DM 7, corrigé

PROBLÈME
Une équation fonctionnelle

Partie I. Solutions deux fois dérivables.

1) Un calcul nous permet de vérifier ceci. Les fonctions cos et ch sont bien continues sur $\mathbb{R}$. De plus, pour $x, y \in \mathbb{R}$, on a :

$$\begin{array}{rcl} \cos(x+y)+\cos(x-y) & = & \cos(x)\cos(y)-\sin(x)\sin(y)+(\cos(x)\cos(y)+\sin(x)\sin(y)) \\ & = & 2\cos(x)\cos(y). \end{array}$$

La fonction cos est dans E. On a également :

$$\begin{array}{rcl} \mathrm{ch}(x+y)+\mathrm{ch}(x-y) & = & \dfrac{e^{x+y}+e^{-x-y}}{2}+\dfrac{e^{x-y}+e^{y-x}}{2} \\ & = & \dfrac{e^x e^y+e^{-x}e^{-y}+e^x e^{-y}+e^{-x}e^y}{2} \\ & = & \dfrac{e^x(e^y+e^{-y})+e^{-x}(e^{-y}+e^y)}{2} \\ & = & (e^x+e^{-x})\mathrm{ch}(y) \\ & = & 2\mathrm{ch}(x)\mathrm{ch}(y). \end{array}$$

La fonction ch est donc dans E.

2) Soit $f \in E$.

a) Soit $\alpha \in \mathbb{R}$. La fonction f_α est continue comme composée de fonctions continues sur $\mathbb{R}$. On a de plus pour $x, y \in \mathbb{R}$:

$$\begin{array}{rcl} f_\alpha(x+y)+f_\alpha(x-y) & = & f(\alpha x+\alpha y)+f(\alpha x-\alpha y) \\ & = & 2f(\alpha x)f(\alpha y) \qquad \text{(car } f \text{ est dans } E.) \\ & = & 2f_\alpha(x)f_\alpha(y). \end{array}$$

La fonction f_α est donc bien dans E.

b) En évaluant la relation vérifiée par f en $x = y = 0$, on obtient $2f(0) = 2f(0)^2$. On en déduit que $f(0)(1-f(0)) = 0$, ce qui entraine que $f(0)$ ne peut valoir que 0 ou 1.

c) Supposons $f(0) = 0$. En évaluant la relation en x quelconque et en $y = 0$, on obtient $2f(x) = 2f(x)f(0)$. Ceci entraine que pour tout $x \in \mathbb{R}$, $f(x) = 0$. f est donc la fonction nulle.

d) Supposons à présent $f(0) = 1$. En appliquant la propriété en $x = 0$ et y quelconque, on obtient $f(y)+f(-y) = 2f(0)f(y)$. On a donc $f(-y) = f(y)$ pour tout y dans $\mathbb{R}$. La fonction f est donc paire.

3) On suppose dans cette question uniquement que f est une fonction de E deux fois dérivable.

a) Fixons $x \in \mathbb{R}$. On peut alors dériver la relation vérifiée par f par rapport à y (en considérant que x est fixé et donc constant). Toutes les fonctions qui apparaissent sont deux fois dérivables comme composées de fonctions deux fois dérivables. On a alors pour tout $y \in \mathbb{R}$:

$$\begin{array}{c} f'(x+y)-f'(x-y) = 2f(x)f'(y) \\ f''(x+y)+f''(x-y) = 2f(x)f''(y) \end{array}$$

On a donc bien la relation voulue.

b) En appliquant la relation précédente en $y = 0$, on obtient que $2f''(x) = 2f(x)f''(0)$. En posant $\alpha = f''(0)$, on a alors bien que $\forall x \in \mathbb{R},\ f''(x) = \alpha f(x)$.

c) L'équation différentielle $y'' - \alpha y = 0$ est une équation différentielle linéaire à coefficients constants d'ordre 2. L'équation caractéristique associée est $X^2 - \alpha = 0$. On en déduit que les solutions sont de la forme :

