Exemple d'anneau principal et non-euclidien

On notera pour tout ce développement $\alpha = \dfrac{1+i\sqrt{19}}{2}$.
On remarque que $\alpha + \overline{\alpha} = 1$, $\alpha\overline{\alpha} = 5$ et que $\alpha^2 - \alpha + 5 = 0$. On a donc : $\mathbb{Z}[\alpha] = \left\{ z = a + b\alpha \in \mathbb{C} \;\middle|\; a, b \in \mathbb{Z} \right\}$.
On définit alors la norme $N : \left| \begin{array}{ccc} \mathbb{Z}[\alpha] & \longrightarrow & \mathbb{N} \\ z = a + b\alpha & \longmapsto & z\overline{z} = a^2 + ab + 5b^2 \end{array} \right.$.

Lemme 1. *Soit A un anneau euclidien. Il existe $x \in A \setminus A^\times$ tel que la restriction à $A^\times \cup \{0\}$ de la projection canonique de A sur $A/(x)$ soit surjective.*

Démonstration du lemme 1.

Si A est un corps, $x = 0$ convient.
Sinon, parmi les éléments de A non nuls et non inversibles, on choisit x tel que $\nu(x)$ soit minimal.
Alors, si $a \in A$, on a $a = xq + r$ avec $r = 0$ ou $\nu(r) = \nu(x)$, donc $a \equiv r \mod x$.
Mais, si $r \neq 0$, comme $\nu(r) < \nu(x)$, r est inversible, et a est bien égal, modulo (x), à 0 ou à un élément de $A^\star$.
$\square$

Théorème 2. *$\mathbb{Z}[\alpha]$ n'est pas euclidien.*

Démonstration du théorème 2.

(i) Montrons que $(\mathbb{Z}[\alpha])^\times = \{1, -1\}$.
Soit $z = a + b\alpha \in (\mathbb{Z}[\alpha])^\times$. On a $N(z)N(z^{-1}) = N(zz^{-1}) = N(1) = 1$.
Comme $N(z), N(z^{-1}) \in \mathbb{N}$, on a $N(z) = a^2 + ab + 5b^2 = 1$.
Or, $b^2 + a^2 + ab \geqslant b^2 + a^2 - |ab| \geqslant (|b| - |a|)^2 \geqslant 0$, donc $1 = a^2 + ab + 5b^2 \geqslant 4b^2$.
On en déduit que $b = 0$, puis que $a = \pm 1$. Donc $(\mathbb{Z}[\alpha])^\times = \{1, -1\}$.

(ii) Supposons que $\mathbb{Z}[\alpha]$ est euclidien.
Alors par la propositon, il existe $x \in \mathbb{Z}[\alpha] \setminus \{1, -1\}$ tel que la restriction à $\{1, -1, 0\}$ de la projection canonique de $\mathbb{Z}[\alpha]$ sur $\mathbb{Z}[\alpha]/(x)$ soit surjective.
$\mathbb{Z}[\alpha]/(x)$ est donc un corps de cardinal inférieur ou égal à 3. Donc $\mathbb{Z}[\alpha]/(x) = \mathbb{K}$, avec $\mathbb{K} \cong \mathbb{F}_2$ ou $\mathbb{F}_3$.
On en déduit l'existence d'un morphisme d'anneaux surjectif $\varphi : \mathbb{Z}[\alpha] \to \mathbb{K}$.
Alors $\beta = \varphi(a)$ vérifie $\beta^2 - \beta + 5 = 0$. Mais cette équation ne possède de solution ni dans $\mathbb{F}_2$ ni dans $\mathbb{F}_3$.
On aboutit donc à une contradiction, et $\mathbb{Z}[\alpha]$ n'est donc pas euclidien.

$\square$

Lemme 3 (Pseudo division euclidienne). *Soient $a, b \in \mathbb{Z}[\alpha] \setminus \{0\}$. Alors il existe $q, r \in \mathbb{Z}[\alpha]$ tels que :*
- *$a = bq + r$ ou $2a = bq + r$*
- *$r = 0$ ou $N(r) < N(b)$*

Démonstration du lemme 3.

