Résolution d'une équation diophantienne

Thème abordé : Structure d'anneau

L'objectif de ce problème est la résolution de l'équation $a^2 - 2b^2 = \pm 1$.

On admettra l'irrationalité de $\sqrt{2}$.

On introduit l'ensemble $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} / (a,b) \in \mathbb{Z}^2\right\}$.

Partie I

1. Montrer que $\mathbb{Z}\left[\sqrt{2}\right]$ muni de l'addition et de la multiplication des réels est un anneau.

2.a Etablir $\forall x \in \mathbb{Z}\left[\sqrt{2}\right], \exists!(a,b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$.

On pose alors $\overline{x} = a - b\sqrt{2}$ appelé conjugué de x.

2.b Montrer que l'application de conjugaison $x \mapsto \overline{x}$ est un automorphisme de l'anneau $\mathbb{Z}\left[\sqrt{2}\right]$.

3. Pour $x \in \mathbb{Z}\left[\sqrt{2}\right]$, on pose $N(x) = x\overline{x}$.

3.a Justifier que $\forall x \in \mathbb{Z}\left[\sqrt{2}\right], N(x) \in \mathbb{Z}$, et

$\forall x, x' \in \mathbb{Z}\left[\sqrt{2}\right], N(xx') = N(x)N(x')$.

3.b Montrer que $x \in \mathbb{Z}\left[\sqrt{2}\right]$ est inversible ssi $N(x) \in \{1,-1\}$.

3.c On forme $H = \left\{x \in \mathbb{Z}\left[\sqrt{2}\right] / N(x) = \pm 1\right\}$.

Justifier par un argument rapide que H est un groupe pour la multiplication des réels.

Partie II

On se propose dans cette partie de décrire l'ensemble H, ce qui correspond à la résolution de l'équation initialement proposée.

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

1.a $a \geq 0$ et $b \geq 0 \Rightarrow x \geq 1$.

1.b $a \leq 0$ et $b \leq 0 \Rightarrow x \leq -1$.

1.c $ab \leq 0 \Rightarrow |x| \leq 1$.

2. On note $H^+ = \{x \in H / x > 1\}$.

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

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

3. Soit $x \in H^+$.

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

3.b En déduire que $x = u^n$.

3.c Conclure que $H = \left\{\pm u^n / n \in \mathrm{Z}\right\}$.

Correction

d'après problème Dunod revu.

Partie I

1. Montrons que $\mathbb{Z}\left[\sqrt{2}\right]$ est un sous-anneau de $(\mathbb{R},+,\times)$.

Bien entendu, $\mathbb{Z}\left[\sqrt{2}\right]\subset\mathbb{R}$.

$1=a+b\sqrt{2}$ avec $a=1\in\mathbb{Z}$ et $b=0\in\mathbb{Z}$ donc $1\in\mathbb{Z}\left[\sqrt{2}\right]$.

Soit $x=a+b\sqrt{2}$ et $x'=a'+b'\sqrt{2}\in\mathbb{Z}\left[\sqrt{2}\right]$.

$x-x'=(a-a')+(b-b')\sqrt{2}\in\mathbb{Z}\left[\sqrt{2}\right]$ car $a-a',b-b'\in\mathbb{Z}$.

$xx'=(aa'+2bb')+\sqrt{2}(ab'+a'b)\in\mathbb{Z}\left[\sqrt{2}\right]$ car $aa'+2bb',ab'+a'b\in\mathbb{Z}$.

Donc $\mathbb{Z}\left[\sqrt{2}\right]$ est un sous anneau de $(\mathbb{R},+,\times)$.

2.a Soit $x\in\mathbb{Z}\left[\sqrt{2}\right]$.

L'existence du couple (a,b) découle de la définition de $\mathbb{Z}\left[\sqrt{2}\right]$.

Etudions l'unicité :

Soit $(a,b)\in\mathbb{Z}^2$ et $(a',b')\in\mathbb{Z}^2$ deux couples solutions.

On a $x=a+b\sqrt{2}=a'+b'\sqrt{2}$ donc $a-a'=(b'-b)\sqrt{2}$.

Si $b\neq b'$ alors $\sqrt{2}=\dfrac{a-a'}{b'-b}\in\mathbb{Q}$ ce qui est faux.

Donc $b=b'$ puis $a-a'=(b'-b)\sqrt{2}=0$ donc $a=a'$.

2.b Notons $\varphi:\mathbb{Z}\left[\sqrt{2}\right]\to\mathbb{Z}\left[\sqrt{2}\right]$ l'application définie par $\varphi(x)=\overline{x}$.

$\varphi(1)=\varphi(1+0.\sqrt{2})=1-0.\sqrt{2}=1$.

Soit $x=a+b\sqrt{2}$ et $x'=a'+b'\sqrt{2}\in\mathbb{Z}\left[\sqrt{2}\right]$.

$$\varphi(x+x')=\varphi((a+a')+(b+b')\sqrt{2})=(a+a')-(b+b')\sqrt{2}$$
$$=(a-b\sqrt{2})+(a'-b'\sqrt{2})=\varphi(x)+\varphi(x')$$

$\varphi(xx')=\varphi((aa'+2bb')+(ab'+a'b)\sqrt{2})=(aa'+2bb')-(ab'+a'b)\sqrt{2}$

et $\varphi(x)\varphi(x')=(a-b\sqrt{2})(a'-b'\sqrt{2})=(aa+2bb')-(ab'+a'b)\sqrt{2}$

donc $\varphi(xx')=\varphi(x)\varphi(x')$.

