Devoir surveillé 5

▸ Exercice 1 : arithmétique de la suite de Fibonacci

Dans tout le problème, on note $(F_n)_{n\in\mathbf{N}}$ la suite définie par $F_0 = 0$, $F_1 = 1$ et pour tout $n \in \mathbf{N}$, $F_{n+2} = F_n + F_{n+1}$.

Partie I. Première propriétés de la suite de Fibonacci

1. Montrer que $(F_n)_{n\geqslant 2}$ est strictement croissante.
2. En déduire la limite de $(F_n)_n$.
3. Montrer qu'il existe deux réels α, β, que l'on déterminera, tels que

$$\forall n \in \mathbf{N}, \quad F_n = \alpha\left(\frac{1+\sqrt{5}}{2}\right)^n + \beta\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Retrouver alors la limite de (F_n).

Partie II. Arithmétique de la suite de Fibonacci

4. a. Prouver que pour tout $n \in \mathbf{N}$, $F_{n+1}^2 - F_nF_{n+2} = (-1)^n$.
   b. En déduire que pour tout $n \in \mathbf{N}$, F_n et F_{n+1} sont premiers entre eux.
5. a. Prouver que pour tout $n \in \mathbf{N}^*$ et tout $p \in \mathbf{N}$, $F_{n+p} = F_{n-1}F_p + F_nF_{p+1}$.
   Indication : on pourra procéder par récurrence sur p.
   b. En déduire que pour $(n, p) \in \mathbf{N}^* \times \mathbf{N}$, $F_{n+p} \wedge F_n = F_n \wedge F_p$.
   c. Montrer alors que pour tout $(n, p, k) \in \mathbf{N}^3$, $F_{n+kp} \wedge F_p = F_n \wedge F_p$.
6. En utilisant l'algorithme d'Euclide, prouver que $\forall (n, p) \in \mathbf{N}^2$, $F_n \wedge F_p = F_{n\wedge p}$.
   En déduire que si p divise n, alors F_p divise F_n.
7. Montrer que si F_n est premier, alors soit $n = 4$, soit n est un nombre premier impair.

Partie III. Puissances de 2 dans la suite de Fibonacci

Dans cette partie, on cherche pour quelles valeurs de n le $n^{\text{ème}}$ nombre de Fibonacci est une puissance de 2, c'est-à-dire qu'il existe $k \in \mathbf{N}$ tel que $F_n = 2^k$.

8. Déterminer tous les entiers naturels n pour lesquels F_n est une puissance de 2 inférieure ou égale à 8.
9. Soit $n \in \mathbf{N}$. On suppose qu'il existe $k > 3$ tel que $F_n = 2^k$.
   a. À l'aide de la question 6, montrer que n est un multiple de 6. On note alors m l'entier tel que $n = 6m$.
   b. Montrer que F_m est une puissance de 2. En notant que $F_3 = 2$, sur le même principe qu'à la question précédente, prouver que 3 divise m.
   c. Prouver que F_n est divisible par F_9, et aboutir à une contradiction.
10. Donner la liste de toutes les valeurs de n pour lesquelles F_n est une puissance de 2.

▸ Exercice 2 : théorème du point fixe de Banach-Picard

Dans tout l'exercice, I désigne un intervalle de $\mathbf{R}$. On ne suppose pas nécessairement I borné, mais on suppose que si I possède une borne supérieure (resp. une borne inférieure), alors $\sup I \in I$ (resp. $\inf I \in I$).
Soit $f : I \to I$ une fonction telle qu'il existe $k \in [0,1[$ tel que

$$\forall (x,y) \in I^2,\ |f(x) - f(y)| \leqslant k|x-y|.$$

On dit alors que f est k-*contractante.* Dans toute la suite, on considère $k \in [0,1[$ comme ci-dessus.

On souhaite prouver le résultat suivant : f possède un unique point fixe ℓ, et pour tout $a \in I$, la suite définie par $\begin{cases} u_0 = a \\ \forall n \in \mathbf{N}, u_{n+1} = f(u_n) \end{cases}$ est convergente de limite ℓ.

1. Montrer que f est continue sur I.
2. Prouver que f possède au plus un point fixe.

Dans la suite, on considère $a \in I$, et on note $(u_n)_n$ la suite définie par $u_0 = a$ et $\forall n \in \mathbf{N}$, $u_{n+1} = f(u_n)$.

3. Montrer que pour tout $n \in \mathbf{N}$, $|u_{n+1} - u_n| \leqslant k^n |u_1 - u_0|$.
4. Prouver alors que pour tout $n \in \mathbf{N}$, $|u_n - u_0| \leqslant \dfrac{1}{1-k}|u_1 - u_0|$.
5. Montrer qu'il existe $\ell \in I$ et $\varphi : \mathbf{N} \to \mathbf{N}$, strictement croissante, telle que $u_{\varphi(n)} \underset{n\to+\infty}{\longrightarrow} \ell$.
6. En remarquant que pour tout $n \in \mathbf{N}$, $f(\ell) - \ell = f(\ell) - f\left(u_{\varphi(n)}\right) + f\left(u_{\varphi(n)}\right) - u_{\varphi(n)} + u_{\varphi(n)} - \ell$, vérifier que ℓ est un point fixe de f.
7. Prouver que pour tout $n \in \mathbf{N}$, $|u_n - \ell| \leqslant k^n |u_0 - \ell|$.
8. Conclure.
9. **Application** : soit f une fonction de classe $\mathscr{C}^1$ sur un intervalle I telle qu'il existe $k \in [0,1[$ telle que $\forall x \in I$, $|f'(x)| \leqslant k$.
   a. En remarquant que $\forall (x,y) \in I^2$, $f(y) - f(x) = \displaystyle\int_x^y f'(t)\,dt$, montrer que f est k-contractante.
   b. Soit $f : \left|\begin{array}{ccc} \mathbf{R}_+^* & \longrightarrow & \mathbf{R}_+^* \\ x & \longmapsto & \dfrac{x}{2} + \dfrac{1}{x} \end{array}\right.$. Montrer que $[1,2]$ est stable par f et que $f_{|[1,2]}$ est k-contractante pour une valeur de $k \in [0,1[$ à déterminer.
   c. En déduire que la suite (u_n) définie par $\begin{cases} u_0 = 2 \\ \forall n \in \mathbf{N},\ u_{n+1} = \frac{u_n}{2} + \frac{1}{u_n} \end{cases}$ est convergente, et déterminer sa limite.

▸ Exercice 3 : groupes finis à un seul automorphisme

Dans tout le problème, $(G, \cdot)$ est un groupe fini d'élément neutre e.
On rappelle qu'un automorphisme de G est un morphisme bijectif de G dans G et on note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.
On note $\mathcal{Z}(G) = \{g \in G \mid \forall h \in G,\ gh = hg\}$.