- Si $\alpha > 0$, de la forme $x \mapsto \lambda e^{\sqrt{\alpha}x} + \mu e^{-\sqrt{\alpha}x},\ \lambda, \mu \in \mathbb{R}$. On peut changer un peu cette expression en remplacement les exponentielles en fonction de ch et sh pour trouver une expression de la forme $x \mapsto (\lambda + \mu)\mathrm{ch}(\sqrt{\alpha}x) + (\lambda - \mu)\mathrm{sh}(\sqrt{\alpha}x)$.
- Si $\alpha = 0$, de la forme $x \mapsto \lambda x + \mu,\ \lambda, \mu \in \mathbb{R}$.
- Si $\alpha < 0$, de la forme $x \mapsto \lambda \cos(\sqrt{-\alpha}x) + \mu \sin(\sqrt{-\alpha}x),\ \lambda, \mu \in \mathbb{R}$.

4) Cherchons les solutions de E qui sont deux fois dérivables par analyse/synthèse.

Analyse : Soit f une solution de E deux fois dérivables. D'après la question précédente, on a la forme de f. Il faut alors vérifier parmi ces solutions lesquels vérifient bien l'équation de départ. Remarquons tout d'abord que si ces fonctions vérifient $f(0) = 0$, alors elles sont égales à la fonction nulle (d'après le 2.c). Supposons donc que ces fonctions vérifient $f(0) = 1$. Elles sont donc impaires d'après le 2.d.

- Si $\alpha > 0$, puisque l'on veut $f(0) = 1$, il faut $\lambda + \mu = 1$. Puisque l'on veut une fonction paire, il faut alors $\lambda - \mu = 0$. On obtient donc une fonction de la forme $x \mapsto \mathrm{ch}(\sqrt{\alpha}x)$.
- Si $\alpha = 0$, alors puisque l'on veut $f(0) = 1$ et f paire, la seule fonction restante est la fonction constante égale à 1.
- Si $\alpha < 0$, puisque l'on veut $f(0) = 1$ et f paire, alors f est forcément de la forme $x \mapsto \cos(\sqrt{-\alpha}x)$ (même calcul que pour le premier cas).

Synthèse : Réciproquement, les fonctions nulles et constantes égale à 1 sont bien solution dans E (elles sont continues sur $\mathbb{R}$ et vérifient la relation demandée). Les fonctions de la forme $x \mapsto \mathrm{ch}(\beta x)$ et $x \mapsto \cos(\beta x)$ pour β quelconque dans $\mathbb{R}$ sont également dans E d'après la question 1 et la question 2.a. On a donc bien trouvé toutes les fonctions deux fois dérivables de E.

Partie II. Solutions qui s'annulent.

5) Puisque f est dans E et n'est pas la fonction nulle, alors $f(0) \neq 0$ d'après le I.2.a. On a alors automatiquement $f(0) = 1$ d'après le 2.b, ce qui entraine que f est paire. Puisque f s'annule au moins une fois sur $\mathbb{R}$, qu'elle ne s'annule pas en 0 (car $f(0) = 1$) et qu'elle est paire, cela entraine que f s'annule au moins une fois sur $\mathbb{R}_+^*$.

6)

a) L'ensemble A est non vide d'après la question précédente et il est minoré. Il admet donc une borne inférieure a. Puisque a est le plus grand des minorants et que 0 minore A, on a aussi $0 \leq a$.

b) Par caractérisation séquentielle de la borne inférieure, il existe une suite (a_n) d'éléments de A qui tend vers a. Par continuité de f, on a donc $f(a_n) \to f(a)$ quand n tend vers l'infini. Or, par définition de la suite (a_n), on a pour tout $n \in \mathbb{N}$, $f(a_n) = 0$. La limite de la suite $(f(a_n))$ est donc 0, ce qui entraine $f(a) = 0$.

Puisque $f(0) = 1$, on a $a \neq 0$. Puisque $a \geq 0$, on en déduit que $a > 0$.

