$\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal non euclidien

Chen Thomas
t.chen.thomas1[at]gmail.com

17 mai 2024

Attention

1. Ce document contient certainement des coquilles. N'hésitez pas à me le signaler. De même si vous avez une question.
2. Pour les recasages, ce sont les miens mais ce développement se case peut-être ailleurs et je n'y ai pas réfléchi.
3. Il se peut que ce développement dure plus de 15 minutes. J'ai essayé de le découper pour faire des recollements personnalisés.

Leçons

- 122 : Anneaux principaux. Exemples et applications.
- 127 : Exemples de nombres remarquables. Exemples d'anneaux de nombres remarquables. Applications.

Références

Lemme 1. Soit A euclidien. Il existe $a \in A\backslash A^\times$ tel qu'en notant $\pi : A \to A/(x)$ surjection canonique, $\pi_{|A^\times \cup \{0\}}$ soit surjective.

Démonstration. Si A est un corps, $x = 0$ convient. Sinon, soit $x \in A\backslash(A^\times \cup \{0\})$ de stathme minimal (celui de A le rendant euclidien, notons le v). Soit $u \in A/(x)$ et $y \in A$ tel que $\pi(y) = u$. On écrit $y = xq + r$ avec $v(r) < v(x)$ ou $r = 0$.

Ainsi, $y \equiv r[x]$ ce qui signifie $\pi(y) = r$. Si $r \neq 0$, comme $v(r) < v(x)$, par minimalité de x, r est nécessairement inversible. Si $r = 0$, $\pi(y) = 0$. Ainsi, $\pi(y) = \pi(r)$ avec $r \in A^\times \cup \{0\}$. Ainsi, u s'écrit $\pi(r)$ avec $r \in A^\times \cup \{0\}$. De plus, $A/(x)$ est un corps car ses éléments sont des images d'un inversible par un morphisme d'anneau. □

Notons $\alpha = \frac{1+i\sqrt{19}}{2}$. Alors $X^2 - X + 5$ annule α et c'est son polynôme minimal. En notant $A = \mathbb{Z}[\alpha]$, on va montrer que A est principal non euclidien. On définit alors $N : z \in A \mapsto z\overline{z} \in \mathbb{N}$ et on admet que $N(zz') = N(z)N(z'), N(z) > 0$ pour $z \neq 0$.

***Proposition* 2.** A n'est pas euclidien.

Démonstration. Supposons par l'absurde que A soit euclidien. Soit x comme dans le lemme. Alors $A/(x)$ est un corps. Or, $A^\times \cup \{0\} = \{-1, 0, 1\}$ et par surjectivité, on a $|A/(x)| \leq 3$. On note ce corps K et K est $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$.

Puisque α est racine de $X^2 - X + 5$, $\beta := \pi(\alpha)$ aussi, et ce, dans K. Or, dans K, ce polynôme n'a pas de racine. Contradiction. □

Théorème 3. *A est principal.*

Démonstration. On va d'abord montrer le lemme suivant.

Lemme 4 (Pseudo division euclidienne)**.** Soit $a, b \in A\backslash\{0\}$. Il existe alors $q, r \in A$ tel que

1. $r = 0$ ou $N(r) < N(b)$
2. $a = bq + r$ ou $2a = bq + r$.

Démonstration. Soit $x = a/b = \dfrac{a\bar{b}}{N(b)} \in \mathbb{C}$. On peut l'écrire $u + \alpha v$ avec $u, v \in \mathbb{Q}$ puisque $x \in A$. Notons $n = \lfloor v \rfloor$, $v \in [n, n+1[$. On coupe cet intervalle en 3.

- Si $v \in [n, n+1[\backslash \left]n + \frac{1}{3}, n + \frac{2}{3}\right[$. Soit s, t les entiers les plus proches de u et v respectivement. On a donc
$$|s - u| \leq \frac{1}{2} \ ; \ |t - v| \leq \frac{1}{3}.$$
Soit $q = s + t\alpha$. On veut $N(x - q) \leq 1$ avec $x = a/b$. On a $q \in A$ et
$$N(x-q) = (s-u)^2 + (s-u)(t-v) + 5(t-v)^2 \leq \frac{1}{4} + \frac{1}{6} + \frac{5}{9} = \frac{35}{36} < 1.$$
Ainsi, en notant $r = a - bq = b(x - q)$, on a $N(r) < N(b)$.
- Sinon, $2x = 2u + 2v\alpha$ et $2v \in \left]2n + \frac{2}{3}, 2n + 1 + \frac{1}{3}\right[$. Avec $m = \lfloor 2v \rfloor$, on a $2v \in [m, m+1[\backslash \left]m + \frac{1}{3}, m + \frac{2}{3}\right[$. (Faire un dessin). On est donc ramené au cas précédent et $2a = bq + r$ avec $N(r) < N(b)$.

□

Avec ce lemme, on peut montrer que A est principal.

1. Montrons que (2) est maximal.
2. On conclut par la pseudo division euclidienne.

1. On a
$$A \simeq \mathbb{Z}[X]/(X^2 - X + 5)$$
donc
$$A/(2) \simeq [\mathbb{Z}[X]/(X^2 - X + 5)]/(2) \simeq (\mathbb{Z}/2\mathbb{Z})[X]/(\underbrace{X^2 - X + 5}_{=X^2+X+1}).$$
Puisque $X^2 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$, $A/(2)$ est un corps donc (2) est maximal.
2. Soit I un idéal différent de $\{0\}$. Soit $a \in I, a \neq 0$ tel que $N(a)$ soit minimal. Si $I = (a)$, c'est terminé. Sinon, soit $x \in I\backslash\{a\}$.
   (a) Si $x = aq + r$ avec $N(r) < N(a)$ ou $r = 0$, alors $r \in I$ donc par minimalité, $r = 0$ et $x = aq$. Absurde.
   (b) Si $2x = aq + r$ avec les mêmes considérations, $2x = aq$ donc $aq|2$. (2) étant maximal, il est premier donc $a|2$ ou $q|2$. Si $q|2$, $x \in (a)$ ce qui est absurde. Donc $q \nmid 2$ et $a|2$. Soit a' tel que $a = 2a'$. On a donc $x = a'q$. *Stratégie : montrer que $a' \in I$.* (2) étant maximal, $q \notin (2)$, on a $(2, q) = A$[1]. On a donc une relation de Bézout : il existe $\lambda, \mu \in A$ tel que $2\lambda + \mu q = 1$. Ainsi, $q' = 2a + \mu q a' \in I$ donc $a' \in I$. Or $N(a')N(2) = N(a)$ donc $N(a') < N(a)$. Absurde.

□

1. C'est un idéal qui contient (2) maximal et $q \notin (2)$ donc est un idéal différent de (2). Par maximalité, c'est A.