2/s_2$.

c) Soient p' et q' des rationnels strictement positifs tels que $r_1/s_1 < p'/q' < r_2/s_2$. On écrit p'/q' sous forme irréductible $p'/q' = r/s$. Alors, il existe $\alpha \in \mathbb{N}^*$ tel que $p' = \alpha r$ et $q' = \alpha s$. Par ailleurs, d'après 2 b), il existe des entiers *strictement* positifs premiers entre eux λ et μ tels que $r = \lambda r_1 + \mu r_2$ et $s = \lambda s_1 + \mu s_2$. On a $\lambda, \mu \geqslant 1$, donc $r \geqslant r_1 + r_2$ et $s \geqslant s_1 + s_2$. En utilisant $\alpha \geqslant 1$, on obtient $p' \geqslant r$ et $p' \geqslant s$, puis $p' \geqslant r_1 + r_2$ et $q' \geqslant s_1 + s_2$.

d) Vérification immédiate.

3. On applique l'algorithme d' Euclide à 355 et 113 : $355 = 3 \times 113 + 16$, $113 = 7 \times 16 + 1$. On en déduit $7 \times 355 - 22 \times 113 = 1$. Donc $\langle 22/7, 355/113 \rangle$ est une paire de Farey. On a : $(113 - 106) \times 355 - (355 - 333) \times 113 = 1$, donc $333 \times 113 - 106 \times 355 = 1$, et $\langle 355/113, 333/106 \rangle$ est une paire de Farey. On a $333/106 < 355/113 < 22/7$ et $\langle r_1/s_1 := 22/7, r_2/s_2 := 333/106 \rangle$ est une paire de Farey. Supposons $22/7 < p'/q' < 333/106$. En utilisant 2 c), on en déduit $p' \geqslant 355$ et $q' \geqslant 113$. On termine en vérifiant :

$$333/106 < 3{,}14151 < \pi - 8 \times 10^{-5} < \pi + 8 \times 10^{-5} < 3{,}1428 < 22/7.$$

L'approximation $355/113 = 3,\underline{14159}292\ldots$ de π a été découverte au v$^{\text{e}}$ siècle par le mathématicien chinois Zu Chongzhi et redécouverte en occident par Peter Metius en 1585.

4. a) On utilise une calculette pour la vérification. On utilise ensuite 2 c).

b) On vérifie numériquement le résultat.

5. On revient à l'étude du cycle positif A de l'application de Collatz. On a $p/q \in J$ (*cf.* (21)). On en déduit, en utilisant 4. b) :

$$p/q \in]r_1/s_1, r_2/s_2[=]357638239/225644606, 272500658/171928773[.$$

Par suite, d'après 3 a) : $p \geqslant 630138897$ et $q \geqslant 397573379$, et :

$$\operatorname{card} A = p + q \geqslant 630138897 + 397573379 = 1027712276.$$

6. a) Les a_n correspondent bijectivement aux A_n. Ils sont deux à deux distincts et forment un sous-ensemble de $\mathbb{N}^*$ que l'on peut numéroter dans l'ordre croissant pour la relation d'ordre de $\mathbb{N}$. Supposons qu'il en soit ainsi. Alors la suite (a_n) est strictement croissante et $\lim\limits_{n\to+\infty} a_n = +\infty$. On en déduit $\lim\limits_{n\to+\infty} \frac{\ln\left(3+\frac{1}{a_n}\right)}{\ln 2} = \frac{\ln 3}{\ln 2}$. D'après l'exercice IV.1.4 de la page 595, $\frac{\ln 3}{\ln 2}$ est irrationnel. En utilisant l'exercice IV.1.33 de la page 600, on en déduit que $\lim\limits_{n\to+\infty} p_n = +\infty$ et $\lim\limits_{n\to+\infty} q_n = +\infty$.
Par suite $\lim\limits_{n\to+\infty} \operatorname{card} A_n = +\infty$.

b) On raisonne par l'absurde. Soit $m \in \mathbb{N}^*$ fixé. On *suppose* que f possède une famille *infinie* de m-cycles positifs deux à deux distincts $\{A_n\}_{n\in\mathbb{N}}$. On peut supposer

que la suite (a_n) est croissante. Alors $\lim\limits_{n\to+\infty} \operatorname{card} A_n = +\infty$, mais, $\forall n \in \mathbb{N}$, $\operatorname{card} A_n = m$ et $\lim\limits_{n\to+\infty} \operatorname{card} A_n = m$. On a une contradiction.

Remarque. Terminons par un mot sur le choix des « mystérieux » entiers apparaissant dans la question 4.

Le problème est de trouver un intervalle de Farey (c'est-à-dire dont les bornes forment une paire de Farey) de longueur « très petite » contenant l'intervalle J. Pour construire un tel intervalle, on peut procéder par une variante du procédé de dichotomie. On commence avec une paire de Farey contenant J, par exemple $\langle 1/1, 2/1\rangle$, puis on la coupe en deux paires de Farey $\langle 1/1, 3/2\rangle$ et $\langle 3/2, 2/1\rangle$ en utilisant 2. d). On garde la paire contenant J, c'est-à-dire $\langle 3/2, 2/1\rangle$ et l'on continue tant qu'il y a l'une des deux paires qui contient J (en programmant le calcul...). Pour cette approche, *cf.* Shalom Eliahou, *le problème* $3N+1$, *C.N.R.S., Images des mathématiques*, 2011, http ://images.math.cnrs.fr/.

Nous avons en fait utilisé une méthode « moins élémentaire » basée sur les notions de fraction continue et de développement en fraction continue d'un nombre réel x (*cf.* le volume L3). Un tel développement donne une suite de rationnels (r_n), la suite des *réduites*, qui converge vers x. On peut calculer des développements en fractions continues en utilisant un système de calcul formel. Par exemple avec *Maple* : **`convert(x,confrac,n+1);`** retourne la fraction continue $[q_0, q_1, \ldots, q_n]$ et ensuite **`identify(numtheory[cfrac],(%));`** retourne la réduite r_n. On vérifie ainsi que les fractions :

$$r_{17} = 272500658/171928773,$$
$$r_{18} = 357638239/225644606,$$
$$r_{19} = 630138897/397573379$$

sont les $17^{ème}$, $18^{ème}$ et $19^{ème}$ réduites du développement en fraction continue de $x := \dfrac{\log_{10} 3}{\log_{10} 2}$. Signalons que :

$$r_2 = 22/7, \quad r_3 = 333/107 \quad \text{et} \quad r_4 = 355/113$$

sont les $2^{ème}$, $3^{ème}$ et $4^{ème}$ réduites du développement en fraction continue de $x := \pi$. La réduite suivante $r_5 = 103993/33102$ donne une excellente approximation de π :

$$103993/33102 = 3, \underline{14159265}30119\ldots$$

Le lecteur intéressé par les fractions continues pourra consulter le livre « J.P. Ramis et A. Warusfel, Cours de Mathématiques Pures et Appliquées, Algèbre et Géométrie, de boeck 2010 » (I.1 6) ou le livre « Michel Demazure, *Cours d'algèbre*, Cassini 1997 » (Ch. 7, 7.4).

IV.1.63 1. Soient $a,\ b,\ c \in \mathbb{R}$ trois points deux à deux distincts. On suppose que $f(a) = b,\ f(b) = c,\ f(c) = a$; (a, b, c) est un 3-cycle de f. Quitte à changer les noms des points, on peut supposer $a < b < c$. On note $I_0 := [a, b]$ et $I_1 := [b, c]$.
On a $a,\ c \in f(I_1)$, donc $I_1 \subset I_0 \cup I_1 = [a, c] \subset f(I_1)$. Par suite, en utilisant l'exercice 29 de la page 551 (avec $J := I_1$), on montre que f admet un point fixe dans I_1.

2. On a $I_1 \subset f(I_0)$, d'après l'exercice 7, il existe un segment $J \subset I_0$ tel que $f(J) = I_1$. On a $J \subset I_0 \subset f(I_1)$, donc $J \subset f \circ f(J)$. En appliquant l'exercice 29 à $f \circ f$, on en déduit que $f \circ f$ a un point fixe ℓ dans J. On a $\ell \leqslant b$ et $f(\ell) \geqslant b$. On ne peut donc pas avoir $f(\ell) = \ell$ (on aurait $\ell = b$ et $f(b) = c \neq b$). Ainsi ℓ est un point périodique de période 2 de f.

3. Soit τ un entier, $\tau \geqslant 4$. On va montrer que f possède un point périodique de plus petite période τ. La première étape est de définir, par récurrence, une suite d'intervalles emboîtés : $A_{\tau-2} \subset A_{\tau-3} \subset \cdots \subset A_1 \subset A_0$, telle que, pour tout $i \in [\![0, \tau-3]\!]$, l'on ait $f(A_{i+1}) = A_i$.

   On pose $A_0 := I_1 = [b, c]$. On a $A_0 \subset f(A_0)$, donc, d'après l'exercice 7, il existe $A_1 \subset A_0$ tel que $f(A_1) = A_0$. On a $A_1 \subset f(A_1)$, donc, d'après l'exercice 7, il existe $A_2 \subset A_1$ tel que $f(A_2) = A_1$. On termine par récurrence de façon évidente.

   On a, pour tout $i \in [\![0, \tau-2]\!]$, $f^{\circ i}(A_i) = A_0 = I_1$. Puisque $I_0 \subset f(I_1)$, on a $I_0 \subset f^{\circ\tau-1}(A_{\tau-2})$. En utilisant encore une fois l'exercice 7 (avec la fonction $f^{\circ\tau-1}$), on obtient un segment $A_{\tau-1} \subset A_{\tau-2}$ tel que $f^{\circ\tau-1}(A_{\tau-1}) = I_0$. On en déduit $A_{\tau-1} \subset I_1 \subset f^{\circ\tau}(A_{\tau-1})$ et, en utilisant l'exercice 29 (pour la fonction $f^{\circ\tau}$), on en déduit qu'il existe un point fixe ℓ de $f^{\circ\tau}$ appartenant à $A_{\tau-1}$.

   Il reste à montrer que τ est la *plus petite* période de ℓ. On raisonne par l'absurde.

   Les $\tau-2$ premiers itérés de ℓ appartiennent à I_1, le $(\tau-1)^{ème}$ appartient à I_0 et le $\tau^{ème}$ est $\ell \in I_1$. S'il existait une période p telle que $2 \leqslant p < \tau$, on aurait $f^{\circ p}(\ell) = \ell$. On a $f^{\circ(\tau-p-1)}(\ell) = f^{\circ(\tau-p-1)}\left(f^{\circ p}(\ell)\right) = f^{\circ(\tau-1)}(\ell) \in I_0$. Mais $\tau - p - 1 \leqslant \tau - 2$, donc $f^{\circ(\tau-p-1)}(\ell) \in I_1$. Ainsi, on doit avoir $f^{\circ(\tau-1)}(\ell) = b$, donc $f^{\circ\tau}(\ell) = c = \ell$.

   On a $\tau > 3$, donc $\tau - 2 > 1$. Par suite $A_{\tau_2} \subset A_1$ et, puisque $\ell \in A_{\tau_2}$, $\ell \in A_1$ et $f(\ell) \in A_0 = I_1$. Mais $f(\ell) = f(c) = a \notin I_1$ et l'on obtient une contradiction.

IV.1.64 On identifie, pour simplifier, toute suite finie à la chaîne de caractères correspondante.

1. a) On raisonne par l'absurde. supposons que l'écriture de c est impropre. Alors, il existe $k \in \mathbb{N}^*$ tel que toutes les décimales de rang strictement supérieur à k soient des 9. Mais la suite S formée de $k+1$ zéros figure dans la suite des décimales de c, donc il existe une décimale de rang strictement supérieur à k de c qui est un zéro et l'on obtient une contradiction.

   b) On raisonne comme dans a).
   Le nombre de Champernowne c est un nombre univers. En effet toute suite finie S ne commençant pas par un 0 a été utilisée dans la construction et, si S commence par 0, la suite finie $1S$, obtenue par concaténation de 1 et S a été utilisée dans la construction.
   À tout nombre réel a, on peut associer un nombre « complémentaire » b, en remplaçant chaque décimale α_k de a par $9 - \alpha_k$. On vérifie que si a est un nombre univers, alors b est aussi un nombre univers. Ainsi le nombre complémentaire de c est un nombre univers.
   Partant de c, on obtient d'autres nombres univers de la façon suivante : par définition la partie réelle est 0 et la suite des décimales est obtenue en concaténant une suite S finie arbitraire de longueur $n \in \mathbb{N}^*$ et $c : 0, Sc$. On vérifie que ces nombres sont des nombres univers et forment un ensemble infini.

   c) Soient a un nombre univers de partie entière nulle et b le nombre « complémentaire » défini comme dans l'exemple 42 de la page 591. On a $a + b = 1$ et 1 n'est pas un nombre univers.

2. a) Soit L une suite finie de m chiffres. Pour tout $n \in \mathbb{N}^*$, on peut définir un entier $s_n := 100\ldots0L$, écrit avec $m+n+1$ chiffres. Cet entier apparaît dans la fabrication de c. On raisonne par l'absurde. On suppose que L ne figure qu'un nombre fini de

fois dans la suite des décimales de c. Il existe alors $p \in \mathbb{N}$ tel que L ne figure pas dans la suite des décimales de c au delà de la $p^{ème}$. On obtient une contradiction en considérant une apparition de s_p dans la suite des décimales de c (par exemple la première) : le mot L écrit dans « ce » s_p figure dans la suite des décimales de c au delà de la $p^{ème}$.

Ainsi L figure une infinité de fois dans la suite des décimales de c.

b) Soit a un nombre univers. Soit L une suite finie de m chiffres. Les suites finies $S_1 := L0$, $S_2 := L10$, $S_3 = L110$, $S_4 := L1110\ldots$ de $m+1$, $m+2$, $m+3$, $m+4\ldots$ chiffres (obtenues par concaténation de L avec 0, 10, 110, $1110\ldots$) figurent chacune au moins une fois dans la suite des décimales de a. Il existe donc une suite $(k(n))_{n\in\mathbb{N}^*}$ telle que, l'on ait $\alpha_{k(1)}\ldots\alpha_{k(1)+m} = L0$, $\alpha_{k(2)}\ldots\alpha_{k(2)+m+1} = L10$, $\alpha_{k(3)}\ldots\alpha_{k(2)+m+2} = L110\ldots$ Montrons que les $(\alpha_{k(n)})$ sont *deux à deux distincts*. On raisonne par l'absurde. Supposons qu'il existe $p, q \in \mathbb{N}^*$ tels que $p < q$ et $\alpha_{k(p)} = \alpha_{k(q)}$. On a $\alpha_{k(p)+m+p-1} = 0$ et $\alpha_{k(q)+m+p-1} = 1$, d'où une contradiction. Ainsi, pour tout $n \in \mathbb{N}^*$, $L = \alpha_{k(n)}\ldots\alpha_{k(n)+m-1}$ et L figure une infinité de fois dans la suite des décimales de a.

c) Soit a un nombre univers. Soit b un nombre obtenu en changeant un certain nombre de décimales parmi les k premières de a, les décimales de rang strictement supérieur à k restant inchangées. Soit S une suite finie. Puisqu'elle figure une infinité de fois dans la suite des décimales de a, elle figure au moins une fois dans la suite des décimales de rang strictement supérieur à k de a. Elle figure donc dans la suite des décimales de b. Ainsi b est un nombre univers.

d) La preuve est similaire à celle faite pour le nombre de Liouville à laquelle le lecteur se reportera pour les détails (*cf.* l'exercice 39 de la page 585). Soit a un nombre univers. On raisonne par l'absurde. Si $a \in \mathbb{Q}$, la suite de ses décimales est périodique, de période m, à partir du rang $k+1$. Par ailleurs, la suite finie $S := \overbrace{00\ldots0}^{m \text{ répétitions}}$ formée de m zéros figure une infinité de fois dans les décimales de a. Il existe donc une suite d'entiers strictement positifs, deux à deux distincts : $(h(n))_{n\in\mathbb{N}^*}$ telle que, pour tout $n \in \mathbb{N}^*$, $\alpha_{h(n)}, \ldots, \alpha_{h(n)+m-1} = \overbrace{00\ldots0}^{m \text{ répétitions}}$. Il n'existe qu'un nombre fini de valeurs de n telles que $h(n) \leqslant k+m$, donc la suite S figure au moins une fois dans la suite des décimales de a de rang strictement supérieur à k. En utilisant l'exercice 38 de la page 581, on en déduit, que les décimales de rang strictement supérieur à k de a sont *toutes nulles*. Donc a est un décimal et l'on obtient une contradiction.

3. On a :

$$c_2 = 0{,}1101110010111011110001001\ldots$$

En reprenant *mutatis mutandis* la preuve faite en base 10, on montre qu'un nombre est rationnel si et seulement si la suite des décimales de son écriture en base b est périodique à partir d'un certain rang. La preuve de l'irrationalité de c_b est alors la même que celle faite plus haut pour un nombre univers en base 10.

4. On peut coder les caractères d'imprimerie (lettres, ponctuation, signes typographiques...) en utilisant les chaînes de 8 caractères formées de 0 et de 1 (8 bits). On peut par exemple utiliser les 128 caractères de la norme ASCII[5] (7 bits) et les complèter pour disposer des

[5] Qui permettent par exemple d'écrire un texte en TeX.

accents nécessaires pour écrire le français (par eemple avec ISO8859-1). On peut ensuite coder les oeuvres complètes de Shakespeare ou de Victor-Hugo (ou le livre que vous êtes en train de lire !) en utilisant ce code. On obtient une (longue...) chaîne de caractères qui figure (une infinité de fois) dans la suite des décimales de n'importe quel nombre univers.

Dans une célèbre nouvelle *La bibliothèque de Babel*, publiée en 1941, l'écrivain argentin Jorge Luis Borges imagine une bibliothèque « contenant tous les livres » (écrits ou à écrire). Plus précisèment la bibliothèque contient tous les livres d'au plus 420 pages (chaque page comporte 40 lignes d'au plus 80 caractères pris dans un alphabet de 25 symboles. Ainisi, en utilisant, par exemple, le codage ASCII, on voit que tout livre de la bibliothèque se trouve (une infinité de fois) dans la suite des décimales de n'importe quel nombre univers. On notera que la bibliothèque de Babel est *finie* (elle contient $2{,}35 \times 10^{1878831}$ ouvrages).

Un disque optique contient environ 5×10^9 bits d'information. Il n'y a donc qu'un nombre fini ($2^{5\times10^9}$) de disques optiques possible différents. Tout disque se trouve dans la suite des décimales de n'importe quel nombre univers. Ainsi tous les morceaux de musiques possibles (dans toutes les interprétations possibles...), par exemple les symphonies de Mozart, se trouvent dans la suite des décimales de n'importe quel nombre univers. De même toutes les photos (par exemple celles du lecteur) et tous les films (y compris ceux qui ne sont pas encore tournés !) figurent dans la suite des décimales de n'importe quel nombre univers.

On pourrait en conclure qu'un nombre univers « contient beaucoup d'information ». Ce n'est pas le cas. Par exemple, on peut définir l'information contenue dans le nombre de Champernowne c par la longueur du plus petit programme permettant de l'écrire. Cette longueur est « très petite » (le lecteur la majorera facilement en écrivant un tel programme).

Il n'y a pas de paradoxe. Vous *savez* qu'une photo de votre petit(e) ami(e) apparaît dans la suite des décimales *mais vous n'avez absolument aucun moyen pratique de la récupèrer* (elle est très très loin dans la suite !).

Remarque On peut montrer que le nombre de Champernowne c est *transcendant*. Une preuve est due au mathématicien allemand Kurt Mahler : *« Arithmetische Eigenschaften einer Klasse von Dezimalbruechen »*, Proc. Kon. Nederl. Akad. Wetensch. 40 (1936), p 421-428.

IV.1.65 1. (i) a) On a $f(0,\alpha_1\alpha_2\alpha_3\ldots\alpha_h\ldots) = 0,\alpha_2\alpha_3\alpha_4\ldots\alpha_{h+1}\ldots$. Par suite l'application f consiste à « effacer la première décimale » et à décaler d'un cran vers la gauche les décimales restantes. On l'appelle aussi *application de décalage* (‘« shift » en anglais). L'application itérée $f^{\circ n}$ consiste à effacer les n premières décimales et à décaler de n crans vers la gauche les décimales restantes. Ainsi $f^{\circ n}(t) = 10^n t - E(10^n t)$.

b) Soient $u = 0,\gamma_1\ldots\gamma_h\ldots$ et $t_0 = 0,\alpha_1\ldots\alpha_h\ldots$. Soit $\varepsilon > 0$. Il existe $n \in \mathbb{N}^*$ tel que $2/10^n < \varepsilon$. On a $(t_0)_n = 0,\alpha_1\ldots\alpha_n$ et, si l'on définit $v := 0,\alpha_1\ldots\alpha_n\gamma_1\ldots\gamma_h\ldots$, alors $v_n = (t_0)_n$ et $f^{\circ n}(v) = u$. On a $|v - t_0| \leqslant |v - v_n| + |v_n - t_0| = |v - v_n| + |(t_0)_n - t_0| \leqslant 2/10^n < \varepsilon$.
Ainsi, puisque le choix de u est *arbitraire*, on peut obtenir *n'importe quel comportement asymptotique* (parmi les comportements possibles) en changeant « aussi peu que l'on veut » la condition initiale t_0.

(ii) a) Il est clair que la suite (u_n) définie par u_0 et f est constante et égale à 0 à partir d'un certain rang si, et seulement si, $u_0 \in \mathbb{D}$ et que $\mathbb{D} \cap [0,1[$ est dense

dans $[0,1[$. Plus généralement, si la suite est constante et égale à $j \in [\![0,8]\!]$ à partir d'un certain rang, sa limite est $j/9$. Les conditions initiales correspondantes sont de la forme $0,\alpha_1 \dots \alpha_h jj \dots j \dots$.

b) Supposons $t \in \mathbb{Q}$. Alors son écriture décimale est périodique, de période m, à partir d'un certain rang $k+1$: $t := 0,\beta_1\beta_2 \dots \beta_k\underline{\alpha_1 \dots \alpha_m}\,\alpha_1 \dots \alpha_m \dots$. On a $f^{\circ k}(t) = 0,\underline{\alpha_1 \dots \alpha_m}\,\alpha_1 \dots \alpha_m \dots$, puis :

$$f^{\circ k}(t) = f^{\circ(k+m)}(t) = f^{\circ m} \circ f^{\circ k}(t).$$

Inversement, supposons qu'il existe $k \in \mathbb{N}$ et $m \in \mathbb{N}^*$ tels que :

$$f^{\circ m} \circ f^{\circ k}(t) = f^{\circ k}(t).$$

Alors $f^{\circ k}(t)$ est périodique de période m :

$$f^{\circ k}(x) = 0,\underline{\alpha_1 \dots \alpha_m}\,\alpha_1 \dots \alpha_m \dots$$

et t est de la forme $t := 0,\beta_1\beta_2 \dots \beta_k\underline{\alpha_1 \dots \alpha_m}\,\alpha_1 \dots \alpha_m \dots$, donc $t \in \mathbb{Q}$.

c) On va choisir $\alpha_1, \dots, \alpha_m$ tels que : $0,\underline{\alpha_1 \dots \alpha_m}\,\alpha_1 \dots \alpha_m \dots$ admette m pour *plus petite* période.
On peut supposer $m \geqslant 2$. Les périodes possibles sont les diviseurs de m. Si m est premier, il n'y a rien à démontrer. Sinon, on choisit $\alpha_1 = 1$ et $\alpha_2 = \dots = \alpha_m = 0$. Il n'y a pas de période srictement plus petite que m. Si m_1 était une telle période, on aurait $\alpha_{m_1+1} = 1$, mais $1 < m_1 + 1 \leqslant m$, donc $\alpha_{m_1+1} = 0$ et l'on aurait une contradiction.
L'écriture décimale $0,\underline{\alpha_1 \dots \alpha_m}\,\alpha_1 \dots \alpha_m \dots$ ne contient pas de 9, elle est donc propre et elle définit un nombre réel.
La suite (u_n) est évidemment périodique de plus petite période m.

d) On utilise (i) b). Soient $m \in \mathbb{N}^*$, $m \geqslant 2$ et $u := 0,\underline{\alpha_1 \dots \alpha_m}\,\alpha_1 \dots \alpha_m \dots$ admettant m pour *plus petite* période. Soit $t_0 \in [0,1[$. Pour tout $\varepsilon > 0$, il existe $n \in \mathbb{N}^*$ et $v \in]t_0 - \varepsilon, t_0 + \varepsilon[\cap [0,1[$ tels que $f^{\circ n}(v) = u$. La suite définie par la condition initiale v est périodique de plus petite période m à partir du rang n.

e) Soient $t_0 \in [0,1[$ et ε. On note $t_0 = 0,\alpha_1 \dots \alpha_h \dots$. On choisit $k \in \mathbb{N}^*$ tel que $2/10^k < \varepsilon$ et l'on définit $u_0 := 0,\underline{\alpha_1 \dots \alpha_k}\alpha_1 \dots \alpha_k \dots$ (dont les décimales sont périodiques de période k). On a $(u_0)_k = (t_0)_k$.
On a :

$$|u_0 - t_0| \leqslant \big|u_0 - (t_0)_k\big| + \big|(t_0)_k - t_0\big| = \big|u_0 - (u_0)_k\big| + \big|(t_0)_k - t_0\big| \leqslant 2/10^k < \varepsilon.$$

La suite définie par u_0 est périodique et l'on a $u_0 \in]t_0 - \varepsilon, t_0 + \varepsilon[\cap [0,1[$.

(iii) a) Soient $t = 0,\alpha_1\alpha_2 \dots \alpha_h \dots$ une écriture décimale et $k \in \mathbb{N}^*$. On considère $t_k = 0,\alpha_1\alpha_2 \dots \alpha_k$. D'après le procédé de définition de c, le mot $(\alpha_1\alpha_2 \dots \alpha_k)$ apparaît dans la liste des décimales de c (il apparaît même une infinité de fois !). Par suite, il existe $n_k \in \mathbb{N}$ tel que $c = \beta_1 \dots \beta_{n_k}\alpha_1\alpha_2 \dots \alpha_k\beta_{n_k+k+1}\beta_{n_k+k+2} \dots$. On a :

$$f^{(n_k)}(c) = \alpha_1\alpha_2 \dots \alpha_k\beta_{n_k+k+1}\beta_{n_k+k+2} \dots$$

et la troncature à l'ordre k de $f^{\circ n_k}(c)$ est $\big(f^{\circ n_k}(c)\big)_k = 0,\alpha_1\alpha_2 \dots \alpha_k = t_k$.

b) Soit $t = 0,\alpha_1\alpha_2 \dots \alpha_h \dots$ une écriture décimale. Soit $\varepsilon > 0$. Il existe $k \in \mathbb{N}^*$ tel que $2/10^k < \varepsilon$. En utilisant a), on obtient $n_k \in \mathbb{N}^*$ tel que $f^{(n_k)}(c) = t_k$.

On a :

$$\left|f^{\circ n_k}(c) - t\right| \leqslant \left|f^{\circ n_k}(c) - t_k\right| + |t_k - t| = \left|f^{\circ n_k}(c) - \left(f^{\circ n_k}(c)\right)_k\right| + |t_k - t|$$
$$\leqslant 2/10^k < \varepsilon.$$

Par suite l'image de la suite $\left(f^{\circ n}(c)\right)_{n\in\mathbb{N}}$ est dense dans $[0,1[$.

(iv) D'après les résultats précédents, on peut, en changeant aussi peu que l'on veut une condition initiale quelconque, obtenir une suite constante à partir d'un certain rang, ou une suite périodique, ou une suite périodique à partir d'un certain rang de plus petite période arbitraire, ou une suite d'image dense.

2. Montrons que l'étude des suites récurrentes de U définies par φ se déduit de celle des suites récurrentes de $[0,1[$ définies par f.

On utilise l'application $\varpi : [0,1[\to U$ définie par $\varpi : t \in [0,1[\mapsto \varpi(t) := e^{2i\pi t} \in U$. Cette application est continue et *bijective*. (On prendra garde au fait que l'application inverse n'est pas continue.) L'image par ϖ d'un sous-ensemble dense de $[0,1[$ est un sous-ensemble dense de U.

Si $\varpi(t) = e^{2i\pi t} = z$, on a :

$$\varpi\left(f(t)\right) = e^{2i\pi f(t)} = e^{2i\pi 10t - E(10t)} = e^{2i\pi 10t} = z^{10} = \varphi(z).$$

L'image par ϖ de la suite récurrente définie par t_0 et f est donc la suite récurrente définie par $z_0 := \varpi(t_0)$ et φ.

Ainsi on peut, en changeant aussi peu que l'on veut une condition initiale $z_0 \in U$ quelconque, obtenir une suite constante à partir d'un certain rang, ou une suite périodique, ou une suite périodique à partir d'un certain rang de plus petite période arbitraire, ou une suite d'image dense.

3. Tous les résultats de 1 restent valables *mutatis mutandis* si l'on remplace la base 10 par une base $b \in \mathbb{N}^*$, $b \geqslant 2$. Il faut remplacer le nombre de Champernowne $c = c_{10}$ par le nombre de Champernowne c_b. On peut ensuite reprendre la méthode de 2 en remplaçant $\varphi = \varphi_{10}$ par φ_b. Les conclusions sont similaires.

Pour $b = 2$, on justifie ainsi les résultats décrits dans l'exemple 3 de la page 573.

Module IV.2 : Fonctions réelles

IV.2.1 1. Écrivons l'expression donnée sous la forme :

$$-5x^4\Big(-\frac{1}{5x^2}+1-\frac{3}{5x^3}\Big).$$

Le second facteur tend vers 1 au voisinage de $+\infty$ et de $-\infty$, il est donc strictement positif pour $|x|$ assez grand et, par suite, les limites respectives en $+\infty$ et $-\infty$ sont toutes deux égales à $-\infty$.

2. La même méthode, en mettant $-12x^3$ en facteur, montre que les limites sont cette fois-ci $-\infty$ en $+\infty$ et $+\infty$ en $-\infty$.

3. La même méthode, en mettant $x/2$ en facteur, montre que les limites sont cette fois-ci $+\infty$ et $-\infty$. Au voisinage de 1, on obtient $-\infty$ si x tend vers 1 par valeurs inférieures, et $+\infty$ par valeurs supérieures.

4. Écrivons l'expression donnée sous la forme :

$$\Big(\frac{1}{x+2}\Big)\Big(\frac{3x-1}{3-5x}\Big).$$

Le second facteur tend vers $-7/13$ au voisinage de -2, on obtient donc $+\infty$ si x tend vers -2 par valeurs inférieures, et $-\infty$ si x tend vers -2 par valeurs supérieures.

5. Écrivons l'expression donnée sous la forme :

$$\Big(\frac{5x}{2}\Big)\Big(\frac{1+1/5x^2}{1-1/2x}\Big).$$

Le second facteur tend vers 1 au voisinage de $+\infty$ et de $-\infty$, il est donc strictement positif pour $|x|$ assez grand ; par suite, les limites respectives en $+\infty$ et $-\infty$ sont respectivement égales à $+\infty$ et à $-\infty$.

L'expression $5x^2+1$ tend vers $9/4$ au voisinage de $1/2$, on obtient, comme plus haut, $-\infty$ si x tend vers $1/2$ par valeurs inférieures, et $+\infty$ si x tend vers $1/2$par valeurs supérieures.

6. Après factorisations, on obtient, pour $x\neq 1$ et $x\neq 1/3$:

$$\frac{(x-1)^2(3x-1)}{(x-1)\,(3x-1)}=x-1.$$

La limite est donc 0 au voisinage de 1 et $-2/3$ au voisinage de $1/3$.

7. La technique traditionnelle de « multiplication par la quantité conjuguée » conduit, pour $x>0$, aux expressions :

$$\frac{(x^2+x+1)-x^2}{\sqrt{x^2+x+1}+x}=\frac{x+1}{\sqrt{x^2+x+1}+x}=\frac{1+1/x}{\sqrt{1+1/x+1/x^2}+1}.$$

La limite en $+\infty$ est donc $1/2$.

8. Après factorisation, on obtient, pour $x\neq 4$, l'expression :

$$\frac{\sqrt{x}-2}{(\sqrt{x}-2)\,(\sqrt{x}+2)}=\frac{1}{\sqrt{x}+2}.$$

La limite est donc $1/4$ au voisinage de 4.

9. Deux factorisations et la multiplication par la quantité conjuguée conduisent en dehors de -1 et 2 aux expressions :

$$\begin{aligned}\frac{(x+1)^2(x+3)}{2-\sqrt{x^2-x+2}} &= \frac{(x+1)^2(x+3)(2+\sqrt{x^2-x+2})}{4-(x^2-x+2)}\\ &= \frac{(x+1)^2(x+3)(2+\sqrt{x^2-x+2})}{(x+1)\,(2-x)}\\ &= \frac{(x+1)\,(x+3)(2+\sqrt{x^2-x+2})}{2-x}.\end{aligned}$$

La limite est donc 0 au voisinage de -1.

10. La limite est 0 puisque tout cosinus est borné par 1.

IV.2.2 Soient les deux suites $(u_n, v_n)_{n\in\mathbb{N}^*}$ définies par $u_n = \dfrac{1}{2n\pi}$ et $v_n = \dfrac{1}{(2n+1)\pi}$.

On a $\cos(1/u_n) = 1$ et $\cos(1/v_n) = -1$, d'où la propriété annoncée.

IV.2.3 1. Une simplification, par multiplication par $3+\sqrt{x+3}$ au numérateur et au dénominateur, donne aussitôt $\dfrac{1}{3+\sqrt{x+3}}$ comme fonction prolongée au voisinage de 6, fonction visiblement dérivable, de valeur $1/6$ et de dérivée $-1/216$ en ce point.

2. Une simplification, par réduction au même dénominateur, donne aussitôt $-\dfrac{1}{1+x}$ comme fonction prolongée au voisinage de 1, fonction visiblement dérivable, de valeur $-1/2$ et de dérivée $1/4$ en ce point. En revanche, la fonction n'est pas prolongeable au voisinage de -1, puisqu'alors $\big|f(x)\big| \to +\infty$.

IV.2.4 Soit $g : [0,1] \to \mathbb{R}$ la fonction continue définie par $x \mapsto g(x) := f(x) - x$.

On a $g(0) = f(0) \geqslant 0$ et $g(1) = f(1) - 1 \leqslant 0$. Par le théorème des valeurs intermédiaires, il existe un $a \in [\,0,1\,]$ tel que $g(a) = 0$, soit $f(a) = a$.

Si f n'est pas continue, le nombre a n'existe pas nécessairement : par exemple si $f(x) := 1-x$ si $x \neq 1/2$, et $f(1/2) := 0$.

Si $f\big([0,1]\big) \not\subset [0,1]$, le nombre a n'existe pas nécessairement : par exemple si $f(x) := x+1$.

IV.2.5 Traduit en termes mathématiques, le résultat à démontrer est le suivant : si deux fonctions f et g continues (c'est la seule façon de marcher...) sur un segment $[\,a,b\,]$ sont telles que $f(a) = g(b)$ et $g(b) = f(a)$, alors il existe un c et un $t \in [a,b]$ tels que $f(t) = g(t) = c$. Cela résulte aussitôt du fait que, si $h(t) := f(t) - g(t)$, alors $h(a)h(b) \leqslant 0$, ce qui implique l'existence d'un t tel que $h(t) = 0$, soit $f(t) = g(t)$. On peut noter qu'il n'y a pas forcément unicité de ce couple (la promenade peut même comporter des allers et retours sur la route).

IV.2.6 1. Supposons f continue périodique et admettant des périodes arbitrairement petites. Si f n'est pas constante, il existe $a \in \mathbb{R}$ tel que $f(a) \neq f(0)$. Par hypothèse, pour tout $\alpha > 0$, il existe une période τ telle que $0 < \tau < \alpha$. Alors l'intervalle $]a-\alpha, a+\alpha[$ contient un multiple entier (relatif) b de τ et en ce point la valeur de f est $f(0)$.

On a $\frac{\left|f(0)-f(a)\right|}{2} > 0$, donc, d'après l'hypothèse de continuité de f en a, il existe $\alpha > 0$ tel que, pour tout $x \in]a-\alpha, a+\alpha[$, l'on ait $\left|f(x)-f(a)\right| < \frac{\left|f(0)-f(a)\right|}{2}$.

Alors $\left|f(b)-f(a)\right| = \left|f(0)-f(a)\right| < \frac{\left|f(0)-f(a)\right|}{2}$ et l'on a une contradiction.

2. Supposons que la fonction continue f admette 1 et $\sqrt{2}$ pour périodes. Alors, pour tout $(m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}$, le réel $m + n\sqrt{2}$ est une période de f ($m + n\sqrt{2} \neq 0$). En particulier, pour tout $p \in \mathbb{N}$, $(\sqrt{2}-1)^p$ est une période de f.

On a $(\sqrt{2}-1)^p > 0$ et, quand p tend vers $+\infty$, $(\sqrt{2}-1)^p$ tend vers 0, donc f admet des périodes arbitrairement petites. D'après 1, la fonction f est donc constante. Inversement les fonctions constantes sont continues et admettent 1 et $\sqrt{2}$ pour périodes.

IV.2.7 1. Il est immédiat que 0 appartient à T. De plus, si τ_1 et τ_2 sont deux éléments de T, on a :

$$\forall x \in \mathbb{R},\ f(x+\tau_1+\tau_2) = f\big((x+\tau_1)+\tau_2\big) = f(x+\tau_1) = f(x)$$

et en appliquant la relation $f(x+\tau_1)$ à $x-\tau_1$, on obtient $f(x) = f(x-\tau_1)$. Ainsi $\tau_1+\tau_2$ et $-\tau_1$ appartiennent aussi à T. Donc T est un sous-groupe de $\mathbb{R}$.

2. L'exercice IV.1.11 de la page 596 nous dit alors que T est soit dense dans $\mathbb{R}$, soit de la forme $a\,\mathbb{Z}$, avec $a > 0$.

Soit f continue. Supposons T dense. Alors $\forall \tau \in T,\ f(\tau) = f(0)$. Or, par densité de T, tout réel x est la limite d'une suite (τ_n) d'éléments de T et par continuité de f, on en déduit $f(x) = \lim f(\tau_n) = f(0)$. Donc f est constante. Par contraposée, on en déduit que si f est non constante, alors T n'est pas dense, donc qu'il existe $a > 0$ tel que $T = a\,\mathbb{Z}$.

IV.2.8 Soit $p \in \mathbb{N}^*$. Soit $\{c_1, \ldots, c_p\}$ une famille strictement croissante de points de $[a,b]$. On choisit une famille de nombres réels $\{d_0, \ldots, d_p\}$ tels que :

- $d_i \in]c_i, c_{i+1}[$ pour $i \in [\![1, p-1]\!]$,
- $d_0 \in]a, c_1[$ si $a \neq c_1$ et $d_0 := a$ si $a = c_1$;
- $d_p \in]c_p, b[$ si $b \neq c_p$ et $d_p := b$ si $b = c_p$.

Alors, pour tout $i \in [\![1,p]\!]$: $\sigma(c_i) \leqslant f(d_i) - f(d_{i-1})$ et, par suite :

$$\sum_{i=1}^{p} \sigma(c_i) \leqslant \sum_{i=1}^{p} (f(d_i) - f(d_{i-1})) = f(d_p) - f(d_0) \leqslant f(b) - f(a).$$

IV.2.9 1. Soit $f : \mathbb{R} \to \mathbb{R}$ une bijection bicontinue décroissante telle que $f(0) = 0$ et $f \circ f = id_{\mathbb{R}}$. On vérifie que la restriction de f à $\mathbb{R}_+$ induit une bijection bicontinue g

de $\mathbb{R}_+$ sur $\mathbb{R}_-$. Puisque $f = f^{-1}$ la restriction de f à $\mathbb{R}_-$ induit la bijection bicontinue g^{-1} de $\mathbb{R}_-$ sur $\mathbb{R}_+$. Les graphes $\Gamma_g \subset \mathbb{R}_+ \times \mathbb{R}_-$ et $\Gamma_{g^{-1}} \subset \mathbb{R}_- \times \mathbb{R}_+$ sont symétriques par rapport à la première bissectrice et leur réunion (dans $\mathbb{R}^2$) est le graphe de f.

Inversement, soit $g : \mathbb{R}_+ \to \mathbb{R}_-$ une bijection bicontinue décroissante. On a nécessairement $g(0) = 0$. On note Γ' le symétrique de Γ_g par rapport à la première bissectrice et $\Gamma := \Gamma_g \cup \Gamma'$. Alors Γ est le graphe d'une bijection bicontinue décroissante $f : \mathbb{R} \to \mathbb{R}$ telle que $f(0) = 0$ et $f \circ f = id_{\mathbb{R}}$.

2. Commençons par deux exemples.

   On définit $g : \mathbb{R}_+ \to \mathbb{R}_-$ par $x \mapsto g(x) := -\sqrt{x}$. Alors $g^{-1} : \mathbb{R}_- \to \mathbb{R}_+$ vérifie $g^{-1}(x) = x^2$. On définit $f : \mathbb{R} \to \mathbb{R}$, comme en 1, par $f(x) := g(x)$ pour $x \in \mathbb{R}_+$ et $f(x) := g^{-1}(x)$ pour $x \in \mathbb{R}_-$; f est une bijection bicontinue décroissante telle que $f(0) = 0$ et $f \circ f = id_{\mathbb{R}}$.

   On définit $g : \mathbb{R}_+ \to \mathbb{R}_-$ par $x \mapsto g(x) := -x - x^2$. Alors $g^{-1} : \mathbb{R}_- \to \mathbb{R}_+$ vérifie $g^{-1}(x) = \frac{1}{2}\left(-1 + \sqrt{1 - 4x}\right)$. On définit ensuite f comme ci-dessus.

   Plus généralement, il y a une infinité de choix possibles pour g, donc une infinité de possibilités pour f.

IV.2.10 Soit $n \in \mathbb{N}^*$, rappelons que l'on note $f^{\circ n} = f \circ \ldots \circ f$ la composée n fois de f par lui même.

1. La composée de deux homéomorphismes est un homéomorphisme ; l'inverse d'un homéomorphisme est un homéomorphisme, d'où le résultat (G est un sous-groupe du groupe des bijections de $\mathbb{R}$ sur $\mathbb{R}$).
2. Les transformations affines $f_{a,b} : x \mapsto ax + b$, avec $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$ forment un sous-groupe infini de G.
3. D'après la proposition 30 de la page 631, les homéomorphismes de $\mathbb{R}$ sont strictement monotones. Soit $H \subset G$ un sous-groupe fini de G. On note n l'ordre de H. D'après le théorème de Lagrange (*cf.* le théorème 22 du module II.2, page 128), si $f \in H$, on a $f^{\circ n} = id_{\mathbb{R}}$.

   Soit $f \in H$ strictement croissante. Montrons que $f = id_{\mathbb{R}}$.

   On raisonne par l'absurde. Si $f \neq id_{\mathbb{R}}$, il existe $a \in \mathbb{R}$ tel que $f(a) \neq a$. On distingue les deux cas $f(a) > a$ et $f(a) < a$.

   - Si $a < f(a)$, on montre par récurrence que :
   $$a < f(a) < f^{\circ 2}(a) < \ldots < f^{\circ n}(a) = a,$$
   d'où une contradiction.
   - Si $f(a) < a$, on montre par récurrence que :
   $$a = f^{\circ n}(a) < \ldots < f^{\circ 2}(a) < f(a) < a,$$
   d'où une contradiction.

   Par suite, si $f \in H \setminus \{id_{\mathbb{R}}\}$, alors f est strictement décroissante. Mais $f \circ f \in H$ est strictement croissante, donc $f \circ f = id_{\mathbb{R}}$. Ainsi, tous les éléments de H sont d'ordre 2.

   Si $f, g \in H \setminus \{id_{\mathbb{R}}\}$, $f \circ g$ est strictement croissante, donc $f \circ g = id_{\mathbb{R}}$ et $g = f^{-1} = f$, donc H a au plus deux éléments. Les sous-groupes finis de G sont donc le sous-groupe

réduit à l'identité et les sous-groupes de la forme $\{id_{\mathbb{R}}, f\}$ où f est une involution strictement décroissante ($f \circ f = id_{\mathbb{R}}$). D'après l'exercice précédent, il y a une infinité de tels sous-groupes.

IV.2.11 Cette fonction paire est définie et continue sur $\mathbb{R}$. Il suffit de s'intéresser à $\mathbb{R}_+$. Il n'existe évidemment pas de dérivée en 0 car $f(x)/x$ tend respectivement vers $-1/2$ et $1/2$ à gauche et à droite.

Pour $0 < x < 1$, on trouve $f'(x) = (2 + x^2)/(2 - x^2)^2$ et, pour $x > 1$, $f'(x) = -1/x^2$. On a $f(1) = 1$ et $(f(x) - 1)/(x - 1)$ tend respectivement vers 3 et -1 à gauche puis à droite en 1. Donc f n'est pas dérivable en 1.

En résumé, f est dérivable en tout point de $\mathbb{R}$ exceptés -1, 0 et 1.

IV.2.12 La restriction de f à $\mathbb{R}_-$ est $x \mapsto e^{-x} + x + 1$ qui est continue et dérivable. D'où la continuité et la dérivabilité de f sur $\mathbb{R}_-^*$, ainsi que sa continuité à gauche et sa dérivabilité à gauche en 0, avec $f(0) = 2$ et $f'_g(0) = 0$.

De même, f est continue et dérivable sur $\mathbb{R}_+^*$ par dérivabilité de $x \mapsto 2 + x^2 \ln x$ et l'on a $\forall x > 0\,,\ f'(x) = 2x \ln x + x$.

Comme $\lim\limits_{x \to 0^+} x^2 \ln x = 0$, on en déduit $\lim\limits_{0^+} f = 2$, donc la continuité à droite de f en 0.

D'autre part, pour $x > 0$, on a $\frac{f(x)-f(0)}{x} = x \ln x \underset{x \to 0^+}{\longrightarrow} 0$, donc f est dérivable à droite en 0 avec $f'_d(0) = 0$.

