

Corrigé du DM 2

Exercice 10 : Anneau $\mathbb{Z}[\sqrt{2}]$

1.

$$A = \{a + b\sqrt{2}; \text{ avec } a, b \in \mathbb{Z}\}$$

- $A \subset \mathbb{R}$.
- Soit $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$ avec $(a, b, c, d) \in \mathbb{Z}^4$.

D'une part :

$$x - y = (a - c) + (b - d)\sqrt{2} \in A$$

car $a - b \in \mathbb{Z}$ et $c - d \in \mathbb{Z}$.

D'autre part :

$$xy = (ac + 2bd) + \sqrt{2}(bc + ad) \in A$$

car $ac + 2bd \in \mathbb{Z}$ et $bc + ad \in \mathbb{Z}$.

Enfin, $1 = 1 + 0 \times \sqrt{2} \in A$, donc A est un sous-anneau de $\mathbb{R}$.

De plus : $\forall a \in \mathbb{Z}, a = a + 0\sqrt{2} \in A$ et $\sqrt{2} = 0 + 1 \times \sqrt{2} \in A$; donc A est un sous-anneau de $\mathbb{R}$ qui contient $\mathbb{Z} \cup \{\sqrt{2}\}$.

- Soit B un sous-anneau de $\mathbb{R}$ qui contient $\mathbb{Z} \cup \{\sqrt{2}\}$.

Soit $x = a + b\sqrt{2} \in A$ avec $a, b \in \mathbb{Z}$ donc $a \in \mathbb{Z} \subset B$, $b \in \mathbb{Z} \subset \sqrt{2} \in B$ et $\sqrt{2} \in B$; donc par stabilité de B par $+$ et $\times$, $x = a + b \times \sqrt{2} \in B$.

On a montré que $A \subset B$, valable pour tout sous-anneau B de $\mathbb{R}$ qui contient $\mathbb{Z} \cup \sqrt{2}$.

Conclusion :

$$A \text{ est le plus petit sous-anneau de } \mathbb{R} \text{ qui contient } \mathbb{Z} \cup \sqrt{2}.$$

2. Soit $x \in A$, par définition de A , il existe $(a, b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$. Montrons l'unicité : soit $(c, d) \in \mathbb{Z}^2$ tel que $x = c + d\sqrt{2}$ et supposons par l'absurde $b \neq d$, donc $a + b\sqrt{2} = c + d\sqrt{2}$, donc $a - c = \sqrt{2} \times (b - d)$ avec $b - d \neq 0$, donc :

$$\sqrt{2} = \frac{a - c}{b - d} \in \mathbb{Q}$$

d'où la contradiction car $\sqrt{2} \notin \mathbb{Q}$.

Donc : $b = d$ et $a - c = \sqrt{2} \times (b - d) = 0$ donc $(a, b) = (c, d)$; ce qui montre l'unicité.

Conclusion :

$$\forall x \in A, \exists! (a, b) \in \mathbb{Z}^2 \mid x = a + b\sqrt{2}.$$

Ainsi pour tout $x = a + b\sqrt{2} \in A$, l'image $|a^2 - 2b^2|$ est définie sans ambiguïté (une seule image possible) et comme $a, b \in \mathbb{Z}$, $|a^2 - 2b^2| \in \mathbb{N}$.

Donc :

$$\text{l'application } N \text{ est bien définie de } A \text{ dans } \mathbb{N}.$$

3. Soit $x = a + b\sqrt{2} \in A$ et $y = c + d\sqrt{2} \in A$.

On a $xy = (ac + 2bd) + \sqrt{2}(bc + ad)$, ce qui entraîne :

$$\begin{aligned} N(xy) &= |(ac + 2bd)^2 - 2(bc + ad)^2| \\ &= |a^2c^2 + 4b^2d^2 - 2b^2c^2 - 2a^2d^2| \end{aligned}$$

Par ailleurs :

$$\begin{aligned} N(x)N(y) &= |(a^2 - 2b^2)(c^2 - 2d^2)| \\ &= |a^2c^2 + 4b^2d^2 - 2b^2c^2 - 2a^2d^2| \end{aligned}$$

Donc :

$$\forall x, y \in A, N(xy) = N(x)N(y).$$

Soit $z \in A$.

- Supposons $z \in U$. Il existe donc $z' \in U$ tel que $zz' = 1$. D'après la question précédente, on en déduit que $N(z)N(z') = N(1) = 1$. Comme $N(z)$ et $N(z')$ appartiennent à $\mathbb{N}$, on conclut que $N(z) = 1$ (car les inversibles de l'anneau $(\mathbb{Z}, +, \times)$ sont 1 et -1).
- Réciproquement, considérons $z = a + b\sqrt{2} \in A$ avec $N(z) = 1$. Remarquons d'abord que : $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$. Or $N(z) = |a^2 - 2b^2| = 1$, donc : $z \times (a - b\sqrt{2}) = 1$ ou $z \times (a - b\sqrt{2}) = -1$; donc : $z \times (a - b\sqrt{2}) = 1$ ou $z \times (-a + b\sqrt{2}) = 1$. Donc z est inversible.