Partie I. Automorphismes d'un groupe

1. Montrer que $\mathrm{Aut}(G)$ est un sous-groupe de $(\mathfrak{S}(G), \circ)$, l'ensemble des bijections de G dans G.
2. Prouver que si G est de cardinal inférieur ou égal à 2, alors $\mathrm{Aut}(G) = \{\mathrm{id}_G\}$.
3. Soit $g \in G$. On note $\varphi_g : \left|\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & gxg^{-1} \end{array}\right.$.
   a. Montrer que $\varphi_g \in \mathrm{Aut}(G)$.
   b. Montrer que $\varphi_g = \mathrm{id}_G$ si et seulement si $g \in \mathcal{Z}(G)$.
4. Montrer que $g \mapsto g^{-1}$ est un automorphisme de G si et seulement si G est abélien.

Partie II. Groupes dont tous les carrés sont triviaux.
Dans cette partie, on suppose que $\mathrm{Card}(G) \geqslant 3$ et que pour tout $g \in G$, $g^2 = e$.

5. Montrer que G est abélien, et pour tout $g \in G$, exprimer g^{-1} en fonction de g.

Une partie A de G est dite génératrice de G si le seul sous-groupe de G qui contient A est G lui-même.
On note $\mathrm{Gen}(G)$ l'ensemble des parties de G qui sont génératrices de G.

6. Montrer que $\mathrm{Gen}(G)$ est non vide.
7. En déduire qu'il existe $A_0 \in \mathrm{Gen}(G)$ tel que $\mathrm{Card}(A_0) = \min\{\mathrm{Card}(A),\ A \in \mathrm{Gen}(G)\}$.
   Un tel A_0 est appelé une partie génératrice minimale de G.

Dans toute la suite de cette partie, A_0 désigne une partie génératrice minimale de G, on note n son cardinal, et on note $A_0 = \{g_1, \ldots, g_n\}$.

8. Prouver que $n \geqslant 2$ et que si $a \in A_0$, alors $A_0 \setminus \{a\}$ n'est pas génératrice de G.
9. Prouver que $\{g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n},\ (\varepsilon_1, \ldots, \varepsilon_n) \in \{0,1\}^n\}$ est un sous-groupe de G qui contient A_0.
10. En déduire que pour tout $g \in G$, il existe un unique n-uplet $(\varepsilon_1, \ldots, \varepsilon_n) \in \{0,1\}^n$ tel que $g = g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n}$.
11. Prouver que $\varphi : \left|\begin{array}{ccc} G & \longrightarrow & G \\ g = g_1^{\varepsilon_1} g_2^{\varepsilon_2} g_3^{\varepsilon_3} \cdots g_n^{\varepsilon_n} & \longmapsto & g_1^{\varepsilon_2} g_2^{\varepsilon_1} g_3^{\varepsilon_3} \cdots g_n^{\varepsilon_n} \end{array}\right.$ est un automorphisme de G.

Partie III. Groupes finis tels que $\mathrm{Aut}(G) = \{\mathrm{id}_G\}$**.**

12. En exploitant les résultats des parties I et II, montrer que la réciproque de la question 2 est vraie, c'est-à-dire que si $\mathrm{Aut}(G) = \{\mathrm{id}_G\}$, alors $\mathrm{Card}(G) \leqslant 2$.

▸ Question subsidiaire : à n'aborder que si vous avez très bien réussi tout le reste.

On définit une fonction f sur $\mathbf{R}$ de la manière suivante : si $x \in \mathbf{R}$ est irrationnel, alors $f(x) = 0$, et si x est rationnel, $f(x) = \dfrac{1}{\min\{q \in \mathbf{N}^* \mid qx \in \mathbf{Z}\}}$.
Déterminer l'ensemble des points en lesquels f est continue.

CORRECTION DU DEVOIR SURVEILLÉ 5

▸ Exercice 1 : arithmétique de la suite de Fibonacci

Partie I. Première propriétés de la suite de Fibonacci.

1. On a $F_2 = F_0 + F_1 = 1$, $F_3 = F_1 + F_2 = 2$ et $F_4 = F_2 + F_3 = 3$.
Prouvons alors par récurrence double sur $n \geqslant 2$, que $F_{n+1} > F_n$.
Nous venons donc de prouver que $F_3 > F_2$ et $F_4 > F_3$, donc la récurrence est initialisée.
Soit $n \geqslant 2$ tel que $F_{n+1} > F_n$ et $F_{n+2} > F_{n+1}$. Alors

$$F_{n+3} = F_{n+1} + F_{n+2} > F_n + F_{n+1} = F_{n+2}.$$

Donc par le principe de récurrence double, pour tout $n \geqslant 2$, $F_{n+1} > F_n$, si bien que $(F_n)_{n\geqslant 2}$ est strictement croissante.

⚠ Attention !
Qui dit récurrence double dit initialisation double.

2. Une récurrence double sans difficultés prouve que pour tout $n \in \mathbf{N}$, $F_n \in \mathbf{N}$.
On serait alors tentés de dire que nous avons un résultat qui a été prouvé au sujet des extractrices qui nous dit que si (u_n) est une suite strictement croissante d'entiers, alors pour tout $n \in \mathbf{N}$, $u_n \geqslant n$.
Mais ici il faut être un peu prudent, puisque ce résultat ne s'applique pas tel quel car (F_n) n'est croissante qu'à partir d'un certain rang. Et de fait, $F_2 = 1 < 2$.
En revanche, on peut par exemple dire que $(F_{n+2})_{n\in\mathbf{N}}$ est strictement croissante et à valeurs entières, si bien que pour tout $n \in \mathbf{N}$, $F_{n+2} \geqslant n$, et donc pour $n \geqslant 2$, $F_n \geqslant n-2$, si bien que $\boxed{\lim_{n\to+\infty} F_n = +\infty.}$

Alternative
On aurait aussi pu directement prouver par récurrence (simple si on utilisait la question précédente) que pour tout $n \in \mathbf{N}$, $F_n \geqslant n-2$.