On a donc montré que a était le minimum de A (il appartient à A d'après ce que l'on vient de vérifier).

c) Soit $x \in [0,a[$. On a $f(0) = 1 > 0$. De plus, par définition de a, on a aussi $f(x) \neq 0$. Supposons par l'absurde que $f(x) < 0$. La fonction f est alors continue sur $[0,x]$ et change de signe. D'après le théorème des valeurs intermédiaires, il existe $y \in [0,x]$ tel que $f(y) = 0$. On a alors $y > 0$ (car $f(0) \neq 0$) et $y \leq x < a$. Ceci entraine que $y \in A$ et $y < a$ ce qui contredit la définition du minimum ! Ceci entraine que pour tout $x \in [0,a[$, $f(x) > 0$.

7)

a) Soit $q \in \mathbb{N}$. En utilisant la relation vérifiée par f en $x = y$, on obtient que $f(2x) + f(0) = 2f(x)^2$. Puisque $f(0) = 1$, on en déduit que $f(2x)+1 = 2f(x)^2$ pour tout $x \in \mathbb{R}$. En appliquant cette propriété en $x = \dfrac{a}{2^{q+1}}$, on obtient :

$$f\left(\frac{a}{2^q}\right) + 1 = 2\left(f\left(\frac{a}{2^{q+1}}\right)\right)^2.$$

b) Montrons par récurrence sur $q \in \mathbb{N}$ la propriété $\mathcal{P}(q)$: « $f\left(\dfrac{a}{2^q}\right) = g\left(\dfrac{a}{2^q}\right)$ ».

- La propriété est vraie au rang $q = 0$. En effet, on a $f(a) = 0$ et $g(a) = \cos(\dfrac{\pi}{2a} \times a) = \cos(\dfrac{\pi}{2}) = 0$.
- Soit $q \in \mathbb{N}$. Supposons la propriété vraie au rang q. En utilisant le résultat de la question précédente, on obtient que :

$$\left(f\left(\frac{a}{2^{q+1}}\right)\right)^2 = \frac{f\left(\frac{a}{2^q}\right)+1}{2}.$$

  Or, on peut passer à la racine carrée car le terme de droite est positif (on a montré que f est positive sur $[0,a]$ et $\dfrac{a}{2^q} \in [0,a]$. Puisque l'on a aussi $\dfrac{a}{2^{q+1}} \in [0,a]$, on a aussi $f\left(\dfrac{a}{2^{q+1}}\right) \geq 0$. Ceci entraine que :

$$f\left(\frac{a}{2^{q+1}}\right) = \sqrt{\frac{f\left(\frac{a}{2^q}\right)+1}{2}}.$$

  Or, la fonction g est dans E d'après la partie I. Elle vérifie donc la même relation que la fonction f. Puisqu'elle est positive sur $[0,a]$, avec le même raisonnement, on obtient :

$$g\left(\frac{a}{2^{q+1}}\right) = \sqrt{\frac{g\left(\frac{a}{2^q}\right)+1}{2}}.$$

  En utilisant l'hypothèse de récurrence, on obtient alors $f\left(\dfrac{a}{2^{q+1}}\right) = g\left(\dfrac{a}{2^{q+1}}\right)$, ce qui est la propriété au rang $q+1$.
- La propriété étant initialisée et héréditaire, elle est vraie pour tout $q \in \mathbb{N}$.

c) On va faire une récurrence sur $p \in \mathbb{N}$ pour montrer $\mathcal{P}(p)$: « $\forall q \in \mathbb{N},\ f\left(\dfrac{pa}{2^q}\right) = g\left(\dfrac{pa}{2^q}\right)$ ».

