1 Un anneau principal non euclidien

Abstract

Un résultat assez connu est qu'un anneau principal est euclidien. Naturellement, on peut se demander si la réciproque est vraie, i.e. si un anneau euclidien est forcément principal. On montre que l'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est un anneau principal non euclidien.

On note $a = \frac{1+i\sqrt{19}}{2}$.

$$\mathbb{Z}[a] = \{x + ay, x, y \in \mathbb{Z}\} \tag{1}$$

On introduit la norme de $z = x + ay$:

$$N(z) = z\bar{z} = \left(x + \frac{y}{2}\right)^2 + \frac{19}{4}y^2 \tag{2}$$

Lemme 1. *Les inversibles de $\mathbb{Z}[a]$ sont ± 1.*

Proof. Soit $z = x + ay$ un élément inversible de $\mathbb{Z}[a]$. On a $N(zz^{-1}) = N(z)N(z^{-1}) = 1$ donc $N(z) = 1$. Or, $\frac{19}{4} > 1$ donc

$$\left(x + \frac{y}{2}\right)^2 + \frac{19}{4}y^2 > \left(x + \frac{y}{2}\right)^2 + y^2 \tag{3}$$

Si $y \neq 0$, alors $N(z) > 1$, donc $y = 0$. On en déduit

$$N(z) = x^2 = 1 \tag{4}$$

donc $x = \pm 1$, i.e. $z = \pm 1$. Et réciproquement, ± 1 sont inversibles dans $\mathbb{Z}[a]$. □

Nous allons premièrement montrer que $\mathbb{Z}[a]$ est un anneau non-euclidien. Pour cela, on montre le lemme suivant

Lemme 2. *Si $\mathcal{A}$ est un anneau euclidien, il existe $x \in \mathcal{A} \setminus \mathcal{A}^\times$ tel que la restriction de la projection de $\mathcal{A}$ sur $\mathcal{A}/(x)$ à $\mathcal{A}^\times \cup \{0\}$ soit surjective.*

Proof. Si $\mathcal{A}$ est un corps, $x = 0$ va convenir. Sinon, on note f le stathme associé à $\mathcal{A}$. On peut choisir x tel que $f(x)$ soit minimal. Si on réalise la division euclidienne d'un élément $a \in \mathcal{A}$ par x, on obtient

$$a = qx + r \tag{5}$$

Si on note π la projection de $\mathcal{A}$ sur $\mathcal{A}/(x)$, on a $\pi(a) = \pi(r)$. Puisque $f(r) < f(x)$, on a alors $r = 0$ ou $r \in \mathcal{A}^\times$, autrement on contredirait la définition de x. On conclut alors que pour tout $a \in \mathcal{A}$, il existe $r \in \mathcal{A}^\times \cup \{0\}$ tel que $\pi(a) = \pi(r)$.

De plus, on montre que (x) est un idéal maximal, si on considère un élément non nul de $\mathcal{A}/(x)$, on sait qu'il existe r inversible tel que $\pi(r) = \pi(a)$. On a alors que $\pi(r)\pi(r^{-1}) = \pi(a)\pi(r^{-1}) = \pi(1)$. On en déduit que $\pi(a)$ est inversible et donc que $\mathcal{A}/(x)$ est un corps. □

Proposition 1. $\mathbb{Z}[a]$ *n'est pas un anneau euclidien.*

Proof. Nous savons que les inversibles de $\mathbb{Z}[a]$ sont $-1, 1$. Supposons que $\mathbb{Z}[a]$ soit euclidien, il existe $z \in \mathbb{Z}[a] \setminus \mathbb{Z}[a]^\times$ vérifiant les propriétés du lemme précédent. On sait que π_z restreinte à $\mathbb{Z}[a]^\times \cup \{0\}$ est surjective. Autrement dit, $\pi_z(\{-1, 0, 1\}) = \mathbb{Z}[a]/(z)$. On a montré que (z) est un idéal maximal donc $\mathbb{Z}[a]/(z)$ est un corps de cardinal 2 ou 3. Or $\pi(\alpha)$ est racine du polynôme $X^2 - X + 5$, qui est irréductible sur $\mathbb{F}_2$ et $\mathbb{F}_3$. On a donc une contradiction. □

On peut ensuite montrer l'existence d'une pseudo-division euclidienne dans $\mathbb{Z}[a]$.

Proposition 2. *Pour tout $z \in \mathbb{Z}[a]$ et $w \in \mathbb{Z}[a] \setminus \{0\}$, il existe $q, r \in \mathbb{Z}[a]$ tels que*

$$z = qw + r \quad ou \quad 2z = qw + r \tag{6}$$

avec $N(r) < N(w)$.

Proof. On note $c = \frac{z}{w}$, on obtient alors

$$\begin{aligned} c &= \frac{x_z + ay_z}{x_w + ay_w} && (7)\\ &= \frac{x_z + ay_z}{x_w + ay_w}\frac{x_w - ay_w}{x_w - ay_w} && (8)\\ &= \frac{x_z x_w + 19y_z y_w}{x_w^2 + 19y_w^2} + a\frac{x_w y_z - x_z y_w}{x_w^2 + 19y_w^2} && (9) \end{aligned}$$

On peut donc écrire $c = t + av$ avec $t, v \in \mathbb{Q}$. On pose ensuite $q = \lfloor t \rceil + a\lfloor v \rceil$ et $r = z - qw$. Supposons que □

Proposition 3. $\mathbb{Z}[a]$ *est un anneau principal.*

Proof. Remarquons premièrement que (2) est un idéal maximal.

$$\mathbb{Z}[a]/(2) \cong \mathbb{Z}[X]/(X^2 - X + 5)/2 \cong \mathbb{Z}[X]/(X^2 + X + 1). \tag{10}$$

On sait que $X^2 + X + 1$ est irréductible sur $\mathbb{Z}$. On déduit que $\mathbb{Z}[a]/(2)$ est un corps.

Soit I un idéal de $\mathbb{Z}[a]$. On considère $z \in I \setminus \{0\}$ tel que $N(z)$ soit minimal. Si $I = (z)$, alors I est principal. Sinon, on peut considère un élément $w \in I \setminus (z)$ et on applique le lemme de pseudo-division euclidienne. On obtient alors $q, r \in \mathbb{Z}[a]$ tels que $w = qz + r$ ou $2w = qz + r$ avec $N(r) < N(z)$. Supposons que $w = qz + r$. Alors $r = w - qz$ est dans I. On a forcément $r = 0$ sinon on contredirait la minimalité de $N(z)$. On en déduit que $w = qz$, ce qui est absurde. On en déduit que $2w = qz + r$. On a de la même manière nécessairement $r = 0$ donc $2w = qz$. (2) est premier et, a fortiori, est premier.

Ainsi, 2 divise q ou z. Si jamais $q = 2q'$, on a $w = 2q'z$ et on déduit que $w \in (z)$, ce qui est une contradiction. On en déduit que $z = 2z'$ et donc que $I = (z)$. □