Devoir Maison N°7

Arithmétique

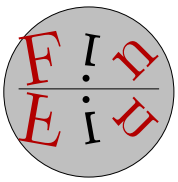
Problème : Résolution d'une équation diophantienne

L'objectif de ce problème est la résolution de l'équation

$$a^2 - 2b^2 = \pm 1, \tag{E}$$

d'inconnues $(a, b) \in \mathbb{Z}^2$.
Pour ce faire, on introduit l'ensemble $\mathbb{Z}[\sqrt{2}] = \left\{a + b\sqrt{2} \ / \ a, b \in \mathbb{Z}\right\}$.

1. Montrer que $(\mathbb{Z}[\sqrt{2}], +, \times)$ est un anneau commutatif.
2. (a) Établir que
$$\forall x \in \mathbb{Z}[\sqrt{2}],\ \exists! a, b \in \mathbb{Z} \ / \ x = a + b\sqrt{2}.$$
On pose alors $\overline{x} = a - b\sqrt{2}$ **le** conjugué de x.
(b) Montrer que l'application de conjugaison $\varphi : x \mapsto \overline{x}$ est une permutation de $\mathbb{Z}[\sqrt{2}]$ vérifiant
$$\forall x, x' \in \mathbb{Z}[\sqrt{2}],\ \varphi(x + x') = \varphi(x) + \varphi(x') \text{ et } \varphi(x \times x') = \varphi(x) \times \varphi(x').$$
3. On pose, pour $x \in \mathbb{Z}[\sqrt{2}]$, $N(x) = x\overline{x}$.
(a) Montrer que, pour tout $x \in \mathbb{Z}[\sqrt{2}]$, $N(x) \in \mathbb{Z}$.
(b) Montrer que, pour tous $x, x' \in \mathbb{Z}[\sqrt{2}]$, $N(xx') = N(x)N(x')$.
(c) Soit $x \in \mathbb{Z}[\sqrt{2}]$. Montrer que x est inversible dans $\mathbb{Z}[\sqrt{2}]$ si, et seulement si, $N(x) = \pm 1$.
(d) Montrer que $H = \left\{x \in \mathbb{Z}[\sqrt{2}] \ / \ N(x) = \pm 1\right\}$ est un groupe pour la multiplication des réels.
4. Soit $x = a + b\sqrt{2} \in H$.
(a) Montrer que si $a \geqslant 0$ et si $b \geqslant 0$ alors $x \geqslant 1$.
(b) Montrer que si $a \leqslant 0$ et si $b \leqslant 0$ alors $x \leqslant -1$.
(c) Montrer que si $ab \leqslant 0$ alors $|x| \leqslant 1$.
5. On note $H^+ = \{x \in H \ / \ x > 1\}$.
(a) Soit $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Montrer que si $x \in H^+$ alors $a > 0$ et $b > 0$.
(b) En déduire que $u = 1 + \sqrt{2}$ est le plus petit élément de H^+.
6. Soit $x \in H^+$.
(a) Montrer qu'il existe $n \in \mathbb{N}$ tel que $u^n \leqslant x < u^{n+1}$.
(b) En déduire que $x = u^n$.
7. Conclure que $H = \{\pm u^n \ / \ n \in \mathbb{Z}\}$.
8. Résoudre l'équation (E).



Corrigé

Problème : Résolution d'une équation diophantienne

1. $Z[\sqrt{2}] \subset \mathbb{C}$ et $(\mathbb{C}, +, \times)$ est un anneau commutatif.
   Montrons que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $(\mathbb{C}, +, \times)$ par caractérisation.
   — $1 = 1 + 0 \times \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.
   — Soient $x = a + b\sqrt{2}, x' = a' + b'\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.
   $$x - x' = (a - a') + (b - b')\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$
   — Soient $z = a + b\sqrt{2}, z' = a' + b'\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.
   $$x \times x' = (aa' + 2bb') + (ab' + a'b)\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$
   On en déduit que $\boxed{(\mathbb{Z}[\sqrt{2}], +, \times) \text{ est un anneau commutatif}}$.

2. (a) *Existence.* Elle est immédiate par définition de $\mathbb{Z}[\sqrt{2}]$.
   Unicité. On suppose que $x = a + b\sqrt{2} = a' + b'\sqrt{2}$ où $a, a', b, b' \in \mathbb{Z}$.
   Ainsi $(b - b')\sqrt{2} = a' - a$. Si $b \neq b'$ alors $\sqrt{2} = \frac{a'-a}{b-b'} \in \mathbb{Q}$. C'est absurde car $\sqrt{2}$ est irrationnel.
   Ainsi $b = b'$ puis $a = a'$.
   $\boxed{\forall x \in \mathbb{Z}[\sqrt{2}],\ \exists! a, b \in \mathbb{Z} \ /\ x = a + b\sqrt{2}}$.