- La propriété est vraie au rang $p = 0$ car $f(0) = g(0) = 1$ et vraie au rang 1 d'après la question ci-dessus.
- Soit $p \in \mathbb{N}^*$. Supposons la propriété vraie jusqu'au rang p (récurrence forte). Fixons $q \in \mathbb{N}$. On a alors, en utilisant que $f \in E$ en $x = \dfrac{pa}{2^q}$ et $y = \dfrac{a}{2^q}$:

$$\begin{aligned} f\left(\frac{(p+1)a}{2^q}\right) &= f\left(\frac{pa}{2^q} + \frac{a}{2^q}\right) \\ &= 2f\left(\frac{pa}{2^q}\right) f\left(\frac{a}{2^q}\right) - f\left(\frac{(p-1)a}{2^q}\right). \end{aligned}$$

  On a alors $p - 1 \geq 0$. Puisque l'on sait que la propriété est vraie au rang 0, 1 et que l'on fait une récurrence forte, on en déduit que :

$$f\left(\frac{(p+1)a}{2^q}\right) = 2g\left(\frac{pa}{2^q}\right) g\left(\frac{a}{2^q}\right) - g\left(\frac{(p-1)a}{2^q}\right).$$

Puisque g est également dans E, en reprenant le calcul effectué sur f pour g, on obtient alors $f\left(\frac{(p+1)a}{2^q}\right) = g\left(\frac{(p+1)a}{2^q}\right)$ ce qui prouve la propriété au rang $p+1$.

- La propriété étant intialisée et hérédiaire, elle est vraie pour tout $p \in \mathbb{N}$.

d) Les fonctions f et g sont paires. On peut donc étendre la propriété précédente à $p \in \mathbb{Z}$.

8) On pose $D = \left\{\frac{pa}{2^q},\ p \in \mathbb{Z},\ q \in \mathbb{N}\right\}$.

a) Soit $x \in \mathbb{R}$. On a $\frac{\lfloor y \rfloor}{y} \to 1$ quand y tend vers l'infini (ceci ce montre en utilisant le théorème des gendarmes et en encadrant $\lfloor y \rfloor$ entre $y-1$ et y). Ceci entraine que :

$$\lim_{n\to+\infty} \frac{\lfloor 2^n x \rfloor}{2^n x} = 1,$$

ce qui en multipliant par x donne le résultat voulu. On a en fait ici pour avoir le droit de divisé par x supposé que $x \neq 0$. On remarque que le résultat demandé s'obtient directement si $x = 0$.

b) La question ci-dessus montre exactement la caractérisation séquentielle de la densité pour l'ensemble D. En effet, si on fixe $x \in \mathbb{R}$, alors la suite précédente tend vers x quand n tend vers l'infini et si l'on pose $p = \lfloor 2^n x \rfloor \in \mathbb{Z}$ et $q = n \in \mathbb{N}$, on remarque que $\frac{\lfloor 2^n x \rfloor}{2^n x} \in D$. On a donc bien une suite d'éléments de D qui tend vers x. L'ensemble D est donc dense dans $\mathbb{R}$.

c) f et g sont deux fonctions continues égales sur un ensemble dense. Elles sont donc égales sur $\mathbb{R}$ tout entier. En effet, si on fixe $x \in \mathbb{R}$, par définition de D est dense dans $\mathbb{R}$, il existe une suite (x_n) d'éléments de D telle que $x_n \to x$ quand n tend vers l'infini. Or, on a démontré a la question 3 que pour tout $n \in \mathbb{N}$, $f(x_n) = g(x_n)$. En passant à la limite quand n tend vers l'infini, puisque f et g sont continues, on obtient $f(x) = g(x)$, ce qui prouve le résultat voulu.

9) On a montré que si f était dans E et s'annulait, alors f est la fonction nulle ou f est de la forme $x \mapsto \cos(\beta x)$ avec $\beta \in \mathbb{R}$. Réciproquement, toutes ces fonctions sont solutions d'après le I.

Partie III. Solutions qui ne s'annulent pas.

On suppose dans cette partie que $f \in E$ et ne s'annule pas.

