

L'anneau $\mathbb{Z}[\sqrt{3}]$

1 Énoncé

Exercice 18. *L'anneau $\mathbb{Z}[\sqrt{3}]$*

On pose $\mathbb{Z}[\sqrt{3}] = \{x \in \mathbb{R} \mid \exists (a, b) \in \mathbb{Z}^2 \ x = a + b\sqrt{3}\}$.

1. Démontrer que $\mathbb{Z}[\sqrt{3}]$ est un sous-anneau de $\mathbb{R}$.
2. Démontrer que tout élément x de $\mathbb{Z}[\sqrt{3}]$ s'écrit de façon unique sous la forme $x = a + b\sqrt{3}$ avec $(a, b) \in \mathbb{Z}^2$ (on utilisera le fait que $\sqrt{3} \notin \mathbb{Q}$ et on pourra commencer par rechercher les entiers relatifs a et b vérifiant : $a + b\sqrt{3} = 0$).
3. Si $x = a + b\sqrt{3}$, avec $(a, b) \in \mathbb{Z}^2$, on pose $\bar{x} = a - b\sqrt{3}$, que l'on appelle le conjugué de x dans $\mathbb{Z}[\sqrt{3}]$. Montrer que l'application $\varphi : x \mapsto \bar{x}$ est un morphisme d'anneaux.
4. Pour tout x élément de $\mathbb{Z}[\sqrt{3}]$, on pose : $N(x) = x\bar{x}$.
 - (a) Démontrer que : $\forall x \in \mathbb{Z}[\sqrt{3}] \quad N(x) \in \mathbb{Z}$.
 - (b) Démontrer que : $\forall (x, y) \in \mathbb{Z}[\sqrt{3}]^2 \quad N(xy) = N(x)N(y)$.
5. Établir qu'un élément x de $\mathbb{Z}[\sqrt{3}]$ est inversible dans l'anneau $\mathbb{Z}[\sqrt{3}]$ si, et seulement si, $N(x) = \pm 1$.
6. Vérifier que les éléments suivants sont inversibles dans $\mathbb{Z}[\sqrt{3}]$ et donner leurs inverses : $7 + 4\sqrt{3}$, $26 - 15\sqrt{3}$.
7. On pose $\mathbb{Q}[\sqrt{3}] = \{x \in \mathbb{R} \mid \exists (a, b) \in \mathbb{Q}^2 \ x = a + b\sqrt{3}\}$.
 - (a) Démontrer que $\mathbb{Q}[\sqrt{3}]$ est un sous-corps de $\mathbb{R}$.
 - (b) Montrer que tout sous-anneau A de $\mathbb{Q}[\sqrt{3}]$ contient $\mathbb{Z}$, i.e. $\mathbb{Z} \subset A$.
 - (c) En déduire que tout sous-corps K de $\mathbb{Q}[\sqrt{3}]$ contient $\mathbb{Q}$, i.e. $\mathbb{Q} \subset K$.
 - (d) Déterminer tous les sous-corps de $\mathbb{Q}[\sqrt{3}]$.

2 Résolution

1. Montrons que $\mathbb{Z}[\sqrt{3}]$ est un sous-anneau de $\mathbb{R}$.
Par définition, $\mathbb{Z}[\sqrt{3}] \subset \mathbb{R}$.
Montrons que $\mathbb{Z}[\sqrt{3}]$ est un sous-groupe pour l'addition.

On a : $0 = 0 + 0\sqrt{3}$.

Donc : $0 \in \mathbb{Z}[\sqrt{3}]$.

D'où : $\mathbb{Z}[\sqrt{3}] \neq \emptyset$.

Soit $(x, y) \in (\mathbb{Z}[\sqrt{3}])^2$.

Montrons que $x - y \in \mathbb{Z}[\sqrt{3}]$.

Il existe $(a_0, b_0, a_1, b_1) \in \mathbb{Z}^4$ tel que : $x = a_0 + b_0\sqrt{3}$ et $y = a_1 + b_1\sqrt{3}$.

On a alors : $x - y = (a_0 + b_0\sqrt{3}) - (a_1 + b_1\sqrt{3}) = (a_0 - a_1) + (b_0 - b_1)\sqrt{3}$.

