UN CORRIGÉ DU DEVOIR LIBRE N°9

Nous définissons la partie $\mathbb{Z}\left[\sqrt{2}\right]$ *de* $\mathbb{R}$ *par* $\mathbb{Z}\left[\sqrt{2}\right] := \left\{a+b\sqrt{2} \,:\, (a,b)\in\mathbb{Z}^2\right\}$.

Q1 — Soit $x\in\mathbb{Z}\left[\sqrt{2}\right]$. Justifier que l'écriture de x sous la forme $a+b\sqrt{2}$, avec $(a,b)\in\mathbb{Z}^2$, est unique.

Soient $(a_1,b_1)\in\mathbb{Z}^2$ et $(a_2,b_2)\in\mathbb{Z}^2$ tels que $x=a_1+b_1\sqrt{2}$ et $x=a_2+b_2\sqrt{2}$. Alors

$$a_1-a_2=(b_2-b_1)\sqrt{2} \tag{1}$$

Si $b_1\neq b_2$, alors $\sqrt{2}=\dfrac{a_1-a_2}{b_2-b_1}\in\mathbb{Q}$, ce qui est faux. Donc $b_1=b_2$ et, d'après (1), $a_1=a_2$.

Q2 — Démontrer que, pour tout $(x_1,x_2)\in\mathbb{Z}\left[\sqrt{2}\right]\times\mathbb{Z}\left[\sqrt{2}\right]$, $-x_1$, x_1+x_2 et x_1x_2 appartiennent à $\mathbb{Z}\left[\sqrt{2}\right]$.

Soit $(x_1,x_2)\in\mathbb{Z}\left[\sqrt{2}\right]^2$. Alors il existe $(a_1,b_1)\in\mathbb{Z}^2$ et $(a_2,b_2)\in\mathbb{Z}^2$ tels que $x_1=a_1+b_1\sqrt{2}$ et $x_2=a_2+b_2\sqrt{2}$.

- Nous calculons
$$-x_1=-a_1+(-b_1)\sqrt{2}$$

Comme $\mathbb{Z}$ est stable par passage à l'opposé, $-a_1\in\mathbb{Z}$ et $-b_1\in\mathbb{Z}$. Ainsi, $-x_1\in\mathbb{Z}\left[\sqrt{2}\right]$.

- On calcule
$$x_1+x_2=(a_1+a_2)+(b_1+b_2)\sqrt{2} \quad\text{et}\quad x_1\cdot x_2=(a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}$$

Comme $\mathbb{Z}$ est stable par addition et par multiplication, les éléments

$$a_1+a_2\,,\ b_1+b_2\,,\ a_1a_2+2b_1b_2\,,\ a_1b_2+a_2b_1$$

appartiennent à $\mathbb{Z}$. Ainsi, $x_1+x_2\in\mathbb{Z}\left[\sqrt{2}\right]$ et $x_1x_2\in\mathbb{Z}\left[\sqrt{2}\right]$.

Remarque Comme de plus 0 et 1 sont des éléments de $\mathbb{Z}\left[\sqrt{2}\right]$, nous avons démontré que $\mathbb{Z}\left[\sqrt{2}\right]$ est un sous-anneau de $(\mathbb{R},+,\times)$.

Soit l'application σ *définie par*

$$\sigma \;\left|\begin{array}{ccc} \mathbb{Z}\left[\sqrt{2}\right] & \longrightarrow & \mathbb{Z}\left[\sqrt{2}\right] \\ a+b\cdot\sqrt{2},\ \textit{avec}\ (a,b)\in\mathbb{Z}^2 & \longmapsto & a-b\cdot\sqrt{2}\,. \end{array}\right.$$

Q3 — Vérifier que, pour tout $(x_1,x_2)\in\mathbb{Z}\left[\sqrt{2}\right]\times\mathbb{Z}\left[\sqrt{2}\right]$

$$\sigma(x_1+x_2)=\sigma(x_1)+\sigma(x_2) \qquad\text{et}\qquad \sigma(x_1x_2)=\sigma(x_1)\sigma(x_2)$$

puis démontrer que σ est bijective.

- L'application σ est bien définie, d'après **Q1**.
- Soient $(x_1,x_2)\in\mathbb{Z}\left[\sqrt{2}\right]^2$. Alors il existe $(a_1,b_1)\in\mathbb{Z}^2$ et $(a_2,b_2)\in\mathbb{Z}^2$ tels que $x_1=a_1+b_1\sqrt{2}$ et $x_2=a_2+b_2\sqrt{2}$. Comme
$$x_1+x_2=\underbrace{a_1+a_2}_{\in\mathbb{Z}}+\underbrace{(b_1+b_2)}_{\in\mathbb{Z}}\sqrt{2}$$
on a
$$\sigma(x_1+x_2)=a_1+a_2-(b_1+b_2)\sqrt{2}=a_1-b_1\sqrt{2}+a_2-b_2\sqrt{2}=\sigma(x_1)+\sigma(x_2)$$
Donc σ respecte l'addition.