10) Puisque f ne s'annule pas, on a $f(0) = 1$. Par l'absurde, si il existait $x \in \mathbb{R}$ tel que $f(x) \leq 0$, alors puisque f est continue et que $f(0) > 1$, on obtiendrait un zéro de f en utilisant le théorème des valeurs intermédiaires. Ceci entraine que f est strictement positive sur $\mathbb{R}$.

11)

a) Soit $n \in \mathbb{N}$. En appliquant la relation vérifiée par f en $x = y = 2^n$, on obtient exactement $u_{n+1} = 2u_n^2 - 1$.

b) On pose $h : x \mapsto 2x^2 - 1 - x$. f est dérivable sur $[0,1]$ et pour tout $x \in [0,1]$, $h'(x) = 4x - 1$. On a donc h' négative sur $[0, \frac{1}{4}]$ et positive sur $[\frac{1}{4}, 1]$. Ceci entraine que g est décroissante sur $[0, \frac{1}{4}]$ et croissante sur $[\frac{1}{4}, 1]$. Or, $h(0) = -1$ et $h(1) = 0$. Ceci entraine que h est négative sur $[0, 1[$.

On remarque que pour $n \in \mathbb{N}$, on a $h(u_n) = 2u_n^2 - 1 - u_n = u_{n+1} - u_n$. Montrons alors par récurrence la propriété $\mathcal{P}(n)$: « $0 \leq u_{n+1} \leq u_n < 1$ ».

- Pour $n = 0$, la propriété est vraie puisque $u_0 = f(1) < 1$ et $0 \leq u_0$ car la suite (u_n) est positive. On a alors $h(u_0) = u_1 - u_0 \leq 0$. Puisque $0 \leq u_1$ (car la suite (u_n) est positive), on en déduit que $1 \leq u_1 \leq u_0 < 1$.
- Si la propriété est vraie au rang $n \in \mathbb{N}$ fixé, alors on a comme ci-dessus $h(u_n) = u_{n+1} - u_n \leq 0$ car $u_n \in [0, 1[$. Puisque l'on a aussi $0 \leq u_{n+1}$ (car la suite (u_n) est positive), on en déduit que $1 \leq u_{n+1} \leq u_n < 1$.

- On a donc montré en particulier que pour tout $n \in \mathbb{N}$, $u_{n+1} \leq u_n$. La suite (u_n) est donc décroissante.

  c) La suite (u_n) est décroissante minorée. Elle converge donc vers $l \in [0,1[$. On a alors $u_{n+1} - u_n \to 0$ quand n tend vers l'infini. On en déduit que $2l^2 - 1 - l = 0$. On a donc $l = 1$ ou $l = -\dfrac{1}{2}$. Puisque la suite (u_n) est positive, elle tend doit tendre vers 1 sauf qu'elle est décroissante et $u_0 = f(1) < 1$. On a donc une absurdité.

12) D'après la question précédente, on a $f(1) \geq 1$. Puisque $\mathrm{ch} : \mathbb{R}_+ \to [1, +\infty[$ est bijective (on peut le montrer avec le théorème de la bijection car ch est continue, strict croissante sur $\mathbb{R}_+$ et vérifie $\mathrm{ch}(0) = 1$ et $\lim\limits_{x \to +\infty} \mathrm{ch}(x) = +\infty$). Il existe donc $\alpha \in \mathbb{R}_+$ tel que $f(1) = \mathrm{ch}(\alpha)$.

13) On pose alors $g : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & \mathrm{ch}(\alpha x) \end{array} \right.$.

On a toujours $\forall q \in \mathbb{N},\ f\left(\dfrac{1}{2^q}\right) + 1 = 2\left(f\left(\dfrac{1}{2^{q+1}}\right)\right)^2$ car pour le montrer, on a utilisé uniquement que $f \in E$ et que f était positive (ce qui est encore vrai ici).