Or : $a_0 - b_0 \in \mathbb{Z}$ et $a_1 - b_1 \in \mathbb{Z}$.

On en déduit que : $x - y \in \mathbb{Z}[\sqrt{3}]$.

Par conséquent, l'ensemble $\mathbb{Z}[\sqrt{3}]$ est un sous-groupe pour l'addition.

On a : $1 = 1 + 0\sqrt{3}$.

Donc : $1 \in \mathbb{Z}[\sqrt{3}]$.

Montrons que $\mathbb{Z}[\sqrt{3}]$ est stable par multiplication.

Montrons donc que : $xy \in \mathbb{Z}[\sqrt{3}]$.

On a : $xy = (a_0 + b_0\sqrt{3})(a_1 + b_1\sqrt{3}) = (a_0a_1 + 3b_0b_1) + (a_0b_1 + a_1b_0)\sqrt{3}$.

Or : $a_0a_1 + 3b_0b_1 \in \mathbb{Z}$ et $a_0b_1 + a_1b_0 \in \mathbb{Z}$.

Donc : $xy \in \mathbb{Z}[\sqrt{3}]$.

L'ensemble $\mathbb{Z}[\sqrt{3}]$ est stable par multiplication.

On en déduit que $\mathbb{Z}[\sqrt{3}]$ est un sous-anneau de $\mathbb{R}$.

2. Soit $(a, b) \in \mathbb{Z}$ tel que : $a + b\sqrt{3} = 0$.

Montrons que $a = b = 0$.

Si $b \neq 0$, alors $\sqrt{3} = -\frac{a}{b} \in \mathbb{Q}$.

Or : $\sqrt{3} \notin \mathbb{Q}$.

On en déduit que $b = 0$.

Donc : $a = a + b\sqrt{3} = 0$.

On en déduit que $a = b = 0$.

Soit $x \in \mathbb{Z}[\sqrt{3}]$ et $(a_0, b_0, a_1, b_1) \in \mathbb{Z}^4$ tel que : $x = a_0 + b_0\sqrt{3}$ et $x = a_1 + b_1\sqrt{3}$.

Montrons que $a_0 = a_1$ et $b_0 = b_1$.

On a : $a_0 + b_0\sqrt{3} = a_1 + b_1\sqrt{3}$.

Donc : $(a_0 - a_1) + (b_0 - b_1)\sqrt{3} = 0$.

Par ce qui précède, on en déduit que : $a_0 - a_1 = b_0 - b_1 = 0$.

Par conséquent, $a_0 = a_1$ et $b_0 = b_1$.

On en déduit que tout élément $x \in \mathbb{Z}[\sqrt{3}]$ s'écrit de manière unique sous la forme $x = a + b\sqrt{3}$ avec $(a, b) \in \mathbb{Z}^2$.

3. Par l'unicité de l'écriture sous la forme $a + b\sqrt{3}$, l'application $\varphi : x \mapsto \bar{x}$ est bien définie.
Soit $(x, y) \in (\mathbb{Z}[\sqrt{3}])^2$.
Il existe $(a_0, b_0, a_1, b_1) \in \mathbb{Z}^4$ tel que : $x = a_0 + b_0\sqrt{3}$ et $y = a_1 + b_1\sqrt{3}$.
Montrons que $\varphi(x + y) = \varphi(x) + \varphi(y)$.

On a : $x + y = (a_0 + b_0\sqrt{3}) + (a_1 + b_1\sqrt{3}) = (a_0 + a_1) + (b_0 + b_1)\sqrt{3}$.
Donc : $\varphi(x + y) = (a_0 + a_1) + (b_0 + b_1)\sqrt{3} = (a_0 + a_1) - (b_0 + b_1)\sqrt{3} = (a_0 - b_0\sqrt{3}) + (a_1 - b_1\sqrt{3})$.

D'où : $\varphi(x + y) = \varphi(x) + \varphi(y)$.

On a : $1 = 1 + 0\sqrt{3}$.

Donc : $\varphi(1) = 1 - 0\sqrt{3}$.

D'où : $\varphi(1) = 1$.

Montrons que $\varphi(xy) = \varphi(x)\varphi(y)$.

On a : $xy = (a_0a_1 + 3b_0b_1) + (a_0b_1 + a_1b_0)\sqrt{3}$.