Finalement, f est dérivable sur $\mathbb{R}$. Sa dérivée est continue et dérivable sur $\mathbb{R}^*$ et continue en 0 puisque $\lim\limits_{x \to 0^-} 1 - e^{-x} = 0 = \lim\limits_{x \to 0^+} 2x \ln x + x$.

Enfin, pour $x > 0$:

$$\frac{f'(x) - f'(0)}{x} = \frac{f'(x)}{x} = 1 + 2 \ln x \underset{x \to 0^+}{\longrightarrow} -\infty,$$

ce qui prouve que f' n'est pas dérivable (à droite) en 0.

IV.2.13 Le domaine de définition de f_1 est $\mathbb{R}$.

Le domaine de définition de f_2 est $\{x \in \mathbb{R} \mid \sin x > 0\}$.

On a $\tan\left(\frac{x}{2} + \frac{\pi}{4}\right) = \frac{1+\tan\frac{x}{2}}{1-\tan\frac{x}{2}}$, donc $\tan\left(\frac{x}{2} + \frac{\pi}{4}\right) > 0$ si, et seulement si :

$$\left(1 + \tan\frac{x}{2}\right)\left(1 - \tan\frac{x}{2}\right) = 1 - \tan^2\frac{x}{2} > 0.$$

En utilisant $\cos x = \frac{1-\tan^2\frac{x}{2}}{1+\tan^2\frac{x}{2}}$, on en déduit que le domaine de définition de f_3 est $\{x \in \mathbb{R} \mid \cos x > 0\}$.

On doit avoir $a \geqslant 0$. On écarte le cas trivial $a = 0$ et l'on suppose $a > 0$. Le domaine de définition de f_4 est alors $\mathbb{R}_+$.

En dérivant les fonctions, on trouve successivement :

$(2 \ln 3)\, 3^{2x}$ sur $\mathbb{R}$, $\quad \big(1 + (1 + \tan^2 x) \ln(\sin x)\big)(\sin x)^{\tan(x)}$ sur $\{x \in \mathbb{R} \mid \sin x > 0\}$,

$\dfrac{1}{\cos x}$ sur $\{x \in \mathbb{R} \mid \cos x > 0\}$, $\quad \dfrac{\sqrt{a}(\sqrt{x} - \sqrt{a})}{2\sqrt{x(x+a)}(\sqrt{a} + \sqrt{x})^2}$ sur $\mathbb{R}_+^*$

IV.2.14 1. Puisque $f(x) = -1 + 2/(1+x)$, il vient $f^{(n)}(x) = 2(-1)^n n!\big((1+x)^{-n-1}\big)$.

2. Puisque $f(x) = (1-\cos 2x)/2$, il vient $f^{(n)}(x) = -2^{n-1}\cos\left(2x + n\,\dfrac{\pi}{2}\right)$.

IV.2.15 Posons $g(x) := f(a-1+1/x)$ pour $0 < x \leqslant 1$. Alors g est bien définie et continue sur $]0,1]$ puisque $a-1+1/x \geqslant a$, et même dérivable avec $g'(x) = -\dfrac{1}{x^2} f'\Big(a-1+\dfrac{1}{x}\Big)$. Si l'on prolonge g à $[0,1]$ en posant $g(0) := g(1) = f(a)$, alors g est continue sur le segment et dérivable sur $]0,1[$ (et même en 1 mais c'est sans importance). Il existe donc $d \in]0,1[$ tel que $g'(d) = 0$; il suffit alors de poser $c = a-1+1/d > a$ pour trouver que :

$$f'(c) = -c^2 g'(d) = 0.$$

Ce résultat est l'une des extensions naturelles du théorème de Rolle.

IV.2.16 1. On suppose que, pour tout $x \in [a,b[$, $f'_d(x) > 0$.

a) Soit $c \in [a,b[$. On a $\lim\limits_{u \overset{>}{\to} c} \frac{f(u)-f(c)}{u-c} = f'_d(c) > 0$. Il existe donc $h > 0$ tel que $c+h \leqslant b$ et, pour tout $u \in]c, c+h]$, $\frac{f(u)-f(c)}{u-c} > 0$, donc $f(c) < f(u)$.

b) Soient $x \in [a,b[$ et $E_x := \{v \in [x,b] \mid \forall u \in [x,v], f(x) \leqslant f(u)\}$.

- On a $x \in E_x$, donc E_x n'est pas vide. Soient $y, z \in E_x$. On peut supposer $y \leqslant z$. D'après la définition de E_x, $x \leqslant y \leqslant z$ et $[x,z] \subset E_x$, donc $[y,z] \subset E_x$. Par suite E_x est une partie *convexe* de $\mathbb{R}$ et d'après la proposition 15 de la page 519, c'est un intervalle.
- L'ensemble E_x est non vide et borné par b. Il admet donc une borne supérieure $\gamma \leqslant b$. D'après les propriétés de la borne supérieure et la définition de E_x, on a $[x,\gamma[\subset E_x$ Montrons que $\gamma \in E_x$, d'où l'on déduira $E_x = [x,\gamma]$. On raisonne par l'absurde. Supposons $\gamma \notin E_x$. Alors il existe $\gamma' \in]x,\gamma]$ tel que $f(x) > f(\gamma')$. D'après la continuité de f en γ', il existe $\gamma'' \in]x,\gamma'[$ tel que $f(x) > f(\gamma'')$. On a $[x,\gamma[\subset E_x$, donc $\gamma'' \in E_x$ et $f(x) \leqslant f(\gamma'')$, d'où une contradiction.
- Montrons $\gamma = b$. On raisonne par l'absurde. Si $\gamma < b$, on peut utiliser a) et l'on obtient $h > 0$ tel que $\gamma + h \leqslant b$ et pour tout $u \in]\gamma, \gamma+h]$, $f(x) \leqslant f(\gamma) < f(u)$. Ainsi $\gamma + h \in E_x$ et γ n'est pas la borne supérieure de E_x.

On a montré $E_x = [x,b]$. Puisque $x \in [a,b[$ peut être choisi arbitrairement, on en déduit que, pour tous $x, y \in [a,b]$ tels que $x < y$, on a $f(x) \leqslant f(y)$, donc f est croissante sur $[a,b]$.

c) Montrons que f est *strictement* croissante. Soient $x, y \in [a,b]$, $x < y$. En utilisant a), on obtient $z \in]x,y]$ tel que $f(x) < f(z)$. On a, en utilisant la croissance de f, $f(x) < f(z) \leqslant f(y)$, donc f est strictement croissante.

2. On suppose que, pour tout $x \in [a,b[$, $f'_d(x) \geqslant 0$.

Pour tout $\varepsilon > 0$, on définit une fonction $g_\varepsilon : [a,b] \to \mathbb{R}$ par $x \mapsto g_\varepsilon(x) := f(x) + \varepsilon x$. On a $(g_\varepsilon)'_d = f'_d + \varepsilon > 0$ et, d'après 1., g_ε est strictement croissante sur $[a,b]$. Ainsi :

$$\forall \varepsilon > 0,\ \forall x, y,\ \text{ tels que } a \leqslant x < y \leqslant b : f(x) < f(y) + \varepsilon(y-x).$$

On en déduit, en passant à la limite quand ε tend vers 0 :

$$\forall x, y, \text{ tels que } a \leqslant x < y \leqslant b : f(x) \leqslant f(y).$$

La fonction f est croissante.

On retrouve, par une autre méthode, un résultat de l'exercice IV.2.0.

IV.2.17 Si I est réduit à un point le résultat est évident. On peut donc supposer que I contient au moins deux points.

Montrons que, pour tous $a, b \in I$, tels que $a < b$, l'intervalle fermé d'extrémités $f'(a)$ et $f'(b)$ est contenu dans $f'(I)$, c'est-à-dire que $f'(I)$ est convexe. Le résultat s'en déduira, d'après la proposition 15.

On définit deux fonctions $\psi_a,\ \psi_b : [a, b] \to \mathbb{R}$, par :

$$\psi_a(a) := f'(a) \quad \text{et} \quad \psi_a(x) := \frac{f(x) - f(a)}{x - a} \ \text{ si } \ x > a,$$

$$\psi_b(b) := f'(b) \quad \text{et} \quad \psi_b(x) := \frac{f(x) - f(b)}{x - b} \ \text{ si } \ x < b.$$

Ces fonctions sont continues, donc $J_a = \psi_a([a, b])$ et $J_b = \psi_b([a, b])$ sont des segments. On a $J_a \subset f'(I)$, puisque $\varphi_a(a) = f'(a)$ et que, d'après la formule des accroissements finis, pour tout $x > a$, il existe $\xi \in]a, x[$ tel que $\psi_a(x) = f'(\xi)$. De même $J_b \subset f'(I)$. Notons $\mu := \frac{f(b)-f(a)}{b-a} = \psi_a(b) = \psi_b(a)$. On a $\mu \in J_a$ et $\mu \in J_b$, donc $\mu \in J_a \cap J_b$ et $J_a \cup J_b \neq \varnothing$. On en déduit que $J_a \cup J_b$ est un intervalle. Cet intervalle est contenu dans $f'(I)$ et il contient $f'(a) \in J_a$ et $f'(b) \in J_b$. D'où le résultat.

IV.2.18 1. Sur l'intervalle $[1, +\infty[$, la fonction $x \mapsto \dfrac{2x^2 + x + 2}{x^2 + 1}$, de dérivée $\dfrac{1 - x^2}{(x^2 + 1)^2} < 0$ (sauf en $x = 1$) décroît strictement de $5/2$ à 2 (exclu). La fonction inverse est donc définie sur $]\,2, 5/2\,]$: l'équation $2x^2 + x + 2 = y(x^2 + 1)$ ayant pour seule racine convenable $\dfrac{1 + \sqrt{(2y - 3)(5 - 2y)}}{2(y - 2)} \geqslant 1$, la fonction cherchée est donc définie par :

$$y \mapsto \frac{1 + \sqrt{-4y^2 + 16y - 15}}{2y - 4}.$$

2. Sur l'intervalle $\left[-\frac{1}{2}, +\infty\right[$, la fonction continue $x \mapsto x^2 + x + 1$ croît strictement de $3/4$ à $+\infty$, et son inverse, continue également, décroît strictement de $4/3$ à 0 (exclu). La fonction inverse est donc définie sur $]\,0, 4/3\,]$: l'équation $x^2 + x + 1 = 1/y$ ayant pour seule racine convenable $\dfrac{-1 + \sqrt{\frac{4}{y} - 3}}{2} \geqslant -\dfrac{1}{2}$, la fonction cherchée est donc définie par :

$$y \mapsto \frac{-1 + \sqrt{\frac{4}{y} - 3}}{2}.$$

IV.2.19 1. L'étude de la fonction auxiliaire impaire définie par $f(x) := x - \sin x$, nulle en 0 et de dérivée $1 - \cos x \geqslant 0$ montre que $\sin x \leqslant x$ pour $x \geqslant 0$.

Par imparité, on a bien $|\sin x| \leqslant |x|$, avec même inégalité stricte si $x \neq 0$.

2. L'étude de la fonction auxiliaire définie par $g(x) := x\sin x - 1 + \cos x$, nulle en 0 et de dérivée $x\cos x \geqslant 0$ sur l'intervalle considéré montre qu'alors $1 - \cos x \leqslant x\sin x$. (Puisque le premier membre est toujours positif ou nul, on voit que l'inégalité ne peut subsister partout, par exemple pour des réels $x > 0$ tels que $\sin x < 0$.)
3. La fonction $\arcsin$ est définie dans le module suivant ; on a $y = \arcsin x$ si, et seulement si, $x = \sin y$ et $|x| \leqslant \dfrac{\pi}{2}$.

   Alors $\cos y = \sqrt{1-x^2}$ et la relation demandée s'écrit $|y| \leqslant |\tan y|$ sur $]-\pi/2, \pi/2[$. Pour prouver cela, introduisons la fonction auxiliaire impaire définie sur cet intervalle par $h(y) := \tan y - y$, nulle en 0 et de dérivée $\tan^2 y \geqslant 0$. Par parité, on a bien $|y| \leqslant |\tan y|$ pour $-1 < x < 1$.

IV.2.20 1. (a) Par hypothèse, $\dfrac{f(x)-f(0)}{x} = \dfrac{f(x)}{x}$ est supérieur ou égal à 1 et admet une limite $f'(0)$ en 0 : celle-ci est donc supérieure ou égale à 1.

   (b) Le théorème des accroissements finis montre que, pour tout $n > 0$, il existe u_n strictement compris entre 0 et $1/n$ tel que $f'(u_n) = \dfrac{f(1/n)-f(0)}{1/n} = nf\Big(\dfrac{1}{n}\Big) \geqslant 1$. La suite (u_n) ainsi construite converge alors vers 0.

2. Par hypothèse, $\dfrac{f'(x)-f'(0)}{x-0} = \dfrac{f'(x)-1}{x}$ a une limite $f''(0)$ en 0. Si l'on pose $x = u_n$, on voit que $x \to 0$ et $f(x) \geqslant 1$, d'où $\dfrac{f'(u_n)-1}{u_n} \geqslant 0$ d'où $f''(0) \geqslant 0$.

3. (a) En 0, on a $\dfrac{g(x)-g(0)}{x-0} = 1 + x + \sin x \sin\dfrac{1}{x} \to 1$ puisque $\sin x \to 0$ et $\big|\sin(1/x)\big| \leqslant 1$. Donc g est dérivable en 0 et $g'(0) = 1$. Pour $x \neq 0$, on trouve par le calcul :

$$g'(x) = 1 + 2x + x\cos x \sin\frac{1}{x} + \frac{\sin x}{x}\Big(x\sin\frac{1}{x} - \cos\frac{1}{x}\Big).$$

   Par suite g est de classe $\mathcal{C}^1$ (et même $\mathcal{C}^\infty$) sur $\mathbb{R}^*$. Sa dérivée n'est pas continue en 0 : en effet, si l'on pose $v_n = \dfrac{1}{2n\pi} \to 0$, on a $\cos\dfrac{1}{v_n} = 1$ et $g'(v_n) \to 0 \neq 1 = g'(0)$.

   (b) La relation $g(x) \geqslant x$ est vraie pour $x = 0$. Si $x > 0$, on a :

$$g(x) - x = x^2 + x\sin x \sin\frac{1}{x} = x^2 + xh(x)$$

   avec $\big|h(x)\big| \leqslant \big|\sin x\big| \leqslant x$, d'où $xh(x) \geqslant -x^2$ et $g(x) \geqslant x$ (il est d'ailleurs facile de montrer qu'en fait l'inégalité est alors stricte).

IV.2.21 Considérons les fonctions auxiliaires $f(x) := \ln(1+x) - \dfrac{x}{x+1}$ et $g(x) := \ln(1+x) - x$. Alors $f(0) = g(0) = 0$ et, pour $x > -1$:

$$f'(x) = \frac{x}{(x+1)^2}, \qquad g'(x) = -\frac{x}{x+1}.$$

Par suite, $0 = f(0)$ est un minimum pour f, qui est donc positive, et un maximum pour g, qui est donc négative, d'où l'encadrement désiré.

IV.2.22 On note :

$$A := \frac{f(a) - 2f(a+h) + f(a+2h)}{h^2}.$$

Soit $\varphi : [0, h] \to \mathbb{R}$ la fonction définie par $x \mapsto \varphi(x) := f(a) - 2f(a+x) + f(a+2x) - Ax^2$. Cette fonction est deux fois dérivable sur $[0, h]$ et l'on a $\varphi(0) = 0$ et $\varphi(h) = 0$ (d'après la définition de A). D'après le théorème de Rolle, il existe $c \in]0, h[$ tel que $\varphi'(c) = 0$, c'est-à-dire $f'(a + 2c) - f'(a + c) = Ac$.

En appliquant la formule des accroissements finis à f' sur $[a + c, a + 2c]$, on obtient $d \in]a + c, a + 2c[$ tel que $cf''(d) = Ac$, c'est-à-dire $f''(d) = A$, puisque $c \neq 0$. On a $d \in]a + h, a + 2h[$, il existe donc $\theta \in]0, 1[$ tel que $d = a + 2\theta h$.

IV.2.23 Soient $x, y \in \mathbb{R}$, $y \neq 0$. En utilisant la formule de Taylor-Lagrange à l'ordre deux, on obtient $\theta_+, \theta_- \in]0, 1[$ tels que :

$$f(x + y) = f(x) + yf'(x) + \frac{y^2}{2} f''(x + \theta_+ y)$$

$$f(x - y) = f(x) - yf'(x) + \frac{y^2}{2} f''(x - \theta_- y).$$

En utilisant $f(x + y)f(x - y) - f^2(x) \leqslant 0$ et $y^2 \neq 0$, on en déduit :

$$-f'^2(x) + \frac{1}{2} f(x) \left(f''(x + \theta_+ y) + f''(x - \theta_- y)\right) + \frac{y}{2} f'(x) \left(-f''(x + \theta_+ y) + f''(x - \theta_- y)\right) + \frac{y^2}{4} f''(x + \theta_+ y) f''(x - \theta_- y) \leqslant 0.$$

Dans l'inégalité ci-dessus on fixe x et l'on fait tendre y vers 0. Alors $\theta_+ y$ et $\theta_- y$ tendent vers 0 et, en utilisant la continuité de f'', on montre que le premier membre de l'inégalité tend vers $-f'^2(x) + f(x)f''(x)$, donc $-f'^2(x) + f(x)f''(x) \leqslant 0$.

IV.2.24 D'après l'exercice 6 de la page 629, il existe un réel a tel que $P(a) = 0$. On en déduit que, pour tout $n \in \mathbb{N}$, $\left|f^{(n)}(a)\right| \leqslant \left|P(a)\right| = 0$ donc $f^{(n)}(a) = 0$.

On applique la formule de Taylor-Lagrange au point a. La partie régulière est nulle, donc, pour tout n et tout $x \in \mathbb{R}$, il existe c_n appartenant à l'intervalle ouvert d'extrémités a et x tel que $f(x) = f^{(n+1)}(c_n) \frac{(x-a)^{n+1}}{(n+1)!}$. On en déduit $\left|f(x)\right| \leqslant \left|P(c_n)\right| \frac{|x-a|^{n+1}}{(n+1)!}$. La fonction $|P|$ est continue, donc majorée par $M > 0$ sur l'intervalle d'extrémités a et x. Par suite, $\left|P(c_n)\right| \frac{|x-a|^{n+1}}{(n+1)!} \leqslant M \frac{|x-a|^{n+1}}{(n+1)!}$ et, à x fixé, le terme majorant tend vers 0 quand n tend vers $+\infty$. On en déduit $f(x) = 0$.

Soient $f := \sin$ et $P := x^2 + 1$. On a, pour tout $x \in \mathbb{R}$, et tout $n \in \mathbb{N}$, $\left|f^{(n)}(x)\right| \leqslant 1 \leqslant P(x)$. Le résultat est donc faux pour un polynôme de degré pair.

IV.2.25 1. On a $f''(t) = \frac{e^t}{(1+e^t)^2} \geqslant 0$, donc f est convexe sur $\mathbb{R}$.

2. Le résultat est trivial si $x = 0$ ou $y = 0$. On peut donc supposer $x > 0$ et $y > 0$. Notons $u := \ln x$ et $v := \ln y$. Puisque f est convexe, on a : $f(\lambda u + \mu v) \leqslant \lambda f(u) + \mu f(v)$, c'est-à-dire :
$$\ln(1 + e^{\lambda u + \mu v}) \leqslant \lambda \ln(1 + e^u) + \mu \ln(1 + e^v)$$
et, en utilisant la croissance de la fonction exponentielle $1 + x^\lambda y^\mu \leqslant (1 + x)^\lambda (1 + y)^\mu$.

IV.2.26 La fonction $\ln$ est concave. En utilisant la proposition 59 pour la fonction convexe $-\ln$, on obtient :
$$\frac{1}{n}\sum_{n=1}^{n} \ln x_i \leqslant \ln\left(\frac{1}{n}\sum_{n=1}^{n} x_i\right),$$
d'où, en utilisant la croissance de la fonction exponentielle :
$$\sqrt[n]{x_1 \dots x_n} \leqslant \frac{1}{n}\sum_{n=1}^{n} x_i.$$

IV.2.27 Soient $x,\ y \in I$ et $\lambda \in [0, 1]$.

Supposons $x \leqslant y$. On a, en utilisant l'hypothèse pour le triplet $(x, \lambda x + (1 - \lambda)y, y)$:
$$\begin{vmatrix} 1 & 1 & 1 \\ x & \lambda x + (1-\lambda)y & y \\ f(x) & f(\lambda x + (1-\lambda)y) & f(y) \end{vmatrix} \geqslant 0.$$
Par combinaison linéaire de colonnes, on en déduit :
$$\begin{vmatrix} 1 & 0 & 1 \\ x & 0 & y \\ f(x) & f(\lambda x + (1-\lambda)y) - \lambda f(x) - (1-\lambda) f(y) & f(y) \end{vmatrix} \geqslant 0.$$
De l'inégalité ci-dessus et de $x - y \leqslant 0$, l'on déduit :
$$f(\lambda x + (1 - \lambda)y) - \lambda f(x) - (1 - \lambda) f(y) \leqslant 0,$$
d'où (21) et la convexité de f.

IV.2.28 Soient $\mu_1, \dots,\ \mu_n$ des réels positifs non tous nuls et $x_1, \dots,\ x_n$ des réels positifs. En utilisant la convexité de la fonction $x \mapsto x^p$ pour $p > 1$ et la proposition 59, on obtient :
$$\left(\frac{\sum_{i=1}^{n} \mu_i x_i}{\sum_{i=1}^{n} \mu_i}\right)^p \leqslant \frac{\sum_{i=1}^{n} \mu_i x_i^p}{\sum_{i=1}^{n} \mu_i}.$$
D'où :
$$\sum_{i=1}^{n} \mu_i x_i \leqslant \left(\sum_{i=1}^{n} \mu_i x_i^p\right)^{1/p} \left(\sum_{i=1}^{n} \mu_i\right)^{1-\frac{1}{p}}.$$
On obtient alors le résultat en posant $\mu_i := b_i^q$ et $x_i := a_i b_i^{-q/p}$.

IV.2.29 1. La fonction f est dérivable sur $]0,1[$ et :

$$f'(x) = -x^{\frac{1}{p}-1}(1-x^{1/p})^{p-1}.$$

On vérifie, en utilisant les propriétés des fonctions puissances, que f' est croissante sur $]0,1[$. On en déduit que f est convexe sur $]0,1[$, puis, f étant continue sur $[0,1]$, qu'elle est convexe sur $[0,1]$.

2. On suppose d'abord que, pour tout $i \in [\![1,n]\!]$, $a_i+b_i \neq 0$. On pose, pour tout $i \in [\![1,n]\!]$, $x_i := \frac{a_i^p}{(a_i+b_i)^p}$ et $\lambda_i := \frac{(a_i+b_i)^p}{\sum\limits_{j=1}^{n}(a_j+b_j)^p}$. On a $\sum\limits_{i=1}^{n}\lambda_i = 1$.

D'après la proposition 59, on a :

$$f(\lambda_1 x_1 + \cdots + \lambda_n x_n) \leqslant \lambda_1 f(x_1) + \cdots + \lambda_n f(x_n),$$

c'est-à-dire :

$$\left(1 - \frac{\left(\sum\limits_{j=1}^{n} a_j^p\right)^{1/p}}{\left(\sum\limits_{j=1}^{n}(a_j+b_j)^p\right)^{1/p}}\right)^p \leqslant \frac{\sum\limits_{j=1}^{n} b_j^p}{\sum\limits_{j=1}^{n}(a_j+b_j)^p}$$

et

$$1 - \frac{\left(\sum\limits_{j=1}^{n} a_j^p\right)^{1/p}}{\left(\sum\limits_{j=1}^{n}(a_j+b_j)^p\right)^{1/p}} \leqslant \frac{\left(\sum\limits_{j=1}^{n} b_j^p\right)^{1/p}}{\left(\sum\limits_{j=1}^{n}(a_j+b_j)^p\right)^{1/p}}.$$

L'inégalité (28) s'en déduit.

Supposons que, pour certaines valeurs de i, l'on ait $a_i + b_i = 0$. Alors $a_i = b_i = 0$ et l'on est ramené à prouver le résultat pour une valeur strictement inférieure de n.

3. Les propriétés (i) et (ii) sont faciles. La propriété (iii) résulte immédiatement de l'inégalité de Minkowski (28).

Si $p = 2$, $\|x\|_2$ est la norme euclidienne de $x \in \mathbb{R}^n$ dont on retrouve les propriétés (*cf.* la définition 16 et la proposition 28 de la page 458 du module III.1).

Dans ce cas l'inégalité de Hölder est l'inégalité de Cauchy-Schwarz (*cf.* le théorème 32 de la page 460 du module III.1).

IV.2.30 On utilise les notations de l'exercice précédent :

$$a := (a_1,\ldots,a_n),\ \ b := (b_1,\ldots,b_n),\ \ \|a\|_p := \left(\sum_{i=1}^{n} a_i^p\right)^{1/p},\ \ \|b\|_q := \left(\sum_{i=1}^{n} b_i^q\right)^{1/q}.$$

On pose, pour tout $i \in [\![1,n]\!]$, $x_i := a_i/\|a\|_p$ et $y_i := b_i/\|b\|_p$. En utilisant l'inégalité de Young (26) de la page 661, on obtient :

$$\forall i \in [\![1,n]\!],\ \ x_i y_i \leqslant \frac{x_i^p}{p} + \frac{y_i^q}{q}.$$

En sommant, on en déduit :

$$\sum_{i=1}^{n} x_i y_i \leqslant \frac{1}{p}\frac{\sum_{i=1}^{n} x_i^p}{\sum_{i=1}^{n} x_i^p} + \frac{1}{q}\frac{\sum_{i=1}^{n} y_i^q}{\sum_{i=1}^{n} y_i^q} = \frac{1}{p} + \frac{1}{q} = 1.$$

On a $\sum_{i=1}^{n} x_i y_i = \frac{1}{\|a\|_p \|b\|_q} \sum_{i=1}^{n} a_i b_i$, donc $\sum_{i=1}^{n} a_i b_i \leqslant \|a\|_p \|b\|_q$, c'est-à-dire l'inégalité de Hölder.

IV.2.31 1. On considère la fonction $\varphi_1 : x \in \mathbb{R}_+^* \setminus \{1\} \mapsto \varphi_1(x) := \frac{f(x)-f(1)}{x-1}$. Elle est croissante, donc elle admet une limite $\ell \in \mathbb{R} \cup +\infty$ quand x tend vers $+\infty$. On a $\frac{f(x)}{x} = \frac{x-1}{x}\varphi_1(x) + \frac{f(1)}{x}$, donc $f(x)/x$ tend vers $\ell \in \mathbb{R} \cup +\infty$ quand x tend vers $+\infty$.

2. On supose $\ell \leqslant 0$. On raisonne par l'absurde. Supposons que f n'est pas décroissante. Alors, il existe $a, b \in R_+^*$, tels que $a < b$ et $f(a) < f(b)$. On a :

$$\forall x \geqslant b, \quad 0 < \varphi_a(b) = \frac{f(b)-f(a)}{b-a} \leqslant \varphi_a(x) = \frac{f(x)-f(a)}{x-a}.$$

Mais $\frac{f(x)-f(a)}{x-a}$ tend vers $\ell \geqslant 0$ quand x tend vers $+\infty$ et l'on obtient une contradiction.

IV.2.32 La fonction est définie partout sauf pour 1 et -1. Sa dérivée vaut :

$$f'(x) = \frac{2x^3(x^2-2)}{(x^2-1)^2}.$$

Par parité de f, il suffit d'étudier son graphe sur $[\,0, 1\,[\cup]\,1, +\infty\,[$. Sur le premier intervalle, il y a décroissance stricte de $0 = f(0)$ jusqu'à $-\infty$. Sur le second, il y a d'abord décroissance stricte de $+\infty$ jusqu'à $f(\sqrt{2}) = 4$, puis croissance stricte de 4 à $+\infty$. Le graphe comporte deux asymptotes verticales en ± 1 ; en $\pm\infty$, la branche est parabolique puisque $f(x)$ « se comporte alors comme x^2 ».

On peut remarquer qu'un grapheur (par exemple une calculatrice de poche à petit écran), utilisé trop rapidement, risque de faire oublier les branches positives pour $|x| > 1$, puisque l'ordonnée minimale $y = 4$ sort généralement des limites de l'affichage (hors réglage spécial).

IV.2.33 1. Soit ε le signe de x. Alors :

$$\frac{f(x)}{x} = 3 + \frac{2}{x} - \varepsilon\sqrt{4 - \frac{1}{x}}$$

a pour limites 1 en $+\infty$ et 5 en $-\infty$. Dans chacun de ces cas :

$$\begin{aligned} f(x) - x &= 2x + 2 - \sqrt{4x^2 - x} \\ &= \frac{(2x+2)^2 - (4x^2 - x)}{2x + 2 + \sqrt{4x^2 - x}} = \frac{5x+4}{2x+2+\sqrt{4x^2-x}} \to \frac{5}{4}. \\ f(x) - 5x &= -2x + 2 - \sqrt{4x^2 - x} \\ &= \frac{(2x-2)^2 - (4x^2 - x)}{-2x + 2 + \sqrt{4x^2 - x}} = \frac{-3x+4}{-2x+2+\sqrt{4x^2-x}} \to \frac{3}{4}. \end{aligned}$$

Il y a donc deux asymptotes, d'équations respectives $y = x + 5/4$ et $y = 5x + 3/4$.

2. Il est tout à fait clair que $y = 3x - 5$ est une asymptote du graphe de f au voisinage de $+\infty$. Au voisinage de $x = 0$, nous avons une asymptote verticale d'équation $x = 0$. Au voisinage de $-\infty$, le rapport :

$$\frac{f(x)}{x} = 3 - \frac{5}{x} - \left(x + \frac{3}{x}\right) \frac{1}{1 - e^{2x}}$$

tend vers $+\infty$, d'où une branche parabolique dans la direction de l'axe des ordonnées négatives.

3. Il est clair que $f(x)/x$ tend vers 2 au voisinage de $+\infty$, mais $f(x) - 2x = 1 - \sqrt{x}$ tend vers $-\infty$, d'où une branche parabolique dans la direction $y = 2x$.

Module IV.3 : Fonctions transcendantes

IV.3.1 On trouve $A = \cos 2\theta$ avec $\sin\theta = 3/5$, d'où $A = 1 - 2\sin^2\theta = 7/25$.

De même $\tan B = \dfrac{(1/2)+(1/3)}{1-(1/2)(1/3)} = 1$.

De plus, $0 \leqslant B \leqslant \arctan 1 + \arctan 1 = \pi/2$, donc $B = \pi/4$.

Enfin la formule d'addition sur les tangentes permet de trouver :

$$\tan C = \frac{2\sqrt{3}/2}{1-(\sqrt{3}/2)^2} = 4\sqrt{3}.$$

IV.3.2 On trouve aussitôt $A = |x|$ et $B = \dfrac{1}{\sqrt{1-x^2}}$ puisque $1 - \tanh^2 u = \dfrac{1}{\cosh^2 u}$.

IV.3.3 Une condition nécessaire s'obtient en écrivant que le membre de gauche a 1 pour tangente, soit :

$$1 = \tan(\arctan 2x + \arctan x) = \frac{2x+x}{1-2x^2} = \frac{3x}{1-2x^2}.$$

On est ainsi conduit à une équation du second degré $T(x) := 2x^2 + 3x - 1 = 0$, de racines :

$$x' = \frac{\sqrt{17}-3}{4} > 0 \qquad \text{et} \qquad x'' = \frac{-\sqrt{17}-3}{4} < 0.$$

Il est clair que x'' n'est pas solution, puisque $\arctan x'' < 0$ et $\arctan 2x'' < 0$.

Posons $A := \arctan 2x' + \arctan x'$. Comme $\tan A = 1$, on sait que A est congru à $\pi/4$ modulo π. Or, $0 \leqslant A \leqslant \pi/2$, donc $A = \pi/4$.

L'équation admet donc une unique solution x'.

> ***Remarque***. On aurait aussi pu montrer l'existence d'une solution (positive) en étudiant les variations (évidentes) de $x \mapsto \arctan 2x + \arctan x$, ce qui aurait montré que x' était bien solution puisque c'était la seule possible.

IV.3.4 Soit donc à calculer $f(x) = \cos^2\theta$ où θ est tel que $\tan\theta = x$ (le fait que $|\theta| < \pi/2$ sera ici sans importance). On a $1+x^2 = 1+\tan^2\theta = 1/\cos^2\theta$ montre aussitôt que $f(x) = 1/(1+x^2)$.

Soit maintenant $g(x) = \arctan t$ où $t := \sqrt{\dfrac{1-\cos x}{1+\cos x}} = \sqrt{\tan^2(x/2)} = \big|\tan(x/2)\big|$. On remarque d'abord que g est paire et périodique de période 2π. Supposons donc $x \in [\,0, \pi\,[$ (la valeur maximale est interdite puisqu'alors $\cos x = -1$). On a aussitôt dans ce cas $g(x) = x/2$. La solution générale, définie pour $\cos x \neq -1$ est donc $g(x) = |(x/2) - k\pi|$ où k est la partie entière de $(x+\pi)/(2\pi)$, c'est-à-dire encore l'entier le plus proche de $x/2\pi$.

IV.3.5 1. Posons $t := \mathrm{e}^x > 0$. On est alors conduit à résoudre l'équation :

$$0 = t - \frac{1}{t} - \frac{1}{2}\Big(t + \frac{1}{t}\Big) - 1 = \frac{t^2-2t-3}{2t} = \frac{(t+1)(t-3)}{2t}.$$

La racine $t = -1$ est négative et donc à rejeter ; reste la seconde, $t = 3$, qui conduit à $x = \ln 3$ qui convient effectivement.

2. L'équation posée équivaut aux suivantes (bien vérifier que c'est le cas pour chaque passage à la ligne) :

$$\ln(x+\sqrt{x^2-1}) = \ln(2-x+\sqrt{(2-x)^2+1}),$$
$$x+\sqrt{x^2-1} = 2-x+\sqrt{x^2-4x+5},$$
$$(2x-2+\sqrt{x^2-1})^2 = x^2-4x+5,$$
$$5x^2-8x+3+4(x-1)\sqrt{x^2-1} = x^2-4x+5$$

ce qui implique enfin :

$$0 = 16(x-1)^2(x^2-1) - (-4x^2+4x+2)^2 = 16x-20.$$

La seule racine possible est donc $x = 5/4 > 1$. Or il existe au moins une racine, puisque le premier membre de l'équation est une fonction croissante A et le second une fonction décroissante B, telles que $B(1) - A(1) = \ln(1+\sqrt{2}) > 0$ et que $B - A$ décroît vers $-\infty$ au voisinage de $+\infty$.
D'ailleurs, pour $A(5/4) = \ln 2 = B(5/4)$.

IV.3.6 1. On trouve $\cosh 3x = 4\cosh^3 x - 3\cosh x$.

2. Ce domaine est défini par l'inégalité $4x^3 - 3x \geqslant 1$, soit $x \geqslant 1$ ou $x = -1/2$ puisque :

$$4x^3 - 3x - 1 = (x-1)(2x+1)^2.$$

3. Cela résulte de la première question puisque, posant $x = \cosh t$, on a :

$$\cosh 3t = 4\cosh^3 t - 3\cosh t = 4x^3 - 3x.$$

IV.3.7 1. On a $1+ab-a-b = (1-a)(1-b) > 0$, donc $0 \leqslant \frac{a+b}{1+ab} < 1$ et $\operatorname{argtanh}\frac{a+b}{1+ab}$ est bien défini. La fonction $\tanh$ est un isomorphime de $\mathbb{R}$ sur $]-1,1[$.

Par suite, pour montrer $\operatorname{argtanh} a + \operatorname{argtanh} b = \operatorname{argtanh}\frac{a+b}{1+ab}$, il suffit de montrer que les images par $\tanh$ des deux membres de l'égalité sont égales, c'est-à-dire :

$$\tanh(\operatorname{argtanh} a + \operatorname{argtanh} b) = \frac{a+b}{1+ab}.$$

Cette égalité est vraie d'après la formule d'addition pour $\tanh$ (*cf.* la proposition 24).

2. On associe à $0 \leqslant v < c$, $w := c\operatorname{argtanh}\frac{v}{c}$. On dit que w est la *rapidité* associée à la vitesse v. Montrons que la loi de composition des vitesses se traduit par *l'addition* des rapidités.

Notons w_1, w_2 et w les rapidités associées respectivement à v_1, v_2 et $v_1 \oplus v_2$. On a :

$$\begin{aligned} w_1 + w_2 &= c\operatorname{argtanh}\frac{v_1}{c} + c\operatorname{argtanh}\frac{v_2}{c} \\ &= c\operatorname{argtanh}\frac{1}{c}\frac{v_1+v_2}{1+\frac{v_1v_2}{c^2}} \\ &= c\operatorname{argtanh}\frac{v_1 \oplus v_2}{c} = w. \end{aligned}$$

IV.3.8 1. Le déterminant de $\Phi(\theta)$ est $\cosh^2\theta - \sinh^2\theta = 1 \neq 0$, donc $\Phi(\theta) \in GL_2(\mathbb{R})$. En utilisant les formules d'addition (*cf.* la proposition 24 de la page 694), on vérifie, pour tous $\theta_1, \theta_2 \in \mathbb{R}$:

$$\begin{aligned}\Phi(\theta_1+\theta_2) &= \begin{pmatrix} \cosh(\theta_1+\theta_2) & -\sinh(\theta_1+\theta_2) \\ -\sinh(\theta_1+\theta_2) & \cosh(\theta_1+\theta_2)\end{pmatrix} \\ &= \begin{pmatrix} \cosh\theta_1 & -\sinh\theta_1 \\ -\sinh\theta_1 & \cosh\theta_1\end{pmatrix}\begin{pmatrix} \cosh\theta_2 & -\sinh\theta_2 \\ -\sinh\theta_2 & \cosh\theta_2\end{pmatrix}\end{aligned}$$

et $\Phi(0)$ est la matrice identité I, donc Φ est un homomorphisme de groupes.

Si $\Phi(t) = I$, on a $\cosh t = 1$, donc $t = 0$. Par suite le noyau de Φ est réduit à $\{0\}$ et Φ est injective (*cf.* le théorème 20 de II.2 2.2, page 126). L'image de l'homomorphisme Φ est un sous-groupe de $GL_2(\mathbb{R})$.

Si la matrice $M := \begin{pmatrix} a & b \\ c & d\end{pmatrix}$ appartient à l'image de Φ, on a $a = d \geqslant 0$, $b = c$ et $a^2 - b^2 = 1$. Supposons inversement que ces conditions soient satisfaites. On a $a \geqslant 1$. Posons $\tau := \operatorname{argcosh} a$. On a $\cosh^2\tau - b^2 = a^2 - b^2 = 1 = \cosh^2\tau - \sinh^2\tau$, donc $\sinh\tau = \pm b$. On a $\tau \geqslant 0$, donc $\sinh\tau \geqslant 0$.

Si $b \geqslant 0$, on a $\Phi(-\tau) = M$. Si $b < 0$, on a $\Phi(\tau) = M$. Donc M appartient à l'image de Φ.

2. On écrit $\Phi(\theta)$ sous forme de transformation de Lorentz L_γ en posant $\gamma := \tanh\theta$:

$$\begin{aligned}\Phi(\theta) &:= \begin{pmatrix} \cosh\theta & -\sinh\theta \\ -\sinh\theta & \cosh\theta\end{pmatrix} = \cosh\theta\begin{pmatrix} 1 & -\tanh\theta \\ -\tanh\theta & 1\end{pmatrix} \\ &= \frac{1}{\sqrt{1-\tanh^2\theta}}\begin{pmatrix} 1 & -\tanh\theta \\ -\tanh\theta & 1\end{pmatrix} = \frac{1}{\sqrt{1-\gamma^2}}\begin{pmatrix} 1 & -\gamma \\ -\gamma & 1\end{pmatrix}.\end{aligned}$$

Inversement, à $\gamma \in]-1, 1[$ on associe $\theta := \operatorname{argtanh}\gamma$ et l'on a $L_\gamma = \Phi(\theta)$. On en déduit que le produit de deux transformations de Lorentz L_{γ_1} et L_{γ_2} est une transformation de Lorentz L_γ. En effet $L_{\gamma_1} = \Phi(\theta_1)$ et $L_{\gamma_2} = \Phi(\theta_2)$, donc $L_{\gamma_1}L_{\gamma_2} = \Phi(\theta_1+\theta_2) = \Phi(\theta) = L_\gamma$, en posant $\theta := \theta_1 + \theta_2$ et $\gamma = \operatorname{argth}\theta$.

En utilisant $\operatorname{argth}\theta = \operatorname{argth}(\theta_1+\theta_2) = \frac{\operatorname{argth}\theta_1 + \operatorname{argth}\theta_2}{1+\operatorname{argth}\theta_1\operatorname{argth}\theta_2}$, la loi de produit se traduit par $\gamma_1 \oplus \gamma_2 := \gamma := \frac{\gamma_1+\gamma_2}{1+\gamma_1\gamma_2}$. On retrouve la loi de composition des vitesses de l'exercice précédent IV.3.7 : si $c = 1$, θ est la rapidité associée à la vitesse γ.

En relativité on note (t, x) au lieu de (u, v) (t est la variable de temps et x celle d'espace). Si l'on ne suppose pas $c = 1$, on remplace dans les formules t par ct et γ par v/t (v étant la vitesse relative d'un repère par rapport à l'autre).

3. C'est un calcul simple (on utilise $\cosh^2\theta - \sinh^2\theta = 1$). Si $\mu := u^2 - v^2$ n'est pas nul, les points (u, v) et (u_θ, v_θ) dans le plan euclidien appartiennent à une même hyperbole équilatère H_μ d'équation $X^2 - Y^2 = \mu$. Par suite les hyperboles H_μ sont conservées par les applications linéaires $\Phi(t)$. Pour $\mu = 0$, on vérifie que les deux droites $X + Y = 0$ et $X - Y = 0$ sont conservées par $\Phi(\theta)$ (ce sont les sous-espaces propres de $\Phi(\theta)$ associés respectivement aux valeurs propres $\mathrm{e}^{-\theta}$ et e^{θ}).

4. On a, pour tout $\theta \in \mathbb{R}$:

$$\mathrm{e}^{\theta} = \sum_{n\in\mathbb{N}} \frac{\theta^n}{n!} = \sum_{p\in\mathbb{N}} \frac{\theta^{2p}}{(2p)!} + \sum_{p\in\mathbb{N}} \frac{\theta^{2p+1}}{(2p+1)!},$$

d'où , en prenant les parties paires et impaires (en vérifiant les convergences) :

$$\cosh\theta = \sum_{p\in\mathbb{N}} \frac{\theta^{2p}}{(2p)!} \quad \text{et} \quad \sinh\theta = \sum_{p\in\mathbb{N}} \frac{\theta^{2p+1}}{(2p+1)!}.$$

On a $A^2 = I$, donc, pour tout $p \in \mathbb{N}$, $A^{2p} = I$ et $A^{2p+1} = A$. En utilisant la définition de l'exponentielle d'une matrice (*cf.* la définition 25 de la page 795) on a alors :

$$\mathrm{e}^{\theta A} = I + \theta A + \frac{\theta^2}{2!}A^2 + \cdots + \frac{\theta^n}{n!}A^n + \cdots = \sum_{p\in\mathbb{N}} \frac{\theta^{2p}}{(2p)!}\, I + \sum_{p\in\mathbb{N}} \frac{\theta^{2p+1}}{(2p+1)!}\, A$$
$$= \cosh\theta\, I + \sinh\theta\, A = \Phi(\theta).$$

On a $\frac{d}{d\theta}\mathrm{e}^{\theta A} = A\,\mathrm{e}^{\theta A}$ (*cf.* la proposition 33 de la page 795), donc $\left(\frac{d}{d\theta}\mathrm{e}^{\theta A}\right)_{\theta=0} = A$. Pour que $\Phi(\theta) = \mathrm{e}^{\theta A}$, il est donc nécessaire que $\Phi'(0) = A$, ce que l'on vérifie immédiatement en utilisant $\Phi'(\theta) := \begin{pmatrix} \sinh\theta & -\cosh\theta \\ -\cosh\theta & \sinh\theta \end{pmatrix}$.

5. On remplace $\Phi(\theta)$ par la matrice de rotation $R(\theta) := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. Le déterminant de $R(\theta)$ est égal à 1 et $R : \mathbb{R} \mapsto GL_2(\mathbb{R})$ est un homomorphisme de groupes de $(\mathbb{R}, +)$ dans le groupe multiplicatif $GL_2(\mathbb{R})$. Le noyau de R est le groupe $2\pi\mathbb{Z}$ et son image est formée des matrices $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ telles que $a^2 + b^2 = 1$.

Soient $(x, y) \in \mathbb{R}^2$ et $\theta \in \mathbb{R}$. On note $\begin{pmatrix} x_\theta \\ y_\theta \end{pmatrix} := R(\theta)\begin{pmatrix} x \\ y \end{pmatrix}$. On a alors $x_\theta^2 + y_\theta^2 = x^2 + y^2$. Par suite, les matrices $R(\theta)$ conservent les cercles centrés à l'origine du plan vectoriel euclidien.

Soit $B := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. On vérifie que, pour tout $\theta \in \mathbb{R}$, $\mathbb{R}(\theta) = \mathrm{e}^{\theta B}$ (on utilise $B^2 = -I$, $B^3 = -B$, $B^4 = I$). On a $R'(0) = B$.

IV.3.9 Cette fonction est bien définie sur $\mathbb{R}_+^*$. En écrivant $f(x) = \exp(\ln x/x)$, on voit que f a pour limite 0 lorsque $x \to 0^+$. On peut même montrer que la limite de $f(x)/x$ est alors nulle car $\left(\frac{1}{x} - 1\right)\ln x \to -\infty$.