3. La relation $F_{n+2} = F_n + F_{n+1}$ signifie que la suite (F_n) est récurrente linéaire d'ordre 2.
Son polynôme caractéristique est $X^2 - X - 1$, qui possède deux racines réelles distinctes égales à $\dfrac{1+\sqrt{5}}{2}$ et $\dfrac{1-\sqrt{5}}{2}$.
D'après un résultat du cours, il existe alors deux réels α et β tels que pour tout $n \in \mathbf{N}$, $F_n = \alpha\left(\dfrac{1+\sqrt{5}}{2}\right)^n + \beta\left(\dfrac{1-\sqrt{5}}{2}\right)^n$.
On a alors $F_0 = 0 = \alpha + \beta$ si bien que $\beta = -\alpha$.
Et $1 = F_1 = \alpha\dfrac{1+\sqrt{5}}{2} + \beta\dfrac{1-\sqrt{5}}{2} = \alpha\left(\dfrac{1+\sqrt{5}}{2} - \dfrac{1-\sqrt{5}}{2}\right) = \alpha\sqrt{5}$.
On en déduit que $\alpha = \dfrac{1}{\sqrt{5}}$, et donc pour tout $n \in \mathbf{N}$,

$$\boxed{F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n.}$$

Puisque $\frac{1+\sqrt{5}}{2} > 1$, $\left(\frac{1+\sqrt{5}}{2}\right)^n \underset{n\to+\infty}{\longrightarrow} +\infty$.
De même, $-1 < \frac{1-\sqrt{5}}{2} < 1$, et donc $\left(\frac{1-\sqrt{5}}{2}\right)^n \underset{n\to+\infty}{\longrightarrow} 0$, si bien que $\boxed{\lim_{n\to+\infty} F_n = +\infty.}$

Partie II. Arithmétique de la suite de Fibonacci

4.a. Prouvons le résultat par récurrence simple sur n.
Pour $n = 0$, on a $F_1^2 - F_0F_2 = 1 = (-1)^0$.
Ssoit $n \in \mathbf{N}$ tel que $F_{n+1}^2 - F_nF_{n+2} = (-1)^n$. Alors

$$\begin{aligned} F_{n+2}^2 - F_{n+1}F_{n+3} &= F_{n+2}^2 - F_{n+1}(F_{n+2} + F_{n+1}) \\ &= F_{n+2}\left(F_{n+2} - F_{n+1}\right) - F_{n+1}^2 \\ &= F_{n+2}F_n - F_{n+1}^2 = -(-1)^n = (-1)^{n+1}. \end{aligned}$$

Donc par le principe de récurrence, $\boxed{\text{pour tout } n \in \mathbf{N},\ F_{n+1}^2 - F_nF_{n+2} = (-1)^n.}$

4.b. Soit $n \in \mathbf{N}$. Posons $u = (-1)^n F_{n+1}$ et $v = (-1)^{n+1} F_{n+2}$. Alors $F_{n+1}u + F_n v = 1$, de sorte que par le théorème de Bézout, $\boxed{F_n \text{ et } F_{n+1} \text{ sont premiers entre eux.}}$

5.a. Prouvons le résultat par récurrence simple sur p, en prouvant la proposition $\mathscr{P}(p)$: «$\forall n \in \mathbf{N}^*$, $F_{n+p} = F_{n-1}F_p + F_n F_{p+1}$».
Pour $p = 0$, cette proposition est correcte puisque pour tout $n \in \mathbf{N}^*$,

$$F_n = F_{n-1} \times 0 + F_n \times 1 = F_{n-1}F_0 + F_n F_1.$$

Soit $p \in \mathbf{N}$ tel que $\mathscr{P}(p)$ soit vraie. Alors pour tout $n \in \mathbf{N}^*$,

$$\begin{aligned} F_{n+p+1} &= F_{n+1+p} = F_n F_p + F_{n+1}F_{p+1} \\ &= F_n F_p + F_n F_{p+1} + F_{n-1}F_{p+1} \\ &= F_{n-1}F_{p+1} + F_n(F_p + F_{p+1}) = F_{n-1}F_{p+1}F_n F_{p+2}. \end{aligned}$$

Donc par le principe de récurrence, pour tout $p \in \mathbf{N}$ et pour tout $n \in \mathbf{N}^*$,

$$\boxed{F_{n+p} = F_{n-1}F_p + F_n F_{p+1}.}$$

Détails
On utilise l'hypothèse avec $n+1$ au lieu de n. D'où l'importance de mettre un «pour tout n» dans l'hypothèse de récurrence et de ne pas travailler à n fixé.

5.b. Soient $(n, p) \in \mathbf{N}^* \times \mathbf{N}$, et notons $d = F_{n+p} \wedge F_n$, $\delta = F_n \wedge F_p$.
Alors $\delta \mid F_n$ et $\delta \mid F_p$, de sorte que $\delta \mid F_n F_{p+1} + F_p F_{n-1} = F_{n+p}$.
Donc δ divise F_{n+p} et F_n, donc divise d.

Rappel
Un entier divise deux entiers a et b si et seulement si c'est un diviseur de $a \wedge b$.

Inversement, d divise F_{n+p} et F_p, donc divise $F_{n+p} - F_{n-1}F_p = F_n F_{p+1}$.
Or d divise F_p, et F_p est premier avec F_{p+1}, donc d est premier avec F_{p+1}.
Puisque $d \mid F_{p+1}F_n$ et $d \wedge F_{p+1} = 1$, par le lemme de Gauss, $d \mid F_n$. Et donc $d \mid F_n$ et $d \mid F_p$, de sorte que $d \mid \delta$.
Comme d et δ sont positifs, on a donc $d = \delta$, soit encore $\boxed{F_{n+p} \wedge F_p = F_n \wedge F_p.}$

5.c. C'est une récurrence facile sur k : $F_{n+kp} \wedge F_p = F_{n+(k-1)p} \wedge F_p = F_{n+(k-2)p} \wedge F_p = \cdots = F_n \wedge F_p$.

6. Soient n, p deux entiers tels que $n \geqslant p$. La question précédente prouve que si $n = bp + r$ est la division euclidienne de n par p, alors $F_n \wedge F_p = F_{n-bp} \wedge F_p = F_r \wedge F_p$.

Supposons donc à présent, quitte à échanger n et p que $n \geqslant p$ et reprenons alors les notations utilisées dans le cours pour l'algorithme d'Euclide, avec r_1 le reste de la division euclidienne de n par p, r_2 le reste de la division euclidienne de b par r_1, etc, et $r_N = n \wedge p$ le reste de la division euclidienne de r_{N-2} par r_{N-1}. Alors le reste de la division euclidienne de r_{N-1} par r_N est nul.
Alors $F_n \wedge F_p = F_p \wedge F_{r_1} = F_{r_1} \wedge F_{r_2} = \cdots = F_{r_{N-1}} \wedge F_{r_N} = F_{r_N} \wedge F_0 = F_{r_N} \wedge 0 = F_{r_N} = \boxed{F_{n \wedge p}.}$

Si de plus $p \mid n$, alors $p \wedge n = p$. Et donc $F_n \wedge F_p = F_{n \wedge p} = F_p$.
Par définition du pgcd[1], on a donc $F_p \mid F_n$.

