Sujet d'étude

Exercice 1 *Anneau $\mathbb{Z}[\sqrt{n}]$ et équation de Pell-Fermat*

Soit n un entier strictement positif tel que $\sqrt{n}$ ne soit pas rationnel. On veut résoudre l'équation d'inconue $(a, b) \in \mathbb{N}^{\star 2}$,

$$a^2 - nb^2 = \pm 1. \tag{E}$$

Dans la suite, on note

$$\mathbb{Z}[\sqrt{n}] = \left\{ z \in \mathbb{R} \;\middle|\; \exists (a, b) \in \mathbb{Z}^2, z = a + b\sqrt{n} \right\}.$$

Dans cet ensemble, les lois de composition interne sont l'addition et la multiplication des réels.

Partie A

A1. Montrer que si a, a', b, b' sont des rationnels tels que $a + b\sqrt{n} = a' + b'\sqrt{n}$, alors $a = a'$ et $b = b'$.

A2. Montrer que $\mathbb{Z}[\sqrt{n}]$ est un anneau.

A3. Pour tout élément $z = a + b\sqrt{n}$ de $\mathbb{Z}[\sqrt{n}]$, on définit

$$\bar{z} = a - b\sqrt{n} \quad \text{et} \quad N(z) = z\bar{z}.$$

Montrer que l'application qui à z associe $\bar{z}$ est un automorphisme de l'anneau $\mathbb{Z}[\sqrt{n}]$.

Montrer que si z est dans $\mathbb{Z}[\sqrt{n}]$, alors $N(z)$ est entier et que

$$\forall (z, z') \in \mathbb{Z}[\sqrt{n}]^2, N(zz') = N(z)N(z').$$

Partie B

Soit $G = U\left(\mathbb{Z}[\sqrt{n}]\right)$ l'ensemble des éléments de $\mathbb{Z}[\sqrt{n}]$ inversibles (pour la multiplication).

B1. Montrer que G est un groupe (pour la multiplication).

B2. Montrer qu'un élément z de $\mathbb{Z}[\sqrt{n}]$ est dans G si, et seulement si $N(z) = \pm 1$.

B3. Soit $z = a + b\sqrt{n} \in G$. Montrer les implications suivantes.

(a) $a \geq 0$ et $b \geq 0 \implies z \geq 1$.

(b) $a \leq 0$ et $b \leq 0 \implies z \leq -1$.

(c) $ab \leq 0 \implies |z| \leq 1$.

B4. Soit $H = \{ z \in G \mid z > 1 \}$. On suppose *dans toute la suite de cette partie* que H est non vide (cela sera démontré dans la prochaine partie).

Montrer que si $z = a + b\sqrt{n}$ et $z' = a' + b'\sqrt{n}$ sont deux éléments de H, alors $a < a'$ si, et seulement si $b < b'$.

En déduire que H admet un plus petit élément u_0.

À titre d'exemple, calculer u_0 si $n = 2$.

B5. Montrer que pour tout élément u de H, il existe un entier naturel m tel que

$$u_0^m \leq u < u_0^{m+1},$$

puis montrer que $u = u_0^m$. En déduire

$$H = \left\{ u_0^m \;\middle|\; m \in \mathbb{N}^\star \right\}.$$

B6. En déduire toutes les solutions de l'équation (E) en fonction de u_0.
Si $n = 2$, déterminer toutes les solutions de (E) telles que $a \leq 100$ et $b \leq 100$.

Partie C

C1. Soit m un entier strictement positif.

(a) Montrer qu'il existe $m + 1$ réels distincts $b\sqrt{n} - a$ de $\mathbb{Z}[\sqrt{n}]$ tels que

$$0 \leq b \leq m \quad \text{et} \quad b\sqrt{n} - a \in [0, 1[.$$

(b) En déduire l'éxistence d'un élément $a - b\sqrt{n}$ de $\mathbb{Z}[\sqrt{n}]$ vérifiant

$$\left|a - b\sqrt{n}\right| < \frac{1}{m} \quad \text{et} \quad 0 < b \leq m.$$

(c) Montrer que pour cet élément

$$|a^2 - nb^2| < 1 + 2\sqrt{n}.$$

C2. Montrer que l'équation $|a^2 - nb^2| < 1 + 2\sqrt{n}$ admet une infinité de solutions dans $\mathbb{Z}^2$.

C3. (a) Montrer qu'il existe un entier k tel que l'équation $a^2 - nb^2 = k$ possède une infinité de solutions.

(b) En déduire l'existence d'entiers k, a, a', b, b' tels que k divise $a - a'$ et $b - b'$ et

$$a^2 - nb^2 = a'^2 - nb'^2 = k$$

(c) Pour les éléments précédents, montrer que

$$A = \frac{aa' - nbb'}{k} \quad \text{et} \quad B = \frac{ab' - ba'}{k}$$

sont des entiers vérifiant $A^2 - nB^2 = 1$.

C4. En déduire que H est toujours non vide et que l'équation (E) admet une infinité de solutions.