Lorsque $x \to +\infty$, on voit que f tend (lentement...) vers 1 par valeurs supérieures.

Le maximum de f est obtenu lorsque $\ln x/x$ est maximum ; un calcul de dérivée immédiat montre que l'abscisse de ce maximum est e, voisin de $2{,}718$, et que sa valeur est $\mathrm{e}^{1/\mathrm{e}}$, soit approximativement $1{,}445$.

IV.3.10 Cette fonction impaire est 2π-périodique. Il suffit de l'étudier sur $[0, \pi]$ puis compléter son graphe par une symétrie relative à l'origine et une infinité de translations. Sur cet intervalle,

il existe deux valeurs de discontinuité, à savoir $\pi/2$ et $2\pi/3$, correspondant à des asymptotes dites verticales.

Le calcul de la dérivée est facile :

$$f'(x) = \frac{-2\cos^3 x + 4\cos x + 1}{\cos^2 x(1+2\cos x)^2} = \frac{g(\cos x)}{\cos^2 x(1+2\cos x)^2}.$$

L'étude des variations de g est triviale. Dans l'intervalle $[-1,1]$ g décroît à partir de la valeur négative -1 puis croît et enfin décroît jusqu'à la valeur positive 3 ; il existe donc une seule valeur de x dans $[0,\pi]$ qui annule f'. Puisque $g\big(\cos(2\pi/3)\big) = g(-1/2) = -3/4 < 0$ et $g\big(\cos(\pi/2)\big) = g(0) = 1 > 0$, il s'agit de l'abscisse d'un maximum, compris entre les deux asymptotes. Un calcul numérique à la machine donne environ $-7{,}737$ pour la valeur de ce maximum.

Cet exemple montre bien le danger de l'utilisation d'une calculatrice graphique standard pour résoudre cet exercice. Si son propriétaire ne lui donne pas des instructions de cadrage très précises, il y a toutes chances que la branche très étroite située entre les deux asymptotes échappe à son attention : les NTIC (alias nouvelles technologies de l'information et de la communication), tant vantées par les media…, peuvent simplifier et embellir la vie, mais aussi la rendre très aléatoire même dans des cas à l'apparence très anodine.

IV.3.11 Considérons les deux fonctions auxiliaires définies par :

$$g(x) := \mathrm{e}^x - x - 1 \qquad \text{et} \qquad h(x) := 1 - (1-x)\mathrm{e}^x.$$

Leurs dérivées valent respectivement $g'(x) = \mathrm{e}^x - 1$ et $h'(x) = x\mathrm{e}^x$, de signes évidents. Comme $g(0) = h(0) = 0$, il en résulte que $g(x) \geqslant 0$ et $h(x) \geqslant 0$ pour tout entier x, d'où la première inégalité de l'énoncé ; pour obtenir la seconde, il faut diviser par $1-x$ ce qui restreint son intervalle de vérité à $]-\infty, 1[$.

IV.3.12 1. Par hypothèse $x, y \in \mathbb{R}_+^*$, donc $\arctan x, \arctan y \in]0, \pi/2[$.

Montrons que $\arctan x + \arctan y = \pi/2$ si, et seulement si, $xy = 1$. Nous avons déjà vu que $\arctan x + \arctan 1/x = \pi/2$. Inversement, supposons que $\arctan y = \pi/2 - \arctan x$. En prenant les tangentes, on obtient $y = 1/x$.

Supposons $xy < 1$. Si $\arctan x + \arctan y \neq \pi/2$, on a :

$$\tan(\arctan x + \arctan y) = \frac{x+y}{1-xy}.$$

On a $0 \leqslant \arctan x < \pi/2$ et $0 \leqslant \arctan y < \pi/2$, donc $0 \leqslant \arctan x + \arctan y < \pi$. On ne peut pas avoir :

$$\arctan x + \arctan y = \pi/2$$

(puisque $xy \neq 1$), ni :

$$\pi/2 < \arctan x + \arctan y < \pi$$

(puisque l'on aurait alors $\tan(\arctan x + \arctan y) = \frac{x+y}{1-xy} < 0$ et $1 < xy$). On a donc $0 \leqslant \arctan x + \arctan y < \pi/2$ et, par suite $\arctan x + \arctan y = \arctan\left(\frac{x+y}{1-xy}\right)$.

2. On a $\frac{1}{(p+r)(p+q)} < 1$ si, et seulement si, $2p^2 + pr + pq + qr > 1$, c'est-à-dire $2p^2 + pr + pq > 0$, et cette dernière inégalité est vérifiée. On vérifie facilement l'égalité :
$$\arctan\left(\frac{1}{p+r}\right) + \arctan\left(\frac{1}{p+q}\right) = \arctan\left(\frac{1}{p}\right). \tag{48}$$
en posant $x := \frac{1}{p+r}$ et $y := \frac{1}{p+q}$ et en utilisant 1.
Soient $p := \sqrt{3}$ et $q = r = 2$. On a $1 + p^2 = 4 = qr$.
La formule donne $2\arctan\frac{1}{\sqrt{3}+2} = \arctan(\frac{1}{\sqrt{3}}) = \frac{\pi}{6}$, c'est-à-dire $\arctan\frac{1}{\sqrt{3}+2} = \frac{\pi}{12}$.
Soient $p := 1$, $q = 1$ et $r = 2$. On a $1 + p^2 = 2 = qr$. La formule donne $\arctan\frac{1}{2} + \arctan\frac{1}{2} = \arctan 1 = \frac{\pi}{4}$.

3. On pose $r := \frac{1+p^2}{q}$. On a $r > 0$. On utilise (48) :
$$\arctan\left(\frac{1}{p+r}\right) + \arctan\left(\frac{1}{p+q}\right) = \arctan\left(\frac{1}{p}\right)$$
$$\arctan\left(\frac{1}{p+\frac{1+p^2}{q}}\right) + \arctan\left(\frac{1}{p+q}\right) = \arctan\left(\frac{1}{p}\right).$$
$$\arctan\left(\frac{q}{pq+1+p^2}\right) + \arctan\left(\frac{1}{p+q}\right) = \arctan\left(\frac{1}{p}\right).$$
Cette dernière égalité est due à Euler.

IV.3.13 1. Par sommation partielle d'une suite géométrique de raison $-x^2$, on trouve :
$$u_n'(x) = \sum_{k=0}^{n}(-x^2)^k = \frac{1+(-1)^n x^{2n+2}}{1+x^2}.$$
La majoration demandée résulte alors immédiatement de la relation :
$$x^{2n+2} \leqslant (1+x^2)\,x^{2n}.$$

2. Par intégration, on trouve :
$$\left|\arctan x - u_n(x)\right| = \left|\int_0^x \left(\frac{1}{1+t^2} - u_n'(t)\right)dt\right| \leqslant \int_0^{|x|} t^{2n}dt = \frac{|x|^{2n+1}}{2n+1} \leqslant a^{2n+1}.$$

3. Puisque $|x|$ est strictement inférieur à 1, on voit que $u_n(x)$ converge vers $\arctan x$ lorsque $n \to +\infty$,

ce que l'on peut écrire en utilisant une somme de série : $\arctan x = \sum_{k=0}^{n} \frac{(-1)^k}{2k+1}x^{2k+1}$.

C'est la formule de Madhawa-Gregory.

IV.3.14 1. On utilise la formule de Moivre. Prenant les parties réelle et imaginaire de $cos4x + i\sin 4x = (\cos x + i\sin x)^4$, on obtient :

$\sin 4x = 4\cos^3 x \sin x - 4\cos x \sin^3 x$ et $\cos 4x = \cos^4 x - 6\cos^2 x \sin^2 x + \sin^4 x$,

d'où :

$$\tan 4x = 4\tan x\frac{\cos^3 x - \cos x\sin^2 x}{\cos^3 x - 6\cos x\sin^2 x + \sin^4 x/\cos x} = 4\tan x\frac{-\tan^2 x + 1}{1 - 6\tan^2 x + \tan^4 x},$$

$$\tan 4x = \frac{4\tan x\,(1-\tan^2 x)}{1 - 6\tan^2 x + \tan^4 x}.$$

Par suite, $\tan(4\arctan 1/5) = 120/119$.

2. La formule donnant $\tan(a-b)$ en fonction de $\tan a$ et $\tan b$ donne aussitôt :

$$\tan\Big(4\arctan\frac{1}{5} - \arctan\frac{1}{239}\Big) = \frac{120\times 239 - 119}{119\times 239 + 120} = 1.$$

3. Notons $t := \tan\pi/8$. On a $1 = \tan\pi/4 = \frac{2t}{1-t^2}$, donc $t^2 + 2t - 1 = 0$. On en déduit $\tan\pi/8 = \sqrt{2} - 1$. De $1/5 < \sqrt{2} - 1$ on déduit $\arctan 1/5 < \pi/8$. Donc $4\arctan 1/5 < \pi/2$.

   Notons $\alpha := 4\arctan\frac{1}{5} - \arctan\frac{1}{239}$. On a : $0 < \alpha < 4\arctan 1/5 < \pi/2$. Puisque, par ailleurs, $\tan\pi/4 = 1$, on a $\tan\alpha = \tan\pi/4$ et l'on en déduit $\alpha = \pi/4$ (en utilisant la proposition 19 de la page 686) :

$$\Big(4\arctan\frac{1}{5} - \arctan\frac{1}{239}\Big) = \pi/4.$$

4. Cherchons un entier $d > 0$ tel que :

$$\tan\Big(4\arctan\frac{1}{5} - \arctan\frac{1}{d}\Big) = 1.$$

   On doit avoir $120\times d - 119 = 119\times d + 120$, c'est-à-dire $d = 239$.

5. Le produit de s_n par $(2n+1)!\,5^{2n+1}\,239^{2n+1}$ étant entier, s_n est rationnel. D'autre part cette suite converge, d'après l'exercice précédent et la question 3, vers π.

6. Les majorations $\big|\arctan x - u_n(x)\big| \leqslant a^{2n+1}$ montrent que la différence $s_n - \pi$ est majorée, en valeur absolue, par les nombres :

$$16\frac{1}{5^{2n+1}} + 4\frac{1}{239^{2n+1}} < \frac{20}{5^{2n+1}} < \frac{1}{5^{2n-1}}.$$

   En se basant sur cette majoration finale, il faut calculer jusqu'à s_2, s_{12} et s_{73} pour être certain d'obtenir respectivement π à 10^{-2}, à 10^{-16} près et à 10^{-100} près (on a $1/5^{2n-1} < 10^{-m}$ si, et seulement si, $(2n-1)\log_{10}5 > m$). En fait, un calcul naïf, opéré par exemple à l'aide d'un logiciel, montre que $s_1 = 3,\underline{14}059\ldots$ et $s_{10} = 3,\underline{14159265358979}32947\ldots$, supérieur à π par moins de 6.10^{-17}, conviennent déjà ($\pi = 3,14159265358979323846\ldots$).

IV.3.15 On a $\tan 2\arctan 1/2 = 4/3$, puis $\tan(2\arctan 1/2 - \arctan 1/7) = \frac{28-3}{21+4} = 1$.

On a $0 < \arctan 1/2 < \pi/4$, donc $0 < 2\arctan 1/2 - \arctan 1/7 < \pi/2$. On en déduit $2\arctan 1/2 - \arctan 1/7 = \pi/4$.

On a $\tan 2\arctan 1/3 = 3/4$, puis $\tan(2\arctan 1/3 + \arctan 1/7) = \frac{21+4}{28-3} = 1$.

On a $1/3 < \sqrt{2} - 1$, donc $\arctan 1/3 < \pi/8$. Par ailleurs $0 < \arctan 1/7 < \pi/4$, donc $0 < 2\arctan 1/3 + \arctan 1/7 < \pi/2$. On en déduit $2\arctan 1/3 + \arctan 1/7 = \pi/4$.

IV.3.16 Soit $y \in \mathbb{R}$. L'équation $y = \sinh x$ s'écrit $\mathrm{e}^{2x} - 2y\,\mathrm{e}^x - 1 = 0$. C'est une équation du second degré en $X := \mathrm{e}^x$ dont le discriminant $4(1 + x^2)$ est strictement positif. On obtient ainsi deux racines réelles dont une seule $X = y + \sqrt{1 + y^2}$ est strictement positive. Donc $x = \ln X = \ln(x + \sqrt{1 + x^2})$.

Pour la deuxième relation, on procède de la même façon : l'équation $y = \cosh x$ s'écrit $X^2 - 2y\,X + 1$, avec $X := \mathrm{e}^x$, et n'admet de solution que lorsque $y \geqslant 1$. Ses deux solutions sont strictement positives puisque leur produit vaut 1 et leur somme $2y > 0$, ce qui permet bien de trouver les deux solutions $\pm \operatorname{argcosh} y$ de l'équation $y = \cosh x$. On ne garde donc que la plus grande, ce qui donne $\operatorname{argcosh} y = \ln(y + \sqrt{y^2 - 1})$.

Pour la dernière relation, l'équation $y = \tanh x$ (avec $y \in]-1, 1[$) se ramène à :

$$y = \frac{\mathrm{e}^{2x} - 1}{\mathrm{e}^{2x} + 1}$$

qui se résout, en considérant e^{2x} comme inconnue, en $\mathrm{e}^{2x} = (1 + y)/(1 - y)$. Donc :

$$x = \frac{1}{2} \ln\left(\frac{1 + y}{1 - y}\right).$$

IV.3.17 1. Cela résulte aussitôt de la formule donnant la somme d'une suite de termes d'une suite géométrique ici de raison $\mathrm{e}^b \neq 1$ qui donne :

$$E_n = \mathrm{e}^a \frac{\mathrm{e}^{nb} - 1}{\mathrm{e}^b - 1} = \mathrm{e}^a \frac{\mathrm{e}^{nb/2}}{\mathrm{e}^{b/2}} \frac{\sinh(nb/2)}{\sinh(b/2)}.$$

2. On trouve $C + S = E_n$ et $C - S = E'_n$, où a et b ont été multipliés par -1 (ce qui ne change pas le fait que b n'est pas nul). Par suite :

$$C = \cosh\Big(a + \frac{n-1}{2}\,b\Big) \frac{\sinh(nb/2)}{\sinh(b/2)}, \qquad S = \sinh\Big(a + \frac{n-1}{2}\,b\Big) \frac{\sinh(nb/2)}{\sinh(b/2)}.$$

Le cas exclu $b = 0$ se traite directement : on trouve $C = n \cosh a$ et $S = n \sinh a$.

3. Le calcul est absolument analogue en trigonométrie circulaire, sauf à changer $C + S$ et $C - S$ en $C + iS$ et $C - iS$. Pour b non multiple de 2π, on obtient :

$$C = \cos\Big(a + \frac{n-1}{2}\,b\Big) \frac{\sin(nb/2)}{\sin(b/2)}, \qquad S = \sin\Big(a + \frac{n-1}{2}\,b\Big) \frac{\sin(nb/2)}{\sin(b/2)}.$$

Les cas $b = 2m\pi$ se traitent immédiatement : il suffit de remplacer la dernière fraction par l'entier n.

On notera que, dans ce cas comme dans l'autre, apparaît une « valeur moyenne » multipliée par un facteur ne dépendant que de b.

IV.3.18 1. Montrons que $\sqrt[m]{10}$ est irrationnel. On raisonne par l'absurde. Supposons que $\sqrt[m]{10} = p/q$, avec $p \in \mathbb{N}$, $q \in \mathbb{N}^*$ et p *et* q *premiers entre eux*. Alors $10 = p^m/q^m$ et $p^m = 10q^m = 2 \times 5q^m$. On a $p > 1$. Soit a un diviseur *premier* de p. Il divise p^m donc $2 \times 5q^m$. Il est premier avec q ; il divise donc 2×5 et, par suite, il divise 2 ou 5 et l'on a nécessairement $a = 2$ ou $a = 5$.

Supposons $a = 2$. Alors $p = 2p_1$ et $2^{m-1}p_1^m = 5q^m$. On a $m - 1 > 0$, donc 2 divise $5q^m$. Puisque 2 divise p, il ne divise pas q, ni q^m, il divise donc 5 et l'on a une contradiction.

Supposons $a = 5$. Alors $p = 5p_2$ et $5^{m-1}p_2^m = 2q^m$. On a $m - 1 > 0$, donc 5 divise $2q^m$. Puisque 5 divise p, il ne divise pas q, ni q^m, il divise donc 2 et l'on a une contradiction.

2. Montrons que $\log_{10} 2$ est irrationnel. On raisonne par l'absurde. Supposons que $\log_{10} 2 = p/q$, avec $p \in \mathbb{N}$ et $q \in \mathbb{N}^*$. Alors :

$$2 = 10^{\log_{10} 2} = 10^{p/q} \iff 2^q = 10^p = 2^p 5^p.$$

L'exposant de 5 doit être nul (sinon 5 diviserait 2^q), donc $p = 0$, et l'on aboutit à une contradiction.

On a :

$$\sqrt{10}^{\log_{10} 4} = \sqrt{10}^{2\log_{10} 2} = 10^{\log_{10} 2} = 2.$$

Posons $\alpha := \sqrt{10}$ et $\beta := \log_{10} 4 = 2\log_{10} 2$. Alors α et β sont *irrationnels* (on utilise 1 pour $m := 2$) et $\alpha^\beta = 2$ est *rationnel*. On répond ainsi à une question de l'exercice 5.

3. Montrons que $\log_2 3$ est irrationnel. On raisonne par l'absurde.

Supposons que $\log_2 3 = p/q$, avec $p \in \mathbb{N}$ et $q \in \mathbb{N}^*$. Alors :

$$3 = 2^{\log_2 3} = 2^{p/q} \iff 3^q = 2^p.$$

Alors $p = q = 0$, ce qui et une contradiction. On a :

$$\sqrt{2}^{\log_2 6} = \sqrt{2}^{2\log_2 3} = 2^{\log_2 3} = 3.$$

On termine comme dans 1. Posons $\alpha' := \sqrt{2}$ et $\beta' := \log_2 6 = \log_2 3 + 1$. Alors α' et β' sont *irrationnels* et $\alpha'^{\beta'} = 3$ est *rationnel*. On répond ainsi à une question de l'exercice 5.

IV.3.19 1. On note,

$$\forall x \in \mathbb{R},\ h(x) := f(x)\mathrm{e}^{-ix}.$$

On vérifie $h'(x) = if(x)\mathrm{e}^{-ix} - if(x)\mathrm{e}^{-ix} = 0$, donc h est constante et il existe $C \in \mathbb{C}$ tel que, pour tout $x \in \mathbb{R}$, $f(x) = C\mathrm{e}^{ix}$. On a $1 = f(0) = C$, donc $f(x) = \mathrm{e}^{ix}$.

2. Il existe une solution unique φ de (16) telle que $\varphi(0) = 1$ et $\varphi'(0) = 0$. Notons, pour tout $x \in \mathbb{R}$, $\psi(x) = \varphi(-x)$. Alors ψ est aussi une solution de (16) et l'on a $\psi(0) = 1$ et $\psi'(0) = -0 = 0$, donc $\psi = \varphi$ et φ est *paire*. Sa dérivée est impaire. Les fonctions φ et $-\varphi'$ sont indépendantes sur $\mathbb{R}$ (une fonction à la fois paire et impaire est nulle) ; elles forment donc une base de E. On note $\cos := \varphi$ et $\sin := -\varphi'$. On a $\cos' = -\sin$ et $\sin' = -(\cos)' = \cos$.

Posons $g := \cos + i\sin$. On a $g' = -\sin + i\cos = i(\cos + i\sin) = ig$ et $g(0) = 1$, donc, d'après 1, pour tout $x \in \mathbb{R}$, $g(x) = \mathrm{e}^{ix}$. Ainsi, les fonctions $\cos$ et $\sin$ ainsi définies coïncident avec les fonctions définies classiquement.

Si l'on ne connaît pas l'exponentielle complexe, on peut utiliser cette méthode pour *définir* $\cos$ et $\sin$ et étudier *directement* leurs propriétés. On peut montrer qu'elles sont périodiques et *définir* π comme la moitié de leur plus petite période. On peut aussi prouver les formules d'addition.

IV.3.20 1. Si $a = 0$ l'équation $\mathrm{e}^z = a$ n'a pas de solution. On suppose $a \neq 0$. On a $\mathrm{e}^z = a$ si, et seulement si, $\mathrm{e}^{\mathrm{Re}\, z} = |a|$ *et* $\mathrm{Im}\, z$ est l'un des arguments de a.

Notons $u + iv := a/|a|$. Il existe un unique argument θ de a appartenant à $]-\pi, \pi]$. Calculons le en fonction de a. On a $\cos\theta = u$ et $\sin\theta = v$. Si $v \geqslant 0$, on a $\theta = \arccos u$ et si $v < 0$, on a $\theta = -\arccos u$.

On a : $\mathrm{e}^z = a$ si, et seulement si, $\mathrm{Re}\, z = \ln|a|$ *et* $\mathrm{Im}\, z \in \theta + 2\pi\mathbb{Z}$.

2. Considérons l'équation $\cos z = \cos z_0$. En posant $Z := \mathrm{e}^{iz}$, elle s'écrit, $Z^2 - 2\cos z_0 Z + 1 = 0$, c'est-à-dire $(Z - \cos z_0)^2 = i^2 \sin^2 z_0$. Cette dernière équation est équivalente à $Z = \mathrm{e}^{iz_0}$ ou $Z = \mathrm{e}^{-iz_0}$, c'est-à-dire à $\mathrm{e}^{i(z-z_0)} = 1$ ou $\mathrm{e}^{i(z+z_0)} = 1$.

On a $\mathrm{e}^{iu} = 1$ si, et seulement si, $u \in 2\pi\mathbb{Z}$, donc $\cos z = \cos z_0$ si, et seulement si, $z = \pm z_0 + 2\pi\mathbb{Z}$.

On a $\sin z = \sin z_0$ si, et seulement si, $\cos(\pi/2 - z) = \cos(\pi/2 - z - 0)$. En utilisant le résultat ci-dessus, on en déduit que $z \in z_0 + 2\pi\mathbb{Z}$ ou $z \in \pi - z_0 + 2\pi\mathbb{Z}$.

3. On procède comme dans le cas réel. On montre que $\tan z = \tan z_0$ si, et seulement si, $\sin(z - z_0) = 0$. On en déduit, en utilisant 2 : $z \in z_0 + \pi\mathbb{Z}$.

4. Considérons l'équation $\cos z = a$. En posant $Z := \mathrm{e}^{iz}$, elle s'écrit, $Z^2 - 2aZ + 1 = 0$, c'est-à-dire $(Z - a)^2 = a^2 - 1$. Cette dernière équation est équivalente à $Z = a + b$ ou $Z = a - b$, avec $b^2 = a^2 - 1$, c'est-à-dire à $\mathrm{e}^{iz} = a + b$ ou $\mathrm{e}^{iz} = a - b$. On termine en utilisant la question 1.

IV.3.21 1. Soit $x > 0$. On a $x + i \notin \mathbb{R}_-$, $0 \leqslant \mathrm{Arg}(x + i) < \pi/2$, $\cos \mathrm{Arg}(x + i) = \frac{x}{\sqrt{1+x^2}}$, $\sin \mathrm{Arg}(x + i) = \frac{1}{\sqrt{1+x^2}}$ et $\tan \mathrm{Arg}(x + i) = 1/x$. Donc $\mathrm{Arg}(x + i) = \arctan 1/x$ et, par suite : $x + i = |x + i|\, \mathrm{e}^{i \mathrm{Arg}(x+i)} = \sqrt{x^2 + 1}\, \mathrm{e}^{i \arctan \frac{1}{x}}$.

On a :

$$\frac{x+i}{x-i} = \frac{(x+i)^2}{x^2+1} = \left(\frac{x+i}{\sqrt{x^2+1}}\right)^2 = \mathrm{e}^{2i \arctan \frac{1}{x}}.$$

2. Soit $x > 0$. On a $x \pm i \notin \mathbb{R}_-$ et l'on vérifie $\frac{x+i}{x-i} \notin \mathbb{R}_-$. On a $\left|\frac{x+i}{x-i}\right| = 1$ et, d'après 1 : $\mathrm{Arg}\, \frac{x+i}{x-i} = 2 \arctan \frac{1}{x}$. Donc :

$$\mathrm{Log}\, \frac{x+i}{x-i} = \ln \left|\frac{x+i}{x-i}\right| + i\, \mathrm{Arg}\, \frac{x+i}{x-i} = 2i \arctan \frac{1}{x},$$

et $\frac{1}{2i} \mathrm{Log}\, \frac{x+i}{x-i} = \arctan \frac{1}{x}$.

3. On vérifie facilement la relation $(2 + i)(3 + i) = i(2 - i)(3 - i)$. Par ailleurs, en multipliant par $2i$ la relation $\arctan 1/2 + \arctan 1/3 = \pi/4$, on obtient $2i \arctan 1/2 + 2i \arctan 1/3 = \frac{\pi}{2}$. En prenant les exponentielles des deux membres, on obtient $\mathrm{e}^{2i \arctan 1/2} \mathrm{e}^{2i \arctan 1/3} = i$.

En utilisant 1, l'on retrouve la relation $\frac{2+i}{2-i} \frac{3+i}{3-i} = i$.

On peut procéder de la même façon pour les trois autres relations en utilisant la formule de Machin et ses deux variantes.

4. On prouve, en raisonnant comme en 3, qu'une condition *nécessaire* est :
$$\left(\frac{u+i}{u-i}\right)^m \left(\frac{v+i}{v-i}\right)^n = i.$$

IV.3.22 1. On note $U := \{z \in \mathbb{C} \mid \operatorname{Re} z > 0\}$
$$V^+ := \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\} \qquad \text{et} \qquad V^- := \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}.$$
On a $U \cup V^+ \cup V^- = \mathbb{C} \setminus \mathbb{R}_-$.

Si $z \in U$, on a $\operatorname{Arg} z \in]-\pi/2, \pi/2[$, donc $\operatorname{Arg} z = \arcsin \operatorname{Im} z$. Si $z \in V^+$, on a $\operatorname{Arg} z \in]0, \pi[$, donc $\operatorname{Arg} z = \arccos \operatorname{Re} z$. Si $z \in V^-$, on a $\operatorname{Arg} z \in]-\pi, 0[$, donc $\operatorname{Arg} z = \arccos(-\operatorname{Im} z)$. On en déduit la continuité de la fonction Arg sur U, V^+ et V^- et par suite sur leur réunion $\mathbb{C} \setminus \mathbb{R}_-$.

2. Soit $g : \mathbb{C} \setminus \mathbb{R}_- \mapsto \mathbb{R}$ une application continue dont l'image est contenue dans $\mathbb{Z}$. Soit $u \notin \mathbb{R}_-$ fixé. On définit une fonction $\varphi : [0,1] \to \mathbb{C}$ par $\varphi(t) := (1-t) + tu$. On vérifie que son image est contenue dans $\mathbb{C} \setminus \mathbb{R}_-$. L'application $g \circ \varphi : [0,1] \to \mathbb{R}$ est continue et son image est contenue dans $\mathbb{Z}$. D'après le théorème 32 de la page 632 cette image est un segment. Mais un segment contenu dans $\mathbb{Z}$ est nécessairement réduit à un point, donc l'application $g \circ \varphi$ est *constante* et l'on a, en particulier, $g \circ \varphi(0) = g \circ \varphi(1)$, c'est-à-dire $g(1) = g(u)$. En faisant varier u, on en déduit que g est constante sur $\mathbb{C}^* \setminus \mathbb{R}_-$.

3. Soit $F : \mathbb{C} \setminus \mathbb{R}_- \mapsto \mathbb{R}$ une application continue telle que, pour tout $z \in \mathbb{C}$, $F(z)$ soit un argument de z, c'est-à-dire $\mathrm{e}^{iF(z)} = z/|z|$. Notons $h := \frac{1}{2\pi}(F - \operatorname{Arg})$.

On a, pour tout $z \in \mathbb{C} \setminus \mathbb{R}_-$:
$$\mathrm{e}^{2i\pi h(z)} = \mathrm{e}^{iF(z)} \mathrm{e}^{-i \operatorname{Arg} z} = z/|z|(z/|z|)^{-1} = 1,$$
donc l'image de h est contenue dans $\mathbb{Z}$. En utilisant 2, on en déduit que h est constante, d'où le résultat.

4. On raisonne par l'absurde. Supposons qu'il existe une fonction continue $G : \mathbb{C}^* \to \mathbb{R}$, dont la restriction à $\mathbb{C} \setminus \mathbb{R}_-$ est égale à la fonction Arg.

Soit $\psi : \mathbb{R} \mapsto \mathbb{C}^*$ définie par $\psi : t \mapsto \mathrm{e}^{it}$. Cette fonction est continue et la fonction composée $G \circ \psi$ est continue sur $\mathbb{R}$. Si $t \in]-\pi, \pi[$, on a $\psi(t) \in \mathbb{C}^* \setminus \{\mathbb{R}_-\}$ et $G \circ \psi(t) = \operatorname{Arg} \circ \psi(t) = t$. Notons $a := G(-1) = G \circ \psi(\pi) = G \circ \psi(-\pi)$. En faisant tendre t vers π par valeurs inférieures on obtient $a = \pi$. En faisant tendre t vers $-\pi$ par valeurs supérieures on obtient $a = -\pi$. On a donc une contradiction.

5. On raisonne par l'absurde. Supposons qu'il existe une fonction continue $f : \mathbb{C}^* \to \mathbb{C}$ telle que, pour tout $z \in \mathbb{C}^*$, l'on ait $\mathrm{e}^{f(z)} = z$. On a donc : $\mathrm{e}^{i \operatorname{Im} f} = z/|z|$ et $\operatorname{Im} f \in \arg z$.

D'après la question 3, il existe $n \in \mathbb{Z}$, tel que la restriction de $\operatorname{Im} f$ à $\mathbb{C} \setminus \mathbb{R}_-$ soit égale à $\operatorname{Arg} + 2n\pi$. Alors $\operatorname{Im} f - 2n\pi$ est une fonction continue sur $\mathbb{C}^*$ dont la restriction à $\mathbb{C} \setminus \mathbb{R}_-$ est égale à Arg. En utilisant la question 4 on obtient une contradiction.

IV.3.23 On a $Qf - P = 0$ sur I.

IV.3.24 1. On a $f^3 = \sqrt{x-1} + \sqrt{2x-3}$, donc $f^6 = 3x - 4 + 2\sqrt{x-1}\sqrt{2x-3}$ et :

$$\left(f^6 - 3x + 4\right)^2 = 4(x-1)(2x-3) = 8x^2 - 20x + 12.$$

Par suite, l'on a $f^{12} - 2(3x-4)f^6 + (x-2)^2 = 0$. Ainsi f est algébrique.

2. Si $x \geqslant 2$, la dérivée de la fonction $x \mapsto \sqrt{x-1} + \sqrt{2x-3}$ est strictement positive, donc la dérivée de f est strictement positive et f est strictement croissante.
On réécrit l'égalité :

$$f^{12} - 2(3x-4)f^6 + (x-2)^2 = 0$$

sous la forme $x^2 - 2(3f^6+2)x + f^{12} + 8f^6 + 4 = 0$. En notant $y := f(x)$, on a $x = g(y)$, donc $g(y)^2 - 2(3y^6+2)g(y) + y^{12} + 8y^6 + 4$, ce qui montre que g est une fonction algébrique. On peut la calculer en résolvant une équation du second degré.
Considérons, pour $y \geqslant \sqrt[3]{2}$ fixé, l'équation $T^2 - 2(3y^6+2)T + y^{12} + 8y^6 + 4$. On a :

$$T := 3y^6 + 2 \pm 2y^3\sqrt{2y^6+1}. \tag{49}$$

On note $T^+ := 3y^6 + 2 \pm 2y^3\sqrt{2y^6+1}$ et $T^- := 3y^6 - 2 \pm 2y^3\sqrt{2y^6+1}$. Ce sont des fonctions *continues* sur $[\sqrt[3]{2}, +\infty[$ et sur cet intervalle $T^+ > T^-$. On a $T^+(\sqrt[3]{2}) = 26$ et $T^-(\sqrt[3]{2}) = 2 = g(\sqrt[3]{2})$. Montrons que, pour tout $y \geqslant \sqrt[3]{2}$, l'on a $g(y) = T^-(y)$.
On considère l'ensemble :

$$A := \{y \geqslant \sqrt[3]{2} \mid \forall t \in [\sqrt[3]{2}, y],\ g(t) = T^-(t)\}.$$

Il est non vide, puisque $\sqrt[3]{2} \in A$. S'il n'est pas borné, il est égal à $[\sqrt[3]{2}, +\infty[$ et le résultat est vrai. Sinon, notons a sa borne supérieure. Puisque T^- est continue, on a $T^-(a) = g(a)$. Pour tout $y > a$, il existe t tel que $a < t \leqslant y$ et $g(y) \neq T^-(y)$. Alors $g(y) = T^+(t)$. Puisque T est continue, on en déduit que $g(a) = T^+(a)$, d'où une contradiction, puisque $T^+(a) \neq T^-(a)$.
Ainsi $g = T^-$: $g(y) = 3y^6 + 2 - 2y^3\sqrt{2y^6+1}$.

3. En reprenant *mutatis mutandis* la même démarche que pour f, on montre que f_1 est algébrique et inversible. Sa fonction réciproque est la fonction $g_1 : [\sqrt[3]{2}, +\infty[\to \infty$, définie par $g_1 : y \mapsto g_1(y) = 3y^6 + 2 + 2y^3\sqrt{2y^6+1}$ (c'est-à-dire $g_1 = T^+$). Elle est algébrique.

IV.3.25 On a $f^2 - x^2 = 0$ et $g^2 - x^2 + 2x - 1 = 0$, donc f et g sont algébriques.
On a $h^2 = f^2 + g^2 + 2fg = 2x^2 - 2x + 1 + 2fg$, donc :

$$0 = (h^2 - 2x^2 + 2x - 1)^2 - 4f^2g^2 = (h^2 - 2x^2 + 2x - 1)^2 - 4x^2(x-1)^2$$

et $(h^2-1)(h^2 - 4x^2 + 4x - 1) = h^4 - (4x^2 - 4x + 2)h^2 + 4x^2 - 4x + 1 = 0$. Par suite h est algébrique.

IV.3.26 On raisonne par l'absurde. On suppose $\ln = P/Q$. En simplifiant si nécessaire la fraction rationnelle P/Q par un monôme de la forme x^m (avec $m \in \mathbb{N}^*$), on peut supposer que $P(0) \neq 0$ *ou* $Q(0) \neq 0$.

- Supposons $Q(0) = 0$. On a $P(0) \neq 0$. De $Q(x)\ln x = P(x)$, l'on déduit, en utilisant $\lim\limits_{x\to 0^+} x^k \ln x$ (pour tout $k \in \mathbb{N}^*$) : $0 = \lim\limits_{x\to 0^+} P(x) = P(0)$, d'où une contradiction.

- Supposons $Q(0) \neq 0$. De $Q(x)\ln x = P(x)$, l'on déduit $Q(x) = \frac{P(x)}{\ln x}$.
  On a $\lim\limits_{x\to 0^+} Q(x) = Q(0) \neq 0$ et $\lim\limits_{x\to 0^+} \dfrac{P(x)}{\ln x} = 0$ (puisque $\lim\limits_{x\to 0^+} \dfrac{1}{\ln x} = 0$), d'où une contradiction.

IV.3.27 On suppose que $\ln$ est une fonction algébrique. Alors, il existe une égalité de la forme $a_n(\ln)^n + a_{n-1}(\ln)^{n-1} + \cdots + a_0 = 0$, avec $a_0, \ldots, a_n \in \mathbb{R}[X]$, $a_n \neq 0$ et $n \in \mathbb{N}^*$. Si l'on considère l'ensemble des égalités de cette forme, il en existe une pour laquelle n est *minimal*. On choisit une telle égalité et nous allons en déduire une contradiction.

On note, pour $k \in [\![0, n-1]\!]$, $b_k := a_k/a_n$. Les b_k sont des fractions rationnelles et $a_n^2 b_k'$ est un polynôme.

On a :

$$(\ln)^n + b_{n-1}(\ln)^{n-1} + \cdots + b_0 = 0,$$

d'où, par dérivation, $\frac{n}{x}(\ln)^{n-1} + b'_{n-1}(\ln)^{n-1} + \cdots + b'_0 = 0$. On réécrit cette égalité sous la forme $c_{n-1}(\ln)^{n-1} + c_{n-1}(\ln)^{n-1} + \cdots + c_0 = 0$ où les c_k sont des fractions rationnelles et $c_{n-1} = \frac{n}{x} + b'_{n-1}$.

En utilisant l'exercice précédent, on montre que $\frac{n}{x} \neq -b'_{n-1} = (-b_{n-1})'$, donc $c_{n-1} \neq 0$. En multipliant par a_n^2, on obtient une égalité de la forme :

$$d_{n-1}(\ln)^{n-1} + d_{n-1}(\ln)^{n-1} + \cdots + d_0 = 0, \tag{50}$$

où les d_k sont des *polynômes* et $d_{n-1} = a_n^2 c_{n-1} \neq 0$. On ne peut pas avoir $n-1 = 0$, sinon l'égalité (50) s'écrirait $d_0 = 0$ et l'on aurait une contradiction. Ainsi $n - 1 \geqslant 1$, mais alors n n'est pas minimal et l'on a aussi une contradiction.

IV.3.28 1. Soit $\mu := \deg r$. D'après l'exercice 4, il existe $a \in \mathbb{R}^*$ tel que la fraction rationnelle r soit équivalente à ax^μ au voisinage de $+\infty$. D'après les théorèmes de comparaison, la fonction $x \mapsto x^\mu \mathrm{e}^{-x}$ tend vers 0, quand x tend vers $+\infty$, donc $\lim\limits_{x\to+\infty} r(x)\mathrm{e}^{-x} = 0$.

2. a) Supposons que l'exponentielle est algébrique. Alors, il existe une égalité de la forme $p_n(\exp)^n + p_{n-1}(\exp)^{(n-1)} + \cdots + p_0 = 0$, avec $p_0, \ldots, p_n \in \mathbb{R}[X]$, $n \in \mathbb{N}^*$ et $p_n \neq 0$. On pose, pour tout $k \in [\![0, n-1]\!]$, $r_k := p_k/p_n$. Les r_k sont des fractions rationnelles.
   On a, pour tout $x \in \mathbb{R}$ assez grand : $1 = -r_{n-1}\mathrm{e}^{-x} - \cdots - r_1\mathrm{e}^{-(n-1)x} - r_0\mathrm{e}^{-nx}$. D'après 1, le second membre tend vers 0 quand x tend vers $+\infty$. On obtient donc une contradiction.

   b) Supposons que le logarithme népérien est algébrique. Alors, il existe une égalité de la forme $a_n(\ln)^n + a_{n-1}(\ln)^{n-1} + \cdots + a_0 = 0$, avec $a_0, \ldots, a_n \in \mathbb{R}[X]$, $a_n \neq 0$ et $n \in \mathbb{N}^*$. On la réécrit $a_n + a_{n-1}/\ln + \cdots + a_0/(\ln)^{n-1} = 0$. Notons αx^m le terme de plus haut degré de a_n ($\alpha \neq 0$). On a, pour tout $x > 1$: $\alpha = \frac{\alpha x^m - a_n}{x^m} - \frac{a_{n-1}}{x^m \ln x} - \cdots - \frac{a_0}{x^m (\ln x)^n}$.
   On vérifie que le second membre tend vers 0 quand x tend vers $+\infty$. On obtient donc une contradiction.

IV.3.29 Par hypothèse, il existe une égalité de la forme $a_n f^n + \cdots + a_0 = 0$, avec $a_0, \ldots, a_n \in \mathbb{R}[X]$, $a_n \neq 0$ et $n \in \mathbb{N}^*$.

1. On suppose que f ne s'annule pas. Si $a_0 = 0$, on peut diviser l'égalité par f et l'on obtient $a_n f^{n-1} + \cdots + a_1 = 0$. Si $a_1 = 0$, on peut à nouveau diviser par $f \ldots$ On en déduit qu'il existe $h \in \mathbb{N}$, $h < n$, tel que $a_n f^{n-h} + \cdots + a_h = 0$ et $a_h \neq 0$. En posant $m := n - h$ et $b_k := a_{k+h}$, on obtient une égalité $b_m f^m + \cdots + b_0 = 0$, avec $m \in \mathbb{N}^*$ et $b_m b_0 \neq 0$. On en déduit $b_0 f^{-m} + \cdots + b_m = 0$. Donc $1/f$ est algébrique.

2. En notant, pour $k \in [\![0, n]\!]$, $\delta_k = \deg a_k$ et $a_k(x) = \sum_{j=0}^{\delta_k} \alpha_{k,j} x^j$ si $a_k \neq 0$, l'égalité $a_n(x) f(x)^n + \cdots + a_0(x) = 0$ s'écrit :
$$\sum_{k=0}^{n} \left(\sum_{j=0}^{\delta_k} \alpha_{k,j} x^j \right) f(x)^k = 0 \tag{51}$$
(en convenant que le terme entre parenthèses est nul si $a_k = 0$).
Notons que, puisque $a_n \neq 0$, le coefficient α_{n,δ_n} de son monôme de plus haut degré *n'est pas nul*. ceci jouera un rôle important dans la suite de la preuve.
On note $y = f(x)$, donc $x = g(y)$. L'égalité $a_n(x) f(x)^n + \cdots + a_0(x) = 0$ s'écrit $a_n(g(y)) y^n + \cdots + a_0(g(y)) = 0$ et, en utilisant (51), on a :
$$\sum_{k=0}^{n} \left(\sum_{j=0}^{\delta_k} \alpha_{k,j} g(y)^j \right) y^k = 0.$$
Notons $h := \max_{k \in [\![0,n]\!]} \delta_k$. En convenant de $\alpha_{k,j} := 0$ si le terme $y^k g(y)^j$ ne figure pas, on obtient la double somme :
$$\sum_{k=0}^{n} \sum_{j=0}^{h} \alpha_{k,j} y^k g(y)^j = 0.$$
En intervertissant les sommations, on obtient :
$$\sum_{j=0}^{h} \sum_{k=0}^{n} \alpha_{k,j} y^k g(y)^j = 0,$$
D'où, en notant, pour $j \in [\![0, h]\!]$, $b_j(y) := \sum_{k=0}^{n} \alpha_{k,j} y^k$, l'égalité :
$$b_h(y) g(y)^h + \cdots + b_0 = 0, \tag{52}$$
avec $b_0, \ldots, b_h \in \mathbb{R}[Y]$ et $h := \max_{k \in [\![0,n]\!]} \delta_k$.
On a $b_{\delta_n}(y) = \sum_{k=0}^{n} \alpha_{k,\delta_n} y^k$. Son monôme de plus haut degré est $\alpha_{n,\delta_n} y^n$, qui, comme nous l'avons noté plus haut, n'est pas nul, donc $b_{\delta_n} \neq 0$.
Dans l'égalité (52), on supprime, si nécessaire, pour tout $j > \delta_n$, les b_j nuls. On obtient une égalité $b_r(y) g(y)^r + \cdots + b_0 = 0$, avec $r \geqslant \delta_n$ et $b_r \neq 0$. On ne peut pas avoir $r = \delta_n = 0$, sinon l'on aurait $b_0 = 0$ ce qui contredirait $b_{\delta_n} \neq 0$. Donc $r \geqslant \delta_n > 0$ et g est algébrique.

IV.3.30 1. Les preuves sont similaires pour $\sinh$ et $\cosh$. Nous ne traiterons que le cas de $\sinh$. Nous allons raisonner par l'absurde. Supposons que $\sinh$ est algébrique. Alors, il existe une égalité de la forme :

$$a_n \sinh^n + \cdots + a_0 = 0, \tag{53}$$

avec $a_0, \ldots, a_n \in \mathbb{R}[X]$, $n \in \mathbb{N}^*$ et $a_n \neq 0$.

On a $\sinh x = \frac{1}{2}(\mathrm{e}^x - \mathrm{e}^{-x})$. Par suite, pour tout $k \in [\![0, n]\!]$, on a :

$$\mathrm{e}^{nx} \sinh^k x = 2^{-k} \mathrm{e}^{nx} (\mathrm{e}^x - \mathrm{e}^{-x})^k,$$

donc, en utilisant la formule du binôme, on peut écrire la fonction $(\exp)^n \sinh^k$ comme un polynôme à coefficients constants de degré $n + k$ « en l'exponentielle $\exp$ ». En multipliant l'égalité (53) par $(\exp)^n$ et en réordonnant les termes, on obtient une égalité de la forme $p_{2n}(\exp)^{2n} + p_{2n-1}(\exp)^{2n-1} + + \cdots + a_0 = 0$, avec $p_0, \ldots, p_{2n} \in \mathbb{R}[X]$, $2n \in \mathbb{N}^*$. On vérifie que $p_{2n} = a_n \neq 0$. Ceci entraîne que la fonction exponentielle est algébrique, ce qui n'est pas vrai d'après l'exercice IV.3.28. Ainsi l'égalité (53) est impossible et la fonction $\sinh$ est transcendante.

2. Pour la fonction $\mathrm{argsinh}$, le résultat se déduit immédiatement de 1 et de l'exercice IV.3.29. Pour la fonction $\mathrm{argcosh}$ il y a une petite difficulté due aux domaines de définition.

On raisonne par l'absurde. Si la fonction $\mathrm{argcosh}$ était algébrique, alors *la restriction à* $\mathbb{R}_+$ de la fonction $\cosh$ serait algébrique. Il existerait donc $n \in \mathbb{N}^*$ et $a_0, \ldots, a_n \in \mathbb{R}[X]$, tels que $a_n \neq 0$, et, pour tout $x \in \mathbb{R}_+$:

$$a_n(x) \cosh^n(x) + a_{n-1}(x) \cosh^{n-1}(x) + \cdots + a_0(x) = 0, \tag{54}$$

On peut supposer que a_n n'est pas impair. Sinon, on multiplie (54) par x et, pour $k \in [\![0, n]\!]$ on remplace a_k par xa_k (si $a_n \neq 0$ est impair, alors xa_n est pair et $xa_n \neq 0$).