[1] C'est un diviseur commun de F_n et F_p, et en particulier un diviseur de F_n.

7. Supposons que F_n soit un nombre premier, et soit p un facteur premier de n.
Alors nous savons que $F_p \mid F_n$.
Si $p > 2$, alors $F_p > F_2 = 1$, donc par primalité de F_n, $F_p = F_n$.
Or la suite de Fibonacci étant strictement croissante à partir de 2, ceci signifie que $n = p$, et donc que n est premier.

Stricte croissance
Autrement dit, l'application définie sur $\mathbf{N} \setminus \{0, 1\}$ par $n \mapsto F_n$ est injective.

Si n n'est pas un nombre premier impair, n possède donc 2 comme unique facteur premier.
Notons $k = v_2(n)$, de sorte que $n = 2^k$. Il est clair que $k = 0$ et $k = 1$ ne conviennent pas puisque F_1 et F_2 ne sont pas premiers.
Si $k \geqslant 2$, alors 2^k est divisible par 4, et donc $F_4 = 5$ divise F_n.
Mais F_n étant premier, on a alors $F_n = 5$, ce qui, toujours pas stricte croissance de $(F_n)_{n \geqslant 2}$, ne se produit que pour $n = 4$.
Donc $\boxed{\text{si } F_n \text{ est premier, alors } n = 4 \text{ ou } n \text{ est premier impair.}}$
Remarque : *la réciproque est fausse : 5 est premier, mais $F_5 = 8$ ne l'est pas.*

Partie III. Puissances de 2 dans la suite de Fibonacci

8. En calculant les premiers nombres de Fibonacci, on constate que $F_6 = 8$. Puisque $(F_n)_{n \geqslant 2}$ est strictement croissante, pour tout $n \geqslant 7$, $F_n > 8$.

Donc il suffit de lister les puissances de 2 parmi $F_0, F_1, \dots, F_6$: il y en a quatre, à savoir $\boxed{F_1 = F_2 = 1,\ F_3 = 2 \text{ et } F_6 = 8.}$

9.a. Si $F_n = 2^k$, avec $k > 3$, alors F_n est divisible par 8, et donc $F_n \wedge 8 = 8$, soit encore $F_n \wedge F_6 = F_6$.
Par la question 6 cela signifie donc que $F_{n\wedge 6} = F_6$, et donc[2] que $n \wedge 6 = 6$, et donc que n est divisible par 6 : il existe $m \in \mathbf{N}^*$ tel que $n = 6m$.
Notons qu'alors $m \geqslant 2$ puisque n est nécessairement[3] supérieur ou égal à 7.

[2] C'est encore la stricte croissance de $(F_n)_{n\geqslant 2}$: la suite (F_n) ne prend qu'une seule fois la valeur F_6, et c'est pour $n = 6$.

[3] C'est la question précédente.

9.b. Puisque $F_m \mid F_{6m} = F_n$, qui est une puissance de 2, F_m possède un unique facteur premier qui est 2, et donc est également une puissance de 2.
On a alors $F_{3\wedge m} = F_3 \wedge F_m = 2 \wedge F_m = 2$.
Mais le seul terme de la suite de Fibonacci égal à 2 est F_3, donc $3 \wedge m = 3$ si bien que $\boxed{3 \mid m.}$

9.c. Puisque $n = 6m$ et que 3 divise m, alors $9 \mid n$, et par conséquent, $F_9 \mid F_n$. Mais $F_9 = 34$ ne divise pas F_n, car 17 est premier avec $F_n = 2^k$.

$\boxed{\text{Il n'existe donc pas de valeur de } n \text{ pour laquelle } F_n \text{ est de la forme } 2^k \text{ avec } k > 3.}$

10. La liste a été donnée à la question 5 : les seules puissances de 2 dans la suite de Fibonacci sont 1, 2 et 8, égaux respectivement à F_1, F_2, F_3 et F_6.

▸ Exercice 2 : théorème du point fixe de Banach-Picard

1. Donnons deux solutions : une purement «epsilonesque» et une à l'aide de la caractérisation séquentielle de la continuité.
Nous pouvons tout de suite laisser de côté le cas où $\varepsilon = 0$, puisqu'alors pour tout $x, y \in I$, $|f(x) - f(y)| \leqslant 0$, et donc $f(x) = f(y)$. Donc f est constante, et donc continue.

Méthode
La continuité est une notion *ponctuelle* : pour prouver qu'une fonction est continue, à moins de disposer d'un théorème (par exemple un résultat sur les sommes/produits/etc de fonctions continues sur I) prouvant directement le continuité sur I, il faut prouver qu'elle est continue *en chaque point de I*.

▸ **Preuve epsilonesque** : soit $x_0 \in I$, et soit $\varepsilon > 0$. Posons alors $\eta = \frac{\varepsilon}{k}$. Alors pour $x \in I$, si $|x - x_0| < \eta$, alors $|f(x) - f(x_0)| \leqslant k|x - x_0| < k\frac{\varepsilon}{k} \leqslant \varepsilon$.
Et donc on a bien prouvé que :

$$\forall \varepsilon > 0,\ \exists \eta > 0,\ \forall x \in I,\ |x - x_0| < \eta \Rightarrow |f(x) - f(x_0)| < \varepsilon.$$

C'est la définition de $\lim\limits_{x \to x_0} f(x) = f(x_0)$, et donc de la continuité de f en x_0.
Ceci étant vrai pour tout $x_0 \in I$, f est continue sur I.
▸ **Preuve séquentielle** : soit $x \in I$, et soit $(x_n) \in I^{\mathbf{N}}$ une suite d'éléments de I qui converge vers x.
Alors pour tout $n \in \mathbf{N}$, $0 \leqslant |f(x_n) - f(x)| \leqslant k|x_n - x|$ si bien que par le théorème des gendarmes, $|f(x_n) - f(x)| \underset{n\to+\infty}{\longrightarrow} 0$, et donc $f(x_n) \underset{n\to+\infty}{\longrightarrow} f(x)$.
Ceci étant vrai pour toute suite (x_n) de limite x, f est continue en x. Et ceci étant vrai pour tout $x \in I$, f est continue sur I.