- Comme
$$x_1x_2 = \underbrace{a_1a_2+2b_1b_2}_{\in\mathbb{Z}} + \underbrace{(a_1b_2+a_2b_1)}_{\in\mathbb{Z}}\sqrt{2}\,.$$
on a
$$\sigma(x_1x_2) = a_1a_2+2b_1b_2-(a_1b_2+a_2b_1)\sqrt{2} \tag{2}$$
D'autre part
$$\sigma(x_1)\,\sigma(x_2) = \left(a_1-b_1\sqrt{2}\right)\left(a_2-b_2\sqrt{2}\right) = a_1a_2+2b_1b_2-(a_1b_2+a_2b_1)\sqrt{2} \tag{3}$$
En comparant (2) et (3), il vient $\sigma(x_1x_2) = \sigma(x_1)\,\sigma(x_2)$. Donc σ respecte la multiplication.
- Soit $x \in \mathbb{Z}\left[\sqrt{2}\right]$. Alors il existe $(a,b) \in \mathbb{Z}^2$ tel que $x = a+b\sqrt{2}$. On calcule
$$\sigma^2(x) = \sigma(\sigma(x)) = \sigma\left(\underbrace{a}_{\in\mathbb{Z}} + \underbrace{(-b)}_{\in\mathbb{Z}}\sqrt{2}\right) = a+b\sqrt{2} = x$$
et on en déduit $\sigma^2 = \mathrm{id}_{\mathbb{Z}[\sqrt{2}]}$. L'application σ est donc bijective et a pour application inverse elle-même (on parle alors d'involution).

Remarque Comme de plus $\sigma(1) = 1$, nous avons démontré que σ est un isomorphisme d'anneaux. L'application σ est l'unique endomorphisme de l'anneau $\left(\mathbb{Z}\left[\sqrt{2}\right],+,\times\right)$ tel que $\sigma\left(\sqrt{2}\right) = -\sqrt{2}$.

Soit l'application norme, notée N, définie par :
$$N \;\left|\begin{array}{ccc}\mathbb{Z}\left[\sqrt{2}\right] & \longrightarrow & \mathbb{N} \\ x & \longmapsto & |x\cdot\sigma(x)|\,.\end{array}\right.$$

Q4 — Démontrer que, pour tout $x \in \mathbb{Z}\left[\sqrt{2}\right]$, $x = 0$ si et seulement si $N(x) = 0$.

Nous raisonnons par double implication.
$\boxed{\Longrightarrow}$ Si $x = 0$, alors $N(x) = 0$ est clair.
$\boxed{\Longleftarrow}$ Supposons $N(x) = 0$. Comme $x \in \mathbb{Z}\left[\sqrt{2}\right]$, il existe $(a,b) \in \mathbb{Z}^2$ tel que $x = a+b\sqrt{2}$. De $N(x) = 0$, nous déduisons
$$a^2 = 2b^2 \tag{4}$$
Si $b \neq 0$, alors $\left(\frac{a}{b}\right)^2 = 2$ et donc $\left|\frac{a}{b}\right| = \sqrt{2}$. Comme $\left|\frac{a}{b}\right| \in \mathbb{Q}$, ceci est en contradiction avec $\sqrt{2} \notin \mathbb{Q}$. Nous en déduisons que $b = 0$, puis que $a = 0$, d'après (4). Ainsi, $x = 0$.

Q5 — Démontrer que, pour tout $(x_1,x_2) \in \mathbb{Z}\left[\sqrt{2}\right] \times \mathbb{Z}\left[\sqrt{2}\right]$, $N(x_1x_2) = N(x_1)N(x_2)$.

Nous calculons
$$\begin{array}{rcll} N(x_1x_2) & := & |x_1x_2\sigma(x_1x_2)| & \\ & = & |x_1\,x_2\,\sigma(x_1)\,\sigma(x_2)| & \left[\sigma \text{ respecte la multiplication}\right] \\ & = & |x_1\,\sigma(x_1)\;x_2\,\sigma(x_2)| & \\ & = & |x_1\,\sigma(x_1)|\,|x_2\,\sigma(x_2)| & \left[\text{la valeur absolue est multiplicative}\right] \\ & = & N(x_1)\,N(x_2) & \end{array}$$

Un élément x de $\mathbb{Z}[\sqrt{2}]$ est appelé unité s'il existe $y \in \mathbb{Z}[\sqrt{2}]$ tel que $x \cdot y = 1$. L'ensemble des unités de $\mathbb{Z}[\sqrt{2}]$ est noté U.