En changeant x en $-x$ dans (54), on obtient, pour tout $x \in \mathbb{R}_+$:

$$a_n(-x) \cosh^n(x) + a_{n-1}(-x) \cosh^{n-1}(x) + \cdots + a_0(-x) = 0,$$

puis, par addition, pour tout $x \in \mathbb{R}_+$:

$$b_n(x) \cosh^n(x) + b_{n-1}(x) \cosh^{n-1}(x) + \cdots + b_0(x) = 0, \tag{55}$$

où, pour $k \in [\![0, n]\!]$, $b_k(x) := a_k(x) + a_k(-x)$. Les b_n et la fonction $\cosh$ étant pairs, l'équation (55) est vraie pour tout $x \in \mathbb{R}$. Par ailleurs $b_n \neq 0$ (sinon a_n serait impair, ce qui n'est pas le cas par hypothèse). Ainsi $\cosh$ est algébrique et l'on aboutit à une contradiction.

Module IV.4 : Séries numériques

IV.4.1 1) Lorsque n tend vers $+\infty$, u_n est équivalent à $1/n^p$. Comme dans l'exercice IV.4.0, la série $\sum_{n\geqslant 1} 1/n^p$ converge parce que $p>1$, et donc la série $\sum_{n\geqslant 0} u_n$ converge.

2) Démontrons la formule annoncée par récurrence sur n. Commençons par le cas $n := 0$; $U_0 = u_0 = 1/p!$, alors que le second membre de la formule s'écrit :

$$\frac{1}{p-1}\left[\frac{1}{(p-1)!}-\frac{1}{p!}\right]=\frac{p-1}{(p-1)p!}=\frac{1}{p!}.$$

La formule est donc vraie pour $n := 0$. Supposons cette formule vraie pour un certain $n\in\mathbb{N}$. Alors $U_{n+1} = U_n + u_{n+1}$ vaut :

$$\frac{1}{p-1}\left[\frac{1}{(p-1)!}-\frac{1}{(n+2)(n+3)\cdots(n+p)}\right]+\frac{1}{(n+2)(n+3)\cdots(n+p+1)}$$
$$=\frac{1}{(p-1)(p-1)!}-\frac{(n+p+1)-(p-1)}{(p-1)(n+2)(n+3)\cdots(n+p+1)}.$$

Après simplification par $n+2$, on obtient :

$$U_{n+1}=\frac{1}{p-1}\left[\frac{1}{(p-1)!}-\frac{1}{(n+3)(n+4)\cdots(n+p+1)}\right],$$

c'est la formule annoncée à l'ordre $n+1$.

Dans l'égalité que nous venons de démontrer, à l'ordre n, faisons tendre n vers $+\infty$. Puisque la série proposée converge, U_n tend vers la somme S de la série. Comme le produit $(n+2)(n+3)\cdots(n+p)$ tend vers $+\infty$, son inverse tend vers 0, d'où :

$$S \;=\; \frac{1}{(p-1)(p-1)!}.$$

IV.4.2 Puisque $u_n\geqslant 0$ pour tout $n\geqslant 1$, il nous suffit de majorer convenablement les sommes partielles U_n de cette série. Commençons par majorer chaque « tranche » T_p, où $p\in\mathbb{N}$ est donné. Les entiers k tels que $10^p\leqslant k\leqslant 10^{p+1}-1$ sont ceux qui ont $p+1$ chiffres décimaux, *i.e.* ceux qui s'écrivent en base 10 : $k := a_p a_{p-1}\cdots a_1 a_0$, où $a_p\in[\![1,9]\!]$ et $a_i\in[\![0,9]\!]$ pour $i=0,1,\ldots,p-1$.

Parmi les entiers k ci-dessus, comptons ceux dont l'écriture décimale ne comporte pas le chiffre 8. La seule contrainte sur les a_i est que $a_p\in[\![1,9]\!]\setminus\{8\}$ et $a_i\in[\![0,9]\!]\setminus\{8\}$ pour $i=0,\ldots,p-1$. Cela donne 8 choix possibles pour a_p et 9 pour chacun des autres a_i. Le nombre de tels entiers k est donc : 8×9^p. Pour chacun de ces k, $u_k=1/k$ est majoré par $1/10^p$, et on en déduit l'encadrement :

$$0\;\leqslant\; T_p\;\leqslant\; 8\times\left(\frac{9}{10}\right)^p.$$

Soient alors $P\in\mathbb{N}$ et $N := 10^{P+1}-1$. Pour tout entier $n\in[\![1,N]\!]$, il existe un unique $p\in[\![0,P]\!]$ tel que $10^p\leqslant n\leqslant 10^{p+1}-1$. Il en résulte que la somme partielle U_N est la somme des T_p pour $p=0,\ldots,P$. D'où :

$$U_N\;\leqslant\; 8\sum_{p=0}^{P}\left(\frac{9}{10}\right)^p\;\leqslant\; 8\sum_{p=0}^{+\infty}\left(\frac{9}{10}\right)^p\;=\;\frac{8}{1-\frac{9}{10}}\;=\;80.$$

Soit maintenant $n \in \mathbb{N}^*$. Il existe un unique entier $P \geqslant 0$ tel que l'on ait $10^P \leqslant n \leqslant 10^{P+1}-1 = N$. Alors $U_n \leqslant U_N \leqslant 80$. Ainsi $U_n \leqslant 80$ pour tout $n \geqslant 1$. Puisque les u_n sont positifs, cela montre que la série $\sum_{n\geqslant 1} u_n$ converge (théorème 9 de la page 715).

Le résultat obtenu peut paraître étonnant. En effet la série harmonique $\sum_{n\geqslant 1} 1/n$ diverge. La série étudiée est obtenue en supprimant « seulement » les $1/n$ pour tous les entiers $n \geqslant 1$ dont l'écriture décimale comporte au moins un 8. On pourrait penser que ces entiers n sont peu nombreux, et que la divergence de la série en résulte. Ce n'est pas le cas : les calculs ci-dessus montrent en fait que la « plupart » des entiers $n \geqslant 1$ sont supprimés.

IV.4.3 Pour tous $N \in \mathbb{N}^*$ et $K \in \mathbb{N}$, posons :

$$U_N := \sum_{n=1}^{N} u_n \quad \text{et} \quad V_K := \sum_{k=0}^{K} 2^k u_{2^k}\,.$$

Par ailleurs, pour tous entiers p, q tels que $1 \leqslant p < q$, posons $S(p,q) := \sum_{n=p}^{q} u_n$. Pour tout $k \in \mathbb{N}$, on a ainsi :

$$S(2^k, 2^{k+1}-1) \;=\; \sum_{n=2^k}^{2^{k+1}-1} u_n\,.$$

Le second membre de cette égalité est une somme de $2^{k+1} - 2^k = 2^k$ termes. Comme la suite (u_n) est décroissante, on a : $u_{2^{k+1}} \leqslant u_n \leqslant u_{2^k}$ pour tout $n \in [\![2^k, 2^{k+1}-1]\!]$, d'où l'encadrement :

$$2^k u_{2^{k+1}} \;\leqslant\; S(2^k, 2^{k+1}-1) \;\leqslant\; 2^k u_{2^k}\,.$$

Sommons ces inégalités pour $k = 0, \ldots, K$, où $K \in \mathbb{N}$. La somme des $S(2^k, 2^{k+1}-1)$ pour $k = 0, \ldots, K$ est évidemment $S(1, 2^{K+1}-1) = U_{2^{K+1}-1}$, d'où :

$$\frac{1}{2}\left[V_{K+1} - u_1\right] \;=\; \sum_{k=0}^{K} 2^k u_{2^{k+1}} \;\leqslant\; U_{2^{K+1}-1} \leqslant \sum_{k=0}^{K} 2^k u_{2^k} \;=\; V_K\,.$$

On en déduit que la série $\sum_{k\geqslant 0} 2^k u_{2^k}$ converge, *i.e.* la suite (V_K) est majorée, si, et seulement si, la suite $(U_{2^{K+1}-1})$ est majorée. Comme la suite (U_n) est croissante, cela revient à dire que (U_n) est majorée, *i.e.* que la série $\sum_{n\geqslant 1} u_n$ converge.

Prenons maintenant $u_n := 1/n^a$, où $a > 0$ est un réel fixé. Pour tout $k \in \mathbb{N}$, on a : $v_k := 2^k u_{2^k} = 2^k/(2^k)^a = (2^{1-a})^k$. Ainsi $\sum_{k\geqslant 0} v_k$ est une série géométrique de premier terme 1 et de raison 2^{1-a}, elle converge si, et seulement si, $2^{1-a} < 1$, *i.e.* si $a > 1$. D'après la première partie de cet exercice, la série de Riemann $\sum_{n\geqslant 1} 1/n^a$ converge si, et seulement si, $a > 1$, ce qui donne une autre démonstration du théorème 14 de la page 718.

IV.4.4 Supposons donc que la série $\sum_{n\geqslant 0} u_n$ converge. Soit $\varepsilon > 0$. D'après le théorème 6 de la page 713, il existe un entier $N \geqslant 0$ tel que, dès que $p, q \in \mathbb{N}$ et $N \leqslant p < q$, on ait $\sum_{n=p}^{q} u_n \leqslant \varepsilon$.

Pour tout $n \in [\![p, q]\!]$, on a $u_n \geqslant u_q$, parce que la suite (u_n) est décroissante. D'où l'encadrement :

$$(q-p+1)u_q \;\leqslant\; \sum_{n=p}^{q} u_n \;\leqslant\; \varepsilon\,.$$

D'où $qu_q \leqslant \varepsilon + (p-1)u_q$. Dans cet inégalité, fixons $p := N$. Puisque la suite (u_n) converge vers 0 (théorème 5 de la page 713), il existe un entier $N' > N$ tel que $(N-1)u_q \leqslant \varepsilon$ pour tout entier $q \geqslant N'$. Ainsi, pour tout $q \geqslant N'$, on a $qu_q \leqslant 2\varepsilon$, ce qui montre bien que la suite (nu_n) converge vers 0.

Prenons maintenant $u_n := 1/(n \ln n)$ pour $n \geqslant 2$. La suite (u_n) tend vers 0 en décroissant, mais la série $\sum\limits_{n\geqslant 2} u_n$ diverge, vu l'exercice IV.4.10 de la page 731. Et pourtant, $nu_n = 1/\ln n$ tend vers 0 lorsque n tend vers $+\infty$. La réciproque en question est donc fausse.

IV.4.5 Notons u_n le terme général de la série proposée. Soit $n \in \mathbb{N}^*$, explicitons u_n. Posons $p := E(\sqrt{n})$, c'est le seul entier tel que $p \leqslant \sqrt{n} < p+1$, soit $p^2 \leqslant n < (p+1)^2$, ce qui équivaut à $p^2 \leqslant n \leqslant p^2 + 2p$. Si $n < p^2 + 2p$, on a encore $n+1 < (p+1)^2$, d'où $p \leqslant \sqrt{n+1} < p+1$. Dans ce cas, $E(\sqrt{n+1}) = p$, donc $u_n = 0$. Si par contre $n = p^2 + 2p$, on a $n+1 = (p+1)^2$, donc $E(\sqrt{n+1}) = p+1$. Dans ce cas, $E(\sqrt{n+1}) - E(\sqrt{n}) = 1$, donc $u_n = 1/n = 1/\big(p(p+2)\big)$. Ainsi :

$$u_n \;=\; \begin{cases} \dfrac{1}{p(p+2)} & \text{si } n := p(p+2),\ p \in \mathbb{N}^*, \\ 0 & \text{sinon.} \end{cases}$$

On en déduit que, pour tout $P \in \mathbb{N}^*$, on a :

$$U_{P(P+2)} \;=\; \sum_{n=1}^{P(P+2)} u_n \;=\; \sum_{p=1}^{P} \frac{1}{p(p+2)}\cdot$$

Lorsque p tend vers $+\infty$, $1/\big(p(p+2)\big)$ est équivalent à $1/p^2$. Comme la série $\sum\limits_{p\geqslant 1} 1/p^2$ converge, la série $\sum\limits_{p\geqslant 1} 1/\big(p(p+2)\big)$ converge aussi. Ainsi la suite $(U_{P(P+2)})$ est majorée, ce qui montre que la série $\sum\limits_{n\geqslant 1} u_n$ converge, avec de plus :

$$S \;:=\; \sum_{n=1}^{+\infty} u_n \;=\; \sum_{p=1}^{+\infty} \frac{1}{p(p+2)} \;=\; \lim_{p\to+\infty} \left(\sum_{p=1}^{P} \frac{1}{p(p+2)} \right).$$

Pour tout $p \in \mathbb{N}^*$, on a :

$$\frac{1}{p(p+2)} \;=\; \frac{1}{2}\left[\frac{1}{p} - \frac{1}{p+2}\right], \quad \text{d'où}$$

$$\sum_{p=1}^{P} \frac{1}{p(p+2)} \;=\; \frac{1}{2}\left[\sum_{p=1}^{P} \frac{1}{p} - \sum_{p=1}^{P} \frac{1}{p+2}\right], \quad \text{soit}$$

$$\sum_{p=1}^{P} \frac{1}{p(p+2)} \;=\; \frac{1}{2}\left[\sum_{k=1}^{P} \frac{1}{k} - \sum_{k=3}^{P+2} \frac{1}{k}\right].$$

On obtient ainsi :

$$\sum_{p=1}^{P} \frac{1}{p(p+2)} \;=\; \frac{1}{2}\left[1+\frac{1}{2}-\frac{1}{P+1}-\frac{1}{P+2}\right].$$

En faisant tendre P vers $+\infty$, on en déduit ceci :

$$S \;=\; \lim_{P\to+\infty}\left(\sum_{p=1}^{P}\frac{1}{p(p+2)}\right) \;=\; \lim_{P\to+\infty}\frac{1}{2}\left[1+\frac{1}{2}-\frac{1}{P+1}-\frac{1}{P+2}\right] \;=\; \frac{3}{4}\cdot$$

Ainsi $\sum\limits_{n=1}^{+\infty} u_n = 3/4$.

IV.4.6 Notons u_n le terme général de la première série et v_n le terme général de la deuxième série. Si $n \geqslant 9$, on a $\ln n \geqslant 2$, d'où $u_n \leqslant 1/n^2$ et $v_n \leqslant 1/2^n$. Les séries $\sum\limits_{n\geqslant 1} 1/n^2$ et $\sum\limits_{n\geqslant 0} 1/2^n$ convergent, donc, par comparaison, les séries $\sum\limits_{n\geqslant 1} u_n$ et $\sum\limits_{n\geqslant 2} v_n$ convergent (ces séries étant à termes réels positifs, on peut appliquer le théorème 10 de la page 715).

IV.4.7 Posons $u_n := a^{H_n}$ pour $n \geqslant 1$. Pour déterminer la nature de la série $\sum\limits_{n\geqslant 1} u_n$, cherchons un équivalent de u_n lorsque n tend vers $+\infty$. Reprenons l'égalité (18) :

$$H_n \;=\; 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n} \;=\; \ln n + C + \varepsilon_n\,, \quad \text{où} \quad \lim_{n\to+\infty}\varepsilon_n = 0.$$

On en déduit ceci :

$$u_n \;=\; a^{H_n} \;=\; a^{\ln n}\, a^C a^{\varepsilon_n} \;=\; n^{\ln a}\, a^C a^{\varepsilon_n}\,.$$

Lorsque n tend vers $+\infty$, a^{ε_n} tend vers 1, donc $u_n \sim K n^{\ln a}$, en posant $K := a^C > 0$. Compte tenu du théorème 14 de la page 718 et du théorème 11 de la page 716, la série $\sum\limits_{n\geqslant 1} u_n$ converge si, et seulement si, $\ln a < -1$, c'est-à-dire $a < 1/e$.

IV.4.8 1) Démontrons donc, par récurrence sur $n \geqslant 1$, la formule :

$$(b-a-1)U_n \;=\; bu_1 - (n+b)u_{n+1}\,, \qquad (*)$$

c'est-à-dire $(b-a-1)U_n = bu_1-(n+a)u_n$. C'est vrai pour $n := 1$, car $U_1 = u_1$. Supposons la formule $(*)$ vraie pour un certain $n \in \mathbb{N}^*$. Alors :

$$(b-a-1)U_{n+1} = (b-a-1)(U_n+u_{n+1}) = bu_1-(n+b)u_{n+1}+(b-a-1)u_{n+1}\,,$$

c'est-à-dire $(b-a-1)U_{n+1} = bu_1-(n+a+1)u_{n+1}$, d'où l'égalité $(*)$ au rang $n+1$.

2) Supposons d'abord que $b := a+1$. Dans ce cas, l'égalité $(*)$ donne, pour tout $n \geqslant 1$, $0 = bu_1-(n+a)u_n$, soit $u_n = bu_1/(n+a)$. Or $bu_1 \neq 0$, et la série $\sum\limits_{n\geqslant 1} 1/(n+a)$ diverge $\big($car $1/(n+a) \sim 1/n$ lorsque n tend vers $+\infty\big)$, donc la série $\sum\limits_{n\geqslant 1} u_n$ diverge.

Supposons désormais $b-a-1 \neq 0$. Compte tenu de l'égalité $(*)$, la série $\sum\limits_{n\geqslant 1} u_n$ converge, *i.e.* la suite (U_n) converge, si, et seulement si, la suite $\big((n+a)u_n\big)$ converge. Si c'est le

cas, la limite ℓ de la suite $\big((n+a)u_n\big)$ est nécessairement nulle : si $\ell \neq 0$, l'équivalence $u_n \sim \ell/(n+a)$ montre que la série $\sum_{n\geqslant 1} u_n$ diverge. Ainsi, notant S la somme de la série $\sum_{n\geqslant 1} u_n$, on a $(b-a-1)S = bu_1$, en passant à la limite dans l'égalité $(*)$ (lorsque n tend vers $+\infty$). D'où :

$$S \;=\; \frac{bu_1}{b-a-1}\cdot$$

Mais $bu_1 > 0$, et $S > 0$ parce que les u_n sont strictement positifs, de sorte que $b-a-1 > 0$, *i.e.* $b > a+1$. Nous avons ainsi montré que, si la série $\sum_{n\geqslant 1} u_n$ converge, d'une part $b > a+1$, et d'autre part la somme S est donnée par la formule ci-dessus.

Pour conclure, il reste à montrer que, si $b > a+1$, la série $\sum_{n\geqslant 1} u_n$ converge. Or, dans ce cas, l'égalité $(*)$ donne, pour tout $n \geqslant 1$:

$$U_n \;=\; \frac{bu_1}{b-a-1} - \frac{(n+b)u_{n+1}}{b-a-1} \;\leqslant\; \frac{bu_1}{b-a-1}\cdot$$

Ainsi la suite (U_n) (qui est croissante) est majorée, elle est donc convergente, *i.e.* la série $\sum_{n\geqslant 1} u_n$ converge.

IV.4.9 1) Pour tout $n \in \mathbb{N}$, posons $t_n := a^n + b^n$. On a $a+b = 4$ et $ab = -1$, donc a et b sont les deux racines de l'équation $x^2 - 4x - 1 = 0$. Ainsi $a^2 = 4a+1$, d'où $a^{n+2} = 4a^{n+1} + a^n$ pour tout $n \in \mathbb{N}$. De même $b^{n+2} = 4b^{n+1} + b^n$ pour tout $n \in \mathbb{N}$. On en déduit l'égalité $t_{n+2} = 4t_{n+1} + t_n$ pour tout $n \in \mathbb{N}$. Comme $t_0 = 2$ et $t_1 = 4$, il en résulte, par récurrence sur n, que chaque t_n est un entier pair.

Une autre solution consistait à appliquer la formule du binôme. Si $n \in \mathbb{N}$, il vient :

$$a^n + b^n \;=\; \sum_{k=0}^{n} \binom{n}{k} \sqrt{5}^{\,k} 2^{n-k} + \sum_{k=0}^{n} \binom{n}{k} (-1)^k \sqrt{5}^{\,k} 2^{n-k}$$

Dans ces sommes, les termes correspondants à des entiers k impairs s'éliminent, il ne reste que les termes correspondants à des entiers k pairs, écrivons $k := 2p$. D'où :

$$t_n \;=\; a^n + b^n \;=\; 2 \sum_{p=0}^{E(n/2)} \binom{n}{2p} 5^p 2^{n-2p}\,,$$

et il en résulte aussitôt que t_n est un entier pair.

2) Soit $n \in \mathbb{N}$. En écrivant $a^n = t_n - b^n$, il vient :

$$\sin(\pi a^n) \;=\; \sin(\pi t_n - \pi b^n) \;=\; -\sin(\pi b^n)\,,$$

la deuxième égalité résultant du fait que t_n soit un entier pair. D'où :

$$|\sin(\pi a^n)| \;=\; |\sin(\pi b^n)| \;=\; \sin\big(\pi |b|^n\big) \;\leqslant\; \pi |b|^n\,.$$

Or $|b| \;=\; \sqrt{5} - 2 \;\in\;]0,1[$, donc la série $\sum_{n\geqslant 0} \pi |b|^n$ converge. Par comparaison, la série $\sum_{n\geqslant 0} \big|\sin(\pi a^n)\big|$ converge. Ainsi la série $\sum_{n\geqslant 0} \sin(\pi a^n)$ est absolument convergente, et par suite elle est convergente (théorème 20 de la page 724).

IV.4.10 Puisque f est décroissante et $f(x)$ tend vers 0 lorsque x tend vers $+\infty$, on a $f(x) \geqslant 0$ pour tout $x > 0$ (le vérifier). Considérons deux entiers p, q tels que $1 \leqslant p < q$. D'après la proposition 13 de la page 718, on a :

$$\sum_{k=p+1}^{q+1} f(k) \;\leqslant\; F(q+1) - F(p) \;\leqslant\; \sum_{k=p}^{q} f(k)\,.$$

Notons S_n les sommes partielles de la série $\sum\limits_{n\geqslant 1} f(n)$. Dans les inégalités précédentes, remplaçons p par 1 et q par un entier $n \geqslant 2$. On obtient :

$$S_{n+1} - f(1) \;\leqslant\; F(n+1) - F(1) \;\leqslant\; S_n\,.$$

Supposons d'abord que $F(x)$ ait une limite finie ℓ lorsque x tend vers $+\infty$. Comme F est croissante (sa dérivée f est positive), $F(x) \leqslant \ell$ pour tout $x > 0$. En particulier $F(n+1) \leqslant \ell$ pour tout $n \in \mathbb{N}^*$, d'où l'on déduit $S_{n+1} \leqslant \ell + f(1) - F(1)$. Ainsi la suite (S_n) est majorée, donc convergente (elle est croissante).

Supposons inversement que la série $\sum\limits_{n\geqslant 1} f(n)$ converge, et soit S sa somme. Pour tout $n \in \mathbb{N}$, on a $S_n \leqslant S$, d'où $F(n+1) \leqslant S + F(1)$. Comme F est croissante, on en déduit que $F(x) \leqslant C := S + F(1)$ pour tout $x > 0$. La fonction F est donc *majorée*. Soit $\ell \in \mathbb{R}$ la borne supérieure de F, *i.e.* la borne supérieure de $\big\{F(x) \;\big|\; x > 0\big\}$. Montrons que $F(x)$ tend vers ℓ lorsque x tend vers $+\infty$. D'abord $F(x) \leqslant \ell$ pour tout x, puisque ℓ majore F. Soit $\varepsilon > 0$. Par définition d'une borne supérieure, $\ell - \varepsilon$ ne majore pas F, *i.e.* il existe $a > 0$ tel que $F(a) > \ell - \varepsilon$. Pour tout $x \geqslant a$, on a $F(x) \geqslant F(a)$ (car F est croissante), d'où $\ell - \varepsilon \leqslant F(x) \leqslant \ell$. Cela montre que $F(x)$ tend vers ℓ lorsque x tend vers $+\infty$, comme annoncé. Noter le résultat que nous avons obtenu : si une fonction F, définie sur un intervalle du type $\left]\alpha, +\infty\right[$, est croissante et majorée, elle a une limite finie en $+\infty$.

Soient maintenant b un réel fixé et f la fonction $x \mapsto 1/\big(x\ln(x)^b\big)$, définie sur $\left]1, +\infty\right[$. Il s'agit de déterminer la nature de la série $\sum\limits_{n\geqslant 2} f(n)$. Cette série est à termes réels positifs. Le cas $b \leqslant 0$ est évident : alors $f(n) \geqslant 1/n$ pour tout $n \geqslant 3$. Comme la série harmonique diverge, la série $\sum\limits_{n\geqslant 2} f(n)$ diverge, par comparaison. Supposons donc $b > 0$. On détermine facilement une primitive F de f sur $\left]1, +\infty\right[$, suivant que b soit égal à 1 ou soit distinct de 1. Si $b := 1$, on peut prendre $F(x) := \ln(\ln x)$. Alors $F(x)$ tend vers $+\infty$ lorsque x tend vers $+\infty$, donc la série $\sum\limits_{n\geqslant 2} f(n)$ diverge, d'après la première partie de l'exercice. Si $b \neq 1$, on peut prendre :

$$F(x) \;:=\; \frac{(\ln x)^{1-b}}{1-b}\cdot$$

Il en résulte que, lorsque x tend vers $+\infty$, $F(x)$ tend vers 0 si $b > 1$ et vers $+\infty$ si $b < 1$. D'où le résultat annoncé : la série $\sum\limits_{n\geqslant 2} f(n)$ converge si, et seulement si, $b > 1$.

IV.4.11 1) Raisonnons par récurrence sur $n \geqslant 1$. L'égalité annoncée est vraie pour $n = 1$, car $B_1 = b_1 = a_1 - a_2 = A_1 - a_2$. Supposons cette égalité vraie pour un certain $n \in \mathbb{N}^*$. Alors :

$$B_{n+1} = B_n + b_{n+1} = \big(A_n - na_{n+1}\big) + (n+1)(a_{n+1} - a_{n+2})\,,$$

c'est-à-dire $B_{n+1} = A_n + a_{n+1} - (n+1)a_{n+2} = A_{n+1} - (n+1)a_{n+2}$, d'où l'égalité au rang $n+1$.

2) Si la série $\sum_{n\geqslant 1} a_n$ converge, notons A sa somme ; de même, si la série $\sum_{n\geqslant 1} b_n$ converge, notons B sa somme. Supposons d'abord que la série $\sum_{n\geqslant 1} a_n$ converge. Comme c'est une série à termes réels positifs, cela signifie que la suite (A_n) est majorée. D'après la question 1), $B_n \leqslant A_n$ pour tout $n \geqslant 1$. Ainsi la suite (B_n) est majorée, *i.e.* la série $\sum_{n\geqslant 1} b_n$ converge ; en effet, puisque la suite (a_n) est décroissante, les b_n sont positifs. En outre $B \leqslant A$. En fait, toujours d'après 1), na_{n+1} a une limite finie lorsque n tend vers $+\infty$, à savoir $A - B$. Nécessairement $A = B$: dans le cas contraire, a_{n+1} serait équivalent à $(A-B)/n$ lorsque n tend vers $+\infty$, et la série $\sum_{n\geqslant 1} a_n$ divergerait. En conclusion $A = B$.

Il reste à démontrer que, si la série $\sum_{n\geqslant 1} b_n$ converge, il en est de même pour $\sum_{n\geqslant 1} a_n$. Ce point est un peu plus subtil. Considérons deux entiers $n, p \in \mathbb{N}^*$. D'après 1), on a :

$$B_{n+p} \;=\; A_{n+p} - (n+p)a_{n+p+1}\,.$$

Dans la somme définissant A_{n+p}, minorons $a_{n+1}, \dots, a_{n+p}$ par a_{n+p+1} $\big($la suite (a_k) est décroissante$\big)$. Il vient :

$$B_{n+p} \;\geqslant\; A_n + pa_{n+p+1} - (n+p)a_{n+p+1} \;=\; A_n - na_{n+p+1}\,.$$

Dans l'inégalité obtenue, fixons n et faisons tendre p vers $+\infty$. Par hypothèse, la suite (a_k) converge vers 0, donc na_{n+p+1} tend vers 0. Par ailleurs, B_{n+p} tend vers B. À la limite, on obtient donc $A_n \leqslant B$. La suite (A_n) est ainsi majorée et croissante, donc convergente. Autrement dit, la série $\sum_{n\geqslant 1} a_n$ converge.

IV.4.12 Si $a < 0$, le terme général de la série proposée tend vers 1, donc cette série diverge. Si $a := 0$, ce terme général n'est pas défini lorsque n est impair. Supposons donc $a > 0$. Pour tout entier $n \geqslant 2$, posons :

$$u_n \;:=\; \frac{(-1)^n}{n^a + (-1)^n} \quad \text{et} \quad v_n \;:=\; \frac{(-1)^n}{n^a}\cdot$$

La série $\sum_{n\geqslant 1} v_n$ converge (exercice 6 de la page 727). Ainsi les séries $\sum_{n\geqslant 1} u_n$ et $\sum_{n\geqslant 1}(v_n - u_n)$ sont de même nature, en vertu du théorème 2 de la page 711 et de son corollaire. Calculons $v_n - u_n$:

$$v_n - u_n \;=\; \frac{(-1)^n}{n^a\big[n^a + (-1)^n\big]}\Big(n^a + (-1)^n - n^a\Big) \;=\; \frac{1}{n^a\big[n^a + (-1)^n\big]}\cdot$$

Ainsi $v_n - u_n > 0$ pour tout n, et en outre $v_n - u_n \sim 1/n^{2a}$ lorsque n tend vers $+\infty$. On en déduit que la série $\sum_{n\geqslant 1}(v_n - u_n)$ converge si, et seulement si, $2a > 1$, soit $a > 1/2$. En conclusion, la série $\sum_{n\geqslant 1} u_n$ converge si, et seulement si, $a > 1/2$. On remarquera que cette série converge absolument si $a > 1$, mais elle est semi-convergente si $1/2 < a \leqslant 1$ (parce que c'est le cas pour la série $\sum_{n\geqslant 1} v_n$).

IV.4.13 Il faut d'abord remarquer que le critère spécial des séries alternées ne s'applique pas : ce critère ne porte que sur des séries à termes *réels*. Écrivons $a := s + it$, où $s, t \in \mathbb{R}$. Pour tout $n \in \mathbb{N}$, on a :

$$\frac{1}{n+a} \;=\; \frac{n+\bar{a}}{|n+a|^2} \;=\; \frac{(n+s)-it}{(n+s)^2+t^2}.$$

Notant u_n le terme général de la série proposée, on a $u_n = a_n + ib_n$, en posant :

$$a_n \;:=\; \frac{(-1)^n(n+s)}{(n+s)^2+t^2} \quad \text{et} \quad b_n \;:=\; \frac{(-1)^{n+1}t}{(n+s)^2+t^2}.$$

La série $\sum\limits_{n\geqslant 0} u_n$ converge si, et seulement si, *chacune* des deux séries $\sum\limits_{n\geqslant 0} a_n$ et $\sum\limits_{n\geqslant 0} b_n$ converge.

La série $\sum\limits_{n\geqslant 0} b_n$ converge absolument (et donc elle converge). C'est évident si $t := 0$, et sinon $|b_n| \sim |t|/n^2$ lorsque n tend vers $+\infty$. Passons à la série $\sum\limits_{n\geqslant 0} a_n$. Il s'agit d'une série alternée (à partir d'un certain rang). Considérons la fonction $x \longmapsto f(x) := x/(x^2+t^2)$. Un calcul immédiat donne sa dérivée : $f'(x) = (t^2-x^2)/(x^2+t^2)^2$. Ainsi f est décroissante sur $\left]|t|, +\infty\right[$. On en déduit que la suite $(|a_n|)$ est décroissante à partir du rang $n_0 := E\big(|s|+|t|\big)+1$. Par ailleurs $\lim\limits_{n\to+\infty} a_n = 0$. Le critère spécial des séries alternées montre donc que la série $\sum\limits_{n\geqslant 0} a_n$ converge. En conclusion, la série $\sum\limits_{n\geqslant 0} u_n$ converge (mais elle ne converge pas absolument).

IV.4.14 1) Le point de départ est le suivant : pour tout $k \in \mathbb{N}$, on a :

$$\frac{1}{ak+1} \;=\; \int_0^1 x^{ak}\mathrm{d}x\,.$$

Soit alors $n \in \mathbb{N}$. Multiplions l'égalité précédente par $(-1)^k$ et sommons pour $k = 0, \ldots, n$. Par linéarité de l'intégrale, il vient :

$$U_n \;=\; \int_0^1 \left(\sum_{k=0}^{n}(-1)^k x^{ak}\right)\mathrm{d}x\,.$$

La somme intervenant dans cette formule est la somme des termes de la progression géométrique de premier terme 1 et de raison $-x^a$. D'où :

$$U_n \;=\; \int_0^1 \frac{1-(-1)^{n+1}x^{a(n+1)}}{1+x^a}\,\mathrm{d}x\,.$$

On en déduit une expression de la différence $I - U_n$:

$$I - U_n \;=\; (-1)^{n+1}\int_0^1 \frac{x^{a(n+1)}}{1+x^a}\,\mathrm{d}x\,,$$

d'où, en majorant $1/(1+x^a)$ par 1 :

$$|I-U_n| \;\leqslant\; \int_0^1 x^{a(n+1)}\mathrm{d}x \;=\; \frac{1}{a(n+1)+1}.$$

Il en résulte bien que la suite (U_n) converge vers I. Autrement dit, la série $\sum_{n\geqslant 0} u_n$ converge, et l'on a :

$$\sum_{n=0}^{+\infty} u_n \;=\; I\,. \qquad (*)$$

La convergence de la série $\sum_{n\geqslant 0} u_n$ résultait aussi évidemment du critère spécial des séries alternées.

2) Considérons un entier $n \geqslant 2$ fixé. Par définition, R_n est la somme de la série $\sum_{k\geqslant 0} u_{n+k+1}$. En particulier, R_n est la limite, lorsque $P \in \mathbb{N}$ tend vers $+\infty$, de la somme partielle S_P d'indice $2P+1$ de ladite série, à savoir :

$$S_P \;:=\; \sum_{k=0}^{2P+1} u_{n+k+1} \;=\; \sum_{p=1}^{P+1} \big(u_{n+2p-1} + u_{n+2p}\big)\,.$$

Pour tout $p \in \mathbb{N}^*$, on a :

$$u_{n+2p-1} + u_{n+2p} \;=\; (-1)^{n-1}\left[\frac{1}{a(n+2p-1)+1} - \frac{1}{a(n+2p)+1}\right], \quad \text{soit}$$

$$u_{n+2p-1} + u_{n+2p} \;=\; \frac{(-1)^{n-1}a}{\big[a(n+2p)+1\big]\big[a(n+2p-1)+1\big]}.$$

Ainsi, lorsque p varie, les sommes $u_{n+2p-1} + u_{n+2p}$ ont toutes le même signe, à savoir $(-1)^{n-1}$. D'où :

$$|S_P| \;=\; \sum_{p=1}^{P+1} \frac{a}{\big[a(n+2p)+1\big]\big[a(n+2p-1)+1\big]}.$$

L'entier n étant toujours fixé, soit f la fonction définie sur $\big[0,+\infty\big[$ par :

$$f(x) \;=\; \frac{a}{\big[a(n+2x)+1\big]\big[a(n+2x-1)+1\big]}.$$

Cette fonction est évidemment décroissante. Par ailleurs, on vérifie facilement qu'une primitive F de f est donnée par la formule :

$$F(x) \;:=\; \frac{1}{2a}\ln\left(\frac{a(n+2x-1)+1}{a(n+2x)+1}\right).$$

Appliquons la proposition 13 de la page 718 à f. Il vient :

$$F(P+2) - F(1) \;\leqslant\; |S_P| \;\leqslant\; F(P+1) - F(0).$$

Lorsque x tend vers $+\infty$, $F(x)$ tend vers 0. En passant à la limite pour P tendant vers $+\infty$, les inégalités précédentes donnent :

$$\ln\left(\frac{a(n+2)+1}{a(n+1)+1}\right) = -2aF(1) \leqslant 2a|R_n| \leqslant -2aF(0) = \ln\left(\frac{an+1}{a(n-1)+1}\right).$$

On sait que, lorsque t tend vers 0, $\ln(1+t)$ est équivalent à t. Faisons tendre n vers $+\infty$. Alors $t := a/(a(n-1)+1)$ tend vers 0, donc :

$$\ln\left(\frac{an+1}{a(n-1)+1}\right) \;=\; \ln(1+t) \;\sim\; t \;=\; \frac{a}{a(n-1)+1} \;\sim\; \frac{1}{n}.$$

De la même manière, $u := a/\big(a(n+1)+1\big)$ tend vers 0, d'où :

$$\ln\left(\frac{a(n+2)+1}{a(n+1)+1}\right) \;=\; \ln(1+u) \;\sim\; u \;=\; \frac{a}{a(n+1)+1} \;\sim\; \frac{1}{n}\cdot$$

Compte tenu des inégalités obtenues précédemment, $2a|R_n| \sim 1/n$, autrement dit $2an|R_n|$ tend vers 1 lorsque n tend vers $+\infty$.

Donnons une solution n'utilisant pas la proposition 13 de la page 718. Pour tout $k \in \mathbb{N}$, posons $v_k := a|u_{2k} + u_{2k+1}|$, autrement dit :

$$v_k \;=\; \frac{a^2}{\big[2ak+1\big]\big[a(2k+1)+1\big]}\cdot$$

La série $\sum\limits_{k\geqslant 0} v_k$ converge : elle est à termes réels positifs, et, lorsque k tend vers $+\infty$, v_k est équivalent à $1/(4k^2)$. Par ailleurs, si $m \in \mathbb{N}$, le début de cette question montre que $a|R_{2m+1}|$ est le reste d'indice m de la série $\sum\limits_{k\geqslant 0} v_k$. Pour estimer ce reste, posons $w_k := 1/\big(4k(k+1)\big)$ pour tout $k \in \mathbb{N}^*$. Ainsi $v_k \sim w_k$ lorsque k tend vers $+\infty$. D'après le théorème 11 de la page 716, $a|R_{2m+1}|$ est équivalent, lorsque m tend vers $+\infty$, au reste d'indice m de la série $\sum\limits_{k\geqslant 0} w_k$. Ce dernier reste vaut $1/\big(4(m+1)\big)$, *cf.* l'exemple 3 de la page 709. D'où $\lim\limits_{m\to+\infty} 4am|R_{2m+1}| = 1$, soit $\lim\limits_{m\to+\infty} 2a(2m+1)|R_{2m+1}| = 1$. De manière analogue, on montre que $\lim\limits_{m\to+\infty} 2a(2m)|R_{2m}| = 1$, en partant de $v_k := a|u_{2k+1} + u_{2k+2}|$. En conclusion, $\lim\limits_{n\to+\infty} 2an|R_n| = 1$.

3) Prenons $a := 2$. La formule $(*)$ s'écrit ici :

$$\sum_{n=0}^{+\infty} \frac{(-1)^n}{2n+1} \;=\; \int_0^1 \frac{\mathrm{d}x}{x^2+1}\cdot$$

La fonction $\arctan$ étant une primitive de $1/(1+x^2)$ sur $\mathbb{R}$, l'intégrale obtenue vaut $\arctan(1) - \arctan(0) = \pi/4$, d'où l'égalité à démontrer.

IV.4.15 Notons $\sum\limits_{n\geqslant 0} u_n$ la série proposée et (U_n) la suite de ses sommes partielles. Observons que les termes positifs de cette série sont ceux dont l'indice est multiple de 3, plus précisément $u_{3p} = 1/(2p+1)$ pour tout $p \in \mathbb{N}$. Pour tout $p \in \mathbb{N}$, on a aussi :

$$u_{3p+1} \;=\; \frac{-1}{4p+2} \quad \text{et} \quad u_{3p+2} \;=\; \frac{-1}{4p+4}\cdot$$

Soit $P \in \mathbb{N}$, calculons S_{3P+2} :

$$S_{3P+2} \;=\; \sum_{n=0}^{3P+2} u_n \;=\; \sum_{p=0}^{P} \big(u_{3p} + u_{3p+1} + u_{3p+2}\big)\,, \quad \text{soit}$$

$$S_{3P+2} \;=\; \sum_{p=0}^{P} \left[\frac{1}{2p+1} - \frac{1}{4p+2} - \frac{1}{4p+4}\right] \;=\; \sum_{p=0}^{P} \left[\frac{1}{4p+2} - \frac{1}{4p+4}\right].$$

En d'autres termes,

$$S_{3P+2} \;=\; \frac{1}{2}\sum_{p=0}^{P}\left[\frac{1}{2p+1}-\frac{1}{2p+2}\right] \;=\; \frac{1}{2}\sum_{n=1}^{2P+2}\frac{(-1)^{n-1}}{n}.$$

Ainsi S_{3P+2} est la moitié de la somme partielle d'indice $2P+2$ de la série harmonique alternée $\sum\limits_{n\geqslant 1}(-1)^{n-1}/n$. D'après la formule (24), cette série harmonique alternée converge et sa somme est $\ln 2$. Il en résulte que la suite $(S_{3P+2})_{P\geqslant 0}$ converge vers $\ln 2/2$.

Pour tout $P\in\mathbb{N}$, on a :

$$S_{3P+1}=S_{3P+2}-u_{3P+2} \quad \text{et} \quad S_{3P}=S_{3P+2}-u_{3P+2}-u_{3P+1}.$$

Comme la *suite* (u_n) converge évidemment vers 0, S_{3P} et S_{3P+1} tendent aussi vers $\ln 2/2$ lorsque P tend vers $+\infty$. Dans ces conditions, la suite $(S_n)_{n\geqslant 0}$ converge vers $\ln 2/2$, *i.e.* la série $\sum\limits_{n\geqslant 0}u_n$ converge et a pour somme $\ln 2/2$.

Remarquons que les termes de la série $\sum\limits_{n\geqslant 0}u_n$ sont exactement les mêmes que ceux de la série harmonique alternée, mais ils ne sont pas écrits dans le même ordre. Ainsi, partant d'une série convergente, si l'on écrit les termes de cette série dans un ordre différent, on peut obtenir une série convergente dont la somme ne soit pas égale à la somme de la série initiale. En L2, nous traduirons ce fait en disant qu'une série convergente n'est pas toujours « commutativement convergente », mais nous verrons aussi qu'une série *absolument* convergente est « commutativement convergente ».

IV.4.16 1) Pour tout $n\in\mathbb{N}$, $|u_n|=1/2^n$. Puisque la série géométrique $\sum\limits_{n\geqslant 0}1/2^n$ converge, la série $\sum\limits_{n\geqslant 0}u_n$ est absolument convergente, donc convergente. De plus, si $n\in\mathbb{N}$, l'inégalité triangulaire donne :

$$|U_n| \;=\; \left|\sum_{k=0}^{n}u_k\right| \;\leqslant\; \sum_{k=0}^{n}\frac{1}{2^k} \;<\; \sum_{k=0}^{+\infty}\frac{1}{2^k} \;=\; 2.$$

Ainsi $|U_n|\leqslant 2$ pour tout n, d'où $|S|\leqslant 2$, en faisant tendre n vers $+\infty$.

2) Nous allons définir par récurrence une suite $(f_n)_{n\geqslant 0}$ où, pour tout n, f_n est une application de $\{-1,1\}^{n+1}$ dans $\big[-2,2\big]$. Définissons d'abord l'application $f_0:\{-1,1\}\to\big[-2,2\big]$ par la formule $f_0(\alpha_0):=\alpha_0\sqrt{2}$. Pour tout $n\in\mathbb{N}$, on définit ensuite f_{n+1} en fonction de f_n comme suit. Pour tous $\alpha_0,\dots,\alpha_{n+1}\in\{-1,1\}$, nous posons :

$$f_{n+1}(\alpha_0,\dots,\alpha_{n+1}) \;:=\; \alpha_0\sqrt{2+f_n(\alpha_1,\dots,\alpha_{n+1})}.$$

Comme $f_n(\alpha_1,\dots,\alpha_{n+1})\in\big[-2,2\big]$, on a $2+f_n(\alpha_1,\dots,\alpha_{n+1})\in\big[0,4\big]$, d'où $f_{n+1}(\alpha_0,\dots,\alpha_{n+1})\in\big[-2,2\big]$.

Revenant à l'énoncé, il suffit maintenant de poser, pour tout $n\in\mathbb{N}$:

$$x_n \;:=\; f_n(\varepsilon_0,\dots,\varepsilon_n).$$

Démontrons ensuite, par récurrence sur n, la formule suivante explicitant f_n : pour tous $\alpha_0,\dots,\alpha_n\in\{-1,1\}$:

$$f_n(\alpha_0,\dots,\alpha_n) \;=\; 2\sin\left(\frac{\pi}{4}\sum_{k=0}^{n}\frac{\alpha_0\alpha_1\cdots\alpha_k}{2^k}\right). \qquad (*)$$

Cette formule est vraie si $n := 0$: pour tout $\alpha_0 \in \{-1, 1\}$, on a bien :

$$f_0(\alpha_0) \;=\; \alpha_0\sqrt{2} \;=\; 2\sin(\alpha_0\pi/4).$$

Supposons que la formule $(*)$ soit vraie pour un certain $n \in \mathbb{N}$.

Soient $\alpha_0, \ldots, \alpha_{n+1} \in \{-1, 1\}$. Compte tenu de la formule donnant f_{n+1} en fonction de f_n, il vient :

$$f_{n+1}(\alpha_0, \ldots, \alpha_{n+1}) \;=\; \alpha_0\sqrt{2 + 2\sin\theta} \;=\; \alpha_0\sqrt{2 + 2\cos(\pi/2 - \theta)}\,,$$

ou encore :

$$f_{n+1}(\alpha_0, \ldots, \alpha_{n+1}) \;=\; 2\alpha_0\big|\cos(\pi/4 - \theta/2)\big| \;=\; 2\alpha_0\big|\sin(\pi/4 + \theta/2)\big|\,,$$

où l'on a posé :

$$\theta \;=\; \frac{\pi}{4}\sum_{k=0}^{n}\frac{\alpha_1\alpha_2\cdots\alpha_{k+1}}{2^k}\cdot$$

Mais $\theta \in \big[-\pi/2, \pi/2\big]$, donc $\pi/4 + \theta/2 \in \big[0, \pi/2\big]$, et par suite le sinus intervenant dans la formule ci-dessus est positif. Ainsi :

$$f_{n+1}(\alpha_0, \ldots, \alpha_{n+1}) \;=\; 2\sin\eta\,, \quad \text{où}$$

$$\eta \;:=\; \frac{\alpha_0\pi}{4}\left[1 + \sum_{k=0}^{n}\frac{\alpha_1\alpha_2\cdots\alpha_{k+1}}{2^{k+1}}\right] \;=\; \frac{\pi}{4}\sum_{k=0}^{n+1}\frac{\alpha_0\alpha_1\cdots\alpha_k}{2^k}\,.$$

D'où la formule $(*)$ à l'ordre $n+1$.