2. Supposons que f possède deux points fixes ℓ_1 et ℓ_2. Alors $f(\ell_1) = \ell_1$ et $f(\ell_2) = \ell_2$. Et donc

$$|\ell_1 - \ell_2| = |f(\ell_1) - f(\ell_2)| \leqslant k|\ell_1 - \ell_2|.$$

Mais k étant strictement inférieur à 1, si $\ell_1 - \ell_2 \neq 0$, on a alors $|\ell_1 - \ell_2| < |\ell_1 - \ell_2|$, ce qui est absurde.
Et donc $\ell_1 = \ell_2$: $\boxed{\text{si } f \text{ possède un point fixe, il est unique.}}$

3. C'est une simple récurrence : pour $n = 0$, on a $|u_1 - u_0| = k^0|u_1 - u_0|$.
Soit $n \in \mathbf{N}$ tel que $|u_{n+1} - u_n| \leqslant k^n|u_1 - u_0|$. Alors

$$|u_{n+2} - u_{n+1}| = |f(u_{n+1}) - f(u_n)| \leqslant k|u_{n+1} - u_n| \leqslant kk^n|u_1 - u_0| \leqslant k^{n+1}|u_1 - u_0|.$$

Donc par le principe de récurrence, $\boxed{\text{pour tout } n \in \mathbf{N},\ |u_{n+1} - u_n| \leqslant k^n|u_1 - u_0|.}$

4. Pour $n = 0$, le résultat est évident, et pour $n \geqslant 1$, on a

$$\begin{aligned}|u_n - u_0| &= |(u_n - u_{n-1}) + (u_{n-1} - u_{n-2}) + \cdots + (u_1 - u_0)| \\ &= \left|\sum_{i=0}^{n-1}(u_{n-i} - u_{n-i-1})\right|\end{aligned}$$

Somme télescopique.

$$\leqslant \sum_{i=0}^{n-1} |u_{n-i} - u_{n-i-1}|$$

Inégalité triangulaire.

$$\leqslant \sum_{i=0}^{n-1} k^{n-i-1}|u_1 - u_0| \leqslant \sum_{j=0}^{n-1} k^j |u_1 - u_0|$$

$$\leqslant \frac{1-k^n}{1-k}|u_1 - u_0| \boxed{\leqslant \frac{1}{1-k}|u_1 - u_0|.}$$

Somme géométrique de raison $\neq 1$.

5. On en déduit en particulier que pour tout $n \in \mathbf{N}$,

$$|u_n| = |u_n - u_0 + u_0| \leqslant |u_n - u_0| + |u_0| \leqslant \frac{1}{1-k}|u_1 - u_0| + |u_0|.$$

Et donc[4] (u_n) est bornée.

[4] Le majorant de $|u_n|$ que nous venons d'obtenir est indépendant de n.

Puisque (u_n) est bornée, par le théorème de Bolzano-Weierstrass, il existe une extractrice $\varphi : \mathbf{N} \to \mathbf{N}$ telle que $(u_{\varphi(n)})_n$ converge vers un réel ℓ.
Il s'agit donc de prouver que la limite ℓ de cette suite extraite est encore dans I.
C'est ici que nous allons avoir besoin des hypothèses de l'énoncé au sujet des éventuelles bornes de l'énoncé. En effet, en utilisant le théorème de classification des intervalles de $\mathbf{R}$, et le fait que les bornes de I, si elles existent, sont dans I, on peut affirmer que I est de l'un des types suivants : $I = \mathbf{R}$, $I =]-\infty, a]$, pour $a \in \mathbf{R}$, $I = [a, +\infty[$ pour $a \in \mathbf{R}$, ou $I = [a, b]$, avec $a \leqslant b$ deux réels.

Autrement dit

I est l'un des types d'intervalles que nous avons appelé *fermé* (ou éventuellement $\mathbf{R}$).

- ►Si $I = \mathbf{R}$, il est évident que $\ell \in I$.
- ►Si $I = [a, b]$ avec $a < b$: alors pour tout $n \in \mathbf{N}$, $a \leqslant u_{\varphi(n)} \leqslant b$ et donc par passage à la limite, $a \leqslant \ell \leqslant b$, de sorte que $\ell \in I$.
- ►Si $I =]-\infty, a]$, avec $a \in \mathbf{R}$: alors, pour tout $n \in \mathbf{N}$, $u_{\varphi(n)} \leqslant a$ et donc $\ell \leqslant a$, de sorte que $\ell \in]-\infty, a]$.
- ►Si $I = [a, +\infty[$, avec $a \in \mathbf{R}$, on conclut comme dans le cas précédent.

Terminologie

L'an prochain vous appellerez *fermée* toute partie I de $\mathbf{R}$ telle que toute suite convergente d'élements de I possède encore une limite dans I.
Ce que nous venons de prouver, c'est précisément que les intervalles fermés sont des parties fermées de $\mathbf{R}$.

6. Par l'inégalité triangulaire, on a, pour tout entier $n \in \mathbf{N}$,

$$\begin{aligned}|f(\ell) - \ell| &= |f(\ell) - f(u_{\varphi(n)}) + f(u_{\varphi(n)}) - u_{\varphi(n)} + u_{\varphi(n)} - \ell| \\ &\leqslant |f(\ell) - f(u_{\varphi(n)})| + |\underbrace{f(u_{\varphi(n)})}_{=u_{\varphi(n)+1}} - u_{\varphi(n)}| + |u_{\varphi(n)} - \ell| \\ &\leqslant k|\ell - u_{\varphi(n)}| + k^{\varphi(n)}|u_1 - u_0| + |u_{\varphi(n)} - \ell| \\ &\leqslant (k+1)|u_{\varphi(n)} - \ell| + k^{\varphi(n)}|u_1 - u_0|.\end{aligned}$$

Puisque pour tout n, $\varphi(n) \geqslant n$, on a donc $0 \leqslant k^{\varphi(n)} \leqslant k^n$, et donc $k^{\varphi(n)} \underset{n\to+\infty}{\longrightarrow} 0$.
Et de même, $|u_{\varphi(n)} - \ell| \underset{n\to+\infty}{\longrightarrow} 0$, et donc par passage à la limite dans les inégalités, $|f(\ell) - \ell| = 0$. Et par conséquent, $\boxed{f(\ell) = \ell \text{ : } \ell \text{ est un}^5 \text{ point fixe de } f.}$

[5] Et donc l'unique point fixe, d'après la question 2.

7. Procédons par récurrence. Pour $n = 0$, c'est évident.
Supposons que $|u_n - \ell| \leqslant k^n |u_0 - \ell|$. Alors

$$|u_{n+1} - \ell| = |f(u_n) - f(\ell)| \leqslant k|u_n - \ell| \leqslant k^{n+1}|u_0 - \ell|.$$

Et donc par le principe de récurrence, pour tout $n \in \mathbf{N}$, $|u_n - \ell| \leqslant k^n |u_0 - \ell|$.