   (b) Il est clair que si $x \in \mathbb{Z}[\sqrt{2}]$ alors $\overline{x} \in \mathbb{Z}[\sqrt{2}]$. Ainsi l'application φ est bien définie.
   On observe que $\varphi \circ \varphi = \mathrm{Id}_{\mathbb{Z}[\sqrt{2}]}$.
   Ainsi $\boxed{\varphi \text{ est une permutation de } \mathbb{Z}[\sqrt{2}]}$.
   Soient $x = a + b\sqrt{2}, x' = a' + b'\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.
   $$\begin{aligned}\varphi(x + x') &= \varphi((a + a') + (b + b')\sqrt{2}) \\ &= (a + a') - (b + b'\sqrt{2}) \\ &= a - b\sqrt{2} + a' - b'\sqrt{2} \\ &= \varphi(x) + \varphi(x').\end{aligned}$$
   $$\begin{aligned}\varphi(x) \times \varphi(x') &= \varphi((aa' + 2bb') + (ab' + a'b)\sqrt{2}) \\ &= (aa' + 2bb') - (ab' + a'b)\sqrt{2} \\ &= (a - b\sqrt{2})(a' - b'\sqrt{2}) \\ &= \varphi(x) \times \varphi(x').\end{aligned}$$
   $$\boxed{\forall x, x' \in \mathbb{Z}[\sqrt{2}],\ \varphi(x + x') = \varphi(x) + \varphi(x') \text{ et } \varphi(x \times x') = \varphi(x) \times \varphi(x').}$$

3. (a) Soit $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Alors
   $$x\overline{x} = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Z}.$$
   $\boxed{\text{Pour tout } x \in \mathbb{Z}[\sqrt{2}],\ N(x) \in \mathbb{Z}}$.

   (b) Soient $x = a + b\sqrt{2}, x' = a' + b'\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.
   $$N(xx') = \varphi(xx')xx' = \varphi(x)\varphi(x')xx' = \varphi(x)x\varphi(x')x' = N(x)N(x').$$
   $\boxed{\text{Pour tous } x, x' \in \mathbb{Z}[\sqrt{2}],\ N(xx') = N(x)N(x').}$

   (c) Soit $x \in \mathbb{Z}[\sqrt{2}]$.
   " $\Rightarrow$ " : Par hypothèse, il existe $y \in \mathbb{Z}[\sqrt{2}]$ tel que $xy = 1$.
   Ainsi $N(xy) = N(1)$. Puis, comme $N(1) = 1$, alors $N(x) \times N(y) = 1$.
   Or $N(x) \in \mathbb{Z}$ et $\mathbb{N}(y) \in \mathbb{Z}$ donc $N(x) \in \mathbb{Z}^\star$. Comme $\mathbb{Z}^\star = \{\pm 1\}$ alors $N(x) = \pm 1$.

" $\Leftarrow$ " : Si $N(x) = \pm 1$ alors $x\overline{x} = \pm 1$.
Si $x\overline{x} = 1$ alors $y = \overline{x} \in \mathbb{Z}[\sqrt{2}]$ vérifie $xy = yx = 1$ donc x est inversible.
Si $x\overline{x} = -1$ alors $y = -\overline{x} \in \mathbb{Z}[\sqrt{2}]$ vérifie $xy = yx = 1$ donc x est inversible.
$\boxed{x \text{ est inversible dans } \mathbb{Z}[\sqrt{2}] \text{ si, et seulement si, } N(x) = \pm 1}$.

(d) Par la question précédente, $H = \mathbb{Z}[\sqrt{2}]^\star$.
D'après le cours, $\boxed{(H, \times) \text{ est un groupe}}$.

4. (a) $x \in H$ donc $a^2 - 2b^2 = \pm 1$.
Si $a = 0$ alors $-2b^2 = \pm 1$. Ce qui est impossible. Ainsi $a \neq 0$.
Comme $a \geqslant 0$ alors $a \geqslant 1$. Ainsi $\boxed{x = a + b\sqrt{2} \geqslant 1}$ puisque $b \geqslant 0$.

(b) $x \in H$ donc $a^2 - 2b^2 = \pm 1$.
Si $a = 0$ alors $-2b^2 = \pm 1$.
Comme $a \leqslant 0$ alors $a \leqslant -1$. Ainsi $\boxed{x = a + b\sqrt{2} \leqslant -1}$ puisque $b \leqslant 0$.

(c) On a : $x \times \overline{x} = \pm 1$ puis $|x| \times |\overline{x}| = 1$.
Comme $ab \geqslant 0$ alors $\overline{x} = a - \sqrt{2}b$ avec $a \times (-b) \leqslant 0$. Par 4.(a) et 4.(b), on en déduit que $|\overline{x}| \geqslant 1$. Ainsi $\boxed{|x| \leqslant 1}$.