Soit $x = \frac{a}{b} = \frac{a\overline{b}}{b\overline{b}} \in \mathbb{C}$, que l'on écrit $x = u + v\alpha$, avec $u, v \in \mathbb{Q}$. Soit $n = \lfloor v \rfloor$. On a $v \in [n, n+1[$.

— Supposons que $v \notin \left]n + \frac{1}{3}, n + \frac{2}{3}\right[$.
Soient alors s et t les entiers les plus proches de u et v respectivement. On a $|s-u| \leqslant \frac{1}{2}$ et $|t-v| \leqslant \frac{1}{3}$.
On pose alors $q = s + t\alpha$, de sorte que q est dans A et on a :

$$N(x-q) = (s-u)^2 + (s-u)(t-v) + 5(t-v)^2 \leqslant \frac{1}{4} + \frac{1}{6} + \frac{5}{9} = \frac{35}{36} < 1$$

Si on pose $r = a - bq = b(x-q)$, on a bien $N(r) < N(b)$.

— Supposons que $v \in \left]n + \frac{1}{3}, n + \frac{2}{3}\right[$.
On considère alors $2x = 2u + 2v\alpha$ et $m = \lfloor 2v \rfloor$, et on a :

$$2v \in \left]2n+1-\frac{1}{3}, 2n+1+\frac{1}{3}\right[\text{ puis } 2v \notin \left]m+\frac{1}{3}, m+\frac{2}{3}\right[$$

On est ramené au cas précédent, et on a $2a = bq + r$ avec $N(r) < N(b)$.

□

Théorème 4. $\mathbb{Z}[\alpha]$ *est principal.*

Démonstration du théorème 4.

(i) L'idéal (2) est maximal dans $\mathbb{Z}[\alpha]$. Comme on a $\mathbb{Z}[\alpha]/(2) \cong (\mathbb{Z}[X]/(X^2 - X + 5))/(2)$, on en déduit que :

$$\mathbb{Z}[\alpha]/(2) \cong \mathbb{Z}[X]/(2, X^2 - X + 5) \cong (\mathbb{Z}[X]/(2))/(X^2 + X + 1) \cong (\mathbb{Z}/2\mathbb{Z})[X]/(X^2 + X + 1)$$

Or le polynôme $X^2 + X + 1$ est irréductible sur $\mathbb{Z}/2\mathbb{Z}$, donc $\mathbb{Z}[\alpha]/(2)$ est un corps, donc (2) est maximal.

(ii) Soit I un idéal non trivial de $\mathbb{Z}[\alpha]$, et soit $a \in I \setminus \{0\}$ tel que $N(a)$ soit minimal.
Si $I = (a)$, on a terminé. Sinon, soit $x \in I \setminus (a)$, et appliquons le lemme :
— Si $x = aq + r$, avec $N(r) < N(a)$ ou $r = 0$.
Comme $r \in I$, on a $r = 0$ par minimalité de $N(a)$, donc $x \in (a)$, c'est une contradiction.

— Si $2x = aq + r$, avec $N(r) < N(a)$ ou $r = 0$, on a de la même manière $r = 0$ puis $2x = aq$.
Comme (2) est maximal, donc premier, on a soit $a \in (2)$ soit $q \in (2)$.
Si $q \in (2)$, $q = 2q'$ et $x \in (a)$, contradiction.
On a donc $q \notin (2)$ et $a \in (2)$. On note $a = 2a'$, d'où $x = a'q \in (a')$.
Comme (2) est maximal et ne contient pas q, on a $(2, q) = \mathbb{Z}[\alpha]$.
On a donc l'existence de $\lambda, \mu \in \mathbb{Z}[\alpha]$ tels que $2\lambda + q\mu = 1$.
On en déduit $a' = 2\lambda a' + q\mu a' = \lambda a + \mu x$, donc $a' \in I$, ce qui contredit la minimalité de $N(a)$.

Ainsi forcément $I = (a)$, donc $\mathbb{Z}[\alpha]$ est principal.

□

Conclusion. $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est un exemple d'anneau principal non-euclidien. ◁

Références

[Per] Daniel Perrin. *Cours d'Algèbre.* Ellipses