8. On a donc $0 \leqslant |u_n - \ell| \leqslant k|u_0 - \ell|$.
Et puisque $k^n \underset{n\to+\infty}{\longrightarrow} 0$, par le théorème de gendarmes, $|u_n - \ell| \underset{n\to+\infty}{\longrightarrow} 0$ et donc $\boxed{u_n \underset{n\to+\infty}{\longrightarrow} \ell.}$

9. Application

9.a. Soient $(x, y) \in I^2$, avec $x \leqslant y$. Alors pour tout $t \in [x, y]$, $|f'(t)| \leqslant k$, et donc par inégalité triangulaire[6],

[6] Ce qui nécessite que les bornes soient dans le bon sens.

$$\left|\int_x^y f'(t)\,dt\right| \leqslant \int_x^y |f'(t)|\,dt \leqslant \int_x^y k\,dt \leqslant k(y-x) \leqslant k|y-x|.$$

Et si $y > x$, alors

$$\left|\int_x^y f'(t)\,dt\right| = \left|-\int_y^x f'(t)\,dt\right| = \left|\int_y^x f'(t)\,dt\right| \leqslant k|x-y| \leqslant k|y-x|.$$

Détails
Puisque $y < x$, une fois les bornes «remises dans le bon sens», on peut utiliser la majoration obtenue au premier cas.

Et donc au final pour tout $(x,y) \in I^2$,

$$|f(x) - f(y)| = \left|\int_x^y f'(t)\,dt\right| \leqslant k|x-y|.$$

Et donc $\boxed{f \text{ est } k\text{-contractante.}}$

9.b. La fonction f est dérivable sur $\mathbf{R}_+^*$ et a pour dérivée $f' : x \mapsto \dfrac{1}{2} - \dfrac{1}{x^2} = \dfrac{x^2-2}{2x^2}$.
Elle est donc décroissante sur $]0, \sqrt{2}]$ et croissante sur $[\sqrt{2}, +\infty[$.
On a alors $f(1) = \dfrac{3}{2} \in [1,2]$, $f(\sqrt{2}) = \sqrt{2} \in [1,2]$ et $f(2) = \dfrac{3}{2} \in [1,2]$.
Soit $x \in [1,2]$. Alors soit $x \in [1,\sqrt{2}]$, et alors $\sqrt{2} = f(\sqrt{2}) \leqslant f(x) \leqslant f(1) = \frac{3}{2}$, donc $f(x) \in [1,2]$.
Soit $x \in [\sqrt{2}, 2]$, et alors $\sqrt{2} = f(\sqrt{2}) \leqslant f(x) \leqslant f(2) = \frac{3}{2}$, donc $f(x) \in [1,2]$.
Au final, $\forall x \in [1,2]$, $f(x) \in [1,2]$, donc $\boxed{[1,2] \text{ est stable par } f.}$

De plus, f' est encore dérivable avec $\forall x \in [1,2]$, $f''(x) = \frac{2}{x^3} \leqslant 0$. Donc f' est croissante sur $[1,2]$, si bien que pour tout $x \in [1,2]$, $-\frac{1}{2} = f'(1) \leqslant f'(x) \leqslant f'(2) = \frac{1}{4}$. Et en particulier, pour tout $x \in [1,2]$, $|f'(x)| \leqslant \frac{1}{2}$.
Par la question précédente, $f_{|[1,2]}$ est $\dfrac{1}{2}$-contractante.

9.c. Par ce qui précède, toute suite (u_n) de premier terme dans $[1,2]$ et vérifiant la relation de récurrence $u_{n+1} = f(u_n)$ sera convergente, de limite l'unique point fixe de $f_{|[1,2]}$.
C'est notamment le cas si $u_0 = 2$.

Pour la culture
Cette suite a été décrite au 1er siècle par HÉRON D'ALEXANDRIE, mais était probablement déjà connue des mathématiciens égyptiens.
Sa convergence vers $\sqrt{2}$ est plutôt rapide, et donc elle fournit rapidement de bonnes approximations de $\sqrt{2}$.
On peut facilement généraliser la méthode pour obtenir une suite qui converge vers $\sqrt{a}$.

Reste à déterminer la valeur du point fixe de $f_{|[1,2]}$. Mais pour $x \in [1,2]$, on a

$$f(x) = x \Leftrightarrow \frac{x}{2} + \frac{1}{x} = x \Leftrightarrow x^2 = 2 \Leftrightarrow x = \sqrt{2}.$$

Et ainsi, $\boxed{u_n \xrightarrow[n\to+\infty]{} \sqrt{2}.}$

▸ Exercice 2 : groupes finis à un seul automorphisme

Partie I. Automorphismes d'un groupe

1. Il est évident que id_G, qui est le neutre de $\mathfrak{S}(G)$ est un automorphisme de G.
Soient φ, ψ deux automorphismes de G. Alors ψ^{-1} est encore un automorphisme de G, et par composition de morphismes, $\varphi \circ \psi^{-1}$ aussi.
Donc $\forall \varphi, \psi \in \mathrm{Aut}(G)$, $\varphi \circ \psi^{-1} \in \mathrm{Aut}(G)$, donc $\boxed{\mathrm{Aut}(G) \text{ est un sous-groupe de } (\mathfrak{S}(G), \circ).}$

Rappel
Un morphisme envoie nécessairement le neutre sur le neutre.

2. Si G est de cardinal 1, $G = \{e\}$. Et si $\varphi \in \mathrm{Aut}(G)$, alors $\varphi(e) = e$, donc $\varphi = \mathrm{id}_G$.
Si G est de cardinal 2, soit $x \in G \setminus \{e\}$ de sorte que $G = \{e, x\}$. Soit alors $\varphi \in \mathrm{Aut}(G)$. Alors $\varphi(e) = e$, et par injectivité de φ, $\varphi(x) \neq e$, si bien que $\varphi(x) = x$.
Dans les deux cas, on a prouvé que $\mathrm{Aut}(G) \subset \{\mathrm{id}_G\}$, l'inclusion réciproque étant évidente.

3.a. Soient $g, x, y \in G$. Alors

$$\varphi_g(x)\varphi_g(y) = gxg^{-1}gyg = gxeyg^{-1} = gxyg^{-1} = \varphi_g(xy).$$

Donc φ_g est un morphisme.
De plus, pour tout $x, y \in G$, on a $\varphi_g(x) = y \Leftrightarrow gxg^{-1} = y \Leftrightarrow gx = yg \Leftrightarrow x = g^{-1}yg$.
Ainsi, tout $y \in G$ possède un unique antécédent par φ_g, si bien que φ_g est bijective, et donc est un automorphisme de G.

