Problème

Sur l'équation diophantienne $a^2 - 2b^2 = 1$

Le but du problème est de résoudre l'équation diophantienne $a^2 - 2b^2 = 1$, c'est à dire l'équation aux inconnues *entières* a et b. Pour cela, on va étudier un anneau noté $\mathbb{Z}[\sqrt{2}]$ et plus particulièrement le groupe de ses éléments inversibles qui sera noté dans la suite H.

Pour toute la suite, on note $\mathbb{Z}[\sqrt{2}] = \left\{a + b\sqrt{2}/(a,b) \in \mathbb{Z}^2\right\}$.
On rappelle que $\sqrt{2}$ est un nombre irrationnel.

1. Montrer que $(\mathbb{Z}[\sqrt{2}], +, \times)$ avec les lois usuelles est un anneau.
2. Démontrer que tout élément $x \in \mathbb{Z}[\sqrt{2}]$ s'écrit de manière unique sous la forme $x = a + b\sqrt{2}$ avec $(a,b) \in \mathbb{Z}^2$.

3. Pour tout $x = a + b\sqrt{2}$, on note $\overline{x} = a - b\sqrt{2}$ et $N(x) = x\overline{x} = a^2 - 2b^2$.
   (a) Vérifier que pour tous $(x, x') \in \mathbb{Z}[\sqrt{2}]^2$ on a $N(x) \in \mathbb{Z}$ et $N(xx') = N(x)N(x')$.
   (b) Démontrer l'équivalence : $N(x) = 0 \Leftrightarrow x = 0$.
   (c) Démontrer que x est inversible (pour la multiplication) dans $\mathbb{Z}[\sqrt{2}]$ si et seulement si $N(x) \in \{1, -1\}$.

4. Justifier que l'ensemble des éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ pour la multiplication noté $(H, \times)$ est un groupe.

5. Pour cette question, on note $x = a + b\sqrt{2}$ un élément de H d'inverse $x' = a' + b'\sqrt{2}$.
   (a) Démontrer que si a et b sont de même signe on a $|x| \geqslant 1$ et que sinon on a $|x| \leqslant 1$.
   (b) On note $H^+ = H \cap]1, +\infty[$. Démontrer que H^+ admet un plus petit élément qui est $\alpha = 1 + \sqrt{2}$.
   (c) Si $x \in H^+$, on note $E = \{n \in \mathbb{N}/\alpha^n \leqslant x\} \subset \mathbb{N}$. Démontrer que E admet un plus grand élément p qui vérifie $\alpha^p \leqslant x < \alpha^{p+1}$.
   (d) Conclure alors que $H^+ = \{\alpha^n/n \in \mathbb{N}\}$ et déterminer H.

6. Résoudre enfin l'équation $a^2 - 2b^2 = 1$ où $(a,b) \in \mathbb{Z}^2$. On pourra utiliser H.

Indications

1. Vérification facile. On pensera à l'interpréter comme un sous-anneau de $\mathbb{R}$ par exemple.

2. Si l'on suppose deux écritures $a + b\sqrt{2} = a' + b'\sqrt{2}$ avec par exemple $b \neq b'$, on peut réexprimer $\sqrt{2}$ qui mène à une contradiction.

3. (a) $N(x) \in \mathbb{Z}$ est clair. Pour $N(xx') = N(x)N(x')$, calculer séparément les deux membres.

   (b) Si $N(x) = 0$, on peut en supposant $b \neq 0$ réexprimer $\sqrt{2}$ et obtenir une contradiction.

   (c) Si x est inversible soit $xx' = 1$, on peut montrer que $N(x) = \pm 1$ puisque $N(x) \in \mathbb{Z}$. Si $N(x) = \pm 1$, il est possible d'exprimer l'inverse de x (dans $\mathbb{R}$) et constater qu'il est élément de $\mathbb{Z}[\sqrt{2}]$.

4. C'est un résultat de cours.

5. (a) Si a et b sont de même signe (disons positifs), déterminer le plus petit élément possible. Si a et b sont de signe contraire, passer par l'inverse de $a + b\sqrt{2}$.

   (b) Etudier tous les cas possibles des éléments (voir question précédente).

   (c) Pour qu'une partie de $\mathbb{N}$ admette un plus grand élément p, il faut et il suffit qu'elle soit non vide et majorée. Dans ce cas, $p + 1$ n'est pas dans E.

   (d) L'inclusion $\{\alpha^n / n \in \mathbb{N}\} \subset H^+$ est facile. Pour la réciproque, raisonner par l'absurde en supposant que $\alpha^p < x < \alpha^{p+1}$ donc que $1 < x(\alpha)^p < \alpha$. Pour alors déterminer H, étudier $H \cap]0, 1[$ en passant aux inverse puis on trouve facilement les éléments négatifs de H.

6. $a^2 - 2b^2 = 1$ équivaut à $N(a + b\sqrt{2}) = 1$. Utiliser alors l'ensemble H en déterminant ses éléments x tels que $N(x) = 1$. On sait que $N(\alpha^n) = N(\alpha)^n$.