Le fait que $\forall q \in \mathbb{N},\ f\left(\dfrac{1}{2^q}\right) = g\left(\dfrac{1}{2^q}\right)$ est encore vrai car elle est vraie en $q = 0$ et la récurrence marche de la même façon car f et g sont toutes les deux dans E (d'après la fin du I pour g). La récurrence de la question suivante marche de la même façon (on utilisait seulement le fait que f et g vérifient la relation donnée), on peut encore étendre la propriété à $\mathbb{Z}$ car les deux fonctions sont encore paires.

Aucun changement dans la question 4, les fonctions f et g sont égales sur un ensemble dense et continues. Elles sont donc égales sur $\mathbb{R}$.

14) Les fonctions f de E ne s'annulant pas sont donc de la forme $x \mapsto \mathrm{ch}(\alpha x)$ où $\alpha \in \mathbb{R}_+$. Or, ces fonctions appartiennent toutes à E d'après la partie I.

Les fonctions présentes dans l'ensemble E sont donc exactement les fonctions trouvées dans la partie I.

PROBLÈME
Résolution d'une équation diophantienne

Partie I. Étude de $\mathbb{Z}[\sqrt{2}]$

1) La loi + est bien associative, commutative. L'élément neutre pour cette loi est 0 qui est bien dans $\mathbb{Z}[\sqrt{2}]$ (on prend $a = b = 0$). $(\mathbb{Z}[\sqrt{2}], +)$ est stable par addition et par passage à l'opposé (car on considère $a, b \in \mathbb{Z}$). Il s'agit donc d'un groupe commutatif. De plus, la loi $\times$ est bien associative, distributive par rapport à l'addition. L'élément neutre pour la loi $\times$ est 1 qui est bien dans $\mathbb{Z}[\sqrt{2}]$ (on prend $a = 1$ et $b = 0$). Il reste à montrer que $\mathbb{Z}[\sqrt{2}]$ est bien stable pour cette loi. Si $a + b\sqrt{2}$ et $a' + b'\sqrt{2}$ sont dans $\mathbb{Z}[\sqrt{2}]$, alors, on a :

$$(a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' - 2bb') + (ab' + a'b)\sqrt{2}.$$

On a alors $aa' - 2bb' \in \mathbb{Z}$ et $ab' + a'b \in \mathbb{Z}$. On a donc bien $(a + b\sqrt{2})(a' + b'\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]$.

On a donc montré que $(\mathbb{Z}[\sqrt{2}], +, \times)$ est un anneau (commutatif).

2) Soit $x \in \mathbb{Z}[\sqrt{2}]$. Il existe alors $(a, b) \in \mathbb{Z}^2$ tels que $x = a + b\sqrt{2}$. Supposons qu'il existe $(a', b') \in \mathbb{Z}^2$ tels que $x = a' + b'\sqrt{2}$. On a alors :

$$(a - a') = \sqrt{2}(b - b').$$

Supposons par l'absurde $b \neq b'$. On a alors $\sqrt{2} = \dfrac{a - a'}{b - b'} \in \mathbb{Q}$. Ceci est absurde puisque $\sqrt{2}$ est irrationnel. On a donc $b = b'$, ce qui implique $a = a'$. On a donc montré l'unicité de l'écriture de x.

3) Un calcul direct permet de vérifier cette question.

4)

a) Soit $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. On a alors $N(x) = a^2 - 2b^2 \in \mathbb{Z}$ car a et b sont entiers.

b) Soient $x, x' \in \mathbb{Z}[\sqrt{2}]$. On a :

$$\begin{aligned} N(xx') &= xx'\overline{xx'} \\ &= xx'\overline{x}\overline{x'} \\ &= x\overline{x} \times x'\overline{x'} \\ &= N(x)N(x'). \end{aligned}$$

c) On va procéder par double implication.

($\Rightarrow$) Soit $x \in \mathbb{Z}[\sqrt{2}]$ inversible. Il existe donc $y \in \mathbb{Z}[\sqrt{2}]$ tel que $xy = 1$. On a alors $N(xy) = 1$ et donc $N(x)N(y) = 1$. Puisque $N(x)$ et $N(y)$ sont entiers, on en déduit que $N(x)$ divise 1. On a alors $N(x) = \pm 1$.