3.b. Soit $g \in G$. Procédons directement par équivalence :

$$\varphi_g = \mathrm{id}_G \Leftrightarrow \forall x \in G,\ \varphi_g(x) = x \Leftrightarrow \forall x \in G,\ gxg^{-1} = x$$
$$\Leftrightarrow \forall x \in G,\ gx = xg \Leftrightarrow g \in \mathcal{Z}(G).$$

4. Il est évident que $g \mapsto g^{-1}$ est bijective, égale à sa propre bijection réciproque puisque pour tout $g \in G$, $\left(g^{-1}\right)^{-1} = g$.
Donc $f : g \mapsto g^{-1}$ est un automorphisme si et seulement si c'est un morphisme.
Si G est abélien, alors pour tout $x, y \in G$, $f(xy) = (xy)^{-1} = y^{-1}x^{-1} = f(y)f(x) = f(x)f(y)$, donc f est un automorphisme.

Et inversement, si f est un morphisme, alors pour tous $x, y \in G$, on a

$$xy = (y^{-1}x^{-1})^{-1} = f\left(y^{-1}x^{-1}\right) = f\left(y^{-1}\right)f\left(x^{-1}\right) = yx$$

et donc G est abélien.

Partie II. Groupes dont tous les carrés sont triviaux.

5. Soient $g \in G$. Alors $g^2 = e$, si bien que $g^{-1} = g$.
Et donc l'application $x \mapsto x^{-1}$ n'est autre que l'identité, et en particulier est un automorphisme de G. Par la question 4, c'est donc que $\boxed{G \text{ est abélien.}}$

6. Puisqu'un sous-groupe de G contenant G est nécessairement égal à G, $G \in \mathrm{Gen}(G)$.

7. Puisque $\mathrm{Gen}(G)$ est non vide, $\{\mathrm{Card}(A),\ A \in \mathrm{Gen}(G)\}$ est une partie non vide de $\mathbf{N}$. Elle possède donc un plus petit élément n. Et alors par définition, il existe $A_0 \in \mathrm{Gen}(G)$ tel que $\mathrm{Card}(A_0) = n$.

8. L'ensemble vide n'est pas une partie génératrice de G puisque $\emptyset \subset \{e\}$, et $\{e\}$ est un sous-groupe de G différent[7] de G.
À présent, soit $g \in G$, et prouvons que le singleton $\{g\}$ n'est pas une partie génératrice de G.
Si $g = e$, alors comme précédemment, $\{e\}$ est un sous-groupe de G contenant $\{e\}$ et différent de G.
Si $g \neq e$, alors $\langle g \rangle$ est un sous-groupe de G contenant g.
Mais si $x \in \langle g \rangle$, alors il existe $n \in \mathbf{Z}$ tel que $x = g^n$.
Si n est pair, soit $q \in \mathbf{Z}$ tel que $n = 2q$. Alors $x = g^n = (g^2)^q = e^q = e$.
Et si n est impair, soit $q \in \mathbf{Z}$ tel que $n = 2q + 1$. Alors $x = g^n = (g^2)^q g = e^q g = g$.
Ainsi, $\langle g \rangle \subset \{e, g\}$, et la réciproque étant évidente[8], $\langle g \rangle = \{e, g\}$.
Donc $\langle g \rangle$ est un sous-groupe de G, différent de G (car $\mathrm{Card}(G) \geqslant 3$) contenant $\{g\}$.

Ainsi, toute partie génératrice de G est de cardinal supérieur ou égal à 2, ce qui s'applique notamment à A_0.

Et si $a \in A_0$, alors $A_0 \setminus \{a\}$ est de cardinal $n - 1 \leqslant n$. Par définition de n, ceci signifie que $A_0 \setminus \{a\}$ n'est plus génératrice de G.

[7] Car $\mathrm{Card}(G) \neq 1$.

Mieux

Nous avons prouvé en cours que $\langle g \rangle$ est le plus petit (au sens de l'inclusion) sous-groupe de G contenant g.

[8] Un sous-groupe contenant g doit contenir g par définition, et comme tout sous-groupe qui se respecte, doit contenur e.

9. Notons donc $H = \left\{g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n},\ (\varepsilon_1, \dots, \varepsilon_n) \in \{0,1\}^n\right\}$.
Alors $e = g_1^0 g_2^0 \cdots g_n^0 \in H$.
Soient $x, y \in H$. Alors il existe $(\varepsilon_1, \dots, \varepsilon_n) \in \{0,1\}^n$ et $(\varepsilon_1', \dots, \varepsilon_n') \in \{0,1\}^n$ tels que

$$x = g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n} \text{ et } y = g_1^{\varepsilon_1'} g_2^{\varepsilon_2'} \cdots g_n^{\varepsilon_n'}.$$

Alors

$$xy = g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n} g_1^{\varepsilon_1'} g_2^{\varepsilon_2'} \cdots g_n^{\varepsilon_n'} = g_1^{\varepsilon_1 + \varepsilon_1'} g_2^{\varepsilon_2 + \varepsilon_2'} \cdots g_n^{\varepsilon_n + \varepsilon_n'}.$$

Pour tout $i \in [\![1, n]\!]$, notons q_i, r_i le quotient et le reste de la division euclidienne de $\varepsilon_i + \varepsilon_i'$ par 2, de sorte que $\varepsilon_i + \varepsilon_i' = 2q_i + r_i$, avec $r_i \in \{0, 1\}$.
Alors $xy = g_1^{2q_1 + r_1} g_2^{2q_2 + r_2} \cdots g_n^{2q_n + r_n} = (g_1^2)^{q_1} g_1^{r_1} (g_2^2)^{q_2} g_2^{r_1} \cdots (g_n^2)^{q_n} g_n^{r_n} = g_1^{q_1} g_2^{q_2} \cdots g_n^{q_n} \in H$.
Enfin, puisque pour tout $g \in G$, $g^{-1} = g$, on a en particulier pour tout $x \in H$, $x^{-1} = x \in H$.
Donc H est un sous-groupe de G. Il contient évidemment g_i pour tout $i \in [\![1, n]\!]$, puisque $g_i = g_1^0 \cdots g_{i-1}^0 g_i^1 g_{i+1}^0 \cdots g_n^0$.

Remarque

Notons qu'il est possible de regrouper les puissances d'un même élément car G est abélien.

10. Puisque A_0 est une partie génératrice de G, le sous-groupe H de la question précédente est égal à G tout entier.
Et donc pour tout $g \in G$, il existe $(\varepsilon_1, \dots, \varepsilon_n) \in \{0,1\}^n$ tel que $g = g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n}$.