Donc :

$$\text{un élément } z \text{ de } A \text{ est inversible si et seulement si } N(z) = 1.$$

4. $N(1 + \sqrt{2}) = |1 - 2 \times 1| = 1$, donc d'après la question 3,

$$1 + \sqrt{2} \in U.$$

Or $(U, \times)$ est le groupe des inversibles de $(A, +, \times)$; donc :

$$\forall n \in \mathbb{Z}, (1 + \sqrt{2})^n \in U.$$

5. $z = a + b\sqrt{2} \in U$ avec $a, b \in \mathbb{N}$.

a) Supposons par l'absurde $a = 0$. Donc : $N(z) = 2b^2 = 1$, donc $b^2 = \frac{1}{2}$: contradiction avec $b \in \mathbb{N}$. Donc :

$$a \neq 0.$$

b) Soit $n \in \mathbb{N}$. La fonction $\ln$ est strictement croissante sur $\mathbb{R}_+^*$ et $z = a + b\sqrt{2}, 1 + \sqrt{2} \in \mathbb{R}_+^*$, donc

$$\begin{aligned} (1 + \sqrt{2})^n &\leq z < (1 + \sqrt{2})^{n+1} \\ \Leftrightarrow n \ln(1 + \sqrt{2}) &\leq \ln z < (n + 1) \ln(1 + \sqrt{2}) \\ \Leftrightarrow n &\leq \frac{\ln z}{\ln(1 + \sqrt{2})} < n + 1 & (\ln(1 + \sqrt{2}) > 0) \\ \Leftrightarrow n &= \left\lfloor \frac{\ln z}{\ln(1 + \sqrt{2})} \right\rfloor \end{aligned}$$

et $a \neq 0$, donc $a \geq 1$ et $z = a + b\sqrt{2} \geq 1$, donc : $\left\lfloor \frac{\ln z}{\ln(1 + \sqrt{2})} \right\rfloor \geq 0$.

Donc :

$$\boxed{\text{il existe un unique } n \in \mathbb{N} \text{ tel que : } (1 + \sqrt{2})^n \leq z < (1 + \sqrt{2})^{n+1}}$$

c) On sait que $z \in U$ et $(1 + \sqrt{2})^{-n} \in U$, or $(U, \times)$ est un groupe, donc : $z(1 + \sqrt{2})^{-n} \in U \subset A$. Donc : il existe $c, d \in \mathbb{Z}$ tels que :

$$\frac{z}{(1 + \sqrt{2})^n} = c + d\sqrt{2}.$$

Or $(1 + \sqrt{2})^n \leq z < (1 + \sqrt{2})^{n+1}$, donc : $1 \leq c + d\sqrt{2} < 1 + \sqrt{2}$. Donc c ou d est strictement positif.

Supposons par l'absurde $c > 0$ et $d < 0$, donc $1 \leq c + d\sqrt{2} < c - d\sqrt{2}$.

Donc : $c^2 - 2d^2 = (c + d\sqrt{2})(c - d\sqrt{2}) > 1$.

Or : $c + d\sqrt{2} \in U$, donc : $N(c + d\sqrt{2}) = |c^2 - 2d^2| = 1$, d'où la contradiction.

Supposons par l'absurde $c < 0$ et $d > 0$, donc : $d \geq 1$ et $c \leq -1$ donc : $c - d\sqrt{2} \leq -2$.

Or : $c + d\sqrt{2} \geq 1$; donc : $|c^2 - 2d^2| \geq 2$: contradiction.

Donc $c \geq 0$ et $d \geq 0$.

Conclusion :

$$\boxed{\text{il existe } c, d \in \mathbb{N} \text{ tels que } z(1 + \sqrt{2})^{-n} = c + d\sqrt{2}.$$

d) $w = c + d\sqrt{2} \in U$ avec $c, d \in \mathbb{N}$ donc, de même que dans la question 5.a, $N(w) = |c^2 - 2d^2| = 1$, donc $c \neq 0$. Or $c \in \mathbb{N}$ donc $c \geq 1$, or :

$$1 \leq c + d\sqrt{2} < 1 + \sqrt{2}$$

donc : $1 + d\sqrt{2} \leq c + d\sqrt{2} < 1 + \sqrt{2}$, donc : $d < 1$, or $d \in \mathbb{N}$, donc $d = 0$.

Donc : $z(1 + \sqrt{2})^{-n} = c + d\sqrt{2} = 1$, donc :

$$\boxed{z = (1 + \sqrt{2})^n.}$$

6. Soit $z \in U$. Donc : $z = a + b\sqrt{2}$ avec $a, b \in \mathbb{Z}$.

1er cas : $a \geq 0, b \geq 0$: donc, d'après la question précédente, $z = (1 + \sqrt{2})^n$.

2e cas : $a \leq 0, b \leq 0$: donc pour $w = -a - b\sqrt{2}$, on a $N(w) = N(z) = 1$ et $w \in U$ avec $-a \geq 0$ et $-b \geq 0$, donc d'après le premier cas, $w = (1 + \sqrt{2})^n$, donc $z = -(1 + \sqrt{2})^n$.

3e cas : $a \geq 0, b \leq 0$: donc pour $w = a - b\sqrt{2}$, de même $w = (1 + \sqrt{2})^n$ et $zw = 1$, donc : $z = (1 + \sqrt{2})^{-n}$.

4e cas : $a \leq 0, b \geq 0$: de même, $z = -(1 + \sqrt{2})^{-n}$.

Donc, dans tous les cas, $z \in \{\pm(1 + \sqrt{2})^n; \text{ avec } n \in \mathbb{Z}\}$.

Réciproquement, pour tout $n \in \mathbb{Z}$, $(1 + \sqrt{2})^n \in U$, et $(-1) \in U$ car $N(-1) = 1$, donc par stabilité de U par $\times$, $-(1 + \sqrt{2})^n \in U$.

Conclusion :

$$\boxed{U = \{\pm(1 + \sqrt{2})^n; \text{ avec } n \in \mathbb{Z}\}.$$