Revenons à la suite (x_n). En remplaçant dans la formule $(*)$ les α_k par les ε_k, on obtient le résultat annoncé, valable pour tout $n \in \mathbb{N}$:

$$x_n \;=\; 2\sin(\pi U_n/4)\,.$$

Par définition d'une série convergente, la suite (U_n) converge vers S. La fonction sinus étant continue, la formule ci-dessus montre que la suite (x_n) converge. Plus précisément :

$$\lim_{n\to+\infty} x_n \;=\; 2\sin(\pi S/4)\,.$$

IV.4.17 Posons $u_n := \varepsilon_n a_n$ pour tout $n \in \mathbb{N}$. Soit $n \in \mathbb{N}$. Effectuons la division euclidienne de n par m : $n = qm + r$, où $q \in \mathbb{N}$ et $r \in [\![0, m-1]\!]$. Pour chaque $k \in \mathbb{N}$, la somme $\sum_{j=km}^{km+m-1}\varepsilon_j$ est égale, vu la périodicité de la suite (ε_h), à $\sum_{j=0}^{m-1}\varepsilon_j$, c'est-à-dire à S. Ainsi :

$$t_n = \sum_{j=0}^{n}\varepsilon_j = \sum_{k=0}^{q-1}\left(\sum_{j=km}^{km+m-1}\varepsilon_j\right) + \sum_{j=qm}^{qm+r}\varepsilon_j = qS + \sum_{j=qm}^{qm+r}\varepsilon_j.$$

On peut donc écrire $T_n = nS/m + w_n$, en posant :

$$w_n \;:= S\big(q - n/m\big) + \sum_{j=qm}^{qm+r}\varepsilon_j \;=\; -S(r/m) + \sum_{j=qm}^{qm+r}\varepsilon_j.$$

Pour tout n, $|w_n| \leqslant |S| + r + 1 \leqslant |S| + m$, donc la suite (w_n) est bornée.

Démontrons ensuite la formule suivante, pour tout $n \in \mathbb{N}$:

$$U_n \;=\; \frac{S(A_n - a_0)}{m} \;+\; w_n a_{n+1} \;+\; \sum_{k=0}^{n} w_k(a_k - a_{k+1})\,. \qquad (*)$$

Cette formule est vraie si $n := 0$. En effet $w_0 = t_0 = \varepsilon_0$, $A_0 = a_0$, donc le second membre vaut $w_0 a_0 = \varepsilon_0 a_0 = u_0 = U_0$. Supposons la formule $(*)$ vraie pour un certain n. Nous voulons établir la formule au rang $n+1$, soit :

$$U_{n+1} \;=\; \frac{S(A_{n+1} - a_0)}{m} \;+\; w_{n+1} a_{n+2} \;+\; \sum_{k=0}^{n+1} w_k(a_k - a_{k+1})\,.$$

Par différence, il revient au même d'établir la formule suivante :

$$\varepsilon_{n+1} a_{n+1} \;=\; S a_{n+1}/m + w_{n+1} a_{n+2} - w_n a_{n+1} + w_{n+1}(a_{n+1} - a_{n+2}).$$

Il suffit évidemment de vérifier l'égalité $\varepsilon_{n+1} = S/m + w_{n+1} - w_n$, soit :

$$\varepsilon_{n+1} = S/m + \big(T_{n+1} - (n+1)S/m\big) - \big(T_n - nS/m\big)\,,$$

ce qui résulte immédiatement de l'égalité $T_{n+1} - T_n = \varepsilon_{n+1}$.

Puisque la suite (w_n) est bornée et la suite (a_n) converge vers 0, la suite $(w_n a_{n+1})$ converge vers 0. Soit ensuite M un réel tel que $|w_n| \leqslant M$ pour tout n. Rappelons que la suite (a_n) est décroissante. Ainsi, pour tout $n \in \mathbb{N}$, on a :

$$\sum_{k=0}^{n} \big|w_k(a_k - a_{k+1})\big| \;\leqslant\; M \sum_{k=0}^{n} (a_k - a_{k+1}) \;=\; M(a_0 - a_{n+1}) \;\leqslant\; M a_0.$$

Il en résulte que la série $\sum\limits_{n \geqslant 0} w_n(a_n - a_{n+1})$ est absolument convergente, donc convergente.

Autrement dit, la suite de terme général $\sum\limits_{k=0}^{n} w_k(a_k - a_{k+1})$ est convergente. Compte tenu de la formule $(*)$, la suite (U_n) converge, *i.e.* la série $\sum\limits_{n \geqslant 0} u_n$ converge, si, et seulement si, la suite $\big(S(A_n - a_0)\big)$ converge, *i.e.* si la suite (SA_n) converge. C'est évidemment le cas si la suite (A_n) converge, *i.e.* si la série $\sum\limits_{n \geqslant 0} a_n$ converge ; c'est aussi le cas si $S = 0$.

Pour conclure, il reste à montrer que, si $S \neq 0$ et si la série $\sum\limits_{n \geqslant 0} a_n$ diverge, la suite (SA_n) diverge. C'est évident car, $\sum\limits_{n \geqslant 0} a_n$ étant une série divergente à termes réels positifs, la suite de ses sommes partielles a pour limite $+\infty$ (c'est une suite croissante).

Complément. À titre d'illustration de cet exercice, soit p un entier strictement positif. Pour tout $k \in \mathbb{N}$, posons $b(k) := \binom{k+p}{p}$. Considérons la série :

$$\sum_{n \geqslant 1} \frac{(-1)^{b(n)}}{n}. \qquad (**)$$

Nous allons montrer que cette série converge si, et seulement si, p est une puissance de 2. Pour tout $n \in \mathbb{N}^*$, nous posons ici :

$$a_n \;:=\; \frac{1}{n} \quad \text{et} \quad \varepsilon_n \;:=\; (-1)^{b(n)}.$$

La suite $(a_n)_{n\geqslant 1}$ est bien décroissante et converge vers 0, par contre la série $\sum_{n\geqslant 1} a_n$ diverge : c'est la série harmonique.

Montrons ensuite que la suite $(\varepsilon_n)_{n\geqslant 1}$ est périodique. Voici une première méthode. Partons de la formule suivante, valable pour tout $n \in \mathbb{N}$:

$$b(n) \;=\; \binom{n+p}{p} \;=\; \frac{n(n-1)\cdots(n-p+1)}{p!}.$$

Soit $m' := 2p!$. Lorsqu'on remplace n par $n+m'$, le numérateur du second membre de l'égalité précédente n'est pas modifié modulo m' (c'est un polynôme en n à coefficients entiers). Il en résulte que les entiers $b(n)$ et $b(n+m')$ ont la même parité, de sorte que $\varepsilon_{n+m'} = \varepsilon_n$. Ainsi m' est une période de la suite $(\varepsilon_n)_{n\geqslant 1}$. Notons m la plus petite période (strictement positive) de cette suite ; ainsi m' est un multiple de m. Nous expliciterons m plus loin.

Appliquons le présent exercice (que les suites considérées soient indexées par $\mathbb{N}$ ou par $\mathbb{N}^*$ ne change rien à la conclusion obtenue). Posons :

$$S \;:=\; \sum_{n=1}^{m} \varepsilon_n \;=\; \sum_{n=1}^{m} (-1)^{b(n)}\,.$$

Alors la série $(**)$ converge si, et seulement si, $S = 0$. Il nous faut donc évaluer S. Pour cela, pour chaque $n \in \mathbb{N}$, nous devons pouvoir dire si l'entier $b(n)$ est pair ou impair.

Utilisons l'exercice II.1.18. Pour tout entier $t \geqslant 1$, notons $\nu_2(t)$ l'exposant de la plus grande puissance de 2 divisant t. L'exercice cité permet, pour tout entier $k \in \mathbb{N}$, de calculer $\nu_2(k!)$. Voici le résultat dudit exercice : $\nu_2(k!) = k - s(k)$, en notant $s(k)$ la somme des chiffres de k écrit en base 2. Soient $a, b \in \mathbb{N}$. Puisque $\binom{a+b}{a} = (a+b)!/(a!\,b!)$, il vient :

$$\nu_2\left(\binom{a+b}{a}\right) \;=\; s(a) + s(b) - s(a+b)\,.$$

En réfléchissant à l'algorithme de l'addition de deux entiers écrits en base 2, on s'aperçoit que $s(a) + s(b) - s(a+b)$ est le nombre de retenues faites dans l'addition de a et b en base 2. En particulier, $\binom{a+b}{a}$ est *impair* si, et seulement si, cette addition ne comporte aucune retenue. Cela revient à dire que, si l'on écrit :

$$a \;:=\; 2^{\alpha_1} + \cdots + 2^{\alpha_h} \quad \text{et} \quad b \;:=\; 2^{\beta_1} + \cdots + 2^{\beta_k}\,,$$

avec $\alpha_1 > \alpha_2 > \cdots > \alpha_h \geqslant 0$ et $\beta_1 > \beta_2 > \cdots > \beta_k \geqslant 0$, on a $\alpha_i \neq \beta_j$ pour tout $(i,j) \in [\![1,h]\!] \times [\![1,k]\!]$.

Écrivons maintenant p en base 2 :

$$p \;:=\; 2^{c_1} + 2^{c_2} + \cdots + 2^{c_r}\,, \quad \text{avec} \quad c_1 > c_2 > \cdots > c_r \geqslant 0.$$

Soit $n \in \mathbb{N}$. Pour que $b(n)$ soit impair, il faut, et il suffit, que les chiffres (en base 2) de n d'indices $c_1, \ldots, c_r$ soient nuls. Cette propriété n'est pas modifiée si l'on remplace n par $n + 2^{c_1+1}$, car les chiffres en question ne changent pas. Il en résulte que $m := 2^{c_1+1}$ est une période de la suite de terme général $(-1)^{b(n)}$. Par contre $b(0) = 1$, alors que $b(2^{c_1})$ est pair, puisque l'addition de p et 2^{c_1} en base 2 comporte une retenue. Tout cela montre que m est la plus petite période strictement positive de la suite $(\varepsilon_n)_{n\geqslant 1}$.

Calculons maintenant la somme S. C'est une somme de m termes, chacun valant ± 1. Ainsi $S = N - N'$, où N (resp. N') est le nombre de termes valant 1 (resp. -1). Par

définition, N' est le nombres d'entiers $n \in [\![0, 2^{c_1+1} - 1]\!]$ tels que les chiffres (en base 2) de n d'indices $c_1, \ldots, c_r$ soient nuls. Les autres chiffres de n sont arbitraires. Lorsqu'on écrit n sous la forme :

$$n := \sum_{i=0}^{c_1} \gamma_i \, 2^i \,,$$

chaque γ_i valant 0 ou 1, r parmi ces coefficients doivent être nuls, les $c_1 + 1 - r$ autres étant arbitraires. D'où $N' = 2^{c_1+1-r} = m2^{-r}$. Cela étant, puisque $N + N' = m$, S est nulle si, et seulement si, $N = N' = m/2$, *i.e.* si $r = 1$. Mais, vu l'écriture de p en base 2, r vaut 1 si, et seulement si, p est une puissance de 2, d'où la conclusion annoncée.

Module IV.5 : Introduction à l'intégration

IV.5.1 On trouve :

1. $A = \displaystyle\int_1^3 \left(x^2 + 2 + \frac{1}{x^2}\right) \mathrm{d}x = \left[\frac{x^3}{3} + 2x - \frac{1}{x}\right]_1^3 = \frac{40}{3}\cdot$
2. $B = \displaystyle\left[\frac{x^8}{4} - \frac{15x^7}{7} + \frac{19x^6}{2} - \frac{108x^5}{5} + \frac{69x^4}{4} + 60x^3 - \frac{425x^2}{2} + 375x\right]_0^1 = \frac{15803}{70}\cdot$

IV.5.2 On trouve :

1. On reconnaît dans l'intégrande la forme $u'(x)\,u(x)$, avec $u(x) = \ln|x|$, d'où :
$$C(x) = \frac{1}{2}\,\ln^2|x| + C^{te}$$
sur tout intervalle ne contenant pas 0.
2. De même, l'intégrande est de la forme $u'(x)/u(x)$, donc :
$$D(x) = \ln\bigl|\ln|x|\bigr| + C^{te}$$
sur tout intervalle ne contenant ni 0, ni 1, ni -1.

IV.5.3 Lorsque la fraction rationnelle est de la forme $\dfrac{P(x)}{(x-a)^n\,Q(x)}$, avec $Q(a) \neq 0$, le coefficient de $\dfrac{1}{(x-a)^n}$ dans la décomposition en éléments simples est $\dfrac{P(a)}{Q(a)}$ (multiplier par $(x-a)^n$ et faire tendre x vers a).

1. On trouver $a = \dfrac{1+3}{1+6} = \dfrac{3}{7}$ et $b = \dfrac{-6+2}{-6-1} = \dfrac{4}{7}$, d'où :
$$\frac{x+2}{x^2+5x-6} = \frac{3}{7(x-1)} + \frac{4}{7(x+6)} \qquad \text{et} \qquad E = \frac{3}{7}\,\ln|x-1| + \frac{4}{7}\,\ln|x+6| + C^{te}$$
sur tout intervalle ne contenant ni 1, ni -6.
2. La partie entière est évidemment $a = 1$. Ensuite, on trouve :
$$b = \frac{0-2}{0-1} = 2 \qquad \text{et} \qquad d = \frac{1-2}{1} = -1.$$
En retranchant la partie entière, on obtient :
$$\frac{b}{x^2} + \frac{c}{x} + \frac{d}{x-1} = \frac{x^3-2}{x^3-x^2} - 1 = \frac{x^2-2}{x^3-x^2}$$
ce qui, en multipliant par x et en faisant tendre x vers l'infini, donne $c + d = 1$. Donc :
$$\frac{x^3-2}{x^3-x^2} = 1 + \frac{2}{x} + \frac{2}{x^2} - \frac{1}{x-1}, \qquad F = x - \frac{2}{x} + \ln\frac{x^2}{|x-1|} + C^{te}$$
sur tout intervalle ne contenant ni 1, ni 0.

3. On trouve $a = 1$ puis, en retranchant $\dfrac{1}{x^3}$:

$$\frac{3x^4 + 2x^2 + 1}{x^3(x^2+1)^2} - \frac{1}{x^3} = \frac{2x}{(x^2+1)^2} \qquad \text{d'où} \qquad G = -\frac{1}{2x^2} - \frac{1}{x^2+1} + C^{te}$$

sur tout intervalle ne contenant pas 0.

IV.5.4 Dans cet exercice et quelques-uns des suivants, nous utiliserons le théorème d'intégration par parties sous la forme :

$$\int \varphi'\psi = \varphi\psi - \int \varphi\psi'.$$

1. Ici nous prendrons $\varphi(x) = x^3/3$ et $\psi(x) = \ln x$, d'où :

$$H = \frac{x^3 \ln x}{3} - \frac{x^3}{9} + C^{te}$$

sur tout intervalle de $\mathbb{R}_+^*$.

2. Ici nous prendrons $\varphi(x) = x$ et $\psi(x) = \arctan x$, d'où :

$$I = x \arctan x - \frac{1}{2}\ln(x^2+1) + C^{te}.$$

IV.5.5 Pour la première intégrale, on écrit :

$$\frac{1}{\sinh x} = \frac{\sinh x}{\sinh^2 x} = \frac{\sinh x}{\cosh^2 x - 1} = \frac{u'}{u^2-1}\cdot$$

En écrivant $\dfrac{1}{u^2-1} = \dfrac{1}{2}\left(\dfrac{1}{u-1} - \dfrac{1}{u+1}\right)$, on obtient :

$$J = \int \frac{\mathrm{d}u}{u^2-1} = \left[\frac{1}{2}\ln\left|\frac{u-1}{u+1}\right|\right]_{\cosh 1}^{\cosh 2} = \ln\frac{(e+1)^2}{\mathrm{e}^2+1}\cdot$$

Pour la deuxième, on écrit $\dfrac{1}{1+\mathrm{e}^x} = 1 - \dfrac{\mathrm{e}^x}{1+\mathrm{e}^x} = 1 - \dfrac{t'}{1+t}$, d'où :

$$K = \big[t - \ln(1+t)\big]_1^2 = 1 - \ln\frac{\mathrm{e}^2+1}{e+1}\cdot$$

La dernière nous ramène au calcul de $\displaystyle\int \mathrm{e}^{-\theta}\cos\theta\ \mathrm{d}\theta$. On peut alors intégrer deux fois par parties ou trouver une primitive de $\theta \mapsto \mathrm{e}^{(i-1)\theta}$ et en prendre la partie réelle. Avec les deux méthodes, on voit qu'une primitive sera de la forme $a\,e^{-\theta}\cos\theta + b\,e^{-\theta}\sin\theta$. Il suffit donc de dériver cette dernière expression et d'identifier, pour trouver :

$$\int \mathrm{e}^{-\theta}\cos\theta\,\mathrm{d}\theta = \frac{\mathrm{e}^{-\theta}}{2}(\sin\theta - \cos\theta) + C^{te}.$$

On a alors :

$$L = \int_{\pi/4}^{\pi/2} \mathrm{e}^{-\theta}\cos\theta\,\mathrm{d}\theta = \frac{\mathrm{e}^{-\pi/2}}{2}\cdot$$

IV.5.6 Le premier calcul est immédiat en posant le changement de variable $u := \cos x$, ce qui donne :

$$M = -\int (1-u^2)u^2 \mathrm{d}u = -\frac{1}{15}\,(5 - 3\cos^x)\cos^3 x + C^{te}.$$

Le changement de variable indiqué pour le second conduit à :

$$N = \int \frac{2t\,\mathrm{d}t}{2t^2+1} = \frac{1}{2}\,\ln(2t^2+1) = \frac{1}{2}\,\ln(1+\sin^2 x) - \ln|\cos x| + C^{te}$$

sur tout intervalle ne contenant aucun zéro de la fonction $\cos$.

IV.5.7 Il suffit de poser le changement de variable $t := \pi/2 - x$.

IV.5.8 Soit F une primitive de f. L'expression dont on doit déterminer la limite s'écrit :

$$\frac{F(1+x)-F(1-x)}{x} = \frac{F(1+x)-F(1)}{x} + \frac{F(1-x)-F(1)}{-x}$$

ce qui montre que la valeur cherchée existe bien et vaut $2F'(1) = 2f(1)$.

IV.5.9 Soient f la fonction continue définie par $f(t) := \sin(t)/t$ pour $t \neq 0$ et $f(0) := 1$, et F sa primitive nulle en 0. L'expression dont on doit déterminer la limite s'écrit $F(x)/x$, ce qui montre que la valeur cherchée existe bien et vaut $F'(0) = f(0) = 1$.

IV.5.10 Suivant l'indication de l'énoncé, on obtient :

$$(\ln b - \ln a)^2 = \left(\int_a^b \frac{\mathrm{d}x}{x}\right)^2 \leqslant \left(\int_a^b \mathrm{d}x\right)\left(\int_a^b \frac{\mathrm{d}x}{x^2}\right) = (b-a)\left(\frac{1}{a} - \frac{1}{b}\right) = \frac{(b-a)^2}{ab}$$

d'où le résultat puisque $b > a > 0$ et $\ln b > \ln a$.

IV.5.11 1. Il s'agit d'une somme de Riemann régulière à gauche sur le segment $[0,1]$ relative à la fonction f. Comme cette dernière est continue sur $[0,1]$, la limite cherchée existe donc et vaut $\displaystyle\int_0^1 f(x)\,\mathrm{d}x$.

2. La première est le cas particulier où $f(x) := x\mathrm{e}^{-x}$, d'où la limite :

$$\int_0^1 x\mathrm{e}^{-x}\mathrm{d}x = [-(x+1)\mathrm{e}^{-x}]_0^1 = 1 - \frac{2}{e}\cdot$$

Pour la deuxième, il s'agit d'une somme de Riemann régulière à droite sur le segment $[0,1]$ relative à la fonction définie par $f(x) = \sqrt{x}$, et sa limite est donc :

$$\int_0^1 f(x)\,\mathrm{d}x = [2\sqrt{x}]_0^1 = 2.$$

IV.5.12 1. L'inégalité de gauche provient de la (stricte) croissance de la fonction logarithme, celle de droite de sa concavité : la courbe d'équation $y = \ln(1+x)$ se trouve sous sa tangente en 0 d'équation $y = x$.

2. La limite est nulle, comme le montrent les majorations :

$$0 \leqslant \int_0^1 \ln(1+x^n)\,\mathrm{d}x \leqslant \int_0^1 x^n\,\mathrm{d}x = \frac{1}{n+1}\cdot$$

3. Résultat d'une intégration par parties :

$$\int_0^1 \varphi'\psi = [\varphi\psi]_0^1 - \int_0^1 \varphi\psi'$$

pour $\varphi(x) := \ln(1+x^n)$ et $\psi(x) := x/n$.

4. La limite de (u_n) est donc 0, et celle de (nu_n) est $\ln 2$.

IV.5.13 1. Toute fonction continûment dérivable est dérivable et donc continue ; sur un segment, cela implique qu'elle est bornée.

2. Posons $M := \sup|g|$, $M' := \sup|g'|$ (qui sont en fait des maximums), $\varphi(t) := -\cos nt$ et $\psi(t) := g(t)$. Il suffit alors d'écrire :

$$n\int_a^b g(t)\,\sin nt\,\mathrm{d}t = [-g(t)\,\cos nt]_a^b + \int_a^b g'(t)\,\cos nt\,\mathrm{d}t$$

pour en déduire la majoration indépendante de n :

$$\left| n\int_a^b g(t)\,\sin nt\,\mathrm{d}t \right| \leqslant 2M + (b-a)\,M'.$$

On peut montrer directement par le calcul que $\displaystyle\int_a^b \sin nt\,\mathrm{d}t$ tend vers 0 quand n tend vers $+\infty$, mais on peut aussi appliquer ce qui précède à $g = 1$, ce qui donne l'inégalité :

$$\left| \int_a^b \sin nt\,\mathrm{d}t \right| \leqslant \frac{2}{n}$$

et montre le résultat.

3. On pourrait montrer que la fonction $t \mapsto t^p/\sin t$ se prolonge en une fonction continûment dérivable sur $[0, \pi/2]$ et appliquer ce qui précède pour montrer :

$$\lim_{n\to+\infty} \int_0^{\pi/2} t^p\,\frac{\sin nt}{\sin t}\,\mathrm{d}t.$$

Montrons ce résultat autrement. Par concavité de la fonction sinus sur $[0, \pi/2]$, on a :

$$\forall t \in [0, \pi/2]\,,\ \sin t \geqslant \frac{2}{\pi}\,t$$

(la courbe représentative se trouve au dessus de la corde reliant les points d'abscisses 0 et $\pi/2$).

Pour tout $\alpha \in]0, \pi/2]$, on dispose de la majoration :

$$\left| \int_0^\alpha t^p \, \frac{\sin nt}{\sin t} \, \mathrm{d}t \right| \leqslant \int_0^\alpha \frac{\pi}{2} \, t^{p-1} \, |\sin nt| \, \mathrm{d}t \leqslant \int_0^\alpha \Big(\frac{\pi}{2}\Big)^p \mathrm{d}t = \alpha \Big(\frac{\pi}{2}\Big)^p.$$

Il en résulte que, pour tout $\varepsilon > 0$ donné, on peut choisir un $\alpha > 0$ tel que cette intégrale soit majorée par $\varepsilon/2$, d'où la majoration :

$$\left| \int_0^{\pi/2} t^p \, \frac{\sin nt}{\sin t} \, \mathrm{d}t \right| \leqslant \frac{\varepsilon}{2} + \left| \int_\alpha^{\pi/2} g(t) \, \sin nt \, \mathrm{d}t \right|$$

où g est, sur $[\alpha, \pi/2]$, une fonction continûment dérivable (et même de classe infinie). Par suite, il existe un N tel que, pour tout $n \geqslant N$, on ait :

$$\left| \int_0^{\pi/2} t^p \, \frac{\sin nt}{\sin t} \, \mathrm{d}t \right| \leqslant \varepsilon.$$

La limite demandée existe donc, elle vaut 0.

4. L'égalité classique $2 \sin u \cos v = \sin(u+v) + \sin(u-v)$ justifie les égalités :

$$\begin{aligned} A_{p,n} &= \frac{1}{2} \left(\int_0^{\pi/2} t^p \, \frac{\sin(2n+1)t}{\sin t} \, \mathrm{d}t - \int_0^{\pi/2} t^p \, \frac{\sin t}{\sin t} \, \mathrm{d}t \right) \\ &= \frac{1}{2} \left(\int_0^{\pi/2} t^p \, \frac{\sin(2n+1)t}{\sin t} \, \mathrm{d}t - \int_0^{\pi/2} t^p \, \mathrm{d}t \right) \end{aligned}$$

qui montrent que, lorsque n tend vers l'infini, $A_{p,n}$ a une limite, égale à :

$$-\int_0^{\pi/2} t^p \, \mathrm{d}t = -\frac{1}{p+1} \left(\frac{\pi}{2}\right)^{p+1}.$$

IV.5.14 Posons $I(a,b)$ l'intégrale considérée et, pour $b > 0$, $\varphi'(x) := x^a$ et $\psi(x) := (1-x)^b$. Une intégration par parties donne, pour $\varphi(x) = x^{a+1}/(a+1)$:

$$I(a,b) = \int_0^1 \varphi' \psi = [\varphi\psi]_0^1 - \int_0^1 \varphi \psi' = 0 + \frac{b}{a+1} \, I(a+1, b-1).$$

Puisque $I(c,0) = 1/(c+1)$, il vient aussitôt par récurrence :

$$I(a,b) = \int_0^1 x^a (1-x)^b \, \mathrm{d}x = \frac{a! \, b!}{(a+b+1)!}.$$

Module IV.6 : Introduction aux fonctions vectorielles d'une variable réelle

IV.6.1 1. Notons que :

$$\|A_n - A\| = \left\|\frac{1}{n}\mathrm{I}_m\right\| = \frac{1}{n}\|\mathrm{I}_m\| = \frac{1}{n}\sqrt{m} \underset{n\to+\infty}{\longrightarrow} 0.$$

Par conséquent, la suite A_n converge vers A quand n tend vers $+\infty$.

2. Remarquons que la matrice A_n n'est pas inversible si, et seulement si, $1/n$ est valeur propre de A. Or la matrice A n'a qu'un nombre fini de valeur propres. Par conséquent, si n est assez grand, $1/n$ n'est pas valeur propre de A et A_n est inversible.

3. Toute matrice A de $M_m(\mathbb{R})$ peut être approchée par des matrices de la forme $A - \frac{1}{n}\mathrm{I}_m$ qui sont inversibles si n est assez grand.

IV.6.2 Soient $\boldsymbol{v}_1$ et $\boldsymbol{v}_2$ deux vecteurs propres de A associés respectivement à λ_1 et λ_2. Alors, $(\boldsymbol{v}_1, \boldsymbol{v}_2)$ est une base de vecteurs propres de $\mathbb{R}^2$. On peut donc écrire :

$$\boldsymbol{u}_0 = x_1\boldsymbol{v}_1 + x_2\boldsymbol{v}_2$$

avec x_1 et x_2 les coordonnées de $\boldsymbol{u}_0$ dans cette base. On a alors :

$$\boldsymbol{u}_n = A^n\boldsymbol{u}_0 = x_1A^n\boldsymbol{v}_1 + x_2A^n\boldsymbol{v}_2 = \lambda_1^n x_1\boldsymbol{v}_1 + \lambda_2^n x_2\boldsymbol{v}_2.$$

Par conséquent :

$$\frac{1}{\lambda_1^n}\boldsymbol{u}_n = x_1\boldsymbol{v}_1 + \left(\frac{\lambda_2}{\lambda_1}\right)^n x_2\boldsymbol{v}_2.$$

Comme $0 < \lambda_2 < \lambda_1$, la suite $(\lambda_2/\lambda_1)^n$ tend vers 0 quand n tend vers $+\infty$. D'où :

$$\boldsymbol{u}_n \underset{n\to+\infty}{\longrightarrow} x_1\boldsymbol{v}_1.$$

IV.6.3 Les racines de l'équation caractéristique $r^2 - r - 2 = 0$ sont :

$$r_1 := -1 \quad \text{et} \quad r_2 := 2.$$

Par conséquent, il existe des constantes A et B telles que :

$$\boldsymbol{u}_n = A \cdot (-1)^n + B \cdot 2^n.$$

Comme $\boldsymbol{u}_0 = 2$ et $\boldsymbol{u}_1 = -1$, les constantes A et B sont solutions du système :

$$\begin{cases} A + B = 0 \\ -A + 2B = -1. \end{cases}$$

Les solutions sont $A = 1/3$ et $B = -1/3$. On a donc :

$$\boldsymbol{u}_n = \frac{(-1)^n - 2^n}{3}.$$

Or :

$$\frac{(-1)^n - 2^n}{3} = -\frac{2^n}{3} \cdot \left(1 - \left(-\frac{1}{2}\right)^n\right) \underset{n\to+\infty}{\longrightarrow} -\infty.$$

IV.6.4 Soit $t_0 \in [0,1]$. Alors, pour tout $t \in [0,1]$, on a :

$$\boldsymbol{f}(t) - \boldsymbol{f}(t_0) = (t - t_0)(A - \mathrm{I}_m).$$

Par conséquent :

$$\big\|\boldsymbol{f}(t) - \boldsymbol{f}(t_0)\big\| \leqslant |t - t_0|\big\|A - \mathrm{I}_m\big\| \underset{t\to t_0}{\longrightarrow} 0.$$

La fonction $\boldsymbol{f}$ est donc continue en t_0.

De plus, pour $t \in [0,1] \setminus \{t_0\}$:

$$\frac{\boldsymbol{f}(t) - \boldsymbol{f}(t_0)}{t - t_0} = A - \mathrm{I}_m$$

qui ne dépend pas de t (et tend donc vers $A - \mathrm{I}_m$ quand t tend vers t_0). Par conséquent, pour tout $t_0 \in [0,1]$:

$$\lim_{t\to t_0, t\neq t_0} \frac{\boldsymbol{f}(t) - \boldsymbol{f}(t_0)}{t - t_0} = A - \mathrm{I}_m.$$

La fonction $\boldsymbol{f}$ est donc dérivable sur $[0,1]$ et sa dérivée vérifie :

$$\boldsymbol{f}'(t) = A - \mathrm{I}_m.$$

IV.6.5 La fonction $\|\boldsymbol{f}\|$ est la composée de la fonction $\big(\boldsymbol{f} \;\big|\; \boldsymbol{f}\big)$ qui est dérivable en x_0 car $\boldsymbol{f}$ est dérivable en x_0, et de la fonction $t \mapsto \sqrt{t}$ qui est dérivable sur $]0,+\infty[$. Comme $\big(\boldsymbol{f} \;\big|\; \boldsymbol{f}\big)(x_0) > 0$, la composée des deux fonctions est dérivable et la dérivée vaut :

$$\|\boldsymbol{f}\|'(x_0) = \frac{1}{2\sqrt{\big(\boldsymbol{f}(x_0) \;\big|\; \boldsymbol{f}(x_0)\big)}} \cdot \big(\boldsymbol{f} \;\big|\; \boldsymbol{f}\big)'(x_0) = \frac{\big(\boldsymbol{f}(x_0) \;\big|\; \boldsymbol{f}'(x_0)\big)}{\|\boldsymbol{f}(x_0)\|}.$$

IV.6.6 Supposons d'abord que $(\boldsymbol{u}_n)$ et $(\boldsymbol{v}_n)$ sont deux suites de vecteurs de $\mathbb{R}^3$ telles que $\boldsymbol{u}_n \to \ell_1$ et $\boldsymbol{v}_n \to \ell_2$. On peut écrire :

$$\boldsymbol{u}_n \wedge \boldsymbol{v}_n - \ell_1 \wedge \ell_2 = (\boldsymbol{u}_n - \ell_1) \wedge (\boldsymbol{v}_n - \ell_2) + (\boldsymbol{u}_n - \ell_1) \wedge \ell_2 + \ell_1 \wedge (\boldsymbol{v}_n - \ell_2).$$

Rappelons que $\|u \wedge v\| \leqslant \|u\| \cdot \|v\|$. Par conséquent :

$$\big\|\boldsymbol{u}_n \wedge \boldsymbol{v}_n - \ell_1 \wedge \ell_2\big\| \underset{n\to+\infty}{\longrightarrow} 0 \quad \text{et} \quad \boldsymbol{u}_n \wedge \boldsymbol{v}_n \underset{n\to+\infty}{\longrightarrow} \ell_1 \wedge \ell_2.$$

Puisque $\boldsymbol{f}$ et $\boldsymbol{g}$ sont continues, si $x \to x_0$, $\boldsymbol{f}(x) \to \boldsymbol{f}(x_0)$ et $\boldsymbol{g}(x) \to \boldsymbol{g}(x_0)$. Par conséquent :

$$(\boldsymbol{f} \wedge \boldsymbol{g})(x) \to (\boldsymbol{f} \wedge \boldsymbol{g})(x_0)$$

ce qui montre que $\boldsymbol{f} \wedge \boldsymbol{g}$ est continue. De plus, on peut écrire :

$$\begin{aligned}(\boldsymbol{f} \wedge \boldsymbol{g})(x) - (\boldsymbol{f} \wedge \boldsymbol{g})(x_0) = {}& \big(\boldsymbol{f}(x) - \boldsymbol{f}(x_0)\big) \wedge \big(\boldsymbol{g}(x) - \boldsymbol{g}(x_0)\big) \\ &+ \boldsymbol{f}(x_0) \wedge \big(\boldsymbol{g}(x) - \boldsymbol{g}(x_0)\big) \\ &+ \big(\boldsymbol{f}(x) - \boldsymbol{f}(x_0)\big) \wedge g(x_0).\end{aligned}$$

Puisque $\boldsymbol{f}$ et $\boldsymbol{g}$ sont dérivables :

$$\lim_{x\to x_0} \frac{\boldsymbol{f}(x) - \boldsymbol{f}(x_0)}{x - x_0} = \boldsymbol{f}'(x_0) \quad \text{et} \quad \lim_{x\to x_0} \frac{\boldsymbol{g}(x) - \boldsymbol{g}(x_0)}{x - x_0} = \boldsymbol{g}'(x_0).$$

Par conséquent :

$$\lim_{x\to x_0}\frac{(\boldsymbol{f}\wedge\boldsymbol{g})(x)-(\boldsymbol{f}\wedge\boldsymbol{g})(x_0)}{x-x_0}=\boldsymbol{f}'(x_0)\wedge\vec{0}+\boldsymbol{f}(x_0)\wedge\boldsymbol{g}'(x_0)+\boldsymbol{f}'(x_0)\wedge\boldsymbol{g}(x_0)$$
$$=\boldsymbol{f}'(x_0)\wedge\boldsymbol{g}(x_0)+\boldsymbol{f}(x_0)\wedge\boldsymbol{g}'(x_0).$$

IV.6.7 Notons que :

$$h=f_1g_2-f_2g_1.$$

Comme les fonctions vectorielles $\boldsymbol{f}$ et $\boldsymbol{g}$ sont dérivables, les fonctions réelles f_1, f_2, g_1 et g_2 le sont. Par conséquent, h est dérivable et :

$$h'=f_1'g_2-f_2'g_1+f_1g_2'-f_2g_1'=\det\begin{pmatrix}f_1'&g_1\\f_2'&g_2\end{pmatrix}+\det\begin{pmatrix}f_1&g_1'\\f_2&g_2'\end{pmatrix}.$$

IV.6.8 1. Étant $x_0\in\mathbb{R}$ et $x\in\mathbb{R}$, on a :

$$\boldsymbol{F}(x)-\boldsymbol{F}(x_0)=\int_{x_0}^{x}\boldsymbol{f}(t)\,\mathrm{d}t.$$

Par conséquent :

$$\big\|\boldsymbol{F}(x)-\boldsymbol{F}(x_0)\big\|\leqslant\left|\int_{x_0}^{x}\big\|\boldsymbol{f}(t)\big\|\,\mathrm{d}t\right|.$$

Comme $\boldsymbol{f}$ est continue en x_0, si x est suffisamment proche de x_0, $|\boldsymbol{f}(x)-\boldsymbol{f}(x_0)|\leqslant 1$, et donc :

$$\boldsymbol{F}(x)-\boldsymbol{F}(x_0)=\big(\big|\boldsymbol{f}(x_0)\big|+1\big)\,|x-x_0|\underset{x\to x_0}{\longrightarrow}0.$$

La fonction $\boldsymbol{F}$ est donc continue en x_0.

2. Nous allons maintenant montrer que la fonction $\boldsymbol{F}$ est dérivable et que sa dérivée est $\boldsymbol{f}$. Pour cela, écrivons :

$$\frac{\boldsymbol{F}(x)-\boldsymbol{F}(x_0)}{x-x_0}-\boldsymbol{f}(x_0)=\frac{1}{x-x_0}\int_{x_0}^{x}\boldsymbol{f}(t)-\boldsymbol{f}(x_0)\,\mathrm{d}t.$$

Pour tout $\varepsilon>0$, il existe $\eta>0$ tel que $|t-x_0|\leqslant\eta$ implique $\big\|\boldsymbol{f}(t)-\boldsymbol{f}(x_0)\big\|\leqslant\varepsilon$. Si $|x-x_0|\leqslant\eta$, on a alors :

$$\left\|\frac{\boldsymbol{F}(x)-\boldsymbol{F}(x_0)}{x-x_0}-\boldsymbol{f}(x_0)\right\|\leqslant\left|\frac{1}{x-x_0}\int_{x_0}^{x}\big\|\boldsymbol{f}(t)-\boldsymbol{f}(x_0)\big\|\,\mathrm{d}t\right|\leqslant\varepsilon.$$

Par conséquent :

$$\lim_{x\to x_0}\frac{\boldsymbol{F}(x)-\boldsymbol{F}(x_0)}{x-x_0}=\boldsymbol{f}(x_0),$$

ce qui montre que $\boldsymbol{F}$ est dérivable de dérivée $\boldsymbol{f}$.

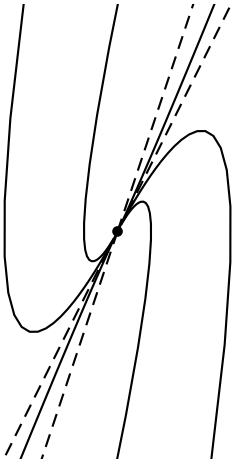
IV.6.9 Il s'agit d'une équation différentielle linéaire à coefficients constants. Les solutions maximales sont définies sur $\mathbb{R}$. Posons $\boldsymbol{A}:=\begin{pmatrix}0&1\\-6&5\end{pmatrix}$. Alors :

$$\boldsymbol{A}\cdot\begin{pmatrix}1\\2\end{pmatrix}=\begin{pmatrix}2\\4\end{pmatrix}=2\begin{pmatrix}1\\2\end{pmatrix}\quad\text{et}\quad\boldsymbol{A}\cdot\begin{pmatrix}1\\3\end{pmatrix}=\begin{pmatrix}3\\9\end{pmatrix}=3\begin{pmatrix}1\\3\end{pmatrix}.$$

Si l'on définit $\boldsymbol{v} := (1,2)$ et $\boldsymbol{w} := (1,3)$, alors $(\boldsymbol{v},\boldsymbol{w})$ est une base de vecteurs propres de $\mathbb{R}^2$. Les solutions de l'équation différentielle $\boldsymbol{y}' = \boldsymbol{A}\cdot\boldsymbol{y}$ sont de la forme :

$$\boldsymbol{f} : t \mapsto C_1 e^{2t}\begin{pmatrix}1\\2\end{pmatrix} + C_2 e^{3t}\begin{pmatrix}1\\3\end{pmatrix}.$$

L'allure de ces solutions est représentée sur la figure suivante. Il y a quatre solutions particulières pour lesquelles les trajectoires sont des demi-droites. Elles sont représentées en pointillés.



IV.6.10 Il s'agit d'une équation différentielle linéaire à coefficients constants. Les solutions maximales sont définies sur $\mathbb{R}$. Posons $\boldsymbol{A} := \begin{pmatrix}0 & 1\\ -4 & 4\end{pmatrix}$. Alors :

$$\boldsymbol{A}\cdot\begin{pmatrix}1\\2\end{pmatrix} = 2\begin{pmatrix}1\\2\end{pmatrix} \quad \text{et} \quad \boldsymbol{A}\cdot\begin{pmatrix}1\\4\end{pmatrix} = 2\left(\begin{pmatrix}1\\2\end{pmatrix} + \begin{pmatrix}1\\4\end{pmatrix}\right).$$

Définissons $\boldsymbol{v} := (1,2)$ et $\boldsymbol{w} := (1,4)$. Si $\boldsymbol{y} = f_1\boldsymbol{v} + f_2\boldsymbol{w}$ est solution de l'équation différentielle $\boldsymbol{y}' = \boldsymbol{A}\cdot\boldsymbol{y}$, alors :

$$\begin{pmatrix}f_1'\\f_2'\end{pmatrix} = 2\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}\cdot\begin{pmatrix}f_1\\f_2\end{pmatrix}.$$

Posons :

$$\boldsymbol{B} := 2\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}.$$

Nous avons vu dans le cours que :

$$e^{t\boldsymbol{B}} = e^{2t}\begin{pmatrix}1 & 2t\\0 & 1\end{pmatrix}.$$

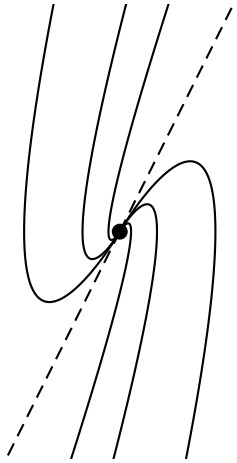
Par conséquent :

$$\begin{pmatrix}f_1(t)\\f_2(t)\end{pmatrix} = e^{2t}\begin{pmatrix}1 & 2t\\0 & 1\end{pmatrix}\begin{pmatrix}C_1\\C_2\end{pmatrix} \quad \text{avec} \quad C_1 := f_1(0) \quad \text{et} \quad C_2 := f_2(0).$$

Les solutions de l'équation différentielle $\boldsymbol{y}' = \boldsymbol{A} \cdot \boldsymbol{y}$ sont de la forme :

$$\boldsymbol{f} : t \mapsto (C_1 + 2tC_2)e^{2t} \begin{pmatrix} 1 \\ 2 \end{pmatrix} + C_2 e^{2t} \begin{pmatrix} 1 \\ 4 \end{pmatrix}.$$

L'allure de ces solutions est représentée sur la figure suivante. Il y a deux solutions particulières pour lesquelles les trajectoires sont des demi-droites. Elles sont représentées en pointillés.



IV.6.11 Il s'agit d'une équation différentielle linéaire à coefficients constants. Les solutions maximales sont définies sur $\mathbb{R}$.

On peut observer que si $\boldsymbol{f} = (f_1, f_2)$ est solution de l'équation différentielle, alors :

$$(f_1', f_2') = a(-f_2, f_1)$$

et donc :

$$(\boldsymbol{f}' \mid \boldsymbol{f}) = a(-f_2)f_1 + af_1f_2 = 0.$$

La fonction $\|\boldsymbol{f}\|^2 = (\boldsymbol{f}' \mid \boldsymbol{f})$ est dérivable comme produit scalaire de deux fonctions dérivables et :

$$\big(\|\boldsymbol{f}\|^2\big)' = 2(\boldsymbol{f}' \mid \boldsymbol{f}).$$

Par conséquent, la fonction $\|\boldsymbol{f}\|^2$ est une fonction constante et la fonction $\boldsymbol{f}$ prend ses valeurs dans un cercle centré à l'origine.

Il est possible d'être plus précis. En effet, $f_1'' = -af_2' = -a^2 f_1$, et donc :

$$f_1(t) = R\cos(at + \varphi) \quad \text{et} \quad f_2(t) = R\sin(at + \varphi)$$

avec R le rayon du cercle et $\varphi \in \mathbb{R}$.