Ainsi φ est un morphisme de l'anneau $\mathbb{Z}\left[\sqrt{2}\right]$ dans lui-même.

On constate $\overline{\overline{x}}=x$, il s'ensuit que φ est involutive et donc bijective, c'est donc un automorphisme de $\mathbb{Z}\left[\sqrt{2}\right]$.

3.a Pour $x=a+b\sqrt{2}\in\mathbb{Z}\left[\sqrt{2}\right]$, $N(x)=a^2-2b^2\in\mathbb{Z}$ car $a,b\in\mathbb{Z}$.

Pour $x,x'\in\mathbb{Z}\left[\sqrt{2}\right]$, $N(xx')=xx'\overline{xx'}=xx'\overline{x}\,\overline{x'}=x\overline{x}x'\overline{x'}=N(x)N(x')$.

3.b Soit $x\in\mathbb{Z}\left[\sqrt{2}\right]$.

Si x est inversible alors $xx^{-1}=1$ et donc $N(x)N(x^{-1})=1$.

Or $N(x),N(x^{-1})\in\mathrm{Z}$ donc $N(x),N(x^{-1})\in\{1,-1\}$.

Inversement, supposons $N(x)\in\{1,-1\}$.

Si $N(x)=1$ alors $x\overline{x}=1$ et donc x est inversible d'inverse $\overline{x}$.

Si $N(x)=-1$ alors $x\overline{x}=-1$ et donc x est inversible d'inverse $-\overline{x}$.
Dans les deux cas x est inversible

3.c H est le groupe des inversibles de l'anneau $(\mathbb{Z}\left[\sqrt{2}\right],+,\times)$

Partie II

1.a Sachant que $0\notin H$, on a $(a,b)\neq(0,0)$.
Si $a\geq 0$ et $b\geq 0$, puisqu'au moins l'un des deux est non nul, $x=a+b\sqrt{2}\geq 1$.

1.b Même principe.

1.c Si $ab\leq 0$ alors $x^{-1}=\pm\overline{x}=\pm(a-b\sqrt{2})$ est formé de deux coefficients de même signe, compte tenu de 1.a et 1.b, on a $\left|x^{-1}\right|\geq 1$ et donc $|x|\leq 1$.

2.a Soit $x=a+b\sqrt{2}\in H^+$.
On a $x>1$, donc, de par la question 1., $a\geq 0$ et $b\geq 0$.
Puisque $N(x)=a^2-2b^2=1$:
+ on ne peut pas avoir $a=0$,
+ on ne peut pas avoir $b=0$ sans que $a=1$ ce qui donne $x=1$ ce qui est exclu.
Par suite $a>0$ et $b>0$.

2.b $u=1+\sqrt{2}\in H^+$ car $u>1$ et $N(u)=a^2-2b^2=-1$.
De plus, grâce à 2.a, $\forall x\in H^+$, $x=a+b\sqrt{2}$ avec $a,b\in\mathbb{N}^*$ donc $x\geq u$.
Ainsi u est le plus petit élément de H^+.

3.a Pour $n=E\left(\dfrac{\ln x}{\ln u}\right)\in \mathrm{N}$, on a $u^n\leq x<u^{n+1}$.

3.b Comme $u\in H$ et que H est un sous groupe, $u^{n+1}\in H$.
De plus $x\in H$ donc $\dfrac{u^{n+1}}{x}\in H$.
Puisque $\dfrac{u^{n+1}}{x}>1$ on a $\dfrac{u^{n+1}}{x}\in H^+$. Or $\dfrac{u^{n+1}}{x}=u.\dfrac{u^n}{x}\leq u$ et u est le plus petit élément de H^+ donc $\dfrac{u^{n+1}}{x}=u$ puis $x=u^n$.

3.c Puisque $u\in H,\forall n\in\mathbb{Z},u^n\in H$.
De plus $-1\in H$ donc $\forall n\in\mathbb{Z},-u^n\in H$.
Ainsi $\left\{\pm u^n/\,n\in\mathbb{Z}\right\}\subset H$.
Inversement.
Soit $x\in H$. Assurément $x\neq 0$.
Si $x>1$ alors $x\in H^+$ donc $\exists n\in\mathbb{N}$ tel que $x=u^n$.
Si $x=1$ alors $x=u^0$.
Si $0<x<1$ alors $\dfrac{1}{x}\in H^+$ et donc $\exists n\in\mathbb{N},\dfrac{1}{x}=u^n$ d'où $x=u^{-n}$.
Si $x<0$ alors $y=-x=(-1)\times x\in H$ et $y>0$ donc $\exists n\in\mathbb{Z}$ tel que $y=u^n$ puis $x=-u^n$.
Dans tous les cas $x\in\left\{\pm u^n/\,n\in\mathbb{Z}\right\}$.
Finalement $H=\left\{\pm u^n/\,n\in\mathbb{Z}\right\}$.