Q6 — Démontrer que, pour tout $x \in \mathbb{Z}[\sqrt{2}]$, $x \in U$ si et seulement si $N(x) = 1$.

Soit $x \in \mathbb{Z}[\sqrt{2}]$. Nous raisonnons par double implication.
$\boxed{\Longrightarrow}$ Supposons que $x \in U(\mathbb{Z}[\sqrt{2}])$. Alors il existe $y \in \mathbb{Z}[\sqrt{2}]$ tel que $xy = 1$. Grâce à **Q5**

$$N(x)N(y) = N(xy) = N(1) = 1$$

Comme $N(x)$ et $N(y)$ sont deux entiers naturels dont le produit vaut 1, chacun des deux est égal à 1. En particulier, $N(x) = 1$.
$\boxed{\Longleftarrow}$ Supposons que $N(x) = 1$. Comme $x \in \mathbb{Z}[\sqrt{2}]$, il existe $(a,b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$. Puisque $N(x) = \left|a^2 - 2b^2\right| = 1$, l'entier $a^2 - 2b^2$ appartient à$\{-1, 1\}$.

- Supposons $a^2 - 2b^2 = 1$. Alors

$$x\left(a + (-b)\sqrt{2}\right) = \left(a + b\sqrt{2}\right)\left(a + (-b)\sqrt{2}\right) = 1$$

  Comme a et $-b$ sont des entiers relatifs, le nombre $y := a + (-b)\sqrt{2}$ appartient à $\mathbb{Z}[\sqrt{2}]$. Nous en déduisons que x est inversible dans l'anneau $(\mathbb{Z}[\sqrt{2}], +, \times)$, d'inverse y.
- Supposons $a^2 - 2b^2 = -1$. Alors

$$x\left((-a) + b\sqrt{2}\right) = \left(a + b\sqrt{2}\right)\left((-a) + b\sqrt{2}\right) = 1$$

  Comme $-a$ et b sont des entiers relatifs, le nombre $y := a + (-b)\sqrt{2}$ appartient à $\mathbb{Z}[\sqrt{2}]$. Nous en déduisons que x est inversible dans l'anneau $(\mathbb{Z}[\sqrt{2}], +, \times)$, d'inverse y.

Dans les deux cas, x est inversible dans l'anneau $(\mathbb{Z}[\sqrt{2}], +, \times)$.

Q7 — Soit x un élément non nul de $\mathbb{Z}[\sqrt{2}]$ et $y \in \mathbb{Z}[\sqrt{2}]$. Démontrer qu'il existe $(q,r) \in \mathbb{Z}[\sqrt{2}] \times \mathbb{Z}[\sqrt{2}]$ tel que

$$y = q \cdot x + r \quad \text{et} \quad N(r) < N(x)\,.$$

Le couple (q,r) est-il nécessairement unique ?

- Comme x et y appartiennent à $\mathbb{Z}[\sqrt{2}]$, il existe $(a,b)\mathbb{Z}^2$ et $(c,d) \in \mathbb{Z}^2$ tels que $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$. Comme σ est un automorphisme de l'anneau $(\mathbb{Z}[\sqrt{2}], +, \times)$:

$$\sigma(x) = a - b\sqrt{2} \neq 0\,.$$

Le calcul suivant est alors licite dans le corps des réels.

$$\frac{y}{x} = \frac{c + d\sqrt{2}}{a + b\sqrt{2}} \times \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \underbrace{\frac{ac - 2bd}{a^2 - 2b^2}}_{=:u \in \mathbb{Q}} + \underbrace{\frac{ad - bc}{a^2 - 2b^2}}_{=:v \in \mathbb{Q}}\sqrt{2} \tag{5}$$

- Remarquons que si α est un nombre rationnel (ou réel)

$$\exists\, n \in \mathbb{Z} \qquad |\alpha - n| \leqslant \frac{1}{2} \qquad [n \text{ est un entier le plus proche de } \alpha]$$

En effet, si $\alpha - \lfloor\alpha\rfloor \leqslant \dfrac{1}{2}$ l'entier relatif $\lfloor\alpha\rfloor$ convient, sinon l'entier relatif $\lfloor\alpha\rfloor + 1$ convient.

- Soient donc e et f des entiers relatifs, respectivement les plus proches de u et v, i.e. tels que

$$|e-u| \leqslant \frac{1}{2} \quad \text{et} \quad |f-v| \leqslant \frac{1}{2} \tag{6}$$

Posons alors

$$q := e + f\sqrt{2} \quad \text{et} \quad r := y - qx$$

Il est clair que $q \in \mathbb{Z}\left[\sqrt{2}\right]$. Comme $\mathbb{Z}\left[\sqrt{2}\right]$ est stable par addition, par multiplication et par passage à l'opposé (cf. **Q2**), le nombre r appartient également à $\mathbb{Z}\left[\sqrt{2}\right]$. La relation $y = qx + r$ découle de la définition même de r. Il reste uniquement à vérifier si $N(r) < N(x)$.