IV.6.12 1. Les racines de l'équation caractéristique $r^2 - 2r - 3 = 0$ sont 3 et -1. Les solutions de l'équation homogène sont donc de la forme :

$$C_1 e^{3t} + C_2 e^{-t} \quad \text{avec} \quad C_1, C_2 \in \mathbb{R}.$$

Utilisons la méthode de variation de la constante, c'est-à-dire, cherchons une solution sous la forme :

$$\boldsymbol{f} = \lambda_1 e^{3t} + \lambda_2 e^{-t} \quad \text{avec} \quad \lambda_1' e^{3t} + \lambda_2' e^{-t} = 0.$$

On a alors :

$$\boldsymbol{f}' = 3\lambda_1 e^{3t} - \lambda_2 e^{-t} \quad \text{et} \quad \boldsymbol{f}'' = 3\lambda_1' e^{3t} - \lambda_2' e^{-t} + 9\lambda_1 e^{3t} + \lambda_2 e^{-t}.$$

En reportant dans l'équation différentielle, on trouve :

$$3\lambda_1' e^{3t} - \lambda_2' e^{-t} = \frac{e^{3t}}{\cosh^2 t}.$$

Il nous faut donc résoudre le système :

$$\begin{cases} \lambda_1' e^{3t} + \lambda_2' e^{-t} = 0 \\ 3\lambda_1' e^{3t} - \lambda_2' e^{-t} = \dfrac{e^{3t}}{\cosh^2 t}. \end{cases}$$

Les solutions sont :

$$\lambda_1' = \frac{1}{4\cosh^2 t} \quad \text{et} \quad \lambda_2' = -\frac{e^{4t}}{4\cosh^2 t}.$$

Une solution particulière de l'équation avec second membre est donnée par :

$$\lambda_1 = \frac{\tanh t}{4} \quad \text{et} \quad \lambda_2 = -\int \frac{e^{4t}}{e^{2t} + 2 + e^{-2t}}\,\mathrm{d}t.$$

Le changement de variable $u = e^{2t}$ pour le calcul de la primitive donnant λ_2 conduit à :

$$\begin{aligned} \int \frac{e^{4t}}{e^{2t} + 2 + e^{-2t}}\,\mathrm{d}t &= \frac{1}{2}\int \frac{u^2}{(u+1)^2}\,\mathrm{d}u \\ &= \frac{1}{2}\int 1 - \frac{2(u+1)}{(u+1)^2} + \frac{1}{(u+1)^2}\,\mathrm{d}u \\ &= \frac{u}{2} - \frac{1}{2}\ln\big((u+1)^2\big) - \frac{1}{2(u+1)} \\ &= \frac{e^{2t}}{2} - \ln(e^{2t}+1) - \frac{1}{2e^{2t}+2}. \end{aligned}$$

En regroupant les termes, on trouve que les solutions sont les fonctions de la forme :

$$\frac{1}{4}\frac{e^{5t} - 3e^{3t} - 2e^t + 2e^{-t}}{e^{2t}+1} + e^{-t}\ln(e^{2t}+1) + C_1 e^{3t} + C_2 e^{-t} \quad \text{avec} \quad C_1, C_2 \in \mathbb{R}.$$

2. L'équation caractéristique $r^2 - 2r + 1 = 0$ a une racine double : 1. Les solutions de l'équation homogène sont donc de la forme :

$$(C_1 t + C_2)e^t \quad \text{avec} \quad C_1, C_2 \in \mathbb{R}.$$

Le second membre est de la forme $P(t)e^{rt}$ avec P un polynôme et r une racine double de l'équation caractéristique. On peut chercher une solution particulière sous la forme $\boldsymbol{f}(t) = at^3 e^t$ avec $a \in \mathbb{R}$. On trouve :

$$\boldsymbol{f}''(t) - 2\boldsymbol{f}'(t) + \boldsymbol{f}(t) = \big((at^3 + 6at^2 + 6at) - 2(at^3 + 3at^2) + at^3\big)e^t = 6ate^t.$$

Par conséquent, les solutions de l'équation avec second membre sont les fonctions de la forme :

$$\frac{t^3}{6}e^t + (C_1 t + C_2)e^t \quad \text{avec} \quad C_1, C_2 \in \mathbb{R}.$$

3. Les racines de l'équation caractéristique $r^2 - 4r + 3 = 0$ sont 1 et -3. Les solutions de l'équation homogène sont donc de la forme :

$$C_1 e^t + C_2 e^{-3t} \quad \text{avec} \quad C_1, C_2 \in \mathbb{R}.$$

On va rechercher une solution particulière de l'équation avec second membre comme somme d'une solution particulière de $y'' - 4y' + 3y = 3t$ et d'une solution particulière de $y'' - 4y' + 3y = e^t$. Dans le premier cas, on peut chercher une solution sous la forme $f_1(t) = at + b$ et on trouve $f_1(t) = t + 4/3$. Dans le second cas, on peut chercher une solution sous la forme $f_2(t) = ate^t$ et on trouve $f_2(t) = -te^t/2$. Les solutions de l'équation avec second membre sont les fonctions de la forme :

$$t + \frac{4}{3} - \frac{t}{2}e^t + C_1 e^t + C_2 e^{-3t} \quad \text{avec} \quad C_1, C_2 \in \mathbb{R}.$$

4. Les racines de l'équation caractéristique $r^2 + 4 = 0$ sont $\pm 2i$. Les solutions de l'équation homogène sont donc de la forme :

$$C_1 \cos(2t) + C_2 \sin(2t) \quad \text{avec} \quad C_1, C_2 \in \mathbb{R}.$$

On peut chercher une solution particulière en utilisant les solutions complexes. Nous proposons d'utiliser la méthode de variation de la constante, c'est-à-dire, de chercher une solution sous la forme :

$$\boldsymbol{f} = \lambda_1 \cos(2t) + \lambda_2 \sin(2t) \quad \text{avec} \quad \lambda_1' \cos(2t) + \lambda_2' \sin(2t) = 0.$$

On a alors :

$$\boldsymbol{f}' = -2\lambda_1 \sin(2t) + 2\lambda_2 \cos(2t)$$

et

$$\boldsymbol{f}'' = -2\lambda_1' \sin(2t) + 2\lambda_2' \cos(2t) + -4\lambda_1 \cos(2t) - 4\lambda_2 \sin(2t).$$

En reportant dans l'équation différentielle, on trouve :

$$-2\lambda_1' \sin(2t) + 2\lambda_2' \cos(2t) = t \sin^2(t).$$

Il nous faut donc résoudre le système :

$$\begin{cases} \lambda_1' \cos(2t) + \lambda_2' \sin(2t) = 0 \\ -2\lambda_1' \sin(2t) + 2\lambda_2' \cos(2t) = t \sin^2(t). \end{cases}$$

Les solutions sont :

$$\lambda_1' = -\frac{1}{2} t \sin^2(t) \sin(2t) \quad \text{et} \quad \lambda_2' = \frac{1}{2} t \sin^2(t) \cos(2t).$$

De manière équivalente, on a :

$$\lambda_1' = -\frac{1}{4} t \sin(2t) + \frac{1}{8} t \sin(4t) \quad \text{et} \quad \lambda_2' = -\frac{t}{8} + \frac{1}{4} t \cos(2t) - \frac{1}{8} t \cos(4t).$$

Une intégration par parties (en dérivant t et en primitivant les sinus et les cosinus) montre que l'on peut choisir :

$$\lambda_1(t) = -\frac{1}{32} t \cos(4t) + \frac{1}{8} t \cos(2t) + \frac{1}{128} \sin(4t) - \frac{1}{16} \sin(2t) \quad \text{et}$$

$$\lambda_2(t) = -\frac{1}{16} t^2 + \frac{1}{8} t \sin(2t) - \frac{1}{32} t \sin(4t) + \frac{1}{16} \cos(2t) - \frac{1}{128} \cos(4t).$$

Les solutions sont alors les fonctions de la forme :

$$\big(\lambda_1(t) + C_1\big) \cos(2t) + \big(\lambda_2(t) + C_2\big) \sin(2t) \quad \text{avec} \quad C_1, C_2 \in \mathbb{R}.$$

Module IV.7 : Première initiation aux fonctions de plusieurs variables

IV.7.1 1. L'intervalle $[0,1[$ n'est pas ouvert dans $\mathbb{R}$. En effet, le point 0 appartient à cet intervalle, mais pour tout $r>0$, la boule $B(0,r)$ contient des réels négatifs qui ne sont pas dans l'intervalle (par exemple $-r/2$). On ne peut donc pas trouver de $r>0$ tel que $B(0,r)\subset[0,1[$.

L'intervalle $[0,1[$ n'est pas fermé dans $\mathbb{R}$ (et n'est donc pas compact). Il faut montrer que son complémentaire $]-\infty,0[\cup[1,+\infty[$ n'est pas ouvert. Le point 1 appartient à ce complémentaire mais pour tout $r>0$, la boule $B(1,r)$ contient des réels plus grand que 1 (par exemple $1+r/2$). Par conséquent, on ne peut pas trouver de $r>0$ tel que $B(1,r)\subset\mathbb{R}\setminus[0,1[$.

2. L'intervalle $]0,1[$ n'est pas ouvert dans $\mathbb{C}$. Par exemple, le point $1/2$ appartient à cet intervalle, mais on ne pas trouver de $r>0$ tel que $B(1/2,r)\subset]0,1[$ (attention, il s'agit de la boule complexe). Par exemple, une telle boule contient le point $1/2+ir/2$.

   L'intervalle $]0,1[$ n'est pas fermé dans $\mathbb{C}$ (et n'est donc pas compact). En effet, son complémentaire n'est pas ouvert dans $\mathbb{C}$: il contient le point 0 et pour tout $r>0$, la boule $B(0,r)$ contient le point $r/2\in]0,1[$.

3. Le segment $[0,1]$ n'est pas ouvert dans $\mathbb{C}$ pour la même raison que précédemment : le point $1/2$ appartient à ce segment mais pour tout $r>0$, la boule $B(1/2,r)$ contient $1/2+ir/2$ qui n'appartient pas au segment.

   Le segment $[0,1]$ est fermé dans $\mathbb{C}$. En effet, si $z\in\mathbb{C}\setminus[0,1]$ alors :
   - soit $\mathrm{Im}(z)\neq 0$ et si l'on choisit, par exemple, $r=\big|\mathrm{Im}(z)\big|$, la boule $B(z,r)$ n'intersecte pas l'axe réel. En particulier, elle est contenue dans $\mathbb{C}\setminus[0,1]$.
   - soit $z\in]1,+\infty[$ et si l'on choisit, par exemple $r=z-1$, la boule $B(z,r)$ est contenue dans $\mathbb{C}\setminus[0,1]$.
   - soit $z\in]-\infty,0[$ et si l'on choisit, par exemple $r=|z|>0$, la boule $B(z,r)$ est contenue dans $\mathbb{C}\setminus[0,1]$.

   Le segment $[0,1]$ est fermé et borné dans $\mathbb{C}$. Il est donc compact.

4. Le demi-plan $H:=\big\{(x,y)\in\mathbb{R}^2\;\big|\;x>y\big\}$ est ouvert dans $\mathbb{R}^2$. Soit $M=(x,y)$ un point de H. Alors $x>y$ et $r:=(x-y)/2>0$. Nous allons montrer que la boule $B(M,r)$ est contenue dans H. Soit $(x',y')\in B(M,r)$. Alors, $|x'-x|<r$ et $|y'-y|<r$. Par conséquent :

$$x'>x-r=\frac{x+y}{2}=y+r>y'.$$

   On a bien $x'>y'$ et donc $(x',y')\in H$.

   Le demi-plan H n'est pas fermé dans $\mathbb{R}^2$ (et n'est donc pas compact). Par exemple, le point $O=(0,0)$ appartient au complémentaire de H mais pour tout $r>0$, la boule $B(O,r)$ contient le point $(r/2,0)$ qui appartient à H.

5. Le demi-plan $H':=\big\{(x,y)\in\mathbb{R}^2\;\big|\;x\geqslant y\big\}$ n'est pas ouvert dans $\mathbb{R}^2$. Par exemple, il contient le point $O=(0,0)$ mais pour tout $r>0$, la boule $B(O,r)$ contient le point $(-r/2,0)$ qui n'appartient à H'.

Le demi-plan H' est fermé dans $\mathbb{R}^2$ puisque $\big\{(x,y) \in \mathbb{R}^2 \;\big|\; x < y\big\}$, son complémentaire, est ouvert dans $\mathbb{R}^2$. En effet, comme précédemment, pour tout $M = (x,y) \in \mathbb{R}^2 \setminus H'$, on a $x < y$ et si l'on choisit $r := (y-x)/2$, la boule $B(M,r)$ est contenue dans $\mathbb{R}^2 \setminus H'$.

Le demi-plan H' n'est pas compact car il n'est pas borné. En effet, pour tout $R > 0$, le point $M = (2R, 0)$ appartient à H' et $\|M\| = 2R > R$.

IV.7.2 1. Remarquons que la fonction f n'est définie que si $x + y > 0$, c'est-à-dire dans le demi-plan ouvert $\big\{(x,y) \in \mathbb{R}^2 \;\big|\; y > -x\big\}$. Quand $(x,y) \to (0,0)$, $x + y \to 0$, donc $\ln(x+y) \to -\infty$. De plus, $\sqrt{x^2+y^2} \to 0$. Par conséquent :

$$\lim_{(x,y)\to(0,0)} f(x,y) = -\infty.$$

La fonction f n'admet pas de limite finie quand $(x,y) \to (0,0)$.

2. Notons que la fonction g est définie dans $\mathbb{R}^2 \setminus \{(0,0)\}$. Quand $(x,y) \to (0,0)$:

$$|x| + |y| \to 0 \quad \text{et} \quad \ln(x^2+y^4) \to -\infty.$$

Nous somme donc en présence d'une forme indéterminée. Cependant, nous pouvons observer que si $|y| < 1$, on a $y^4 < y^2$ et donc :

$$\ln(x^2+y^4) \leqslant \ln(x^2+y^2) = 2\ln\big\|(x,y)\big\|.$$

De plus :

$$|x| + |y| \leqslant 2\big\|(x,y)\big\|.$$

Par conséquent :

$$\big\|g(x,y)\big\| \leqslant 4\big\|(x,y)\big\| \cdot \ln\big\|(x,y)\big\| \underset{\|(x,y)\|\to 0}{\longrightarrow} 0.$$

D'où :

$$\lim_{(x,y)\to(0,0)} g(x,y) = 0.$$

3. La fonction h est définie dans $\mathbb{R}^2 \setminus \{(0,0)\}$. Quand $(x,y) \to (0,0)$, $x^2 - y^2 \to 0$ et $x^2 + y^2 \to 0$. Nous sommes donc en présence d'une forme indéterminée. Notons que

$$h(x,0) = 1 \quad \text{et} \quad h(0,y) = -1.$$

Comme :

$$\lim_{x\to 0} h(x,0) = 1 \neq -1 = \lim_{y\to 0} h(0,y)$$

nous pouvons dire que la fonction h n'admet pas de limite quand (x,y) tend vers $(0,0)$.

IV.7.3 La fonction f est continue comme produit et composée de fonctions continues sur $\mathbb{R}^2$. Cependant :

$$f(0,y) = -y^3 e^{y^3} \underset{y\to+\infty}{\longrightarrow} -\infty.$$

La fonction f ne tend donc pas vers 0 quand $\big\|(x,y)\big\| \to +\infty$. Elle n'est pas non plus bornée.

Nous proposons d'étudier à la place la fonction $f : \mathbb{R}^2 \to \mathbb{R}$ définie par :

$$f(x,y) := (x^2 - y^3)e^{-(x^2+y^2)}.$$

Cette fonction est continue comme produit et composée de fonctions continues sur $\mathbb{R}^2$. De plus, dès que $\big\|(x,y)\big\| \geqslant 1$, on a $x^2 \leqslant \big\|(x,y)\big\|^2 \leqslant \big\|(x,y)\big\|^3$ et $|y^3| \leqslant \big\|(x,y)\big\|^3$. On peut alors écrire :

$$\big|f(x,y)\big| \leqslant 2\big\|(x,y)\big\|^3 e^{-\big\|(x,y)\big\|^2} \underset{\big\|(x,y)\big\|\to+\infty}{\longrightarrow} 0$$

(c'est l'exponentielle qui l'emporte).

Comme $f(x,y) \to 0$ quand $\big\|(x,y)\big\| \to +\infty$, il existe $R > 0$ tel que si $\big\|(x,y)\big\| > R$, alors $\big|f(x,y)\big| < e^{-1}$. Notons que $f(1,0) = e^{-1} > 0$ et $f(0,1) = -e^{-1} < 0$. En particulier $R \geqslant 1$. La fonction f est continue sur le disque fermé de centre $(0,0)$ et de rayon R, qui est compact. Elle y est donc bornée et y atteint ses bornes. On peut donc trouver (x_0,y_0) et (x_1,y_1) tels que pour tout $(x,y) \in \mathbb{R}^2$ avec $\big\|(x,y)\big\| \leqslant R$, on a :

$$f(x_0,y_0) \leqslant f(x,y) \leqslant f(x_1,y_1).$$

Ceci est vrai en particulier pour $(x,y) = (1,0)$ et $(x,y) = (0,1)$. On a donc :

$$f(x_0,y_0) \leqslant -e^{-1} \leqslant e^{-1} \leqslant f(x_1,y_1).$$

Par conséquent, pour tout $(x,y) \in \mathbb{R}^2$ avec $\big\|(x,y)\big\| > R$, on a également :

$$f(x_0,y_0) \leqslant f(x,y) \leqslant f(x_1,y_1).$$

Cet encadrement est donc vrai pour tout $(x,y) \in \mathbb{R}^2$, ce qui montre que f est bornée et atteint ses bornes dans $\mathbb{R}^2$.

IV.7.4 1. La fonction f est définie, continue, différentiable sur $\mathbb{R}^2$ comme somme produit et composée de fonctions différentiables sur $\mathbb{R}^2$. De plus :

$$\frac{\partial f}{\partial x}(x,y) = e^x \sin(x^2+y) + 2xe^x \cos(x^2+y)$$

et

$$\frac{\partial f}{\partial y}(x,y) = e^x \cos(x^2+y).$$

2. La fonction g est définie, continue et différentiable sur l'ouvert :

$$\big\{(x,y) \in \mathbb{R}^2 \;\big|\; x + y^2 > 0\big\}$$

(c'est la région située à droite de la parabole d'équation $x = y^2$). On a :

$$\frac{\partial g}{\partial x}(x,y) = \frac{y^2}{\sqrt{x+y^2}} - \frac{xy^2}{2(x+y^2)^{3/2}}$$

et

$$\frac{\partial g}{\partial y}(x,y) = \frac{2xy}{\sqrt{x+y^2}} - \frac{xy^3}{(x+y^2)^{3/2}}.$$

3. La fonction h est définie, continue et différentiable sur $\mathbb{R}^2$. On a :

$$\frac{\partial h}{\partial x}(x,y) = 2x\cos(x^2-y) + 2y\sin(xy)\cos(xy)$$

et

$$\frac{\partial h}{\partial y}(x,y) = -\cos(x^2-y) + 2x\sin(xy)\cos(xy).$$

IV.7.5 La fonction $\boldsymbol{f}$ est définie sur $\mathbb{R}^2 \setminus \{(0,0)\}$. Elle y est différentiable car chacune de ses coordonnées est la somme, le produit où la composée de fonctions différentiables sur $\mathbb{R}^2 \setminus \{(0,0)\}$. De plus, on a :

$$\frac{\partial \boldsymbol{f}}{\partial x}(x,y) = \begin{pmatrix} 2xy \\ e^x \sin(y) \\ \dfrac{2x}{x^2+y^2} \end{pmatrix} \quad \text{et} \quad \frac{\partial \boldsymbol{f}}{\partial y}(x,y) = \begin{pmatrix} x^2 \\ e^x \cos(y) \\ \dfrac{2y}{x^2+y^2} \end{pmatrix}.$$

IV.7.6 La fonction $\boldsymbol{f}$ est continue et différentiable sur $\mathbb{R}^2$ comme produit de deux fonctions différentiables sur $\mathbb{R}^2$: la fonction $\boldsymbol{x} \mapsto (\,\boldsymbol{x} \mid \boldsymbol{x}\,)$ et la fonction identité. La différentielle de $\boldsymbol{f}$ est donnée par :

$$D_{\boldsymbol{x}}\boldsymbol{f}(\boldsymbol{h}) = (\,\boldsymbol{x} \mid \boldsymbol{x}\,) \cdot \boldsymbol{h} + 2(\,\boldsymbol{x} \mid \boldsymbol{h}\,) \cdot \boldsymbol{x}.$$

IV.7.7

1. La fonction f est définie sur $\mathbb{R}^2 \setminus \{(0,0)\}$. Elle y est différentiable. En effet, c'est la composée de la fonction $(x,y) \mapsto \left\|(x,y)\right\|^2 = x^2+y^2$ qui est différentiable sur $\mathbb{R}^2$ et de la fonction $t \mapsto \dfrac{1}{2}\ln(t^2)$ qui est dérivable sur $]0,+\infty[$. Notons que les dérivées partielles :
$$\frac{\partial f}{\partial x}(x,y) = \frac{x}{x^2+y^2} \quad \text{et} \quad \frac{\partial f}{\partial y}(x,y) = \frac{y}{x^2+y^2}$$
sont continues sur $\mathbb{R}^2 \setminus \{(0,0)\}$. La fonction f y est donc continûment différentiable et :
$$D_{(x,y)}f(h_1,h_2) = \frac{xh_1+yh_2}{x^2+y^2}.$$
2. La fonction g est continue sur $\mathbb{R}^2$ comme composée de fonctions continues. La fonction g est différentiable en dehors de la droite d'équation $x+y=0$. Elle n'est différentiable en aucun point de cette droite. En effet, si $(x_0,-x_0)$ est un point de cette droite, alors :
$$t \mapsto g(x_0+t,-x_0+t) = |2t|$$
n'est pas dérivable en $t=0$. En d'autre termes, la fonction g n'est dérivable dans la direction du vecteur $(1,1)$ en aucun point de la droite d'équation $x+y=0$.

IV.7.8 L'application f est continue, différentiable et même continûment différentiable sur $\mathbb{R}^2$. La matrice jacobienne de f est la matrice dont les colonnes sont les dérivées partielles de f par rapport à x et à y :

$$J_{(x,y)}\boldsymbol{f} = \begin{pmatrix} 2x+3y^2 & 6xy \\ ye^x & e^x \end{pmatrix}.$$

IV.7.9 L'application $\boldsymbol{f}$ est continue et différentiable sur $\mathbb{R}^2$. Les dérivées partielles :

$$\frac{\partial \boldsymbol{f}}{\partial x}(x,y) = \begin{pmatrix} -y\sin(xy) \\ \cos(x+y) \end{pmatrix} \quad \text{et} \quad \frac{\partial \boldsymbol{f}}{\partial y}(x,y) = \begin{pmatrix} -x\sin(xy) \\ \cos(x+y) \end{pmatrix}$$

sont continues sur $\mathbb{R}^2$. L'application $\boldsymbol{f}$ est donc continûment différentiable sur $\mathbb{R}^2$ et sa différentielle est donnée par :

$$D_{(x,y)}\boldsymbol{f}(h_1,h_2)=\begin{pmatrix} -y\sin(xy) & -x\sin(xy)\\ \cos(x+y) & \cos(x+y)\end{pmatrix}\cdot\begin{pmatrix} h_1\\ h_2\end{pmatrix}=\begin{pmatrix} -(yh_1+xh_2)\sin(xy)\\ (h_1+h_2)\cos(x+y)\end{pmatrix}.$$

IV.7.10 La fonction f est continue et continûment différentiable sur $\mathbb{R}^2\setminus\{(0,0)\}$ comme somme et produit de fonctions continûment différentiables. Nous allons étudier la continuité et la différentiabilité en $(0,0)$.

Notons que si $y=0$, on a $f(x,y)=0$. De plus, si $y\neq 0$, $x^2+y^2\geqslant y^2$ et :

$$\big|f(x,y)\big|\leqslant\left|\frac{xy^3}{y^2}\right|=|xy|.$$

Dans les deux cas, on a :

$$\big|f(x,y)\big|\leqslant|xy|\underset{(x,y)\to(0,0)}{\longrightarrow}0=f(0,0).$$

Donc f est continue en $(0,0)$.

Cette majoration montre également que lorsque $\boldsymbol{h}\to(0,0)$, $f(\boldsymbol{h})=\mathrm{o}\big(\|\boldsymbol{h}\|\big)$. Donc f est différentiable en $(0,0)$ et la différentielle est l'application nulle.

Pour déterminer si $\boldsymbol{f}$ est continûment différentiable, nous devons déterminer si les dérivées partielles de f sont des fonctions continues. Comme la différentielle de f en $(0,0)$ est l'application nulle, on a :

$$\frac{\partial f}{\partial x}(0,0)=0\quad\text{et}\quad\frac{\partial f}{\partial y}(0,0)=0.$$

De plus, pour $(x,y)\in\mathbb{R}^2\setminus\{(0,0)\}$, on a :

$$\frac{\partial f}{\partial x}(x,y)=\frac{y^3}{x^4+y^2}-\frac{4x^4y^3}{(x^4+y^2)^2}=\frac{y^3(y^2-3x^4)}{(x^4+y^2)^2}$$

et

$$\frac{\partial f}{\partial y}(x,y)=\frac{3y^2x}{x^4+y^2}-\frac{2xy^4}{(x^4+y^2)^2}=\frac{y^2x(3x^4+y^2)}{(x^4+y^2)^2}.$$

Si $|y|\leqslant x^2$ avec $x>0$, on utilise $x^4+y^2\geqslant x^4$ et l'on obtient :

$$\left|\frac{\partial f}{\partial x}(x,y)\right|\leqslant 4x^2\underset{(x,y)\to(0,0)}{\longrightarrow}0\quad\text{et}\quad\left|\frac{\partial f}{\partial y}(x,y)\right|\leqslant 4x\underset{(x,y)\to(0,0)}{\longrightarrow}0.$$

Si $x^2\leqslant|y|$ avec $y\neq 0$, on utilise $x^4+y^2\geqslant y^2$ et l'on obtient :

$$\left|\frac{\partial f}{\partial x}(x,y)\right|\leqslant 4y\underset{(x,y)\to(0,0)}{\longrightarrow}0\quad\text{et}\quad\left|\frac{\partial f}{\partial y}(x,y)\right|\leqslant 4\sqrt{|y|}\underset{(x,y)\to(0,0)}{\longrightarrow}0.$$

Par conséquent, les dérivées partielles de f sont continues sur $\mathbb{R}^2$ et f est continûment différentiable.

IV.7.11 Il s'agit d'une application de l'inégalité des accroissements finis. Remarquons d'abord que $\boldsymbol{f}$ est continûment différentiable est que la différentielle est identiquement nulle. Pour tout $\boldsymbol{c}\in\mathbb{R}^n$, on a donc :

$$\big\|D_{\boldsymbol{c}}\boldsymbol{f}\big\|=0.$$

Soient $\boldsymbol{a}$ et $\boldsymbol{b}$ deux points de $\mathbb{R}^n$. Alors :

$$\big\|\boldsymbol{f}(\boldsymbol{b}) - \boldsymbol{f}(\boldsymbol{a})\big\| \leqslant \sup_{\boldsymbol{c}\in[\boldsymbol{a},\boldsymbol{b}]} \big\|D_{\boldsymbol{c}}\boldsymbol{f}\big\| \cdot \|\boldsymbol{b} - \boldsymbol{a}\| = 0.$$

Par conséquent, pour tous points $\boldsymbol{a}$ et $\boldsymbol{b}$ de $\mathbb{R}^n$, on a $\boldsymbol{f}(\boldsymbol{b}) = \boldsymbol{f}(\boldsymbol{a})$. L'application $\boldsymbol{f}$ est donc constante.

IV.7.12 Il s'agit d'étudier la fonction f définie par :

$$f(x,y) = \arctan(x) + \arctan(y) - \arctan\frac{x+y}{1-xy}.$$

La fonction f est définie, continue et différentiable en dehors de l'hyperbole d'équation $xy = 1$ comme somme, produit et composée de fonction différentiables. De plus :

$$\begin{aligned}\frac{\partial f}{\partial x}(x,y) &= \frac{1}{1+x^2} - \frac{1}{1+(x+y)^2/(1-xy)^2} \cdot \frac{1-xy+y(x+y)}{(1-xy)^2}\\ &= \frac{1}{1+x^2} - \frac{(1-xy)^2}{1-2xy+x^2y^2+x^2+2xy+y^2} \cdot \frac{1+y^2}{(1-xy)^2}\\ &= 0\end{aligned}$$

et

$$\frac{\partial f}{\partial y}(x,y) = 0$$

en échangeant le rôle de x et de y. En reprenant les arguments de l'exercice précédent, on voit que f est constante sur chacune des trois régions délimitées par l'hyperbole d'équation $xy = 1$.

Dans la région centrale, f est constante égale à $f(0,0) = 0$. Dans la région où $y > 1/x > 0$, la fonction est constante égale à :

$$f(\sqrt{3},\sqrt{3}) = \frac{\pi}{3} + \frac{\pi}{3} - \Big(-\frac{\pi}{3}\Big) = \pi.$$

Dans la région où $y < 1/x < 0$, la fonction est constante égale à :

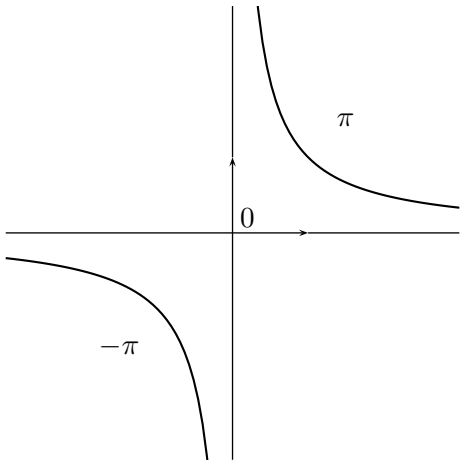
$$f(-\sqrt{3},-\sqrt{3}) = -\frac{\pi}{3} + -\frac{\pi}{3} - \frac{\pi}{3} = -\pi.$$

IV.7.13 Il nous faut supposer que $f : \mathbb{R}^2 \to \mathbb{R}$ est une application différentiable, sinon, on ne peut pas parler de la différentielle de f en $\boldsymbol{x}$. Même dans le cas où f n'est pas différentiable, on peut écrire le développement suivant lorsque $t \in \mathbb{R}$ tend vers 0 :

$$f(\boldsymbol{x}+t\boldsymbol{x}) = f\big((1+t)\boldsymbol{x}\big) = (1+t)^k f(\boldsymbol{x}) = f(\boldsymbol{x}) + ktf(\boldsymbol{x}) + t\varepsilon(t) \quad \text{avec} \quad \varepsilon(t) \underset{t\to 0}{\longrightarrow} 0.$$

Cela montre que pour tout $\boldsymbol{x} \in \mathbb{R}^2 \setminus \{(0,0)\}$, l'application f admet une dérivée suivant le vecteur $\boldsymbol{x}$ égale à $kf(\boldsymbol{x})$. Si f est différentiable en $\boldsymbol{x}$, cela s'écrit :

$$D_{\boldsymbol{x}} f(\boldsymbol{x}) = kf(\boldsymbol{x}).$$



IV.7.14 1. En identifiant $M_2(\mathbb{R})$ à $\mathbb{R}^4$, on peut écrire :

$$\frac{\partial f}{\partial a}\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = d, \qquad \frac{\partial f}{\partial b}\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = -c,$$

$$\frac{\partial f}{\partial c}\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = -b \quad \text{et} \quad \frac{\partial f}{\partial d}\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = a.$$

2. Les dérivées partielles de f existent et sont continues sur $\mathbb{R}^4$. La fonction f est donc continûment différentiable.

3. La matrice de l'application différentielle de f en I_2 est la matrice jacobienne de f :

$$J_{\mathrm{I}_2} f = \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}.$$

On voit donc que :

$$D_{\mathrm{I}_2} f \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = a + d.$$

Par conséquent, l'image de la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ par la différentielle de f en I_2 est le nombre $a + d$.

IV.7.15 1. Le déterminant de M est une fonction polynomiale des coefficients de M. C'est donc une application différentiable (comme somme et produit de fonctions différentiables).

2. Les coefficients de la matrice $\mathrm{I}_3 + hM$ dépendent de manière affine de h. Comme le déterminant de la matrice $\mathrm{I}_3 + hM$ est une fonction polynomiale des coefficients de $\mathrm{I}_3 + hM$, on voit que P est un polynôme. D'ailleurs :

$$\det(\mathrm{I}_3 + hM) = -h^3 \det(-h^{-1}\mathrm{I}_3 - M) = -h^3 \chi_M(-1/h)$$

avec χ_M le polynôme caractéristique de la matrice M. Or, χ_M est un polynôme de degré 3, le coefficient de X^3 est 1, le coefficient de X^2 est égal à $-\mathrm{tr}(M)$ et le coefficient constant est égal à $-\det(M)$:

$$\chi_M(X) = X^3 - \mathrm{tr(M)X^2} + \alpha \mathrm{X} - \det(\mathrm{M}) \quad \text{avec} \quad \alpha \in \mathbb{R}.$$

Par conséquent :

$$\begin{aligned}\det(\mathrm{I}_3 + hM) &= -h^3 \left(-\frac{1}{h^3} - \frac{\mathrm{tr(M)}}{h^2} - \frac{\alpha}{h} - \det(M) \right) \\ &= 1 + \mathrm{tr(M)h} + \alpha \mathrm{h}^2 + \det(\mathrm{M})\mathrm{h}^3.\end{aligned}$$

3. On a donc

$$\det(\mathrm{I}_3 + hM) = 1 + \mathrm{tr}(M)h + h\varepsilon(h) \quad \text{avec} \quad \varepsilon(h) \underset{h\to 0}{\longrightarrow} 0.$$

Cela montre que :

$$\lim_{\substack{h\to 0 \\ h\neq 0}} \frac{f(\mathrm{I}_3 + hM) - f(\mathrm{I}_3)}{h} = \mathrm{tr}(M).$$

4. La différentielle de f en I_3 est donc l'application tr.

IV.7.16 1. L'application $f : z \mapsto |z|$ peut également s'écrire

$$f(x+iy) = P(x,y) + iQ(x,y) \quad \text{avec} \quad P(x,y) = \sqrt{x^2+y^2} \quad \text{et} \quad Q(x,y) = 0.$$

Les applications P et Q sont différentiables en dehors de $(0,0)$ et la matrice jacobienne de l'application (P,Q) est :

$$J = \begin{pmatrix} \dfrac{x}{\sqrt{x^2+y^2}} & \dfrac{y}{\sqrt{x^2+y^2}} \\ 0 & 0 \end{pmatrix}.$$

Les conditions de Cauchy ne sont vérifiées que lorsque :

$$\frac{x}{\sqrt{x^2+y^2}} = 0 \quad \text{et} \quad \frac{y}{\sqrt{x^2+y^2}} = -0,$$

c'est-à-dire si, et seulement si, $x = y = 0$. L'application f n'est donc holomorphe sur aucun ouvert de $\mathbb{C}$.

2. Les fonctions $z \mapsto z+1$ et $z \mapsto z^2+2$ sont holomorphes sur $\mathbb{C}$. La fonction $z \mapsto z^2+2$ s'annule si, et seulement si, $z = \pm i\sqrt{2}$. Par conséquent, la fonction g est holomorphe sur $\mathbb{C} \setminus \{i\sqrt{2}, -i\sqrt{2}\}$.

3. La fonction $z \mapsto \mathrm{Arg}(z)$ est définie sur $\mathbb{C}\setminus]-\infty, 0]$ et prend ses valeurs dans l'intervalle $]-\pi, \pi[$. On a :

$$\mathrm{Arg}(x+iy) = 2\arctan \frac{y}{x + \sqrt{x^2+y^2}}.$$

L'application $h : z \mapsto \ln|z| + i\,\mathrm{Arg}(z)$ est donc définie sur $\mathbb{C} \setminus]-\infty, 0]$. Elle peut également s'écrire $f(x+iy) = P(x,y) + iQ(x,y)$ avec :

$$P(x,y) = \frac{1}{2}\ln(x^2+y^2) \quad \text{et} \quad Q(x,y) = 2\arctan\frac{y}{x+\sqrt{x^2+y^2}}.$$

Les applications P et Q sont différentiables sur $\mathbb{R}^2 \setminus \big\{(x,y) \;\big|\; y = 0 \text{ et } x \leqslant 0\big\}$. Notons que :

$$\frac{\partial P}{\partial x}(x,y) = \frac{1}{2}\frac{2x}{x^2+y^2} \quad \text{et} \quad \frac{\partial P}{\partial y}(x,y) = \frac{1}{2}\frac{2y}{x^2+y^2}.$$

De plus :

$$\begin{aligned}\frac{\partial Q}{\partial x}(x,y) &= 2\frac{1}{1+y^2/(x+\sqrt{x^2+y^2})^2}\cdot(-y)\frac{1+x/\sqrt{x^2+y^2}}{(x+\sqrt{x^2+y^2})^2}\\ &= \frac{1}{x^2+y^2+x\sqrt{x^2+y^2}}\cdot\frac{-y(x+\sqrt{x^2+y^2})}{\sqrt{x^2+y^2}}\\ &= \frac{-y}{x^2+y^2} = -\frac{\partial P}{\partial y}(x,y)\end{aligned}$$

et

$$\begin{aligned}\frac{\partial Q}{\partial y}(x,y) &= 2\frac{1}{1+y^2/(x+\sqrt{x^2+y^2})^2}\cdot\frac{x+\sqrt{x^2+y^2}-y^2/\sqrt{x^2+y^2}}{(x+\sqrt{x^2+y^2})^2}\\ &= \frac{1}{x^2+y^2+x\sqrt{x^2+y^2}}\cdot\frac{x(x+\sqrt{x^2+y^2})}{\sqrt{x^2+y^2}}\\ &= \frac{x}{x^2+y^2} = \frac{\partial P}{\partial x}(x,y).\end{aligned}$$

Les conditions de Cauchy sont vérifiées sur $\mathbb{R}^2 \setminus \big\{(x,y) \;\big|\; y = 0 \text{ et } x \leqslant 0\big\}$. La fonction h est donc holomorphe sur $\mathbb{C} \setminus]-\infty, 0]$.

IV.7.17 Bien entendu, il faut supposer que $(a,b) \neq (0,0)$ sinon la matrice n'est pas inversible. Les matrices de la forme $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ sont les matrices de similitudes. L'inverse d'une similitude (de rapport non nul) est une similitude (de rapport inverse). Plus précisément, on a :

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\cdot\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax-by \\ bx+ay \end{pmatrix} \quad \text{et} \quad (a+ib)(x+iy) = (ax-by)+i(bx+ay).$$

Or :

$$\frac{1}{a+ib} = \frac{a-ib}{a^2+b^2} = a'+ib' \quad \text{avec} \quad a' = \frac{a}{a^2+b^2} \quad \text{et} \quad b' = -\frac{b}{a^2+b^2}.$$

L'inverse de la matrice $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ est la matrice $\begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix}$.

IV.7.18 On recherche sous quelles conditions :

$$f(x,y) = \sum_{n=0}^{d} b_n(x+iy)^n = \sum_{n=0}^{d}\sum_{k=0}^{n} b_n C_n^k i^{n-k}x^k y^{n-k} \quad \text{avec} \quad C_n^k := \frac{k!(n-k)!}{n!}.$$

Le polynôme :

$$f(x,y)=\sum_{n=0}^{d}\sum_{k=0}^{n}a_{n,k}x^k y^{n-k}$$

est un polynôme en $z:=x+iy$ si, et seulement si :

$$b_{n,k}:=\frac{1}{i^{n-k}}\frac{k!(n-k)!}{n!}a_{n,k}$$

ne dépend pas de k, donc si, et seulement si, pour tout $n\in[\![1,d]\!]$ et tout $k\in[\![0,n-1]\!]$, on a :

$$a_{n,k+1}=-i\frac{n-k}{k+1}a_{n,k}.$$

Par ailleurs, si $f(x,y)=P(x,y)+iQ(x,y)$ avec P et Q des polynômes à coefficients réels, les conditions de Cauchy-Riemann sont vérifiées si, et seulement si :

$$\frac{\partial P}{\partial x}=\frac{\partial Q}{\partial y}\quad\text{et}\quad\frac{\partial P}{\partial y}=-\frac{\partial Q}{\partial x},$$

donc si, et seulement si :

$$\frac{\partial f}{\partial x}=\frac{\partial P}{\partial x}+i\frac{\partial Q}{\partial x}=\frac{\partial Q}{\partial y}-i\frac{\partial P}{\partial y}=-i\frac{\partial f}{\partial y}.$$

Par conséquent, le polynôme :

$$f(x,y)=\sum_{n=0}^{d}\sum_{k=0}^{n}a_{n,k}x^k y^{n-k}$$

vérifie les conditions de Cauchy-Riemann si, et seulement si :

$$\sum_{n=0}^{d}\sum_{k=1}^{n}ka_{n,k}x^{k-1}y^{n-k}=-i\sum_{n=0}^{d}\sum_{k=0}^{n-1}(n-k)a_{n,k}x^k y^{n-k-1}$$

donc si, et seulement si, pour tout $n\in[\![1,d]\!]$ et tout $k\in[\![0,n-1]\!]$, on a :

$$a_{n,k+1}=-i\frac{n-k}{k+1}a_{n,k}.$$

Pour déterminer les conditions sous lesquelles $f(x,y)$ est un polynôme en $\bar{z}:=x-iy$, il suffit d'échanger le rôle de i et de $-i$. Le polynôme :

$$f(x,y)=\sum_{n=0}^{d}\sum_{k=0}^{n}a_{n,k}x^k y^{n-k}$$

est un polynôme en $z:=x+iy$ si, et seulement si, pour tout $n\in[\![1,d]\!]$ et tout $k\in[\![0,n-1]\!]$, on a :

$$a_{n,k+1}=i\frac{n-k}{k+1}a_{n,k},$$

donc si, et seulement si :

$$\frac{\partial P}{\partial x}+i\frac{\partial Q}{\partial x}=\frac{\partial f}{\partial x}=i\frac{\partial f}{\partial y}=-\frac{\partial Q}{\partial y}+i\frac{\partial P}{\partial y},$$

donc si, et seulement si :

$$\frac{\partial P}{\partial x}=-\frac{\partial Q}{\partial y}\quad\text{et}\quad\frac{\partial P}{\partial y}=\frac{\partial Q}{\partial x}.$$

Module IV.8 : Approximation

IV.8.1 On calcule $f'(t) = \frac{2t}{1+t^2}$ et $f''(t) = \frac{2(1-t^2)}{(1+t^2)^2}$.

On a, en utilisant la formule de Taylor avec reste intégral à l'ordre 1 :

$$f(1) = f(0) + f'(0) + \int_0^1 \frac{2(1-t^2)}{(1+t^2)^2}(1-t)\,\mathrm{d}t,$$

donc : $I = \displaystyle\int_0^1 \frac{(1-t^2)}{(1+t^2)^2}(1-t)\,\mathrm{d}t = \frac{f(0)}{2} = \frac{\ln 2}{2}$.

IV.8.2 1. On a évidemment $0 \leqslant g_n$. On a $g_n'(t) = -n(1-t)^{n-1}\mathrm{e}^t + (1-t)^n\mathrm{e}^t = -(1-t)^{n-1}\mathrm{e}^t(n-1+t)$. La fonction est donc décroissante sur $[0,1]$. On a $g_n(0) = 1$, donc $g_n \leqslant 1$.

2. La formule de Taylor avec reste intégral pour la fonction exponentielle s'écrit :

$$e = 1 + \sum_{k=1}^{n} \frac{1}{k!} + \frac{1}{n!}\int_0^1 (1-t)^n\mathrm{e}^t\,\mathrm{d}t,$$

d'où l'encadrement cherché en utilisant 1.

IV.8.3 1. a) On a deux formules de Taylor-Lagrange au point c, respectivement entre c et a et entre c et b :

$$f(a) = f\left(c + a - c)\right) = f(c) + (a-c)f'(c) + \frac{(a-c)^2}{2}f''(c_1)$$

$$f(b) = f\left(c + b - c)\right) = f(c) + (b-c)f'(c) + \frac{(b-c)^2}{2}f''(c_2)$$

avec $c_1, c_2 \in]a,b[$. On en déduit par combinaison linéaire :

$$\begin{aligned} P(c) - f(c) &= \frac{b-c}{b-a}f(a) + \frac{c-a}{b-a}f(b) - f(c) \\ &= \frac{b-c}{b-a}\frac{(a-c)^2}{2}f''(c_1) + \frac{c-a}{b-a}\frac{(b-c)^2}{2}f''(c_2) \\ &= \frac{(c-a)(b-c)}{2}\left(\frac{c-a}{b-a}f''(c_1) + \frac{b-c}{b-a}f''(c_2)\right). \end{aligned}$$

On a $\frac{c-a}{b-a} \geqslant 0$, $\frac{b-c}{b-a} \geqslant 0$ et $\frac{c-a}{b-a} + \frac{b-c}{b-a} = 1$, donc $\gamma := \frac{c-a}{b-a}f''(c_1) + \frac{b-c}{b-a}f''(c_2)$ appartient au segment d'extrémités $f''(c_1)$ et $f''(c_2)$. La fonction f'' est continue, donc d'après le théorème des valeurs intermédiaires, il existe d appartenant au segment d'extrémités c_1 et c_2 (et donc appartenant à $]a,b[$) tel que $f''(d) = \gamma$. Ainsi on a (36), puis (37). On en déduit immédiatement (38), puis :

$$\left|f(c) - P(c)\right| \leqslant \frac{(c-a)(b-c)}{2}\sup_{x\in[a,b]}\left|f''(x)\right|.$$

On vérifie, par ailleurs que $\dfrac{(c-a)(b-c)}{2(b-a)^2} \leqslant \dfrac{1}{8}$, donc :

$$\frac{(c-a)(b-c)}{2}\sup_{x\in[a,b]}\left|f''(x)\right| \leqslant \frac{(b-a)^2}{8}\sup_{x\in[a,b]}\left|f''(x)\right|.$$

b) Soit $\varphi : t \in [0,1] \mapsto \varphi(t) := (1-t)a + tb \in [a,b]$. Cette application est bijective et, si $c \in [a,b]$, $t = \varphi^{-1}(c) = \frac{c-a}{b-a}$ et $1-t = \frac{b-c}{b-a}$.
Notons $c := (1-t)a + tb$. Si $f'' \geqslant 0$, on a :

$$(1-t)f(a) + tf(b) - f\left((1-t)a + tb\right) = P(c) - f(c) \geqslant 0,$$

donc f est convexe.
Si $f'' \leqslant 0$, on a :

$$(1-t)f(a) + tf(b) - f\left((1-t)a + tb\right) \leqslant 0,$$

donc f est concave.
Inversement, notons $\lambda := \inf_{x\in[a,b]} f''(x)$ et considérons les fonctions :

$$h : x \in [a,b] \mapsto h(x) := (x-a)(b-x) \quad \text{et} \quad g := f + \frac{\lambda}{2}h.$$

On a $h" = -2$, donc $g'' = f'' - \lambda \geqslant 0$ et g est convexe.
L'inégalité de convexité pour g s'écrit :

$$(1-t)f(a) + tf(b) - f\left((1-t)a + tb\right) - \lambda t(1-t)\frac{(b-a)^2}{2} \geqslant 0$$

et l'on retrouve l'une des inégalités (38). On retrouve l'autre en considérant $-f$.