5. (a) D'après ce qui précède, $a \geqslant 1$ et $b \geqslant 0$. Si $b = 0$ alors $x = a \in \mathbb{Z}$ et $N(x) = a^2 = \pm 1$. Donc $a = \pm 1$ et cela contredit le fait que $x > 1$. C'est absurde. Par conséquent, $b \neq 0$ puis $b \geqslant 1$.
Ainsi, $\boxed{\text{si } x \in H^+ \text{ alors } a > 0 \text{ et } b > 0}$.

(b) H^+ est une partie de $\mathbb{R}$, non vide (car contenant $1 + \sqrt{2}$) et minoré par $1 + \sqrt{2}$ par ce qui précède.
On en déduit que H^+ admet une borne inférieure vérifiant $\inf(H^+) \geqslant 1 + \sqrt{2}$.
Comme $1 + \sqrt{2} \in H^+$ alors $\inf(H^+) = \min(H^+) = 1 + \sqrt{2}$.
$\boxed{u = 1 + \sqrt{2} \text{ est le plus petit élément de } H^+}$.

6. (a) On pose $n = \left\lfloor \frac{x}{\ln(u)} \right\rfloor \in \mathbb{N}$ qui vérifie $\boxed{u^n \leqslant x < u^{n+1}}$.

(b) On a : $1 \leqslant \frac{x}{u^n} < u$. Si $\frac{x}{u^n} > 1$ alors $\frac{x}{u^n} \in H^+$ et la minimalité de u est contredite.
Ainsi $\frac{x}{u^n} = 1$ puis $\boxed{x = u^n}$.

7. L'inclusion $H \subset \{\pm u^n \ / \ n \in \mathbb{Z}\}$ est claire car $u \in H$ et que $(H, \times)$ est un groupe stable par passage à l'opposé.
Soit $x \in H$.
Nécessairement $x \neq 0$.
Si $x = 1$ alors $x = u^0 \in \{\pm u^n \ / \ n \in \mathbb{Z}\}$.
Si $x > 1$ alors il existe $n \in \mathbb{N}$ tel que $x = u^n$. Ainsi $x \in \{\pm u^n \ / \ n \in \mathbb{Z}\}$.
Si $0 < x < 1$ alors $\frac{1}{x} > 1$ et $\frac{1}{x} \in H^+$. Ainsi, il existe $n \in \mathbb{N}$ tel que $\frac{1}{x} = u^n$. Par conséquent, $x = u^{-n} \in \{\pm u^n \ / \ n \in \mathbb{Z}\}$.
Si $0 < x$ alors $-x > 0$ et $-x \in H$. Ainsi $-x \in \{\pm u^n \ / \ n \in \mathbb{Z}\}$ puis $x \in \{\pm u^n \ / \ n \in \mathbb{Z}\}$.
Par double inclusion, $\boxed{H = \{\pm u^n \ / \ n \in \mathbb{Z}\}}$.

8. On observe que $(a, b) \in \mathbb{Z}^2$ est solution de (E) si, et seulement si, $x = a + b\sqrt{2} \in H$ si, et seulement si, il existe $n \in \mathbb{Z}$ tel que $a + b\sqrt{2} = \pm(1 + \sqrt{2})^n$.
Il y a 4 cas à traiter.
Cas où $n = 2p$ avec $p \in \mathbb{N}$. Dans ce cas,

$$(1 + \sqrt{2})^n = \sum_{k=0}^{p} \binom{2p}{2k} 2^k + \sqrt{2} \sum_{k=0}^{p-1} \binom{2p}{2k+1} 2^k.$$

Cas où $n = 2p+1$ avec $p \in \mathbb{N}$. Dans ce cas,

$$(1+\sqrt{2})^n = \sum_{k=0}^{p} \binom{2p+1}{2k} 2^k + \sqrt{2} \sum_{k=0}^{p} \binom{2p+1}{2k+1} 2^k.$$

Cas où $n = -2p$ avec $p \in \mathbb{N}$. Dans ce cas,

$$(1+\sqrt{2})^n = (1-\sqrt{2})^{-n} = \sum_{k=0}^{p} \binom{2p}{2k} 2^k - \sqrt{2} \sum_{k=0}^{p-1} \binom{2p}{2k+1} 2^k.$$

Cas où $n = -2p-1$ avec $p \in \mathbb{N}$. Dans ce cas,

$$(1+\sqrt{2})^n = -(1-\sqrt{2})^{-n} = -\sum_{k=0}^{p} \binom{2p+1}{2k} 2^k + \sqrt{2} \sum_{k=0}^{p} \binom{2p+1}{2k+1} 2^k.$$

On conclut que

$$\mathcal{S} = \left\{ \left(\pm \sum_{k=0}^{p} \binom{2p}{2k} 2^k, \pm \sum_{k=0}^{p-1} \binom{2p}{2k+1} 2^k \right), \left(\pm \sum_{k=0}^{p} \binom{2p+1}{2k} 2^k, \pm \sum_{k=0}^{p} \binom{2p+1}{2k+1} 2^k \right) \ / \ p \in \mathbb{N} \right\},$$