- En utilisant (5) et la définition de q, nous calculons

$$r = \left(\frac{y}{x} - q\right) x = \left(\underbrace{(u-e)}_{\in\mathbb{Q}} + \underbrace{(v-f)}_{\in\mathbb{Q}}\sqrt{2}\right)\left(a + b\sqrt{2}\right) \tag{7}$$

On vérifie alors, par un calcul qui ne découle pas strictement de **Q3**, mais qui repose sur les mêmes ressorts

$$\sigma(r) = \left((u-e) - (v-f)\sqrt{2}\right)\left(a - b\sqrt{2}\right) \tag{8}$$

D'après (7) et (8)

$$N(r) = \left|\left((u-e) + (v-f)\sqrt{2}\right)\left((u-e) - (v-f)\sqrt{2}\right)\right| \left|\left(a + b\sqrt{2}\right)\left(a - b\sqrt{2}\right)\right| = \left|(u-e)^2 - 2(v-f)^2\right| N(x) \tag{9}$$

En utilisant les inégalités (6), nous établissons

$$-\frac{1}{2} \leq (u-e)^2 - 2(v-f)^2 \leqslant \frac{1}{4}$$

d'où

$$\left|(u-e)^2 - 2(v-f)^2\right| \leqslant \frac{1}{2} \tag{10}$$

Enfin, en combinant (9) et (10), on obtient le résultat manquant

$$N(r) \leqslant \frac{1}{2} N(x) < N(x)$$

Pour obtenir cette dernière inégalité, $N(x) > 0$ est essentiel (cf. ensemble d'arrivée de l'application N et **Q4**).

- Étudions à présent l'unicité éventuelle d'un couple $(q, r) \in \mathbb{Z}\left[\sqrt{2}\right] \times \mathbb{Z}\left[\sqrt{2}\right]$ tel que

$$y = q \cdot x + r \quad \text{et} \quad N(r) < N(x)$$

En analysant la construction précédente, nous remarquons que si u (resp. v) égale $\dfrac{1}{2}$ alors on dispose de deux choix (0 et 1) pour e (resp. f). Cette situation se produit, par exemple pour $x = 2 \in \mathbb{Z}\left[\sqrt{2}\right]$ et $y = 1 + \sqrt{2} \in \mathbb{Z}\left[\sqrt{2}\right]$, puisque, pour ces valeurs

$$\frac{y}{x} = \underbrace{\frac{1}{2}}_{u} + \underbrace{\frac{1}{2}}_{v}\sqrt{2}$$

Dans ce cas, les différents choix pour $e \in \{0,1\}$ et $f \in \{0,1\}$ dans notre construction, livrent quatre couples (q,r), qui conviennent tous.

$$y = \underbrace{0}_{q_1 \in \mathbb{Z}[\sqrt{2}]} \cdot x + \underbrace{y}_{r_1 = 1+\sqrt{2} \in \mathbb{Z}[\sqrt{2}]} \quad \text{avec} \quad N(r_1) = 1 < 4 = N(x)$$

$$y = \underbrace{1}_{q_2 \in \mathbb{Z}[\sqrt{2}]} \cdot x + \underbrace{y-x}_{r_2 = -1+\sqrt{2} \in \mathbb{Z}[\sqrt{2}]} \quad \text{avec} \quad N(r_2) = 1 < 4 = N(x)$$

$$y = \underbrace{\sqrt{2}}_{q_3 \in \mathbb{Z}[\sqrt{2}]} \cdot x + \underbrace{y-\sqrt{2}x}_{r_3 = 1-\sqrt{2} \in \mathbb{Z}[\sqrt{2}]} \quad \text{avec} \quad N(r_3) = 1 < 4 = N(x)$$

$$y = \underbrace{\left(1+\sqrt{2}\right)}_{q_4 \in \mathbb{Z}[\sqrt{2}]} \cdot x + \underbrace{y-\left(1+\sqrt{2}\right)x}_{r_4 = -1-\sqrt{2} \in \mathbb{Z}[\sqrt{2}]} \quad \text{avec} \quad N(r_4) = 1 < 4 = N(x)$$

Cet exemple met en défaut l'unicité.

Q8 — Justifier que $1+\sqrt{2} \in U$.

Nous calculons $N\left(1+\sqrt{2}\right) = 1$. D'après **Q6**, $1+\sqrt{2} \in U\left(\mathbb{Z}\left[\sqrt{2}\right]\right)$.