2. La fonction K_t est évidemment continue et positive.
On calcule facilement $\displaystyle\int_0^1 K_t(s)\,\mathrm{d}s = \frac{t(1-t)}{2}$.

3. Rappelons que le reste dans la formule de Taylor avec reste intégral au point $c \in [a,b]$ peut s'écrire (*cf.* (3) page 850) : $\displaystyle(x-c)^2 \int_0^1 (1-s)f''\left(c + s(x-c)\right)\mathrm{d}s$.
Soit $c \in [a,b]$. On note, comme plus haut, $t := \frac{c-a}{b-a}$ et l'on a $c = (1-t)a + tb$, $c - a = t(b-a)$ et $b - c = (1-t)(b-a)$.
On réécrit les deux formules de Taylor en c de la solution de la question 1 en remplaçant les restes de Lagrange par des restes intégraux et l'on utilise $(a-c)^2 = t^2(b-a)^2$ et $(b-c)^2 = (1-t)^2(b-a)^2$. On obtient :

$$f(a) = f(c) + t(a-b)f'(c) + t^2(b-a)^2 \int_0^1 (1-s)f''\left((1-t)a + tb + st(a-b)\right)\mathrm{d}s,$$

$$f(b) = f(c) + (1-t)(b-a)f'(c)$$
$$+ (1-t)^2(b-a)^2 \int_0^1 (1-s)f''\left((1-t)a + tb + s(1-t)(b-a)\right)\mathrm{d}s.$$

Si $t \neq 0$, on a, en utilisant le changement de variable $\sigma := t(1-s)$, puis en remplaçant σ par s :

$$t^2 \int_0^1 (1-s)f''\left((1-s)\left((1-t)a + tb\right) + sa\right)\mathrm{d}s = \int_0^t sf''\left((1-s)a + sb\right)\mathrm{d}s,$$

Cette formule reste vraie pour $t = 0$.
Si $t \neq 1$, on a, en utilisant le changement de variable $\tau := (1-t)(1-s)$, puis en

remplaçant τ par s :

$$(1-t)^2\int_0^1 (1-s)f''\left((1-t)a+tb+s(1-t)(b-a)\right)\mathrm{d}s$$
$$=\int_0^{1-t} sf''\left((1-s)b+sa\right)\mathrm{d}s$$
$$=\int_t^1 (1-s)f''\left((1-s)a+sb\right)\mathrm{d}s.$$

Cette formule reste vraie pour $t=1$.
Par combinaison linéaire on obtient :

$$(1-t)\int_0^t sf''\left((1-s)a+sb\right)\mathrm{d}s + t\int_t^1 (1-s)f''\left((1-s)a+sb\right)\mathrm{d}s$$
$$=\int_0^1 f''\left((1-s)a+sb\right)K_t(s)\,\mathrm{d}s.$$

On obtient ensuite (39) en calculant $(1-t)f(a)+tf(b)$.
On retrouve les inégalités (38) en utilisant $K_t\geqslant 0$ et $\displaystyle\int_0^1 K_t(s)\,\mathrm{d}s=\frac{t(1-t)}{2}$.

4. – Si α et β sont les valeurs données par la table respectivement pour $f(a)$ et $f(b)$ et si t est décimal, on peut calculer exactement le nombre décimal $\gamma:=t\alpha+(1-t)\beta$. On a $|\gamma-(tf(a)+(1-t)f(b))|\leqslant t\,10^{-m}+(1-t)10^{-m}=10^{-m}$. Pour obtenir l'erreur totale dans le calcul de $f(c)$, il faut donc ajouter 10^{-m} à l'erreur de méthode.
   – Si $f(x)=\log_{10}x=\ln x/\ln 10$. On a $0{,}43<1/\ln 10<0{,}44$. Supposons $a\in[10^3,10^4[$ et $b:=a+1$. On a alors $\left|f''(x)\right|\leqslant\frac{1}{\ln 10}\frac{1}{x^2}<0{,}44.10^{-6}$ et l'erreur de méthode est majorée par $6.10^{-8}<10^{-7}$. Elle est donc négligeable devant l'erreur due à la table et à l'arrondi qui est de l'ordre de 10^{-5}.
   – On note $sin(x):=\sin\left(\frac{\pi}{180}x\right)$. La table donne :

$$sin(40)\approx 0{,}64278761\quad\text{et}\quad sin(41)\approx 0{,}65605903.$$

Par interpolation linéaire on obtient :

$$sin(40{,}25)\approx 0{,}75\times 0{,}64278761+0{,}25\times 0{,}65605903\approx 0{,}64610546.$$

On a $sin''(x)=-\left(\frac{\pi}{180}\right)^2 sin(x)$. L'erreur de méthode est donc majorée par $3{,}808\times 10^{-5}$ et l'erreur totale par $3{,}809\times 10^{-5}$.
En fait $sin(40{,}25)\approx 0{,}64612398$ et l'erreur est donc voisine de $1{,}9.10^{-5}$.

IV.8.4 1. On a :

$$g(x)=xg'(0)+\frac{x^3}{6}g'''(0)+\int_0^x\frac{(x-t)^4}{24}g^{(5)}(t)\,\mathrm{d}t$$
$$g'(x)=g'(0)+\frac{x^2}{2}g'''(0)+\int_0^x\frac{(x-t)^3}{6}g^{(5)}(t)\,\mathrm{d}t,$$

d'où :

$$g(x) - \frac{x}{3}g'(x) = \frac{2x}{3}g'(0) + \int_0^x g^{(5)}(t)\left(\frac{(x-t)^4}{24} - \frac{x(x-t)^3}{18}\right)\mathrm{d}t.$$

2. Soit $x \in]0,1]$. Posons $h_x : t \in]0,x[\to h_x(t) := \frac{(x-t)^4}{24} - \frac{x(x-t)^3}{18}$. Cette fonction est continue. Montrons qu'elle est *strictement négative* sur $]0,x[$. On a :

$$h_x(t) = \frac{(x-t)^3}{6}\left(\frac{x-t}{4} - \frac{x}{3}\right) = -\frac{(x-t)^3}{72}(3t+x) < 0.$$

Calculons $\displaystyle\int_0^x h_x(t)\,\mathrm{d}t = \left[-\frac{(x-t)^5}{120} + \frac{x(x-t)^4}{72}\right]_0^x = x^5\left(\frac{1}{120} - \frac{1}{72}\right) = -\frac{x^5}{180}$.

D'après les exercices 2 et 3 (première formule de la moyenne), il existe $d_x \in]0,x[$ tel que :

$$\int_0^x g^{(5)}(t)h_x(t)\,\mathrm{d}t = g^{(5)}(d_x)\int_0^x h_x(t)\,\mathrm{d}t = -\frac{x^5}{180}\,g^{(5)}(d_x).$$

On en déduit :

$$g(x) = \frac{2x}{3}g'(0) + \frac{x}{3}g'(x) - \frac{x^5}{180}\,g^{(5)}(d_x),$$

puis (40) en faisant $x := 1$ et en notant $d_1 = d$.

IV.8.5 En écrivant :

$$\frac{x+1}{x-2} = -\frac{1+x}{2}\left(1 - \frac{x}{2}\right)^{-1} \qquad \text{et} \qquad \frac{x^2-x}{2x^2-x+5} = -\frac{x-x^2}{5}\left(1 - \frac{x}{5} + \frac{2x^2}{5}\right)^{-1},$$

on trouve respectivement $-\frac{1}{2} - \frac{3x}{4} - \frac{3x^2}{8} - \frac{3x^3}{16} + \mathrm{o}(x^3)$ et $-\frac{x}{5} + \frac{4x^2}{25} + \mathrm{o}(x^2)$.

IV.8.6 On a $f(x) := \sinh x \sin x \sim x^2$, donc $f(x) = x^2 + \mathrm{o}(x^2)$. Comme f est paire et de classe $\mathcal{C}^\infty$, elle admet un développement limité à tout ordre, ce développement ne comportant que des termes de degré pair. Donc $f(x) = x^2 + \mathrm{o}(x^3)$.

Comme $(1-x^4)^{-1} = 1 + \mathrm{o}(x^3)$, le développement limité à l'ordre 3 de $g(x) := \frac{1}{(1+x)(1-x^4)}$ est le même que celui de $(1+x)^{-1}$, soit $g(x) = 1 - x + x^2 - x^3 + \mathrm{o}(x^3)$.

Puisque $\sin x \sim x$ et $\ln(1+x) \sim x$, il suffit d'utiliser des développements limités à l'ordre 2 de ces deux fonctions pour obtenir un développement limité à l'ordre 3 de leur produit. Comme $\sin x = x + \mathrm{o}(x^2)$ et $\ln(1+x) = x - x^2/2 + \mathrm{o}(x^2)$, on obtient $(\sin x)\ln(1+x) = x^2 - \dfrac{x^3}{2} + \mathrm{o}(x^3)$.

IV.8.7 On trouve respectivement $-1 + \mathrm{o}(x^3)$ et $-4(x+1) + 6(x+1)^2 - 4(x+1)^3 + \mathrm{o}(x^3)$.

IV.8.8 On trouve $f'(x) = \dfrac{1}{\sqrt{1+x^2}} = 1 - \dfrac{x^2}{2} + \dfrac{3x^4}{8} + \mathrm{o}(x^4)$, d'où le développement :

$$f(x) = f(0) + x - \frac{x^3}{6} + \frac{3x^5}{40} + \mathrm{o}(x^5) = x - \frac{x^3}{6} + \frac{3x^5}{40} + \mathrm{o}(x^5).$$

IV.8.9 On trouve respectivement $1 - \dfrac{x}{2} + \dfrac{x^2}{4} - \dfrac{x^3}{8} + \mathrm{o}(x^3)$ et, en changeant x en $x-2$,

$$\frac{1}{x} = \frac{\frac{1}{2}}{1+\frac{x-2}{2}} = \frac{1}{2} - \frac{x-2}{4} + \frac{(x-2)^2}{8} - \frac{(x-2)^3}{16} + \mathrm{o}(x-2)^3.$$

IV.8.10 On trouve $\ln\left(1+\dfrac{x}{e}\right) = \dfrac{x}{e} - \dfrac{x^2}{2\mathrm{e}^2} + \mathrm{o}(x^2)$ et, en changeant x en $x-e$:

$$\ln x = 1 + \ln\left(1+\frac{x-e}{e}\right) = 1 + \frac{x-e}{e} - \frac{(x-e)^2}{2\mathrm{e}^2} + \mathrm{o}(x-e)^2.$$

IV.8.11 Voici les limites demandées :

1. 0, car le numérateur est équivalent à $-x^3/6$;
2. $3/4$, car le numérateur et le dénominateur sont respectivement équivalents à $-x^3/2$ et $-2x^3/3$;
3. $1/3$, comme on le voit en écrivant, pour $x>0$ et $y := 1/x$:
$$\sqrt[3]{x^3+x^2+7} = x\sqrt[3]{1+y+7y^3} = x\left(1+\frac{y}{3}+\mathrm{o}(y)\right);$$
4. $-1/2$, comme on le voit en écrivant, pour $y := x - \dfrac{\pi}{2}$:
$$\sqrt[4]{1+2\cos x} = \sqrt[4]{1-2\sin y} = 1 - \frac{2\sin y}{4} + \mathrm{o}(\sin y) = 1 - \frac{y}{2} + \mathrm{o}(y).$$

IV.8.12 On trouve respectivement $-\dfrac{x}{6} + \mathrm{o}(x^2)$ et $\dfrac{3}{4} + \dfrac{3x^2}{16} + \mathrm{o}(x^2)$. Rechercher les dérivées successives serait très maladroit ; il vaut mieux chercher des développements du numérateur et du dénominateur à l'ordre $4 = 2+2$ pour la première et $5 = 2+3$ pour la deuxième pour tenir compte des simplifications respectivement par x^2 et x^3.

IV.8.13 1. On trouve aussitôt

$$\cos x = 1 - \frac{x^2}{2} + \frac{x^4}{24} + \mathrm{o}(x^4)$$
$$\cosh x = 1 + \frac{x^2}{2} + \frac{x^4}{24} + \mathrm{o}(x^4),$$

d'où le développement cherché $f(x) = 1 + \dfrac{x}{2} + \dfrac{x^2}{24} + \mathrm{o}(x^2)$.

2. On trouve $f'(x) = \dfrac{\sinh(\sqrt{x})}{2\sqrt{x}}$ pour $x>0$ et $f'(x) = \dfrac{\sin(\sqrt{-x})}{2\sqrt{-x}}$ pour $x<0$. Ces deux quantités ont même limite, $1/2$, lorsque x tend vers 0 ; or la lecture du développement limité ci-dessus montre qu'en 0 la fonction f admet bien une dérivée première égale à $1/2$, d'où le résultat.

IV.8.14 Les développements :

$$f(x+2h) = f(x) + 2hf'(x) + 2h^2 f''(x) + \mathrm{o}(h^2),$$

$$f(x+3h) = f(x) + 3hf'(x) + \frac{9h^2}{2} f''(x) + \mathrm{o}(h^2)$$

montrent que le numérateur peut s'écrire $3h^2 f''(x) + \mathrm{o}(h^2)$; la limite cherchée existe donc bien et vaut $f''(x)$.

IV.8.15 Dans tout ce qui suit, on posera $h := 1/x$ pour $x \neq 0$.

1. On a aussitôt :

$$\frac{f(x)}{x} = \frac{2 - 7h - 9h^2}{1 - 2h} = 2 - 3h - 15h^2 + \mathrm{o}(h^2)$$

d'où les valeurs $a = 2$, $b = -3$ et $c = -15 < 0$: la droite d'équation $y = 2x - 3$ est donc asymptote au graphe de f, à la fois aux voisinages de $-\infty$ et $+\infty$; le graphe est respectivement au-dessus et au-dessous de son asymptote.

2. De la même façon, pour $x < 0$ on a :

$$\frac{f(x)}{x} = 1 - \sqrt[4]{1 - h - h^4} = \frac{h}{4} + \frac{3h^2}{32} + \mathrm{o}(h^2)$$

d'où l'asymptote d'équation $y = 1/4$ pour $x < 0$ (avec position au-dessus de l'asymptote au voisinage de $-\infty$), alors que, pour $x > 0$ on a :

$$\frac{f(x)}{x} = 1 + \sqrt[4]{1 - h - h^4} = 2 - \frac{h}{4} - \frac{3h^2}{32} + \mathrm{o}(h^2)$$

d'où l'asymptote d'équation $y = 2x - 1/4$ pour $x > 0$ (avec position au-dessous de l'asymptote au voisinage de $+\infty$).

3. De la même façon, on a aussitôt :

$$\frac{f(x)}{x} = \frac{1}{h} \arctan\left(\frac{h}{1+h}\right) = \frac{1}{h} \arctan\left(h - h^2 + h^3 + \mathrm{o}(h^3)\right) = 1 - h + \frac{2h^2}{3} + \mathrm{o}(h^2)$$

d'où l'asymptote d'équation $y = x - 1$, le graphe étant au-dessus de l'asymptote aussi bien au voisinage de $-\infty$ que de $+\infty$.

IV.8.16 *Dans les indications permettant de répondre aux questions posées, u est une variable tendant vers 0.*

On trouve les équivalents suivants :

1. (a) $u_n \sim \dfrac{1}{n^3}$ (penser à $\mathrm{e}^u - 1 \sim u$).
   (b) $v_n \sim \mathrm{e}^{15}$ (remplacer $5/n$ par $15/3n$).
   (c) $w_n \sim 1$ (prendre le logarithme).
   (d) $z_n \sim -\ln n$ (remplacer $1/n$ par $\mathrm{e}^{-\ln n}$).
2. (a) $u_n \sim n$ (penser à $\sin u \sim u$).

(b) $u_n \sim \dfrac{1}{2}$ (penser à $1-\cos u \sim u^2/2$).

(c) $u_n \sim \dfrac{n^2}{2}$ (penser à $\sinh u \sim u$).

(d) $u_n \sim 1$ (penser à $\tan u \sim \arctan u \sim u$).

3. $u_n \sim \dfrac{2}{\sqrt{n}}$ (penser à $\arctan u \sim \sinh u \sim u$).

4. $u_n \sim \dfrac{1}{4}$ (penser à $\cos u - 1 \sim -u^2/2$).

5. $v_n \sim \dfrac{1}{24}$ (développer $\exp u$ à l'ordre 4).

IV.8.17 En utilisant la question 1 de l'exercice IV.8.0 de la page 895, on montre que les parties régulières des développements limités à l'ordre 5 à l'origine des deux fonctions sont nulles. Les deux fonctions étant impaires, on calcule les développements limités à l'ordre 7. On trouve $\sinh(\sin(t))-\sin(\sinh(t)) = \frac{1}{45}t^7+\mathrm{o}(t^7)$ et $\tanh(\tan(t))-\tan(\tanh(t)) = -\frac{2}{45}t^7+\mathrm{o}(t^7)$. Par suite $\sinh\circ\sin-\sin\circ\sinh \sim \frac{1}{45}t^7$ et $\tanh\circ\tan-\tan\circ\tanh \sim -\frac{2}{45}t^7$.

IV.8.18 1. a) On montre que $\tilde{A}_p(ix) = iA_p(x)$ et $\tilde{C}_p(ix) = C_p(x)$ en utilisant la table IV.8.2 de la page 867.

b) On a, en considérant les polynômes de $\mathbb{R}[X]$ comme des polynômes de $\mathbb{C}[Z]$, $\tilde{A}_p(z) = \tilde{Q}_p(z)\tilde{C}_p(z) + z^{p+1}\tilde{S}_p(z)$, pour tout $z \in \mathbb{C}$, donc, en particulier, pour tout $x \in \mathbb{R}$:

$$\tilde{A}_p(ix) = \tilde{Q}_p(ix)\tilde{C}_p(ix) + i^{p+1}x^{p+1}\tilde{S}_p(ix)$$

et, en utilisant a) : $iA_p(x) = \tilde{Q}_p(ix)C_p(x) + i^{p+1}x^{p+1}\tilde{S}_p(ix)$.
Ainsi :

$$A_p(x) = \frac{1}{i}\tilde{Q}_p(ix)C_p(x) + i^p x^{p+1}\tilde{S}_p(ix). \tag{56}$$

Le polynôme $\tilde{Q}_p$ est *impair*, donc le polynôme $\frac{1}{i}\tilde{Q}_p(ix)$ est réel et le polynôme $i^{p+1}\tilde{S}_p(ix)$ est également réel puisque $A_p(x)$ l'est. Par suite (56) est l'égalité de division suivant les puissances croissantes dans $\mathbb{R}[X]$ de A_p par C_p à l'ordre p et, d'après l'unicité dans la division, $\frac{1}{i}\tilde{Q}_p(ix) = Q_p(x)$.

2. D'après le théorème 25 de la page 876, $\tilde{Q}_p$ est la partie régulière du développement limité de $\tanh x$ en 0 à l'ordre p. D'après (29), on a :

$$\tilde{Q}_p(ix) = \sum_{k=1}^{p}(-1)^{k+1}2^{2k}(2^{2k}-1)\frac{B_k}{(2k)!}(ix)^{2k-1}.$$

En utilisant $Q_p(x) = \frac{1}{i}\tilde{Q}_p(ix)$, on en déduit :

$$Q_p(x) = \sum_{k=1}^{p}2^{2k}(2^{2k}-1)\frac{B_k}{(2k)!}x^{2k-1}.$$

IV.8.19 1. On a, pour $x+h, x-h \in [a,b]$, deux développements limités de Taylor-Young :

$$f(x+h) = f(x) + h\,f'(x) + \frac{h^2}{2}\,f''(x) + \frac{h^3}{6}\,f'''(x) + \mathrm{o}(h^3),$$

$$f(x-h) = f(x) - h\,f'(x) + \frac{h^2}{2}\,f''(x) - \frac{h^3}{6}\,f'''(x) + \mathrm{o}(h^3)$$

d'où $f(x+h) - f(x-h) = 2h\,f'(x) + \dfrac{h^3}{3}\,f'''(x) + \mathrm{o}(h^3)$, puis :

$$f'(x) - \frac{1}{2h}\big(f(x+h) - f(x-h)\big) = -\frac{h^2}{6}\,f'''(x) + \mathrm{o}(h^2).$$

En faisant $x := x_p$, on obtient :

$$f'(x_p) - \frac{1}{2h}\,(f(x_{p+1}) - f(x_{p-1})) = -\frac{h^2}{6}\,f'''(x_p) + \mathrm{o}(h^2),$$

c'est-à-dire :

$$v_p - \frac{1}{2h}\,(u_{p+1} - u_{p-1}) = -\frac{h^2}{6}\,f'''(x_p) + \mathrm{o}(h^2).$$

Pour montrer que l'on peut remplacer le second membre de l'égalité ci-dessus : $-\frac{h^2}{6}\,f'''(x_p) + \mathrm{o}(h^2)$ par un terme de la forme $-\frac{h^2}{6}\,f'''(\omega)$, on peut considérer la fonction auxiliaire φ définie, sur $[0,h]$, par :

$$\varphi(t) := 2t\,f'(x_p) - f(x_p+t) + f(x_p-t) + \lambda\,\frac{t^3}{3},$$

où la constante λ est choisie de façon à vérifier l'égalité $\varphi(h) = 0$.
Calculons les trois premières dérivées de φ :

$$\varphi'(t) = 2\,f'(x_p) - f'(x_p+t) - f'(x_p-t) + \lambda\,t^2,$$
$$\varphi''(t) = f''(x_p-t) - f''(x_p+t) + 2\lambda\,t,$$
$$\varphi'''(t) = 2\lambda - \big(f'''(x_p-t) + f'''(x_p+t)\big).$$

La fonction φ et ses deux premières dérivées sont continues sur $[0,h]$ et s'annulent pour $t := 0$. La troisième dérivée est continue sur $[0,h]$.

Par trois applications successives du théorème de Rolle, il existe un $c \in\,]0,h[$ tel que $\varphi'(c) = 0$, puis un $d \in\,]0,c[\subset\,]0,h[$ tel que $\varphi''(d) = 0$, et enfin un $k \in\,]0,d[\subset\,]0,h[$ tel que $\varphi'''(k) = 0$. D'où :

$$\lambda = \frac{1}{2}\,\big(f'''(x_p-k) + f'''(x_p+k)\big) = f'''(\omega),$$

où l'existence de $\omega \in [x_p-k, x_p+k] \subset\,]x_p-h, x_p+h[\subset]a,b[$ résulte du théorème des valeurs intermédiaires appliqué à la fonction continue f'''.
Finalement, on déduit de l'égalité $\varphi(h) = 0$:

$$v_p - \frac{1}{2h}\,(u_{p+1} - u_{p-1}) = \frac{\varphi(h)}{2h} - \frac{h^2}{6}\,f'''(\omega) = -\frac{h^2}{6}\,f'''(\omega),$$

ce qui conduit à la relation annoncée.

2. La valeur approchée v_p présentée ici peut être vue comme la pente de la droite $A_{p-1}A_{p+1}$, ou encore la demi-somme des pentes de $A_{p-1}A_p$ et A_pA_{p+1}.

3. On a, pour $x, x+h, x+2h \in [a,b]$, deux développements limités de Taylor-Young :

$$f(x+h) - f(x) = h\,f'(x) + \frac{h^2}{2}\,f''(x) + \frac{h^3}{6}\,f'''(x) + \mathrm{o}(h^3),$$

$$f(x+2h) - f(x) = 2h\,f'(x) + 2h^2 f''(x) + \frac{4h^3}{3}\,f'''(x) + \mathrm{o}(h^3)$$

d'où, en utilisant :

$$4\,(f(x+h) - f(x)) - (f(x+2h) - f(x)) = -3f(x) + 4f(x+h) - f(x+2h),$$

$$-3f(x) + 4f(x+h) - f(x+2h) = 2h\,f'(x) - \frac{2h^3}{3}\,f'''(x) + \mathrm{o}(h^3),$$

puis :

$$f'(x) - \frac{1}{2h}\,\big(-3f(x) + 4f(x+h) - f(x+2h)\big) = \frac{h^2}{3}\,f'''(x) + \mathrm{o}(h^2).$$

en faisant $x := 0$, on obtient :

$$f'(0) - \frac{1}{2h}\,\big(-3f(0) + 4f(h) - f(2h)\big) = \frac{h^2}{3}\,f'''(0) + \mathrm{o}(h^2).$$

Pour montrer que l'on peut remplacer $f'''(x)$ par un terme de la forme $f'''(\theta)$, on peut considérer la fonction auxiliaire ψ définie, sur $[0,h]$, par :

$$\psi(t) := 2t\,f'(0) + 3f(0) - 4f(t) + f(2t) - 2\mu\,\frac{t^3}{3},$$

où la constante μ est choisie de façon à vérifier l'égalité $\psi(h) = 0$. Calculons les deux premières dérivées de ψ :

$$\psi'(t) = 2\,f'(0) - 4f'(t) + 2f'(2t) - 2\mu\,t^2,$$
$$\psi''(t) = -4f''(t) + 4f''(2t) - 4\mu\,t.$$

La fonction ψ et ses deux premières dérivées sont continues sur $[0,h]$ et s'annulent pour $t := 0$. Par deux applications du théorème de Rolle, il existe un $r \in\,]0,h[$ tel que $\psi'(r) = 0$, puis un $s \in\,]0,r[\subset\,]0,h[$ tel que :

$$\psi''(s) = 0, \qquad \text{d'où} \qquad \mu = \frac{f''(2s) - f''(s)}{s} = f'''(\theta),$$

où l'existence de $\theta \in\,]s,2s[\subset\,]0,2h[\subset]a,b[$ résulte du théorème des accroissements finis appliqué à la fonction f''.

Finalement, de l'égalité $\psi(h) = 0$ on déduit :

$$v_0 - \frac{1}{2h}\,(-3u_0 + 4u_1 - u_2) = \frac{\psi(h)}{2h} + \frac{h^2}{3}\,f'''(\theta) = \frac{h^2}{3}\,f'''(\theta),$$

ce qui conduit à la relation annoncée.

4. Considérons, pour $\alpha, \beta \in \mathbb{R}_+$:

$$\alpha\,(f(x+h) - f(x)) - \beta\,(f(x+2h) - f(x)) = (\beta - \alpha)f(x) + \alpha f(x+h) - \beta f(x+2h).$$

En utilisant, comme plus haut, deux développements de Taylor-Young, on obtient :

$$(\beta-\alpha)f(x)+\alpha f(x+h)-\beta f(x+2h)=h(\alpha-2\beta)f'(x)+\frac{h^2}{2}(\alpha-4\beta)f''(x)$$
$$+\frac{h^3}{6}(\alpha-8\beta)+\mathrm{o}(h^3).$$

Supposons $\alpha\neq 2\beta$. Si $\alpha\neq 4\beta$, on obtient :

$$f'(x)-\frac{1}{h(\alpha-2\beta)}\left((\beta-\alpha)f(x)+\alpha f(x+h)-\beta f(x+2h)\right)$$
$$=-\frac{h(\alpha-4\beta)}{2(\alpha-2\beta)}f''(x)+\mathrm{o}(h).$$

Si $\alpha=4\beta$ on améliore le résultat :

$$f'(x)-\frac{1}{h(\alpha-2\beta)}\left((\beta-\alpha)f(x)+\alpha f(x+h)-\beta f(x+2h)\right)$$
$$=-\frac{h^2(\alpha-8\beta)}{6(\alpha-2\beta)}f'''(x)+\mathrm{o}(h^2).$$

Le couple (α,β) peut être choisi à un coefficient de proportionnalité près. Ainsi le choix $\alpha:=4,\ \beta:=1$ fait plus haut, qui conduit aux coefficients $-3,4,-1$, est celui qui donne la meilleure approximation de $f'(x)$.

5. La valeur approchée de v_0 présentée ici peut être vue comme un barycentre : celui des pentes des droites A_0A_1 (avec le poids $3/2$) et A_1A_2 (avec le poids $-1/2$).

6. Pour $p:=n$, la même méthode conduit aux relations :

$$\left|v_n-\frac{1}{2h}\left(-u_{n-2}+4u_{n-1}-3u_n\right)\right|=\left|\frac{h^2}{3}f'''(\tau)\right|\leqslant\frac{Mh^2}{3}\cdot$$

On peut d'ailleurs se ramener au cas précédent en changeant x en $a+b-x$.

7. Supposons $x,x+h\in[a,b]$. De la formule de Taylor-Lagrange :

$$f(x+h)-f(x)=h\,f'(x)+\frac{h^2}{2}f''(\gamma),$$

où $\gamma\in]a,b[$, l'on déduit : $f'(x)-\frac{1}{h}\left(f(x+h)-f(x)\right)=-\frac{h}{2}f''(\gamma)$. Par suite $\left|f'(x)-\frac{1}{h}\left(f(x+h)-f(x)\right)\right|\leqslant\frac{h}{2}M_2$, où M_2 est un majorant de la dérivée seconde de f sur $[a,b]$. L'approximation est moins bonne que celles de (41) et (42). La conclusion est la même en remplaçant h par $-h$ et en comparant à (42) et (43).

IV.8.20 On a, pour $x,x+h,x-h\in[a,b]$, deux développements limités de Taylor-Young :

$$f(x+h)-f(x)=h\,f'(x)+\frac{h^2}{2}f''(x)+\frac{h^3}{6}f'''(x)+\frac{h^4}{24}f^{(4)}(x)+\mathrm{O}(h^5),$$

$$f(x-h)-f(x)=-h\,f'(x)+\frac{h^2}{2}f''(x)-\frac{h^3}{6}f'''(x)+\frac{h^4}{24}f^{(4)}(x)+\mathrm{O}(h^5),$$

d'où, en ajoutant les deux égalités ci-dessus :

$$f(x+h)-2f(x)+f(x-h)=h^2f''(x)+\frac{h^4}{12}f^{(4)}(x)+\mathrm{O}(h^5),$$

et, en choisissant $x = x_p$ $(0 < p < n)$:

$$f''(x_p) - \frac{1}{h^2}\left(f(x_{p+1}) - 2f(x_p) + f(x_{p-1})\right) = -\frac{h^2}{12}f^{(4)}(x_p) + \mathrm{o}(h^2).$$

Pour écrire le second membre de l'égalité ci-dessus sous la forme $-\frac{h^2}{12}f^{(4)}(\rho)$, avec $\rho \in]x_{p-1}, x_{p+1}[$, on introduit la fonction auxiliaire :

$$\chi : t \mapsto \chi(t) := t^2 f''(x_p) - f(x_p + t) + 2f(x_p) - f(x_p - t) + \lambda\frac{t^4}{12},$$

en choisissant λ pour que $\chi(h) = 0$.
On calcule les 4 premières dérivées de χ :

$$\begin{aligned}
\chi'(t) &= 2tf''(x_p) - f'(x_p + t) + f'(x_p - t) + \lambda\frac{t^3}{3}\\
\chi''(t) &= 2f''(x_p) - f''(x_p + t) - f''(x_p - t) + \lambda t^2\\
\chi^{(3)}(t) &= -f^{(3)}(x_p + t) + f^{(3)}(x_p - t) + 2\lambda t\\
\chi^{(4)}(t) &= -f^{(4)}(x_p + t) - f^{(4)}(x_p - t) + 2\lambda.
\end{aligned}$$

Les trois premières fonctions s'annulent en $t = 0$. Par quatre applications successives du théorème de Rolle, on obtient $\nu \in]0, h[$ tel que :

$$0 = \chi^{(4)}(\nu) = -f^{(4)}(x_p + \nu) - f^{(4)}(x_p - \nu) + 2\lambda,$$

c'est-à-dire $\lambda = \frac{f^{(4)}(x_p+\nu)+f^{(4)}(x_p-\nu)}{2}$ et, en appliquant le théorème des valeurs intermédiaires à la fonction continue $f^{(4)}$ sur $[x_p - \nu, x_p + \nu]$, on obtient $\rho \in [x_p - \nu, x_p + \nu]$ tel que $\lambda = f^{(4)}(\rho)$, donc :

$$\left|w_p - \frac{1}{h^2}\left(u_{p+1} - 2u_p + u_{p-1}\right)\right| = \frac{h^2}{12}\left|f^{(4)}(\rho)\right| \leqslant \frac{M'h^2}{12}\cdot$$

IV.8.21 On pose :

$$g : x \in [0, 1] \to g(x) := \int_{c-hx}^{c+hx} f(t)dt.$$

Cette fonction est impaire et de classe $\mathcal{C}^5$. Soit F une primitive de f.
On a $g = F(c + hx) - F(c - hx)$, donc :

$$g'(x) = h\left(F'(c + hx) + F'(c - hx)\right) = h\left(f(c + hx) + f(c - hx)\right)$$

et :

$$g'(0) = 2hf(c) \quad \text{et} \quad g'(1) = h\left(f(c + h) + f(c - h)\right).$$

On a $g^{(5)}(x) = h^5\left(\left(f^{(4)}(c + hx) + f^{(4)}(c - hx)\right)\right.$.
La formule (40) de l'exercice IV.8.4 s'écrit ici :

$$\exists\, d \in]0, 1[, \quad g(1) = \frac{1}{3}\left(2g'(0) + g'(1)\right) - \frac{1}{90}\frac{f^{(4)}(c + d) + f^{(4)}(c - d)}{2}\cdot$$

En appliquant le théorème des valeurs intermédiaires à la fonction continue $f^{(4)}$ sur l'intervalle $[c - d, c + d]$, on obtient $\xi \in [c - d, c + d] \subset]c - h, c + h[$ tel que :

$$\int_{c-h}^{c+h} f(x)\,\mathrm{d}x - \frac{h}{3}\left(f(c + h) + f(c - h) + 4f(c)\right) = -\frac{h^5}{90}f^{(4)}(\xi).$$

Alors :

$$\left|\int_{c-h}^{c+h} f(x)\,\mathrm{d}x - \frac{h}{3}\left(f(c+h)+f(c-h)+4f(c)\right)\right| = \frac{h^5}{90}\left|f^{(4)}(\xi)\right| \leqslant \frac{h^5}{90}M_4.$$

IV.8.22 1. On applique la méthode des rectangles à la fonction $f : x \mapsto x-a$. On a $f' = 1$ et l'on peut choisir $M_1 = 1$. On a $\displaystyle\int_a^b (x-a)^2\,\mathrm{d}x = \frac{(b-a)^2}{2}$ et l'on calcule :

$$R_n(f) = \frac{b-a}{n}\sum_{i=0}^{n-1}\frac{i(b-a)}{n} = \frac{(b-a)^2(n-1)}{2n} = \frac{(b-a)^2}{2} - \frac{(b-a)^2}{2n}.$$

On en déduit $\displaystyle\int_a^b (x-a)\,\mathrm{d}x - R_n(f) = \frac{(b-a)^2}{2n} = \frac{M_1(b-a)^2}{2n}$. L'inégalité (30) est donc optimale. Ainsi, dans la méthode des rectangles, l'ordre 1 ne peut pas être amélioré.

2. On applique la méthode des rectangles médians à la fonction $f : x \mapsto (x-a)^2$. On a $f'' = 2$ et l'on peut choisir $M_2 = 2$. On a $\displaystyle\int_a^b (x-a)^2\,\mathrm{d}x = \frac{(b-a)^3}{3}$ et :

$$A_n(f) = \frac{b-a}{n}\sum_{i=1}^{n}\left(\frac{b-a}{n}\right)^2\left(i-\frac{1}{2}\right)^2.$$

On calcule, en utilisant $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ et $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ (*cf.* l'exercice IV.1.24) :

$$\sum_{i=1}^{n}\left(i-\frac{1}{2}\right)^2 = \sum_{i=1}^{n}\left(i^2-i+\frac{1}{4}\right) = \frac{n(n+1)(2n+1)}{6} - \frac{n(n+1)}{2} + \frac{n}{4} = \frac{n(4n^2-1)}{12}.$$

Par suite :

$$A_n(f) = \frac{(b-a)^3(4n^2-1)}{12n^2} = \frac{(b-a)^3}{3} - \frac{(b-a)^3}{12n^2}.$$

On en déduit $\displaystyle\int_a^b (x-a)^2\,\mathrm{d}x - A_n(f) = \frac{(b-a)^3}{12n^2} = \frac{M_2(b-a)^3}{24n^2}$. L'inégalité (32) est donc optimale. Ainsi, dans la méthode des rectangles médians, l'ordre 2 ne peut pas être amélioré.

3. On applique la méthode des trapèzes à la fonction $f : x \mapsto (x-a)^2$. On a $f'' = 2$ et l'on peut choisir $M_2 = 2$. On a $\displaystyle\int_a^b (x-a)^2\,\mathrm{d}x = \frac{(b-a)^3}{3}$ et l'on calcule :

$$T_n(f) = \frac{b-a}{n}\sum_{i=1}^{n}\left(\frac{b-a}{n}\right)^2\left(\frac{(i-1)^2+i^2}{2}\right) = \frac{b-a}{n}\sum_{i=1}^{n}\left(\frac{b-a}{n}\right)^2\left(i^2-i+\frac{1}{2}\right).$$

On calcule :

$$\sum_{i=1}^{n}\left(i^2-i+\frac{1}{2}\right) = \frac{n(n+1)(2n+1)}{6} - \frac{n(n+1)}{2} + \frac{n}{2} = \frac{n(2n^2-1)}{6}.$$

Par suite :

$$T_n(f) = \frac{(b-a)^3(2n^2-1)}{6n^2} = \frac{(b-a)^3}{3} - \frac{(b-a)^3}{6n^2}.$$

On en déduit $\displaystyle\int_a^b (x-a)^2\,\mathrm{d}x - T_n(f) = \frac{(b-a)^3}{6n^2} = \frac{M_2(b-a)^3}{12n^2}\cdot$ L'inégalité (33) est donc optimale. Ainsi, dans la méthode des trapèzes, l'ordre 2 ne peut pas être amélioré.

4. Supposons f de classe $\mathcal{C}^2$ et convexe. Tout arc du graphe de f est *en dessous* de la corde correspondante et l'on en déduit la majoration $\displaystyle\int_a^b f(x)\,\mathrm{d}x \leqslant T_n(f)$. Par ailleurs le graphe de f est *au-dessus* de ses tangentes et, en utilisant la remarque de la page 888, l'on en déduit la minoration $A_n(f) \leqslant \displaystyle\int_a^b f(x)\,\mathrm{d}x$.

5. La méthode de Simpson est évidemment exacte pour un polynôme de degré 2 au plus. Supposons que $\deg f = 3$. Alors $f^{(4)} = 0$ et l'on peut choisir $M_4 = 0$, donc l'inégalité (32) est une égalité et l'on en déduit que la méthode est exacte pour f.

6. On traite d'abord le cas $f := x^4/4!$. On a $m_4 = 1$. On prouve (45), où le signe d'égalité, est remplacé par celui d'égalité, en utilisant Φ et ses dérivées.
On a :
$$\Phi^{(3)}(t) = -\frac{t}{3}\left(f^{(3)}(c+t) - f^{(3)}(c-t)\right) = -\frac{2}{3}t^2,$$
d'où :
$$\Phi''(t) = -\frac{2}{3}\int_0^t u^2\,\mathrm{d}u = -\frac{2t^3}{9}, \Phi'(t) = -\frac{2}{9}\int_0^t 3^2\,\mathrm{d}u = -\frac{1}{18}t^4$$
et $\Phi(t) = -\frac{1}{18}\displaystyle\int_0^u u^4\,\mathrm{d}u = -\frac{1}{90}t^5$.
L'inégalité (45) est vraie pour tout polynôme g de degré 3 (puisque $g^{(4)} = 0$), donc, par linéarité, elle est vraie pour tout polynôme de la forme $\lambda\frac{x^4}{4!} + g$, avec $\lambda \in \mathbb{R}$ quelconque. Ainsi elle est vraie pour tout polynôme de degré au plus 4.
Soit f un polynôme de degré au plus 4. On a :
$$\begin{aligned}\int_a^b f(x)\,\mathrm{d}x - S_n(f)&\\ &= \sum_{i=1}^n \left(\int_{x_{i-1}}^{x_i} f(x)\,\mathrm{d}x - \frac{b-a}{6n}\left(f(x_{i-1}) + f(x_i) + 4f\left(\frac{x_i + x_{i-1}}{2}\right)\right)\right)\\ &= -n\frac{m_4}{90}\left(\frac{b-a}{2n}\right)^5 = -\frac{m_4(b-a)^5}{2880n^4}\cdot\end{aligned}$$
On en déduit : $\left|\displaystyle\int_a^b f(x)\,\mathrm{d}x - S_n(f)\right| = \frac{M_4(b-a)^5}{2880n^4}$, ce qui prouve que l'inégalité (35) est optimale. Ainsi, dans la méthode de Simpson, l'ordre 4 ne peut pas être amélioré.

Module V.1 : Statistique descriptive

V.1.1 1. On trace le nuage de points sur la figure V.3.6 et on constate visuellement une certaine corrélation positive entre la puissance x et la consommation y d'une voiture.

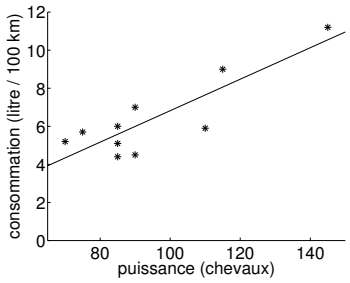


FIGURE V.3.6 – Ajustement linéaire de la consommation d'une voiture (en ordonnée y) par la puissance (en abscisse x).

2. Le coefficient de corrélation est $\mathrm{R}(x,y) \simeq 0{,}858$, ce qui montre qu'une droite de régression linéaire est d'assez bonne qualité.
3. On trace la droite de régression linéaire, qui a pour équation $y = ax+b$ avec $a \simeq 0{,}0827$ et $b \simeq -1{,}45$.
4. La prévision de consommation est $\hat{y} \simeq 9{,}3$ litres/100 km.

V.1.2 1. On a (avec $n = 20$) :

$$(x_i)_{i=1}^n = (8,12,15,17,8,10,8,17,7,15,15,14,15,15,20,12,19,20,15,21)\,,$$
$$(y_i)_{i=1}^n = (9,8,6,6,6,5,6,4,4,4,4,2,3,3,3,3,3,2,1,1)\,.$$

On trouve donc que

$$\bar{x} = 14{,}15\,, \quad \mathrm{Var}(x) = 17{,}5275\,, \quad \bar{y} = 4{,}15\,, \quad \mathrm{Var}(y) = 4{,}4275\,.$$

2. On trouve

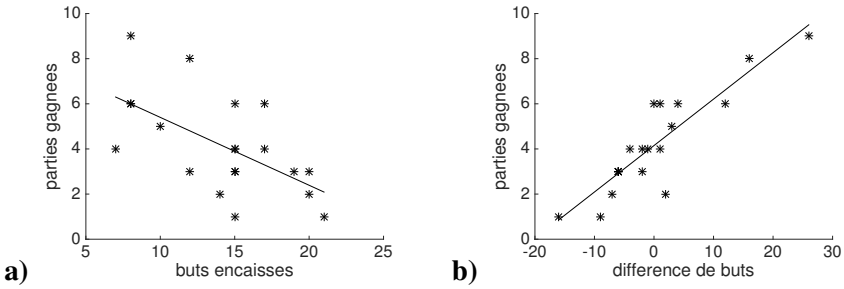
$$\mathrm{Cov}(x,y) = -5{,}2725\,, \quad \mathrm{R}(x,y) = -0{,}5985\,.$$

3. La droite de régression linéaire a pour équation $y = ax+b$ avec $a \simeq -0{,}30$ et $b \simeq 8{,}41$. Évidemment a est négatif : plus une équipe encaisse de buts, moins elle a de chance de gagner des parties. Le coefficient de corrélation est de valeur absolue $|\mathrm{R}(x,y)| \simeq 0{,}60$, ce qui montre que la droite de régression linéaire est de qualité moyenne (voir la figure V.3.7a de la page ci-contre).
4. On recommence avec comme variable explicative la « différence de buts » (colonne « Diff » du tableau) au lieu du « nombre de buts encaissés » :

$$(x'_i)_{i=1}^n = (26,16,12,4,1,3,0,-1,1,-4,-2,2,-2,-6,-6,-6,-6,-7,-9,-16)\,,$$
$$(y_i)_{i=1}^n = (9,8,6,6,6,5,6,4,4,4,4,2,3,3,3,3,3,2,1,1)\,.$$

On trouve donc que

$$\bar{x}' = 0\,, \quad \mathrm{Var}(x') = 83{,}1\,, \quad \bar{y} = 4{,}15\,, \quad \mathrm{Var}(y) = 4{,}4275\,,$$



a) **b)**

FIGURE V.3.7 – Ajustement linéaire du nombre de parties gagnées par le nombre de buts encaissés (figure a) ou par la différence de buts (figure b).

$$\mathrm{Cov}(x', y) = 17{,}1\,, \quad \mathrm{R}(x', y) = 0{,}8915\,.$$

La droite de régression linéaire a pour équation $y = ax' + b$ avec $a' \simeq 0{,}21$ et $b' \simeq 4{,}15$. Le coefficient de corrélation est de valeur absolue $|\mathrm{R}(x', y)| \simeq 0{,}89$, ce qui montre que la droite de régression linéaire est de bonne qualité (voir la figure V.3.7b de la présente page). La différence de buts explique évidemment mieux le nombre de parties gagnées que le nombre de buts encaissés.

V.1.3 1. On peut calculer la moyenne par la formule suivante :

$$\bar{x} = \sum_i f_i c_i\,,$$

où c_i est le centre d'une classe et f_i sa fréquence. On trouve ici $\bar{x} = 1644 + 0{,}195z$.

Si le budget moyen est égal à $1\,995$ euros, alors on doit avoir $1995 = 1644 + 0{,}195z$ et on trouve : $z = 1\,800$.

