DS n°6 : Arithmétique, structures algébriques

Durée : **2h**. Calculatrices non autorisées
Le soin et la clarté de la rédaction pourront faire varier la note de ± 1 point. Il n'est pas attendu que vous arrivez au bout du sujet (le barème dépassera 100 points). Faites primer la qualité sur la quantité.

Exercice 1 : Une équation diophantienne... avec de l'algèbre

On s'intéresse dans ce problème à l'*équation de Pell-Fermat* $x^2 - 3y^2 = 1$ d'inconnue $(x, y) \in \mathbb{N}^2$.
Afin de la résoudre, on pose $\mathbb{Z}[\sqrt{3}] = \left\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\right\}$.

1) **a)** Montrer que $\mathbb{Z}[\sqrt{3}]$ est un sous-anneau de $\mathbb{R}$.

b) Montrer que $\sqrt{3}$ est irrationnel, puis que pour tout $x \in \mathbb{Z}[\sqrt{3}]$, il existe un unique couple $(a, b) \in \mathbb{Z}^2$ pour lequel $x = a + b\sqrt{3}$.

L'élément $a - b\sqrt{3}$ est alors appelé le *conjugué* de x et est noté $\overline{x}$. Cette définition ne pose aucun problème d'ambiguité vis-à-vis du choix de a et b car le couple (a, b) associé à x est unique. Attention, bien que la notation soit similaire, cela n'a rien à voir avec la conjuguaison complexe !

c) Montrer que l'application $x \mapsto \overline{x}$ est un automorphisme d'anneau de $\mathbb{Z}[\sqrt{3}]$.

2) Pour tout $x \in \mathbb{Z}[\sqrt{3}]$, on appelle *norme* de x et on note $N(x)$ le réel $x\overline{x}$.

a) Montrer que pour tous $x, x' \in \mathbb{Z}[\sqrt{3}]$, on a $N(xx') = N(x)N(x') \quad \text{et} \quad N(x) \in \mathbb{Z}$.

b) On pose $G = \left\{x \in \mathbb{Z}[\sqrt{3}] \mid x > 0 \quad \text{et} \quad N(x) = 1\right\}$. Montrer que G est un sous-groupe de $\mathbb{R}^*$.

3) Soit $x = a + b\sqrt{3} \in G \cap]1, +\infty[$.

a) Montrer que $a > 0$.

b) Montrer que $x^2 = 1 + 2bx\sqrt{3}$, puis que $b > 0$.

c) En déduire que $2 + \sqrt{3}$ est le plus petit élément de $G \cap]1, +\infty[$.

4) **a)** Soit $x \in G$. Montrer que $(2 + \sqrt{3})^n \leq x < (2 + \sqrt{3})^{n+1}$ pour un certain $n \in \mathbb{Z}$, puis que $x = (2 + \sqrt{3})^n$.

b) En déduire que $G \cap [1, +\infty[= \left\{(2 + \sqrt{3})^n \mid n \in \mathbb{N}\right\}$. Attention, ici c'est l'intervalle $[1, +\infty[$ fermé en 1.

c) On pose $\mathcal{S}$ l'ensemble des solutions de l'équation de Pell-Fermat $x^2 - 3y^2 = 1$ d'inconnue $(x, y) \in \mathbb{N}^2$. Exhiber une bijection de $\mathcal{S}$ sur $G \cap [1, +\infty[$.

$\boxed{\textbf{Suite au dos}}$

Exercice 2 : propriétés arithmétiques de la suite de Fibonacci

Soit u la suite définie par

$$u_0 = 0 \qquad u_1 = 1 \qquad \text{et} \qquad \forall n \in \mathbb{N} \quad u_{n+2} = u_{n+1} + u_n$$

1) Calculer u_2, u_3, u_4, u_5.

2) Montrer par récurrence que pour tout $n \in \mathbb{N}$,

$$u_{n+1}^2 - u_n u_{n+2} = (-1)^n$$

3) En déduire que pour tout $n \in \mathbb{N}$, u_n et u_{n+1} sont premiers entre eux.

Dans la suite on considère un couple quelconque $(n, p) \in \mathbb{N} \times \mathbb{N}^*$. On admet la propriété suivante :

$$u_{n+p} = u_n u_{p-1} + u_{n+1} u_p$$

4) En déduire que $u_{n+p} \wedge u_n = u_n \wedge u_p$.

5) En déduire que pour tout $q \in \mathbb{N}$, on a $u_{n+qp} \wedge u_n = u_n \wedge u_p$.

6) Démontrer finalement que

$$u_n \wedge u_m = u_{n \wedge m}$$

On pourra s'inspirer de l'algorithme d'Euclide,