Donc : $\varphi(xy) = (a_0a_1 + 3b_0b_1) - (a_0b_1 + a_1b_0)\sqrt{3}$
 $= a_0(a_1 - b_1\sqrt{3}) - b_0\sqrt{3}(-b_1\sqrt{3} + a_1)$
 $= (a_0 - b_0\sqrt{3})(a_1 - b_1\sqrt{3})$

D'où : $\varphi(xy) = \varphi(x)\varphi(y)$.

On en déduit que l'application φ est un morphisme d'anneau.

4. (a) Soit $x \in \mathbb{Z}[\sqrt{3}]$.

Il existe $(a, b) \in \mathbb{Z}^2$ tel que : $x = a + b\sqrt{3}$.

On a alors : $N(x) = x\bar{x} = (a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2$.

Or : $(a, b) \in \mathbb{Z}^2$. Donc : $a^2 - 3b^2 \in \mathbb{Z}.$ (★)

On en déduit que : $\forall x \in \mathbb{Z} \quad N(x) \in \mathbb{Z}$

(b) Soit $(x, y) \in \mathbb{Z}[\sqrt{3}]$.

On a : $N(xy) = xy\bar{xy} = x\bar{x}y\bar{y} = N(x)N(y)$.

On en déduit que : $\forall (x, y) \in \mathbb{Z}[\sqrt{3}] \quad N(xy) = N(x)N(y)$

5. Soit $x \in \mathbb{Z}[\sqrt{3}]$.

On suppose que x est inversible dans $\mathbb{Z}[\sqrt{3}]$.

Montrons que : $N(x) = \pm 1$.

On a : $x^{-1} \in \mathbb{Z}[\sqrt{3}]$.

Donc : $N(xx^{-1}) = N(x)N(x^{-1})$.

Or : $N(xx^{-1}) = N(1) = 1$.

et : N est à valeurs dans $\mathbb{Z}$.

On en déduit que $N(x)$ est inversible dans $\mathbb{Z}$.

Par conséquent, $N(x) = \pm 1$.

On suppose maintenant que : $N(x) = \pm 1$.

Montrons que x est inversible dans $\mathbb{Z}[\sqrt{3}]$.

On a : $N(x) = x\bar{x}$.

et : $N(x) = \pm 1$. Donc : $N(x)^2 = 1$.

Donc : $x(N(x)\bar{x}) = 1$.

Or : $\bar{x} \in \mathbb{Z}[\sqrt{3}]$ et $N(x) \in \mathbb{Z}$. Donc, $N(x)\bar{x} \in \mathbb{Z}[\sqrt{3}]$.

On en déduit que : x est inversible dans $\mathbb{Z}[\sqrt{3}]$.

Remarquons que : $x^{-1} = N(x)\bar{x}.$ (‡)

Par conséquent, un élément $x \in \mathbb{Z}[\sqrt{3}]$ est inversible dans $\mathbb{Z}[\sqrt{3}]$ si et seulement si $N(x) = \pm 1$.

6. Par l'égalité (★), on a : $N(7 + 4\sqrt{3}) = 7^2 - 3 * 4^2 = 49 - 48 = 1$.

Par (‡) et la question 5, $7 + 4\sqrt{3}$ est inversible dans $\mathbb{Z}[\sqrt{3}]$
et $(7 + 4\sqrt{3})^{-1} = 7 - 4\sqrt{3}$

De même, $N(26 - 15\sqrt{3}) = 26^2 - 3 * 15^2 = 676 - 675 = 1$.

Par (‡) et la question 5, $26 - 15\sqrt{3}$ est inversible dans $\mathbb{Z}[\sqrt{3}]$
et $(26 - 15\sqrt{3})^{-1} = 26 + 15\sqrt{3}$

7. (a) Par le même raisonnement qu'à la question 1, l'ensemble $\mathbb{Q}[\sqrt{3}]$ est un sous-anneau (il suffit de remplacer $\mathbb{Z}$ par $\mathbb{Q}$).

Soit $x \in \mathbb{Q}[\sqrt{3}] \setminus \{0\}$.

Il existe $(a, b) \in \mathbb{Q}$ tel que : $x = a + b\sqrt{3}$.

Si $a - b\sqrt{3} = 0$ et $b \neq 0$, alors $\sqrt{3} = \frac{a}{b} \in \mathbb{Q}$.