Reste à prouver l'unicité d'une telle écriture. Soient donc $(\varepsilon_1, \dots, \varepsilon_n)$ et $(\alpha_1, \dots, \alpha_n)$ deux n-uplets de $\{0,1\}^n$ tels que $g = g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n} = g_1^{\alpha_1} \cdots g_n^{\alpha_n}$.
Supposons par l'absurde que ces deux n-uplets sont distincts et notons
$k = \min\{i \in [\![1,n]\!] \mid \varepsilon_i \neq \alpha_i\}$.
Quitte à échanger nos deux n-uplets, on peut supposer que $\varepsilon_k = 0$ et $\alpha_k = 1$.
Et alors $g_1^{\varepsilon_1} \cdots g_{k-1}^{\varepsilon_{k-1}} g_{k+1}^{\varepsilon_{k+1}} \cdots g_n^{\varepsilon_n} = g_1^{\alpha_1} \cdots g_{k-1}^{\alpha_{k-1}} g_k g_{k+1}^{\alpha_{k+1}} \cdots g_n^{\alpha_n}$.
Comme $\varepsilon_1 = \alpha_1, \dots, \varepsilon_{k-1} = \alpha_{k-1}$, il vient $g_{k+1}^{\varepsilon_{k+1}} \cdots g_n^{\varepsilon_n} = g_k g_{k+1}^{\alpha_{k+1}} \cdots g_n^{\alpha_n}$ et donc

$$g_k = g_{k+1}^{\varepsilon_{k+1}-\alpha_{k+1}} \cdots g_n^{\varepsilon_n - \alpha_n}.$$

Soit alors $A = \{g_1, \dots, g_{k-1}, g_{k+1}, \dots, g_n\} = A_0 \setminus \{g_k\}$.
Si H est un sous-groupe de G qui contient A, alors pour tout $i \in [\![k+1, n]\!]$, H contient aussi $g_i^{\varepsilon i - \alpha_i}$.
Et donc par stabilité de H par produit, H contient g_k.
Et donc H contient $\{g_1, \dots, g_n\} = A_0$. Puisque A_0 est génératrice de G, $H = G$.
Autrement dit, on a prouvé que A est une partie génératrice de G, de cardinal $n-1$, ce qui contredit la minimalité de n.

Par conséquent, $(\varepsilon_1, \dots, \varepsilon_n) = (\alpha_1, \dots, \alpha_n)$ si bien que g s'écrit de manière unique sous la forme $g = g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n}$.

> **Remarque**
> Nous venons donc de prouver qu'il existe une bijection entre G et $\{0,1\}^n$, si bien que G a même cardinal que $\{0,1\}^n$, et donc G est de cardinal 2^n.
> Ce résultat avait été prouvé d'une manière complètement différente dans l'exercice 8 du TD 15.
> En poussant un peu plus loin, on prouverait que cette bijection est en fait un isomorphisme entre G et $\{0,1\}^n$

11. Commençons par noter que l'application φ est définie de manière non ambigüe car l'écriture d'un élément $g \in G$ sous la forme $g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n}$ est unique.

Il est aisé de constater que $\varphi \circ \varphi = \mathrm{id}_G$ puisque si $g = g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n}$,

$$\varphi(\varphi(g)) = \varphi(g_1^{\varepsilon_2} g_2^{\varepsilon_1} g_3^{\varepsilon_3} \cdots g_n^{\varepsilon_n}) = g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n} = g.$$

Et donc φ est bijective, égale à sa propre bijection réciproque.

Reste donc à vérifier que φ est un morphisme de groupes.
Soient donc $x, y \in G$, et soient $(\varepsilon_1, \dots, \varepsilon_n), (\alpha_1, \dots, \alpha_n) \in \{0,1\}^n$ tels que $x = g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n}$ et $y = g_1^{\alpha_1} \cdots g_n^{\alpha_n}$.
Comme à la question 9, si on note r_i le reste de la division euclidienne de $\varepsilon_i + \alpha_i$ par 2, alors $xy = g_1^{r_1} \cdots g_n^{r_n}$. Et alors

$$\varphi(xy) = g_1^{r_2} g_2^{r_1} g_3^{r_3} \cdots g_n^{r_n}.$$

Et par ailleurs, $\varphi(x)\varphi(y) = g_1^{\varepsilon_2} g_2^{\varepsilon_1} g_3^{\varepsilon_3} \cdots g_n^{\varepsilon_n} g_1^{\alpha_2} g_2^{\alpha_1} g_3^{\alpha_3} \cdots g_n^{\alpha_n} = g_1^{\varepsilon_2+\alpha_2} g_2^{\varepsilon_1+\alpha_1} g_3^{\varepsilon_3+\alpha_3} \cdots g_n^{\varepsilon_n+\alpha_n}$.
Puisque $g_1^2 = e$, on a encore $g_1^{\varepsilon_2+\alpha_2} = g_1^{r_2}$ et de même, $g_2^2 = e$, et donc $g_2^{\varepsilon_1+\alpha_1} = g_2^{r_1}$.
Et donc on a bien $\varphi(xy) = \varphi(x)\varphi(y)$, si bien que $\varphi \in \mathrm{Aut}(G)$.

Partie III. Groupes finis tels que $\mathrm{Aut}(G) = \{\mathrm{id}_G\}$.

12. Soit $g \in G$. Alors l'automorphisme φ_g défini à la question 3 est égal à id_G, nécessairement $g \in \mathcal{Z}(G)$. Et donc pour tout $g \in G$ et pour tout $h \in G$, $gh = hg$, si bien que G est abélien.

Puisque G est abélien, par la question 4, $g \mapsto g^{-1}$ est un automorphisme de G.
Il est donc égal à id_G si bien que pour tout $g \in G$, $g^{-1} = g$. Soit encore, après multiplication[9] par g, $g^2 = e$.
Ainsi G satisfait les hypothèses de la partie II.
Supposons par l'absurde que $\mathrm{Card}(G) \geqslant 3$.
Donc en reprenant les mêmes notations, l'automorphisme φ défini à la question 11 est bien dans $\mathrm{Aut}(G)$, donc égal à l'identité.
Or cet automorphisme envoie $g_1 = g_1^1 g_2^0 \cdots g_n^0$ sur $g_1^0 g_2^1 \cdots g_n^0 = g_2 \neq g_1$. Ce qui est absurde.
Et donc nécessairement $\boxed{\mathrm{Card}(G) \leqslant 2.}$

> **Remarque**
> Comme mentionné dans la remarque précédente, G est isomorphe à $\{0,1\}^n$.
> Or si $n \geqslant 2$, ce groupe possède des automorphismes non triviaux, par exemple l'application qui échange les deux premières coordonnées.
> Et donc $\mathrm{Aut}(G)$, qui est isomorphe à $\mathrm{Aut}(\{0,1\}^n)$ est non trivial lui aussi.

Remarque *: le résultat reste vrai si on ne suppose pas G fini : un groupe qui ne possède qu'un automorphisme est de cardinal inférieur ou égal à 2. Mais la preuve de ce fait nécessite l'axiome du choix.*