($\Leftarrow$) Soit $x \in \mathbb{Z}[\sqrt{2}]$ tel que $N(x) = \pm 1$. On a alors $x\overline{x} = \pm 1$. On en déduit que $\pm\overline{x}$ est l'inverse de x (puisque son produit avec x vaut 1). On a donc montré que x était inversible.

On a donc montré l'équivalence voulue.

d) Soit $H = \{x \in \mathbb{Z}[\sqrt{2}] \ / \ N(x) = \pm 1\}$.

- H contient 1 (car $N(1) = 1$).
- Si $x, y \in H$, on a alors $N(xy) = N(x)N(y) = \pm 1$. On a donc $xy \in H$. H est donc stable par produit.
- Si $x \in H$, alors on a $N(x) = \pm 1$ et donc d'après la question précédente, il existe $y \in \mathbb{Z}[\sqrt{2}]$ tel que $xy = 1$. On a $y \in H$ car $N(x)N(y) = 1$ et $N(x) = \pm 1$ et donc $N(y) = \pm 1$. On en déduit que x admet un inverse dans H.

On en déduit que $(H, \times)$ est un groupe.

Partie II. Étude de H

5) Soit $x = a + b\sqrt{2} \in H$.

a) Supposons que $a \geq 0$ et $b \geq 0$. Si $a = b = 0$, on a alors $x = 0$ donc $N(x) = 0$ ce qui est absurde (puisque $x \in H$, on a $N(x) = \pm 1$). On en déduit que soit a, soit b est supérieur ou égal à 1 (puisqu'ils sont entiers). Puisque $\sqrt{2} \geq 1$ (et que a et b sont tous les deux positifs), on a alors $x = a + b\sqrt{2} \geq 1$.

b) Supposons que $a \leq 0$ et $b \leq 0$. De la même manière que ci-dessus, on ne peut pas avoir $a = b = 0$. On en déduit que soit a, soit b est inférieur ou égal à -1 (puisqu'ils sont entiers). Puisque $\sqrt{2} \geq 1$ et que a et b sont tous les deux négatifs, on a alors $x = a + b\sqrt{2} \leq -1$.

c) Supposons que $ab \leq 0$ (c'est à dire a et b de signes opposés). On a alors que a et $-b$ sont de même signe. Puisque $\overline{x} = a - b\sqrt{2}$, on déduit des questions précédentes (appliquées à $\overline{x}$) que $|\overline{x}| \geq 1$. Or, on a $x\overline{x} = N(x) = \pm 1$, ce qui implique en prenant la valeur absolue que :

$$|x| \times |\overline{x}| = 1.$$

Puisque $|\overline{x}| \geq 1$ et que $|x| = \dfrac{1}{|\overline{x}|}$, on en déduit que $|x| \leq 1$.

6) Posons $H_+ = \{x \in H \ / \ x > 1\}$.

a) Soit $x = a + b\sqrt{2} \in H_+$. On a alors $x > 1$. D'après les questions précédentes, si on avait $a \leq 0$ et $b \leq 0$, on aurait alors une absurdité (car cela implique que $x \leq -1$). De même si a et b étaient de signe opposé, on aurait $|x| \leq 1$ ce qui contredirait également le fait que $x > 1$. On en déduit que a et b sont tous les deux strictements positifs (puisque si l'un des deux était nul, on aurait $ab \leq 0$ et donc $|x| \leq 1$). On en déduit que $a > 0$ et $b > 0$.

b) Soit $x = a + b\sqrt{2} \in H_+$. D'après la question précédente, $a > 0$ et $b > 0$. Puisqu'ils sont entiers, on a donc $a \geq 1$ et $b \geq 1$. On a donc $x \geq 1 + \sqrt{2}$. On en déduit que u est un minorant de H_+.