Remarque $\left(1+\sqrt{2}\right)^{-1} = -1-\sqrt{2}$.

Q9 — Soit $u \in U$ tel que $u > 1$. Démontrer que $u \geqslant 1+\sqrt{2}$ puis qu'il existe $n \in \mathbb{N}^*$ tel que $u = \left(1+\sqrt{2}\right)^n$.

- Comme $u \in \mathbb{Z}\left[\sqrt{2}\right]$, il existe $(a,b) \in \mathbb{Z}^2$ tel que $u = a+b\sqrt{2}$. Comme u est inversible dans l'anneau $\left(\mathbb{Z}\left[\sqrt{2}\right],+,\times\right)$

$$N(u) = a^2 - 2b^2 = \left(a+b\sqrt{2}\right)\left(a-b\sqrt{2}\right) = 1 \tag{11}$$

d'après **Q6**. Comme

$$u = a+b\sqrt{2} > 1 \tag{12}$$

$a-b\sqrt{2} > 0$ et donc

$$a > b\sqrt{2} \tag{13}$$

En combinant (12) et (13), nous obtenons

$$2a > 1$$

Comme $a \in \mathbb{Z}$, nous en déduisons

$$a \geqslant 1 \tag{14}$$

- D'après (11) et (12)

$$a-b\sqrt{2} < 1$$

d'où

$$a-1 < b\sqrt{2} \tag{15}$$

En combinant (14) et (15), nous obtenons

$$0 < b\sqrt{2}$$

Comme $b \in \mathbb{Z}$, nous en déduisons

$$b \geqslant 1$$

- Puisque $a \geqslant 1$ et $b \geqslant 1$, $u = a + b\sqrt{2} \geqslant 1 + \sqrt{2}$.
- La suite géométrique de raison $\left(\left(1+\sqrt{2}\right)^n\right)_{n\in\mathbb{N}^*}$, de raison $1+\sqrt{2} > 1$, diverge vers $+\infty$. Le nombre u ne la majore donc pas, i.e. il existe un entier N tel que

$$u \leqslant \left(1+\sqrt{2}\right)^N$$

Aussi la partie de $\mathbb{N}$ définie par

$$\left\{k \in \mathbb{N} : u \leqslant \left(1+\sqrt{2}\right)^k\right\}$$

est-elle non vide. Elle admet donc un plus petit élément, noté n. Comme $u > 1$, $n \geqslant 1$.

- Nous démontrons que $u = \left(1+\sqrt{2}\right)^n$, en raisonnant par l'absurde. Supposons donc $u \neq \left(1+\sqrt{2}\right)^n$. Par définition de l'entier n, il vient alors

$$\left(1+\sqrt{2}\right)^{n-1} < u < \left(1+\sqrt{2}\right)^n$$

puis

$$1 < \underbrace{u\left(1+\sqrt{2}\right)^{-(n-1)}}_{=:u'} < 1+\sqrt{2} \tag{16}$$

Comme l'ensemble des éléments inversibles de l'anneau $\left(\mathbb{Z}\left[\sqrt{2}\right], +, \times\right)$ forme un groupe (pour la multiplication)

$$u' := u\left(1+\sqrt{2}\right)^{-(n-1)} \in U\left(\mathbb{Z}\left[\sqrt{2}\right]\right) \tag{17}$$

Les propriétés (16) et (17) contredisent le résultat obtenu dans la première partie de notre réponse. En effet, nous avons trouvé un élément inversible u' de l'anneau $\left(\mathbb{Z}\left[\sqrt{2}\right], +, \times\right)$ qui est strictement plus grand que 1, mais qui n'est pas supérieur ou égal à $1+\sqrt{2}$.

Soit l'application φ définie par

$$\varphi \left| \begin{array}{ccc} \{-1,1\}\times\mathbb{Z} & \longrightarrow & U \\ (\varepsilon, n) & \longmapsto & \varepsilon\left(1+\sqrt{2}\right)^n \end{array} \right.$$

Q10 — Vérifier que, pour tout $(\varepsilon_1, n_1) \in \{-1,1\}\times\mathbb{Z}$ et $(\varepsilon_2, n_2) \in \{-1,1\}\times\mathbb{Z}$:

$$\varphi(\varepsilon_1\varepsilon_2, n_1+n_2) = \varphi(\varepsilon_1, n_1)\,\varphi(\varepsilon_2, n_2)$$

puis démontrer que φ est bijective. Il s'agit d'un cas particulier du théorème des unités de Dirichlet.