Or : $\sqrt{3} \notin \mathbb{Q}$.

Donc, si $a - b\sqrt{3} = 0$, alors $b = 0$ et donc $a = 0$.

Or : $a + b\sqrt{3} \neq 0$ et donc : $a \neq 0$ et $b \neq 0$.

D'où : $a - b\sqrt{3} \neq 0$.

On a alors : $(a + b\sqrt{3})^{-1} = \frac{1}{a + b\sqrt{3}}$
 $= \frac{a - b\sqrt{3}}{(a + b\sqrt{3})(a - b\sqrt{3})}$
 $= \frac{a - b\sqrt{3}}{a^2 - 3b^2}$
 $= \frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{3}$
Or : $(a, b) \in \mathbb{Q}^2$. Donc : $\frac{a}{a^2 - 3b^2} \in \mathbb{Q}$ et $-\frac{b}{a^2 - 3b^2} \in \mathbb{Q}$.

On en déduit que : $(a + b\sqrt{3})^{-1} \in \mathbb{Q}[\sqrt{3}]$.

On en déduit que $\mathbb{Q}[\sqrt{3}]$ est un sous-corps de $\mathbb{R}$.

(b) Soit A un sous-anneau de $\mathbb{Q}[\sqrt{3}]$.

Montrons, par récurrence, que si $a \in A$, alors $\forall n \in \mathbb{N} \quad na \in A$.

Soit $a \in A$.

On a : $0 * a = 0 \in A$.

et : $1 * a = a \in A$.

La propriété est donc vraie au rang 0 et 1.

Soit $n \in \mathbb{N}$.

On suppose que $na \in A$. Montrons que $(n + 1)a \in A$.

On a : $(n + 1)a = na + a$.

Or : $na \in A$ et $a \in A$.

Donc : $(n+1)a \in A$.

Par récurrence, on en déduit que si $a \in A$, alors $\forall n \in \mathbb{N} \quad na \in A$.

Or, on a : $1 \in A$ et donc : $-1 \in A$.

On en déduit que : $\forall n \in \mathbb{Z} \quad n \in A$

et donc : $\boxed{\mathbb{Z} \subset A}$

(c) Soit K un sous-corps de $\mathbb{Q}[\sqrt{3}]$.

L'ensemble K est donc un sous-anneau de $\mathbb{Q}[\sqrt{3}]$.

On a donc : $\mathbb{Z} \subset K$. (†)

Soit $x \in \mathbb{Q}$.

Il existe $(p, q) \in \mathbb{Z} \times \mathbb{Z}^*$ tel que : $x = \frac{p}{q}$.

Par (†), on a : $p \in K$ et $q \in K^*$.

Donc : $\frac{p}{q} \in K$.

On en déduit : $\boxed{\mathbb{Q} \subset K}$

(d) L'ensemble $\mathbb{Q}$ est un sous-corps de $\mathbb{Q}[\sqrt{3}]$.

Soit K un sous-corps de $\mathbb{Q}[\sqrt{3}]$ différent de $\mathbb{Q}$.

Montrons que $K = \mathbb{Q}[\sqrt{3}]$.

On a : $\mathbb{Q} \subset K$.

Or : $\mathbb{Q} \neq K$.

Il existe donc $x \in K$ tel que : $x \notin \mathbb{Q}$.

Il existe $(a, b) \in \mathbb{Q}$ tel que : $x = a + b\sqrt{3}$ et $b \neq 0$.

Par la question 7c, on a : $a \in K$ et $b \in K^*$.

Donc : $\sqrt{3} = \frac{x-a}{b} \in K$.

Soit $y \in \mathbb{Q}[\sqrt{3}]$.

Montrons que $y \in K$.

Il existe $(c, d) \in \mathbb{Q}$ tel que $y = c + d\sqrt{3}$.

On a donc : $c \in K$, $d \in K$ et $\sqrt{3} \in K$.

On en déduit : $y \in K$.

Donc : $K = \mathbb{Q}[\sqrt{3}]$.

$\boxed{\text{On en déduit que les sous-corps de } \mathbb{Q}[\sqrt{3}] \text{ sont } \mathbb{Q} \text{ et } \mathbb{Q}[\sqrt{3}].}$