

L'objectif de ce problème est la résolution de l'équation $a^2 - 2b^2 = \pm 1$, avec $(a, b) \in \mathbb{Z}^2$

On pose $\mathbb{Z}[2] = \{a + b\sqrt{2} : (a, b) \in \mathbb{Z}^2\}$

Partie I

1. Montrer que :

- $\sqrt{2} \notin \mathbb{Q}$
- $1 \in \mathbb{Z}[2]$
- Pour tout $x \in \mathbb{Z}[2]$ et $x' \in \mathbb{Z}[2]$: $x + x' \in \mathbb{Z}[2]$ et $xx' \in \mathbb{Z}[2]$

2.

a. Etablir que pour tout $x \in \mathbb{Z}[2]$, il existe un unique $(a, b) \in \mathbb{Z}$ tel que $x = a + b\sqrt{2}$.

On pose alors $\bar{x} = a - b\sqrt{2}$, et on l'appelle « conjugué de x ».

b. Soit $\varphi: \mathbb{Z}[2] \rightarrow \mathbb{Z}[2]$ l'application définie par :

$$\varphi(x) = \bar{x}$$

Montrer que :

- $\varphi(1) = 1$
- Pour tout $x \in \mathbb{Z}[2]$ et $x' \in \mathbb{Z}[2]$, $\varphi(x + x') = \varphi(x) + \varphi(x')$ et $\varphi(xx') = \varphi(x)\varphi(x')$.
- φ est bijective et déterminer φ^{-1} .

3. Pour $x \in \mathbb{Z}[2]$ on pose $N(x) = x\bar{x}$.

a. Justifier que pour tout $x \in \mathbb{Z}[2]$, $N(x) \in \mathbb{Z}$, et montrer que pour tout $x \in \mathbb{Z}[2]$ et $x' \in \mathbb{Z}[2]$ $N(xx') = N(x)N(x')$.

b. Montrer que $x \in \mathbb{Z}[2]$ admet un inverse dans $\mathbb{Z}[2]$ si et seulement si $N(x) = \pm 1$.

Partie II

On se propose dans cette partie de décrire l'ensemble $H = \{x \in \mathbb{Z}[2] : N(x) = \pm 1\}$, ce qui correspond à la résolution de l'équation initialement proposée.

1. Montrer que le produit de deux éléments de H est dans H .

2. Soit $x = a + b\sqrt{2} \in H$. Montrer que :

- $a \geq 0$ et $b \geq 0$ entraîne que $x \geq 1$.
- $a \leq 0$ et $b \leq 0$ entraîne que $x \leq -1$.
- $ab \leq 0$ entraîne que $|x| \leq 1$. On pourra montrer que $|x^{-1}| \geq 1$.

3. On note $H^+ = \{x \in H : x > 1\}$.

a. Alors montrer que si $x = a + b\sqrt{2} \in H^+$ alors $a > 0$ et $b > 0$.

b. En déduire que $u = 1 + \sqrt{2}$ est le plus petit élément de H^+ .

4. Soit $x \in H^+$

a. Montrer qu'il existe un unique entier naturel n tel que $u^n \leq x < u^{n+1}$.

b. En déduire que $x = u^n$. On pourra montrer que $\frac{u^{n+1}}{x} \in H^+$ et que $\frac{u^{n+1}}{x} \leq u$.

c. Conclure que $H = \{\pm u^n : n \in \mathbb{Z}\}$. On fera une double inclusion. Pour montrer que $H \subset \{\pm u^n : n \in \mathbb{Z}\}$ on distinguera les cas $x > 1$; $x = 1$; $0 < x < 1$ et $x < 0$.