Si le budget médian est égal à $1\,920$ euros : on regarde le tableau des fréquences cumulées :

Budget	Fréquence	Fréquence cumulée
$[800, 1000[$	0,08	0,08
$[1000, 1400[$	0,1	0,18
$[1400, 1600[$	0,16	0,34
$[1600, z[$	0,3	0,64
$[z, 2400[$	0,09	0,73
$[2400, 4000[$	0,27	1

On voit que la médiane est quelque part dans l'intervalle $[1600, z[$. Il faut alors raisonner par interpolation linéaire sur l'intervalle $[1600, z[$. On pose le rapport des distances suivant :

$$\frac{1920 - 1600}{z - 1600} = \frac{0{,}5 - 0{,}34}{0{,}64 - 0{,}34}\,,$$

et on trouve : $z = 2\,200$.

2. Pour donner une représentation graphique correcte de la distribution (histogramme), il faut calculer la hauteur des rectangles en tenan compre du fait que la largeur des classes

n'est pas uniforme :

Budget	Fréquence	Hauteur des rectangles
$[800, 1000[$	0,08	0,08
$[1000, 1400[$	0,1	0,05
$[1400, 1600[$	0,16	0,16
$[1600, 2000[$	0,3	0,15
$[2000, 2400[$	0,09	0,045
$[2400, 4000[$	0,27	0,045

3. La budget moyen est :

$$\bar{x} = \sum_i f_i c_i = 2\,034\,.$$

La médiane est dans l'intervalle $[1600, 2000]$ et est telle que :

$$\frac{\mathrm{Med}(x) - 1600}{2000 - 1600} = \frac{0{,}5 - 0{,}34}{0{,}64 - 0{,}34}\,,$$

et donc $\mathrm{Med}(x) = 1\,813$. Comme souvent, la moyenne est plus grande que la médiane, car la moyenne est entraînee par quelques grandes valeurs.

V.1.4 1. (a) G est un polynôme du second degré en x :

$$G(x) = nx^2 - 2\Big(\sum_{i=1}^{n} x_i\Big)x + \Big(\sum_{i=1}^{n} x_i^2\Big).$$

Le coefficient dominant de ce polynôme est strictement positif. Un tel polynôme admet un unique minimum en x tel que $G'(x) = 0$. Or $G'(x) = 2nx - 2\sum_{i=1}^{n} x_i$, et donc $G'(x) = 0$ si, et seulement si, $x = \bar{x} := \sum_{i=1}^{n} x_i/n$.

(b) On retrouve bien le fait que la meilleure approximation au sens des moindres carrés des données est la moyenne arithmétique $\bar{x}$.

2. (a) On remarque d'abord que la fonction L est une fonction continue affine par morceaux. Les ruptures de pente ont lieu à chaque x_i, la pente augmentant de 2 au passage de chaque x_i. De plus, sur $]-\infty, x_1]$, la pente de L vaut -3. Elle vaut ensuite -1 sur $[x_1, x_2]$, 1 sur $[x_2, x_3]$ et 3 sur $[x_3, +\infty[$. De plus, $L(-3) = 11$. On peut donc représenter graphiquement la fonction à partir de ces informations sans avoir à chercher l'expression de L sur chacun des intervalles.

(b) Le même raisonnement s'applique, mais cette fois on part d'une pente égale à -4 sur $]-\infty, x_1]$. La pente vaut ensuite -2 sur $[x_1, x_2]$, 0 sur $[x_2, x_3]$, 2 sur $[x_3, x_4]$ et 4 sur $[x_4, +\infty[$. De plus, $L(-3) = 21$. On peut là encore représenter la fonction à partir de ces informations.

(c) Supposons d'abord que n est impair, $n = 2p+1$. L est une fonction continue affine par morceaux de pente valant $-n$ si $x \leqslant x_1$, valant $-n+2$ si $x \in [x_1, x_2]$, …, valant $-n + 2p = -1$ si $x \in [x_p, x_{p+1}]$, valant $-n + 2(p+1) = 1$ si $x \in [x_{p+1}, x_{p+2}]$, …, valant $-n + 2n = n$ si $x \geqslant x_n$. Par conséquent L est

strictement décroissante sur $]-\infty, x_{p+1}]$ et strictement croissante sur $[x_{p+1}, +\infty[$. Elle admet son unique minimum en x_{p+1}.

Si $n = 2p$ est pair, alors L est une fonction continue affine par morceaux, de pente valant $-n$ si $x \leqslant x_1$, valant $-n+2$ si $x \in [x_1, x_2]$, ..., valant $-n+2(p-1) = -2$ si $x \in [x_{p-1}, x_p]$, valant $-n+2p = 0$ si $x \in [x_p, x_{p+1}]$, valant $-n+2(p+1) = 2$ si $x \in [x_{p+1}, x_{p+2}]$, ..., valant $-n + 2n = n$ si $x \geqslant x_n$. Par conséquent L est strictement décroissante sur $]-\infty, x_p]$, constante sur $[x_p, x_{p+1}]$, et strictement croissante sur $[x_{p+1}, +\infty[$. La fonction L admet donc un minimum qui est atteint pour tous les réels de l'intervalle $[x_p, x_{p+1}]$.

(d) Rappelons la définition de la médiane d'un échantillon de données quantitatives. On appelle médiane la valeur m qui partage l'échantillon étudié en deux sous-groupes de même effectif, chacun tel que tous les éléments du premier groupe ont des valeurs inférieures ou égales à m et tous les éléments du second groupe ont des valeurs supérieures ou égales à m. Si l'effectif de l'échantillon est un nombre impair, et si les termes sont ordonnés par valeurs croissantes, la médiane est le terme de rang $(n+1)/2$. Si l'effectif est un nombre pair, toute valeur comprise entre les termes de rang $n/2$ et $n/2+1$ pourrait convenir. La valeur située au milieu de cet intervalle définit alors (par convention) la médiane de l'échantillon.

V.1.5 1. Notons I l'ensemble des indices k dans $[\![1, n]\!]$ tels que $x_k \notin [\bar{x} - 2\sigma, \bar{x} + 2\sigma]$. On ne va retenir dans la somme $\sum_{k=1}^{n} (x_k - \bar{x})^2$ que les indices pour lesquels $k \in I$. On sait qu'il y en a $n-p$, et pour un tel indice k, on a $(x_k - \bar{x})^2 \geqslant 4\sigma^2$. D'où l'inégalité demandée :

$$\sum_{k=1}^{n} (x_k - \bar{x})^2 \geqslant \sum_{k \in I} (x_k - \bar{x})^2 \geqslant (n-p)4\sigma^2.$$

Par définition de l'écart-type, on a $\sigma^2 = \frac{1}{n} \sum_{k=1}^{n} (x_k - \bar{x})^2 \geqslant \frac{4(n-p)}{n}\sigma^2$. En simplifiant par σ^2, on en déduit que $\frac{4(n-p)}{n} \leqslant 1$ et donc $p \geqslant 3n/4$. Il y a bien au moins $3/4$ des éléments de l'échantillon qui sont compris entre $\bar{x} - 2\sigma$ et $\bar{x} + 2\sigma$.

2. On reprend la même méthode, mais en remplaçant 2 par t. Si p est le nombre d'éléments de l'échantillon compris entre $\bar{x} - t\sigma$ et $\bar{x} + t\sigma$, on trouve que :

$$\sum_{k=1}^{n} (x_k - \bar{x})^2 \geqslant t^2(n-p)\sigma^2.$$

Utilisant la définition de l'écart-type, on trouve alors $\frac{t^2(n-p)}{n} \leqslant 1$ et donc :

$$p/n \geqslant (t^2 - 1)/t^2 = 1 - 1/t^2.$$

V.1.6 Commençons par donner une équation de D_1 et une équation de D_2. Pour D_1, c'est du cours : l'équation est $y = ax + b$ avec $a = \mathrm{Cov}(x, y)/\mathrm{Var}(x)$ et $b = \bar{y} - a\bar{x}$. Pour D_2, c'est aussi du cours, mais il faut échanger le rôle joué par x et par y. L'équation de D_2 est donc $x = a'y + b'$ avec $a' = \mathrm{Cov}(x, y)/\mathrm{Var}(y)$ et $b' = \bar{x} - a'\bar{y}$. On peut réécrire l'équation de D_2 sous la forme $y = (1/a')x - b'/a'$. Remarquons que les droites D_1 et D_2 passent toutes les

deux par le point moyen $(\bar{x}, \bar{y})$ du nuage. Elles coïncident donc si, et seulement si, elles ont la même pente, si, et seulement si, $\mathrm{Cov}(x,y)/\mathrm{Var}(x) = \mathrm{Var}(y)/\mathrm{Cov}(x,y)$, si, et seulement si, $\mathrm{Cov}(x,y)^2/[\mathrm{Var}(x)\mathrm{Var}(y)] = 1$, si, et seulement si, $|\mathrm{R}(x,y)| = 1$. On conclut en utilisant le fait que $|\mathrm{R}(x,y)| = 1$ si, et seulement si, les points du nuage sont alignés. En effet, d'après l'équation (8),

$$\sum_{i=1}^{n}(y_i - ax_i - b)^2 = \frac{\mathrm{Var}(x)\mathrm{Var}(y) - \mathrm{Cov}(x,y)^2}{\mathrm{Var}(x)} = \mathrm{Var}(y)\big(1 - \mathrm{R}(x,y)^2\big)\,.$$

Le membre de gauche est nul si, et seulement si, les points du nuage sont alignés. Le membre de droite est nul si, et seulement si, $|\mathrm{R}(x,y)| = 1$.

V.1.7 1. On a $\min\limits_{i\in[\![1,n]\!]} x_i \leqslant x_j$ pour tout j, donc $\min\limits_{i\in[\![1,n]\!]} x_i \leqslant \sqrt[n]{x_1\cdots x_n} = M$. De même, on a $x_j \leqslant \max\limits_{i\in[\![1,n]\!]} x_i$ pour tout j, et donc $\bar{x} \leqslant \max\limits_{i\in[\![1,n]\!]} x_i$.

2. On élève au carré et on forme la différence :

$$\big(\sqrt{x_1x_2}\big)^2 - \Big(\frac{x_1+x_2}{2}\Big)^2 = -\frac{x_1^2}{4} - \frac{x_2^2}{4} + \frac{x_1x_2}{2} = -\Big(\frac{x_1-x_2}{2}\Big)^2 \leqslant 0,$$

ce qui donne le résultat $\sqrt{x_1x_2} \leqslant \frac{x_1+x_2}{2}$ car $\sqrt{x_1x_2}$ et $\frac{x_1+x_2}{2}$ sont tous deux positifs.

3. On fait une récurrence sur n. Le résultat est vrai pour $n = 1$.
Soit $n \geqslant 2$ et $x = (x_i)_{i\in[\![1,n]\!]}$ un échantillon de nombres positifs. Si l'un des nombres est nul, alors $\sqrt[n]{x_1\cdots x_n}$ est nul et l'inégalité cherchée est vraie. Supposons dorénavant que tous les nombres sont strictement positifs. On note $y = \sqrt[n-1]{x_2\cdots x_n}$ et $z = \frac{x_2+\cdots+x_n}{n-1}$. On a $y \leqslant z$ par l'hypothèse de récurrence. On considère la fonction :

$$f(x) = x^{1/n}y^{1-1/n} - \frac{x}{n} - \frac{n-1}{n}z,$$

de telle sorte que $f(x_1) = \sqrt[n]{x_1\cdots x_n} - \frac{x_1+\cdots+x_n}{n}$. La fonction f est bien définie et dérivable sur $]0,+\infty[$, et

$$f'(x) = \frac{1}{n}x^{1/n-1}y^{1-1/n} - \frac{1}{n}.$$

La fonction f' est strictement positive sur $]0,y[$ et strictement négative sur $]y,+\infty[$, donc la fonction f est maximale en $x = y$ où elle vaut

$$f(y) = y - \frac{y}{n} - \frac{n-1}{n}z = \frac{n-1}{n}(y-z) \leqslant 0\,.$$

Donc f est négative sur $]0,+\infty[$, ce qui donne le résultat.

Module V.2 : Probabilités finies

V.2.1 Il y a $\binom{32}{5} = 201376$ mains possibles.

1. Il y a $\binom{8}{1}\binom{28}{1} = 224$ mains contenant un carré, car il y a $8 = \binom{8}{1}$ choix possibles de carrés, et $28 = \binom{28}{1}$ choix possibles pour la dernière carte.
2. Il y a $\binom{8}{1}\binom{4}{3}\binom{7}{1}\binom{4}{2} = 1344$ mains contenant un full, car il y a $8 = \binom{8}{1}$ choix possibles pour la hauteur du brelan, $\binom{4}{3}$ choix possibles de brelans de hauteur donnée, $\binom{7}{1}$ choix possibles pour la hauteur de la paire (une fois que la hauteur du brelan est fixée), et $\binom{4}{2}$ choix possibles de paires de hauteur donnée.
3. Il y a $\binom{8}{1}\binom{4}{3}\binom{28}{2} = 12096$ mains avec exactement trois cartes identiques, car il y a $\binom{8}{1}$ choix possibles pour la hauteur, $\binom{4}{3}$ choix possibles de brelans, et $\binom{28}{2}$ choix possibles pour les deux autres cartes. Mais parmi toutes ces mains, il y a les fulls, pour lesquelles on n'annonce pas un brelan, mais un full. Donc il y a $12096 - 1344 = 10752$ mains permettant d'annoncer un brelan.

V.2.2 1. Il y a 2^p applications de E dans F. Parmi toutes ces applications, certaines sont surjectives, d'autres pas. Pour qu'une application $f : E \to F$ ne soit pas surjective, il faut qu'un des éléments de F n'ait pas d'antécédent. Comme $F = \{y_1, y_2\}$, cela revient à demander que toutes les images de f soient égales à y_1, ou bien qu'elles soient toutes égales à y_2. Il y a donc seulement deux applications qui ne sont pas surjectives, et le nombre total d'applications surjectives est $2^p - 2$.

2. Notons $E = \{x_1, \dots, x_p\}$ avec $x_1 < \cdots < x_p$, $\mathcal{C}(E, F)$ l'ensemble des applications strictement croissantes de E dans F, et $\mathcal{P}_p(F)$ l'ensemble des parties de F à p éléments. On définit l'application :

$$\begin{array}{rl} \Psi : & \mathcal{C}(E,F) \to \mathcal{P}_p(F) \\ & f \mapsto f(E) \end{array}$$

- L'application Ψ est bien définie, car une application strictement croissante est injective, et donc $\mathrm{card}(f(E)) = p$.
- L'application Ψ est surjective. En effet, si $\{y_1, \dots, y_p\} \in \mathcal{P}_p(F)$, alors on commence par permuter les y_i de telle manière que $y_{\sigma(1)} < \cdots < y_{\sigma(p)}$. On vérifie ensuite que l'application $f : E \to F$ définie par $f(x_j) = y_{\sigma(j)}$ pour tout $j = 1, \dots, p$ est strictement croissante.
- L'application Ψ est injective. En effet, supposons que deux applications strictement croissantes f et g ont le même ensemble image $\{y_1, \dots, y_p\}$. On permute cet ensemble image de telle manière que $y_{\sigma(1)} < \cdots < y_{\sigma(p)}$. Comme $f(x_1) < \cdots < f(x_p)$, on peut identifier $f(x_j) = y_{\sigma(j)}$ pour tout j. De même $g(x_j) = y_{\sigma(j)}$. Donc $g = f$.

L'application Ψ étant bijective, on doit avoir :

$$\mathrm{card}(\mathcal{C}(E,F)) = \mathrm{card}(\mathcal{P}_p(F)) = \binom{n}{p}.$$

V.2.3 1. On a $A \subset A \cup B$, donc $\mathbb{P}(A \cup B) \geqslant \mathbb{P}(A) = 1/2$.

On ne peut pas proposer une meilleure minoration, car il se pourrait que $B \subset A$, et alors on aurait l'égalité $\mathbb{P}(A \cup B) = 1/2$.
On a $\mathbb{P}(A \cup B) \leqslant \mathbb{P}(A) + \mathbb{P}(B) = 5/6$. On ne peut pas proposer une meilleure majoration, car il se pourrait que A et B soient disjoints, et alors on aurait l'égalité $\mathbb{P}(A \cup B) = 5/6$.
On a $\mathbb{P}(A \cap B) \geqslant 0$, et on ne peut pas proposer une meilleure minoration, car il se pourrait que A et B soient disjoints, et alors on aurait l'égalité $\mathbb{P}(A \cap B) = 0$.
On a $A \cap B \subset B$, donc $\mathbb{P}(A \cap B) \leqslant \mathbb{P}(B) = 1/3$. On ne peut pas proposer une meilleure majoration, car il se pourrait que $B \subset A$, et donc $A \cap B = B$ et alors on aurait l'égalité $\mathbb{P}(A \cap B) = 1/3$.

2. On utilise la formule $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$.
Si A et B sont incompatibles, alors $A \cap B = \varnothing$ et donc :

$$\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) = 5/6.$$

Si $\mathbb{P}(A \cap B) = 1/4$, alors $\mathbb{P}(A \cup B) = 1/2 + 1/3 - 1/4 = 7/12$.

V.2.4 1. Notons A l'événement « il y a au moins un billet gagnant dans les k billets ». On va plutôt calculer la probabilité de l'événement contraire : A^c =« les k billets sont perdants ». Comme chaque billet a une probabilité $1 - 1/n$ d'être perdant, on trouve que :

$$\mathbb{P}(A^c) = \left(1 - \frac{1}{n}\right)^k ,$$

et donc :

$$\mathbb{P}(A) = 1 - \mathbb{P}(A^c) = 1 - \left(1 - \frac{1}{n}\right)^k .$$

On cherche le plus petit k tel que $\mathbb{P}(A) \geqslant 1/2$.

$$\mathbb{P}(A) \geqslant \frac{1}{2} \iff \left(1 - \frac{1}{n}\right)^k \leqslant \frac{1}{2} \iff k \ln\left(1 - \frac{1}{n}\right) \leqslant -\ln(2) .$$

On divise alors par $\ln(1 - 1/n)$ qui est négatif :

$$\mathbb{P}(A) \geqslant \frac{1}{2} \iff k \geqslant \frac{-\ln 2}{\ln(1 - 1/n)} .$$

Le plus petit k entier vérifiant cette inégalité est

$$k_n = \left[\frac{-\ln 2}{\ln(1 - 1/n)}\right] + 1 ,$$

où $[\cdot]$ est la fonction « partie entière ».

Application numérique :

- Si $n = 10$, alors $k_n = 7$.
- Si $n = 100$, alors $k_n = 69$.

2. On peut se servir du développement limité usuel $\ln(1 - x) = -x + o(x)$ au voisinage de 0, ce qui donne :

$$\frac{1}{n} k_n \underset{n \to \infty}{\longrightarrow} \ln(2) \simeq 0{,}69 .$$

V.2.5 Il y a $n!$ permutations possibles, et toutes les permutations sont équiprobables.
Il y a $(n-1)\times 1\times (n-2)!$ permutations qui permettent de trouver les deux volumes côte à côte dans le bon ordre. En effet, il y a $n-1$ choix possibles pour la position du volume 1 (seulement $n-1$, car la dernière position ne permet pas de placer le second volume juste à sa droite). Une fois la position du premier volume choisie, il y a 1 seul choix possible pour la position du second volume (juste à droite du premier volume). Une fois les deux volumes placés, il y a $(n-2)!$ possibilités de placer les $n-2$ livres restants.
La probabilité de trouver les deux volumes côte à côte dans le bon ordre est donc :

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

V.2.6 L'espace de probabilité est $\Omega=\{F,G\}^2$. Une réalisation se note $\omega=(\omega_1,\omega_2)$ où ω_1 est le sexe de l'enfant le plus âgé et ω_2 le sexe du plus jeune. La probabilité sur cet espace est uniforme.

1. On introduit les événements A =« il y a au moins une fille » et B =« il y a au moins un garçon ». On cherche $\mathbb{P}(B|A)$. Or $A=\{(FF),(FG),(GF)\}$, $B=\{(GG),(FG),(GF)\}$, et $A\cap B=\{(FG),(GF)\}$. Donc :
$$\mathbb{P}(B|A)=\frac{\mathbb{P}(A\cap B)}{\mathbb{P}(A)}=\frac{\mathrm{card}\,(A\cap B)}{\mathrm{card}\,(A)}=\frac{2}{3}\cdot$$
2. On introduit les événements C =« l'aîné une fille » et D =« le plus jeune est un garçon ». On cherche $\mathbb{P}(D|C)$. Or $C=\{(FF),(FG)\}$, $D=\{(GG),(FG)\}$, et $C\cap D=\{(FG)\}$. Donc :
$$\mathbb{P}(D|C)=\frac{\mathbb{P}(C\cap D)}{\mathbb{P}(C)}=\frac{\mathrm{card}\,(C\cap D)}{\mathrm{card}\,(C)}=\frac{1}{2}\cdot$$

V.2.7 Pour modéliser l'expérience consistant à tirer une carte au hasard, on prend comme espace fondamental Ω l'ensemble des 52 cartes, muni de la probabilité uniforme.
Soient v une valeur et c une couleur fixées. On introduit les événements A =« la carte tirée a pour valeur a » et B =« la carte tirée a pour couleur c ». On a $\mathrm{card}\,(A)=4$ (car il y a 4 cartes de valeur a), $\mathrm{card}\,(B)=13$ (car il y a 13 cartes de couleur c), et $\mathrm{card}\,(A\cap B)=1$ (car il y a une seule carte de valeur a et de couleur c). Comme $\mathbb{P}$ est la probabilité uniforme sur Ω :

$$\begin{aligned}\mathbb{P}(A\cap B) &= \frac{\mathrm{card}\,(A\cap B)}{\mathrm{card}\,(\Omega)}=\frac{1}{52},\\ \mathbb{P}(A)\mathbb{P}(B) &= \frac{\mathrm{card}\,(A)}{\mathrm{card}\,(\Omega)}\frac{\mathrm{card}\,(B)}{\mathrm{card}\,(\Omega)}=\frac{4}{52}\times\frac{13}{52}=\frac{1}{52}\cdot\end{aligned}$$

On a donc bien $\mathbb{P}(A\cap B)=\mathbb{P}(A)\mathbb{P}(B)$.

V.2.8 L'ensemble fondamental est $[\![1,6]\!]^2=\{1,2,\ldots,6\}^2$. Une réalisation se note $\omega=(\omega_1,\omega_2)$ où ω_1 est le résultat du dé noir et ω_2 le résultat du dé blanc. La probabilité sur cet espace est

uniforme. On introduit les événements :

$$A : \text{« le chiffre du dé noir est pair »},$$
$$B : \text{« le chiffre du dé blanc est pair »},$$
$$C : \text{« les chiffres des deux dés ont même parité »}.$$

On a $\text{card}\,(A) = 3 \times 6 = 18$, $\text{card}\,(B) = 6 \times 3 = 18$, et $\text{card}\,(C) = 6 \times 3 = 18$.
De plus $A \cap B = D :=$ « les deux résultats sont pairs ». On a $A \cap C = D$, $B \cap C = D$ et aussi $A \cap B \cap C = D$. Donc $\text{card}\,(A \cap B) = 3 \times 3 = 9$, $\text{card}\,(A \cap C) = 9$, $\text{card}\,(B \cap C) = 9$, et $\text{card}\,(B \cap C) = 9$. Au total :

$$\begin{aligned}\mathbb{P}(A \cap B) &= \frac{\text{card}\,(A \cap B)}{\text{card}\,(\Omega)} = \frac{9}{36} = \frac{1}{4} = \frac{1}{2} \times \frac{1}{2} \\ &= \frac{18}{36} \times \frac{18}{36} = \frac{\text{card}\,(A)}{\text{card}\,(\Omega)} \frac{\text{card}\,(B)}{\text{card}\,(\Omega)} = \mathbb{P}(A)\mathbb{P}(B)\,,\end{aligned}$$

et on trouve de même que :

$$\mathbb{P}(A \cap C) = \mathbb{P}(A)\mathbb{P}(C) \qquad \text{et} \qquad \mathbb{P}(B \cap C) = \mathbb{P}(B)\mathbb{P}(C)\,,$$

ce qui montre que les événements A, B et C sont deux à deux indépendants. Cependant :

$$\mathbb{P}(A \cap B \cap C) = \frac{\text{card}\,(D)}{\text{card}\,(\Omega)} = \frac{9}{36} = \frac{1}{4},$$
$$\mathbb{P}(A)\mathbb{P}(B)\mathbb{P}(C) = \frac{\text{card}\,(A)}{\text{card}\,(\Omega)} \frac{\text{card}\,(B)}{\text{card}\,(\Omega)} \frac{\text{card}\,(C)}{\text{card}\,(\Omega)} = \frac{18}{36} \times \frac{18}{36} \times \frac{18}{36} = \frac{1}{8}\,,$$

ce qui montre que les événements A, B et C ne sont pas mutuellement indépendants.

V.2.9 On note A l'événement « le joueur est Flamand » et B l'événement « le joueur est un amateur de frites hexagonales ». D'après l'énoncé,
- il y a 7 joueurs sur 11 qui sont Flamands, donc $\mathbb{P}(A) = 7/11$.
- si on sait qu'on a affaire à un Flamand, alors la probabilité que ce soit un mangeur de frites traditionnelles est $0{,}65$, donc $\mathbb{P}(B|A) = 1 - 0{,}65 = 0{,}35$.
- si on sait qu'on a affaire à un Wallon, alors la probabilité que ce soit un mangeur de frites traditionnelles est $0{,}75$, donc $\mathbb{P}(B|A^c) = 1 - 0{,}75 = 0{,}25$.

On cherche $\mathbb{P}(A|B)$. D'après la formule de Bayes :

$$\mathbb{P}(A|B) = \frac{\mathbb{P}(B|A)\mathbb{P}(A)}{\mathbb{P}(B|A)\mathbb{P}(A) + \mathbb{P}(B|A^c)\mathbb{P}(A^c)} = \frac{0{,}35 \times 7}{0{,}35 \times 7 + 0{,}25 \times 4} = \frac{2{,}45}{3{,}45} \simeq 71\%\,.$$

V.2.10 On note A l'événement « le moteur des essuie-glaces est en panne » B l'événement « la commande manuelle des essuie-glaces est en panne » et C l'événement « il pleut ».

1. L'événement en question est $A \cap B^c \cap C$, dont la probabilité est :

$$\mathbb{P}(A \cap B^c \cap C) = \mathbb{P}(A)\mathbb{P}(B^c)\mathbb{P}(C) = \frac{1}{10}\frac{1}{3} \times \frac{3}{4} = \frac{1}{4} = 2{,}5\%\,.$$

On a ici utilisé le fait que A, B et C sont indépendants, donc A, B^c et C le sont aussi.

2. On cherche $\mathbb{P}(A \cap B|C)$:

$$\mathbb{P}(A \cap B|C) = \frac{\mathbb{P}(A \cap B \cap C)}{\mathbb{P}(C)} = \mathbb{P}(A)\mathbb{P}(B) = \frac{1}{10} \times \frac{2}{3} = \frac{1}{15} \simeq 6{,}67\% \,.$$

V.2.11 Pour modéliser ce problème, considérons un espace de probabilité avec les événements suivants. Pour $i \in [\![1, 4]\!]$, T_i est l'événement « le parapluie est dans le i-ème tiroir ». L'énoncé nous dit que $\mathbb{P}(T_1 \cup T_2 \cup T_3 \cup T_4) = p$, et on cherche la probabilité

$$\mathbb{P}(T_4 \mid T_1^c \cap T_2^c \cap T_3^c).$$

On calcule alors :

$$\mathbb{P}(T_4 \mid T_1^c \cap T_2^c \cap T_3^c) = \frac{\mathbb{P}(T_4 \cap T_1^c \cap T_2^c \cap T_3^c)}{\mathbb{P}(T_1^c \cap T_2^c \cap T_3^c)} = \frac{\mathbb{P}(T_4)}{1 - \mathbb{P}(T_1) - \mathbb{P}(T_2) - \mathbb{P}(T_3)}.$$

De plus, on a $\mathbb{P}(T_i|T_1 \cup T_2 \cup T_3 \cup T_4) = 1/4$ pour tout $i \in [\![1, 4]\!]$.
Comme $p = \mathbb{P}(T_1) + \cdots + \mathbb{P}(T_4)$, on en déduit que $\mathbb{P}(T_i) = p/4$. Ainsi,

$$\mathbb{P}(T_4 \mid T_1^c \cap T_2^c \cap T_3^c) = \frac{p/4}{1 - 3p/4} = \frac{p}{4 - 3p}.$$

Module V.3 : Variables aléatoires

V.3.1 On choisit pour ensemble fondamental $\Omega = [\![1,6]\!]^2$ que l'on munit de la probabilité uniforme puisque les deux dés sont équilibrés. Remarquons que le cardinal de Ω vaut 36. X prend ses valeurs dans $[\![1,6]\!]$. L'événement $\{X=1\}$ est égal au singleton $\{(1,1)\}$ et donc $\mathbb{P}(X=1)=1/36$. De même, on a

$$\mathbb{P}(X=2)=\mathbb{P}\big(\{(1,2),(2,1),(2,2)\}\big)=\frac{3}{36}=\frac{1}{12}\,,$$

et $\mathbb{P}(X=3)=5/36$, $\mathbb{P}(X=4)=7/36$, $\mathbb{P}(X=5)=9/36=1/4$, $\mathbb{P}(X=6)=11/36$.

V.3.2 On note V_k l'événement « la porte n'est toujours pas ouverte après k essais ». Il s'agit d'une suite décroissante d'événements, avec $\mathbb{P}(V_0)=1$. La probabilité p_k qu'il faille exactement k essais pour ouvrir la porte est, pour $k \geqslant 1$:

$$p_k=\mathbb{P}(V_k^c\cap V_{k-1})=\mathbb{P}(V_{k-1})-\mathbb{P}(V_k)\,.$$

Pour tout $k\geqslant 1$, on a :

$$\mathbb{P}(V_k)=\mathbb{P}(V_k|V_{k-1})\mathbb{P}(V_{k-1})\,.$$

Or, si V_{k-1} est vraie, alors au $k^{ème}$ essai, le concierge tire une clé parmi les $n-(k-1)$ qui restent, et donc :

$$\mathbb{P}(V_k|V_{k-1})=1-\frac{1}{n-k+1}\,,$$

et il vient :

$$\mathbb{P}(V_k)=\mathbb{P}(V_k|V_{k-1})\mathbb{P}(V_{k-1})=\left(1-\frac{1}{n+1-k}\right)\mathbb{P}(V_{k-1})=\frac{n-k}{n+1-k}\mathbb{P}(V_{k-1})\,,$$

si bien que, pour tout $k\in[\![0,n]\!]$:

$$\mathbb{P}(V_k)=\prod_{j=1}^{k}\frac{n-j}{n+1-j}=\frac{n-k}{n}\,,$$

et $\mathbb{P}(V_k)=0$ pour tout $k\geqslant n$. On trouve donc que la probabilité p_k qu ?il faille exactement k essais pour ouvrir la porte est :

$$p_k=\mathbb{P}(V_{k-1})-\mathbb{P}(V_k)=\frac{n-k+1}{n}-\frac{n-k}{n}=\frac{1}{n}\,,$$

pour tout $k\in[\![1,n]\!]$. C'est la probabilité uniforme sur $[\![1,n]\!]$! Le nombre moyen d'essais nécessaires est :

$$\sum_{k=1}^{n}kp_k=\frac{n(n-1)}{2n}=\frac{n-1}{2}\cdot$$

V.3.3 On note A_k l'événement « il y a rencontre au $k^{ème}$ tirage ». On cherche donc $p_n=\mathbb{P}(\cup_{k=1}^n A_k)$ et on utilise pour cela la formule d'inclusion-exclusion :

$$p_n=\mathbb{P}\left(\cup_{k=1}^n A_k\right)=\sum_{k=1}^{n}(-1)^{k+1}\sum_{1\leqslant i_1<\cdots<i_k\leqslant n}\mathbb{P}(A_{i_1}\cap\cdots\cap A_{i_k})\,.$$

Il y a $n!$ façons de tirer les n boules. Si on fixe la sortie des boules $i_1, \dots, i_k$, alors il reste $(n-k)!$ façons de tirer les $n-k$ autres boules. Comme les tirages sont équiprobables, on a :

$$\mathbb{P}(A_{i_1} \cap \cdots \cap A_{i_k}) = \frac{(n-k)!}{n!}\,,$$

et il vient :

$$\begin{aligned} p_n &= \sum_{k=1}^{n}(-1)^{k+1} \sum_{1\leqslant i_1<\cdots<i_k\leqslant n} \frac{(n-k)!}{n!} = \sum_{k=1}^{n}(-1)^{k+1}\binom{n}{k}\frac{(n-k)!}{n!} \\ &= \sum_{k=1}^{n}(-1)^{k+1}\frac{n!}{k!(n-k)!}\frac{(n-k)!}{n!} = \sum_{k=1}^{n}(-1)^{k+1}\frac{1}{k!}\,. \end{aligned}$$

On a donc :

$$p_n = 1 - \sum_{k=0}^{n}(-1)^k\frac{1}{k!}\,.$$

Lorsque $n \to +\infty$ on trouve que $p_n \to 1-\exp(-1) \simeq 0{,}63$.

V.3.4 1. Lorsque le fumeur s'aperçoit qu'une boîte est vide, il peut rester r allumettes dans l'autre boîte, avec $r \in [\![0, N]\!]$.
Pour qu'il reste exactement r allumettes dans l'autre boîte lorsque le fumeur s'aperçoit qu'une boîte est vide, il faut que le fumeur ait fait en tout $N+(N-r)+1$ tirages : N tirages de la poche vide, $N-r$ tirages de l'autre poche, et 1 ultime tirage de la poche vide, pour s'apercevoir qu'elle est vide. Si le dernier tirage (qui permet de s'apercevoir que la boîte est vide) est dans la poche droite, alors ce tirage était le $N+1^{ème}$ de la poche droite, et les N tirages précédents dans la poche droite ont pu se dérouler n'importe quand lors des $2N-r$ premiers tirages. Donc la probabilité qu'il reste exactement r allumettes dans la boîte de la poche gauche lorsque le fumeur s'aperçoit que la boîte de la poche droite est vide est :

$$2^{-(2N-r+1)}\binom{2N-r}{N}\,.$$

De même, la probabilité qu'il reste exactement r allumettes dans la boîte de la poche droite lorsque le fumeur s'aperçoit que la boîte de la poche gauche est vide est :

$$2^{-(2N-r+1)}\binom{2N-r}{N}\,,$$

et donc :

$$u_r = 2^{r-2N}\binom{2N-r}{N}\,.$$

Comme le nombre d'allumettes restant dans l'autre boîte est compris entre 0 et N, on doit avoir :

$$\sum_{r=0}^{N} u_r = 1\,,$$

ce qu'on peut vérifier avec l'expression de u_r et la formule du binôme.

2. On a :

$$u = u_0 = 2^{-2N}\binom{2N}{N}\,.$$

Avec la formule de Stirling :

$$\binom{2N}{N} = \frac{(2N)!}{(N!)^2} \sim \frac{(2N/e)^{2N}\sqrt{4\pi N}}{(N/e)^{2N}2\pi N} = \frac{2^{2N}}{\sqrt{\pi N}},$$

et donc :

$$u \sim \frac{1}{\sqrt{\pi N}}.$$

V.3.5 1. On note A_k l'aire de la couronne k, et A l'aire totale. Par les hypothèses d'équiprobabilité faites dans l'énoncé, on a $\mathbb{P}(X=k) = A_k/A$ pour k compris entre 1 et 10. Pour la couronne k, le cercle extérieur est de rayon $11-k$ et le cercle intérieur de rayon $10-k$ (un petit dessin pourra aider pour faire attention à l'inversion entre l'ordre des cercles et les rayons). On a donc, en cm^2, $A_k = \pi((11-k)^2 - (10-k)^2) = \pi(21-2k)$ et $A = \pi 10^2$. On en déduit que

$$\mathbb{P}(X=k) = \frac{21-2k}{100}.$$

2. Notons Y la variable aléatoire correspondant au gain du joueur. Y prend ses valeurs dans $\{-2, 6, 7, 8, 9, 10\}$. L'événement $\{Y=-2\}$ est égal à l'événement $\{X \leqslant 5\}$, et donc

$$\mathbb{P}(Y=-2) = \sum_{k=1}^{5} \mathbb{P}(X=k) = \frac{5\times 21 - 5\times 6}{100} = \frac{75}{100},$$

d'après le résultat de la question précédente. D'autre part, pour $k \in [\![6, 10]\!]$, on a $\mathbb{P}(Y=k) = \mathbb{P}(X=k)$. On en déduit l'espérance de Y :

$$\mathbb{E}[Y] = -2\times 75/100 + \big(6\times 9 + 7\times 7 + 8\times 5 + 9\times 3 + 10\times 1\big)/100 = 3/10.$$

L'espérance est positive. Le jeu est favorable au joueur. En moyenne, il peut espérer gagner 0,3 euros par partie.

V.3.6 1. X prend ses valeurs dans $[\![1, 6]\!]$.

Par hypothèse, il existe un réel a tel que $\mathbb{P}(X=k) = ka$. Maintenant, puisque la loi de X est une loi de probabilité, on a : $1 = \sum_{k=1}^{6} \mathbb{P}(X=k) = a\frac{6\times 7}{2}$ et donc $a = 1/21$.

La loi de X est donc :

$$\mathbb{P}(X=k) = \frac{k}{21}, \quad k \in [\![1, 6]\!].$$

Son espérance est :

$$\mathbb{E}[X] = \sum_{k=1}^{6} k\mathbb{P}(X=k) = \frac{1}{21}\sum_{k=1}^{6} k^2 = \frac{1}{21}\frac{6(6+1)(2\times 6+1)}{6} = \frac{13}{3}.$$

2. Y prend ses valeurs dans $\{1, 1/2, 1/3, 1/4, 1/5, 1/6\}$, et sa loi est donnée par :

$$\mathbb{P}\Big(Y = \frac{1}{k}\Big) = \frac{k}{21}, \quad k \in [\![1, 6]\!].$$

Son espérance est :

$$\mathbb{E}[Y] = \sum_{k=1}^{6} \frac{1}{k}\mathbb{P}\Big(Y=\frac{1}{k}\Big) = \sum_{k=1}^{6} \frac{1}{21} = \frac{6}{21} = \frac{2}{7}.$$

V.3.7 On considère la fonction

$$\mathcal{E}(c) = \mathbb{E}[(X-c)^2]\,.$$

C'est un polynôme du second degré :

$$\mathcal{E}(c) = c^2 - 2\mathbb{E}[X]c + \mathbb{E}[X^2]\,,$$

dont le coefficient dominant est strictement positif. Il admet donc un unique minimum au point où $\mathcal{E}'(c) = 0$. Ce point est $c = \mathbb{E}[X]$ et la valeur du minimum est alors $\mathrm{Var}(X)$.

V.3.8 La somme dans (29) est finie, car X est à valeurs dans un sous-espace fini de $\mathbb{N}$ donc $\mathbb{P}(X > n) = 0$ à partir d'un certain rang. Soit $M \in \mathbb{N}$ tel que $\mathbb{P}(X > M) = 0$. On décompose la somme qui constitue la définition de l'espérance :

$$\mathbb{E}[X] = \sum_{k=0}^{M} k\mathbb{P}(X=k) = \sum_{k=1}^{M} k\mathbb{P}(X=k) = \sum_{k=1}^{M}\sum_{n=0}^{k-1} \mathbb{P}(X=k)\,,$$

puis on inverse les sommes :

$$\mathbb{E}[X] = \sum_{n=0}^{M-1}\sum_{k=n+1}^{M} \mathbb{P}(X=k) = \sum_{n=0}^{M-1} \big(\mathbb{P}(X>n) - \mathbb{P}(X>M)\big) = \sum_{n=0}^{M-1} \mathbb{P}(X>n)\,,$$

ce qu'il fallait démontrer.

V.3.9

1. Supposons que les cartes dans le paquet soient numérotées de 1 à 52. Le devin annonce les cartes dans un autre ordre, c'est-à-dire qu'il annonce une permutation de $[\![1,52]\!]$. On se place donc sur $(\mathcal{S}_{52}, \mathcal{P}(\mathcal{S}_{52}))$, où $\mathcal{S}_{52}$ est l'ensemble des permutations de taille 52, avec la probabilité uniforme.

2. Le nombre de cartes que le devin trouvera est :

$$X = \max\{k \mid \omega(1) < \omega(2) < \cdots < \omega(k)\}\,.$$

On a pour $k \in [\![1,52]\!]$

$$\begin{aligned}\mathbb{P}(X \geqslant k) &= \sum_{1\leqslant j_1<\cdots<j_k\leqslant 52} \mathbb{P}(\{\omega \mid \omega(1)=j_1,\ldots,\omega(k)=j_k\}) \\ &= \sum_{1\leqslant j_1<\ldots<j_k\leqslant 52} \frac{(52-k)!}{52!} = \binom{52}{k}\frac{(52-k)!}{52!} = \frac{1}{k!}\,.\end{aligned}$$

On utilise le fait que, comme X est une v.a. entière positive, on a :

$$\mathbb{E}[X] = \sum_{k\geqslant 0} \mathbb{P}(X>k) = \sum_{k\geqslant 1} \mathbb{P}(X\geqslant k).$$

Ainsi, le devin trouvera en moyenne

$$\mathbb{E}[X] = \sum_{k=1}^{52} \frac{1}{k!} \simeq \exp(1) - 1 \simeq 1{,}72$$

cartes.

V.3.10 1. En utilisant les informations de l'énoncé sur l'héritage des gènes, on trouve

$$\mathbb{P}(E=1|(P,M)=(1,1))=1,$$
$$\mathbb{P}(E=1|(P,M)=(1,2))=1/2,$$
$$\mathbb{P}(E=1|(P,M)=(2,1))=1/2,$$
$$\mathbb{P}(E=1|(P,M)=(2,2))=1/4,$$

et les cinq autres probabilités conditionnelles sont nulles.

2. On calcule $\mathbb{P}(E=1)$ par la formule des probabilités totales :

$$\mathbb{P}(E=1)=\sum_{i,j=1}^{3}\mathbb{P}(E=1|(P,M)=(i,j))\mathbb{P}((P,M)=(i,j))\,.$$

Les procréations étant supposées aléatoires, on a aussi :

$$\mathbb{P}((P,M)=(i,j))=u_i(n)u_j(n).$$

On en déduit

$$\begin{aligned}\mathbb{P}(E=1)&=u_1(n)^2+\frac{1}{2}u_1(n)u_2(n)+\frac{1}{2}u_2(n)u_1(n)+\frac{1}{4}u_2(n)^2\\&=\big(u_1(n)+\frac{1}{2}u_2(n)\big)^2\,.\end{aligned}$$

Il est facile de calculer $\mathbb{P}(E=3)$. Par symétrie des rôles de A et B, on a en effet

$$\mathbb{P}(E=3)=\big(u_3(n)+\frac{1}{2}u_2(n)\big)^2\,.$$

Enfin,

$$\begin{aligned}\mathbb{P}(E=2)&=1-\mathbb{P}(E=1)-\mathbb{P}(E=3)\\&=1-\big(u_1(n)+\frac{1}{2}u_2(n)\big)^2-\big(u_3(n)+\frac{1}{2}u_2(n)\big)^2\,.\end{aligned}$$

3. On a $u_1(n+1)=\mathbb{P}(E=1)=\theta(n)^2$. De plus, $u_1(n)+u_2(n)+u_3(n)=1$, ce qui fait que $u_3(n)+\frac{1}{2}u_2(n)=1-\theta(n)$. Ainsi, $u_3(n+1)=(1-\theta(n))^2$ et $u_2(n+1)=1-\theta(n)^2-(1-\theta(n))^2$.

4. Calculons $\theta(n+1)$ en fonction de $\theta(n)$ pour $n\geqslant 1$.
On a $\theta(n+1)=u_1(n+1)+\frac{1}{2}u_2(n+1)=\theta(n)^2+\frac{1}{2}\big[1-\theta(n)^2-(1-\theta(n))^2\big]=\theta(n)$.
Ainsi, pour $n\geqslant 1$, on a $\theta(n+1)=\theta(n)$ et donc d'après la question précédente, $u_i(n+1)=u_i(n)$. La proportion de malades dans la population ne varie plus !

V.3.11 1. Y_n ne prend que deux valeurs, $1/n$ et $1+1/n$. On a en outre : $\{Y_n=1/n\}=$ « aucune vache n'est malade ». Donc $\mathbb{P}(Y_n=1/n)=0{,}85^n$. Comme la loi de Y est une loi de probabilité, on en déduit que $\mathbb{P}(Y_n=1+1/n)=1-(0{,}85)^n$. Le calcul de l'espérance donne :

$$\mathbb{E}[Y_n]=\frac{0{,}85^n}{n}+\frac{n+1}{n}(1-0{,}85^n)=1+\frac{1}{n}-0{,}85^n\,.$$

2. La fonction f est dérivable sur $]0,+\infty[$, et $f'(x) = \frac{1+ax}{x}$. $f'(x)$ est donc du signe de $1+ax$, ce qui permet de dire que f est croissante sur $]0,-1/a[$, et décroissante ensuite. La limite de f en $+\infty$ est $-\infty$, il en est de même en 0. En calculant les valeurs successives de $f(n)$, on a $f(17) > 0{,}07$ et $f(18) < -0{,}03$. 17 est donc la plus grande valeur entière pour laquelle $f(n)$ est positive. En outre, $f(1) < 0$ alors que $f(2) > 0$. L'ensemble d'entiers recherché est donc $[\![2,17]\!]$.
3. On a :

$$\mathbb{E}[Y_n] < 1 \iff 1 + \frac{1}{n} - 0{,}85^n < 1 \iff 0{,}85^n > \frac{1}{n} \iff n \ln 0{,}85 > -\ln n\,.$$

Par suite, $\mathbb{E}[Y_n] < 1 \iff f(n) > 0$. L'étude précédente montre que les entiers n pour lesquels $f(n) > 0$ est $[\![2,17]\!]$. On a intérêt à choisir la deuxième méthode si, et seulement si, il y a de 2 à 17 vaches dans l'étable.