- Soient $(\varepsilon_1, n_1) \in \{-1,1\}\times\mathbb{Z}$ et $(\varepsilon_2, n_2) \in \{-1,1\}\times\mathbb{Z}$. Comme $\left(U\left(\mathbb{Z}\left[\sqrt{2}\right]\right), \times\right)$ est un groupe abélien

$$\varphi\left((\varepsilon_1, n_1).(\varepsilon_2, n_2)\right) = (\varepsilon_1\varepsilon_2, n_1+n_2) = \varepsilon_1\varepsilon_2\left(1+\sqrt{2}\right)^{n_1+n_2} = \underbrace{\varepsilon_1\left(1+\sqrt{2}\right)^{n_1}}_{\varphi((\varepsilon_1,n_1))}\ \underbrace{\varepsilon_2\left(1+\sqrt{2}\right)^{n_2}}_{\varphi((\varepsilon_2,n_2))}$$

- D'après le point précédent, l'application φ est un morphisme de groupes. Pour établir son injectivité, nous démontrons que son noyau ne contient qu'un seul élément, le neutre $(1,0)$ du groupe (produit) à la

source de φ.

- Soit $(\varepsilon, n) \in \mathrm{Ker}(\varphi) \subset \{-1,1\} \times \mathbb{Z}$. Alors

$$\varepsilon \left(1+\sqrt{2}\right)^n = 1$$

Comme $\left(1+\sqrt{2}\right)^n > 0$, nécessairement $\varepsilon > 0$. Par suite $\varepsilon = 1$. Ensuite, comme $\left(1+\sqrt{2}\right)^n = 1$

$$n \underbrace{\ln\left(1+\sqrt{2}\right)}_{\neq 0} = 0$$

et donc $n = 0$. Nous avons établi $(\varepsilon, n) = (1,0)$.

- Soit $u \in U(\mathbb{Z}[\sqrt{2}])$. Alors nous distinguons six cas.
  - Cas 1 : $u > 1$. D'après **Q9**, il existe $n \in \mathbb{N}^*$ tel que $u = \left(1+\sqrt{2}\right)^n$. Donc $u = \varphi((1,n))$.
  - Cas 2 : $u = 1$. $u = \varphi((1,0))$.
  - Cas 3 : $0 < u < 1$. Comme $u \in U\left(\mathbb{Z}[\sqrt{2}]\right)$, $u^{-1} = \dfrac{1}{u} \in U\left(\mathbb{Z}[\sqrt{2}]\right)$. Comme $u^{-1} > 1$, le cas 1, nous permet d'affirmer qu'il existe $n \in \mathbb{N}^*$ tel que $\varphi((1,n)) = u^{-1}$. Puisque φ est un morphisme de groupes, $\varphi((1,-n)) = u$.
  - Cas 4 : $-1 < u < 0$. Comme $N(-u) = N(u) = 1$, $-u \in U\left(\mathbb{Z}[\sqrt{2}]\right)$ (cf. **Q6**). Comme $0 < -u < 1$, le cas 3 nous livre un $n \in \mathbb{Z}$ tel que $\varphi((1,n)) = -u$. Alors on remarque que $\varphi((-1,n)) = u$.
  - Cas 5 : $u = -1$. $u = \varphi((-1,0))$.
  - Cas 6 : $u < -1$. Comme $N(-u) = N(u) = 1$, $-u \in U\left(\mathbb{Z}[\sqrt{2}]\right)$ (cf. **Q6**). Comme $-u < 1$, le cas n°1 nous livre un $n \in \mathbb{N}^*$ tel que $\varphi((1,n)) = -u$. Alors on remarque que $\varphi((-1,n)) = u$.

Dans tous les cas, u possède un antécédent par l'application φ. Donc l'application φ est surjective.

Remarque Nous avons établi que l'application φ est un isomorphisme de groupes.

Q11 — Déterminer l'ensemble solution de l'équation de Pell-Fermat :

$$(E) \qquad a^2 - 2b^2 = 1$$

d'inconnue $(a,b) \in \mathbb{Z}^2$.

Nous raisonnons par analyse et synthèse.

- Analyse. Soit $(a,b) \in \mathbb{Z}^2$ tel que $a^2 - 2b^2 = 1$. Alors $a + b\sqrt{2} \in U\left(\mathbb{Z}[\sqrt{2}]\right)$ (cf. **Q6**). D'après **Q10**, il existe un unique $\varepsilon \in \{-1,1\}$ et un unique $n \in \mathbb{Z}$ tel que

$$a + b\sqrt{2} = \varepsilon \left(1+\sqrt{2}\right)^n.$$

Nous en déduisons $a - b\sqrt{2} = \varepsilon \left(1-\sqrt{2}\right)^n$ (cf. **Q3**). Comme

$$1 = a^2 - 2b^2 = \left(a+b\sqrt{2}\right)\left(a-b\sqrt{2}\right) = \varepsilon \left(1+\sqrt{2}\right)^n \varepsilon \left(1-\sqrt{2}\right)^n = \varepsilon^2 \left(\left(1+\sqrt{2}\right)\left(1-\sqrt{2}\right)\right)^n = (-1)^n$$

l'entier n est nécessairement pair. Posons alors $n = 2p$, où $p \in \mathbb{Z}$.