De plus, on a $N(u) = 1 - 2 = -1$. On a donc $N(u) = \pm 1$ et on a $u > 1$ car $\sqrt{2} > 0$. On en déduit que $u \in H_+$. C'est donc bien le minimum de H_+.

7) Soit $x \in H_+$.

a) Posons $A = \{p \in \mathbb{N}^* \ / \ u^p \leq x\}$. A est non vide (il contient toujours 1 puisque u est le minimum de H_+). De plus, puisque la suite $(u^p)_{p \in \mathbb{N}^*}$ tend vers $+\infty$ (car $u > 1$), il existe $N \in \mathbb{N}$ tel que $u_N > x$. Puisque la suite $(u^p)_{p \in \mathbb{N}^*}$ est strictement croissante (on multiplie à chaque étape par $u > 1$), on en déduit que pour tout $p \geq N$, $u^p > x$. Ceci implique que N est un majorant de A.

A est une partie de $\mathbb{N}$ non vide majorée. Elle admet donc un maximum n. Cet entier vérifie $u^n \leq x$ et $u^{n+1} > x$ (car $n + 1 \notin A$). On a donc bien construit un entier $n \in \mathbb{N}^*$ (puisque $1 \in A$, on a $n \geq 1$) comme demandé.

b) Supposons que $x > u^n$. On a alors $1 < \dfrac{x}{u^n} < u$ (puisque $u^n > 0$, on ne change pas le signe des inégalités). Or, on a $\dfrac{x}{u^n} \in H$ puisque H est un groupe pour la loi $\times$. Puisque $1 < \dfrac{x}{u^n}$, on en déduit que $\dfrac{x}{u^n} \in H_+$. Ceci est absurde puisque cet élément est strictement plus petit que u, le minimum de H_+ !

On en déduit que $x \leq u^n$, ce qui implique, puisque $u^n \leq x$, que $x = u^n$.

c) Notons $B = \{\pm u^n, \ n \in \mathbb{Z}\}$. On va procéder par double inclusion. Puisque H est un groupe pour la loi $\times$ et que $u \in H$, on a que $\{u^n, \ n \in \mathbb{Z}\} \subset H$. De plus, si $x \in H$, on a également $-x \in H$ (car on a $-x \in \mathbb{Z}[\sqrt{2}]$ et que $N(-x) = N(-1)N(x) = N(x)$). On a donc que $B \subset H$.

Réciproquement, soit $x \in H$.

- Si $x > 1$, alors d'après la question précédente, il existe $n \in \mathbb{N}^*$ tel que $x = u^n$. On a donc $x \in B$. Si $x < -1$, on a alors $-x > 1$ et on a alors $-x \in H_+$ (toujours puisque H est stable par passage à l'opposé). Il existe donc $n \in \mathbb{N}^*$ tel que $-x = u^n$. On a donc $x = -u^n$ et donc $x \in B$.

- Si $x = 1$ ou $x = -1$, alors, on a $x = u^0$ ou $x = -u^0$ et on a encore $x \in B$.

- Supposons à présent que $|x| < 1$. On a alors $\left|\dfrac{1}{x}\right| > 1$ et $\dfrac{1}{x} \in H$ (puisque H est un groupe pour la loi $\times$). On a alors, en appliquant le premier point à $\dfrac{1}{x}$, on a que $\dfrac{1}{x} \in B$. Puisque B est stable par passage à l'inverse (puisque l'on autorise les puissances à être dans $\mathbb{Z}$), on en déduit que $x \in B$.

Dans tous les cas, on a montré que $x \in B$. On a donc $H \subset B$. On a bien montré que $H = \{\pm u^n,\ n \in \mathbb{Z}\}$.

Ceci décrit alors l'ensemble des solutions de l'équation proposée comme les $\pm(1+\sqrt{2})^n$ avec $n \in \mathbb{Z}$. En développant cette expression avec le binôme de Newton (en séparant les termes pairs et impairs pour faire apparaitre des entiers et des entiers multipliés par $\sqrt{2}$), on peut trouver une expression explicite des couples d'entiers solutions.