— Cas 1 : $p = 0$. Alors $a + b\sqrt{2} = \varepsilon \left(1+\sqrt{2}\right)^0 = \varepsilon$. On en déduit deux couples candidats pour être solutions de l'équation (E)

$$(a,b) = (\varepsilon, 0) \quad \text{où} \quad \varepsilon \in \{-1,1\}$$

— Cas 2 : $p \in \mathbb{N}^*$. Alors $a+b\sqrt{2} = \varepsilon\left(1+\sqrt{2}\right)^{2p} = \varepsilon\left(3+2\sqrt{2}\right)^p$. Ainsi

$$a = \frac{\varepsilon\left(3+2\sqrt{2}\right)^p + \sigma\left(\varepsilon\left(3+2\sqrt{2}\right)^p\right)}{2} = \frac{\varepsilon}{2}\left(\left(3+2\sqrt{2}\right)^p + \left(3-2\sqrt{2}\right)^p\right)$$

et

$$b = \frac{\varepsilon\left(3+2\sqrt{2}\right)^p - \sigma\left(\varepsilon\left(3+2\sqrt{2}\right)^p\right)}{2} = \frac{\varepsilon}{2}\left(\left(3+2\sqrt{2}\right)^p - \left(3-2\sqrt{2}\right)^p\right)$$

— Cas 2 : $p \in \mathbb{Z}_{\leqslant -1}$. Alors, comme $\left(1+\sqrt{2}\right)^{-1} = -1+\sqrt{2}$

$$a+b\sqrt{2} = \varepsilon\left(1+\sqrt{2}\right)^{2p} = \varepsilon\left(-1+\sqrt{2}\right)^{2q} = \varepsilon\left(3-2\sqrt{2}\right)^q$$

où $q := -p \in \mathbb{N}^*$. Ainsi

$$a = \frac{\varepsilon\left(3-2\sqrt{2}\right)^q + \sigma\left(\varepsilon\left(3-2\sqrt{2}\right)^q\right)}{2} = \frac{\varepsilon}{2}\left(\left(3-2\sqrt{2}\right)^q + \left(3+2\sqrt{2}\right)^q\right)$$

et

$$b = \frac{\varepsilon\left(3-2\sqrt{2}\right)^q - \sigma\left(\varepsilon\left(3-2\sqrt{2}\right)^q\right)}{2} = \frac{\varepsilon}{2}\left(\left(3-2\sqrt{2}\right)^q - \left(3+2\sqrt{2}\right)^p\right)$$

• Conclusion de l'analyse. Les différents couples candidats pour être solutions de (E), obtenus dans les trois cas ci-dessus, peuvent être regroupés en deux familles

— $(a,b) = (\varepsilon, 0)$ où $\varepsilon \in \{-1,1\}$

— $(a,b) = \left(\frac{\varepsilon_1}{2}\left(\left(3+2\sqrt{2}\right)^p + \left(3-2\sqrt{2}\right)^p\right), \frac{\varepsilon_2}{2}\left(\left(3+2\sqrt{2}\right)^p - \left(3-2\sqrt{2}\right)^p\right)\right)$ où $(\varepsilon_1, \varepsilon_2, p) \in \{-1,1\} \times \{-1,1\} \times \mathbb{N}^*$

• Synthèse. Si $\varepsilon \in \{-1,1\}$ alors $(a,b) = (\varepsilon, 0)$ est clairement solution de (E). Considérons à présent

$$(a,b) := \left(\frac{\varepsilon_1}{2}\left(\left(3+2\sqrt{2}\right)^p + \left(3-2\sqrt{2}\right)^p\right), \frac{\varepsilon_2}{2}\left(\left(3+2\sqrt{2}\right)^p - \left(3-2\sqrt{2}\right)^p\right)\right)$$

où $(\varepsilon_1, \varepsilon_2, p) \in \{-1,1\} \times \{-1,1\} \times \mathbb{N}^*$, et vérifions si $a^2 - 2b^2 = 1$. Comme $\varepsilon_1^2 = \varepsilon_2^2 = 1$, il suffit de considérer le cas où $\varepsilon_1 = \varepsilon_2 = 1$.
Par construction de

$$a = \frac{1}{2}\left(\left(3+2\sqrt{2}\right)^p + \left(3-2\sqrt{2}\right)^p\right) = \frac{1}{2}\left(\left(3+2\sqrt{2}\right)^p + \sigma\left(\left(3+2\sqrt{2}\right)^p\right)\right)$$

et

$$b = \frac{1}{2}\left(\left(3+2\sqrt{2}\right)^p - \left(3-2\sqrt{2}\right)^p\right) = \frac{1}{2}\left(\left(3+2\sqrt{2}\right)^p - \sigma\left(\left(3+2\sqrt{2}\right)^p\right)\right)$$

donc

$$a+b\sqrt{2} = \left(3+2\sqrt{2}\right)^p$$

Alors

$$a^2 - 2b^2 = \left(a+b\sqrt{2}\right)\sigma\left(a+b\sqrt{2}\right) = \left(3+2\sqrt{2}\right)^p \sigma\left(\left(3+2\sqrt{2}\right)^p\right) = \left(\left(3+2\sqrt{2}\right)\sigma\left(3+2\sqrt{2}\right)\right)^p = 1^p = 1$$

• Conclusion. Les solutions de l'équation de Pell-Fermat sont les couples d'entiers relatifs (a,b) apparaissant dans l'une des deux familles suivantes

— $(a,b) = (\varepsilon, 0)$ où $\varepsilon \in \{-1,1\}$

— $(a,b) = \left(\dfrac{\varepsilon_1}{2}\left(\left(3+2\sqrt{2}\right)^p + \left(3-2\sqrt{2}\right)^p\right), \dfrac{\varepsilon_2}{2}\left(\left(3+2\sqrt{2}\right)^p - \left(3-2\sqrt{2}\right)^p\right)\right)$ où $(\varepsilon_1,\varepsilon_2,p) \in \{-1,1\}\times\{-1,1\}\times\mathbb{N}^*$

Remarque 1 De **Q10**, on déduit que les éléments figurant dans les familles ci-dessous sont deux-à-deux distincts. Ainsi, l'équation de Pell-Fermat possède-t-elle une infinité de solutions.

Remarque 2 Pour $p \in \mathbb{N}^*$ donné, on peut chercher à avoir une expression plus agréable des sommes

$$\left(3+2\sqrt{2}\right)^p + \left(3-2\sqrt{2}\right)^p \qquad \text{et} \qquad \left(3+2\sqrt{2}\right)^p - \left(3-2\sqrt{2}\right)^p$$

Avec la formule du binôme de Newton, en se remémorant que $3+2\sqrt{2} = \left(1+\sqrt{2}\right)^2$, il vient

$$\begin{aligned}
\left(3+2\sqrt{2}\right)^p &= \left(1+\sqrt{2}\right)^{2p} \\
&= \sum_{k=0}^{2p} \binom{2p}{k} \sqrt{2}^k \\
&= \sum_{k=0}^{p} \binom{2p}{2k} \sqrt{2}^{2k} + \sum_{k=0}^{p-1} \binom{2p}{2k+1} \sqrt{2}^{2k+1} \\
&= \underbrace{\sum_{k=0}^{p} \binom{2p}{2k} 2^k}_{\in\mathbb{Z}} + \underbrace{\left(\sum_{k=0}^{p-1} \binom{2p}{2k+1} 2^k\right)}_{\in\mathbb{Z}} \sqrt{2}
\end{aligned}$$

puis

$$\left(3-2\sqrt{2}\right)^p = \sigma\left(\left(3+2\sqrt{2}\right)^p\right) = \sum_{k=0}^{p} \binom{2p}{2k} 2^k - \left(\sum_{k=0}^{p-1} \binom{2p}{2k+1} 2^k\right)\sqrt{2}$$

Nous en déduisons

$$\frac{\left(3+2\sqrt{2}\right)^p + \left(3-2\sqrt{2}\right)^p}{2} = \sum_{k=0}^{p} \binom{2p}{2k} 2^k \qquad \text{et} \qquad \frac{\left(3+2\sqrt{2}\right)^p - \left(3-2\sqrt{2}\right)^p}{2} = \sum_{k=0}^{p-1} \binom{2p}{2k+1} 2^k$$

mais les sommes qui apparaissent ne semblent pas aisées à calculer, autrement qu'avec les puissances de $3+2\sqrt{2}$ et de $3-2\sqrt{2}$.

Q12 — Donner dix solutions distinctes de l'équation (E).

paramètre $p \in \mathbb{N}^*$	$(a,b) \in \mathbb{N}^2$ tel que $a+b\sqrt{2} = \left(3+2\sqrt{2}\right)^p$
2	(17 , 12)
3	(99 , 70)
4	(577 , 408)
5	(3 363 , 2 378)
6	(19 601 , 13 860)
7	(114 243 , 80 782)
8	(665 857 , 470 832)
9	(3 880 899 , 2 744 210)
10	(22 619 537 , 15 994 428)
30	(46 292 552 162 781 456 490 001 , 32 733 777 552 734 744 709 300)