Étude de l'anneau $\mathbb{Z}\left[\dfrac{1+i\sqrt{19}}{2}\right]$

D. Perrin, *Cours d'Algèbre*, Ellipses. Paragraphe II.5 page 53

Recasage : 122

Théorème 1

L'anneau $A = \mathbb{Z}\left[\dfrac{1+i\sqrt{19}}{2}\right]$ est principal et non-euclidien.

▷ – *Étape 1 : Détermination des inversibles de A.* Notons $\alpha = \dfrac{1+i\sqrt{19}}{2}$. Comme $\alpha+\overline{\alpha} = 1$ et $\alpha\overline{\alpha} = 5$, on a $\alpha^2-\alpha+5 = 0$ donc

$$A = \{a + b\alpha,\ (a,b) \in \mathbb{Z}^2\}$$

est un sous-anneau de $\mathbb{C}$. Il est donc intègre. De plus, A est stable par conjugaison car $\overline{\alpha} = 1-\alpha$. Définissons sur A la norme N par

$$\forall a,b \in \mathbb{Z}, \qquad N(a+b\alpha) = (a+b\alpha)\overline{a+b\alpha} = a^2+ab+5b^2 = \left(a+\frac{b}{2}\right)^2 + \frac{19}{4}b^2 \geq 0.$$

On en déduit que $\forall z \in A$, $N(z) \in \mathbb{N}$ et $N(z) = 0$ si et seulement si $z = 0$. Alors, si $z \in A^\times$, on a $1 = N(zz^{-1}) = N(z)N(z^{-1})$, ce qui impose $N(z) = 1$. En notant $z = a+b\alpha$ avec $a,b \in \mathbb{Z}$,

$$\left(a+\frac{b}{2}\right)^2 + \underbrace{\frac{19}{4}}_{>1} b^2 = 1$$

donc $b = 0$ et $a = \pm 1$. Ainsi, $A^\times = \{\pm 1\}$.

– *Étape 2 : A n'est pas euclidien.* Si A est euclidien, alors il existe $x \in A\backslash A^\times$ tel que la restriction de la projection canonique $A \to A/(x)$ à $A^\times \cup \{0\}$ est surjective. Mais alors, $A/(x)$ est un corps à deux ou trois éléments. On a donc un morphisme d'anneaux $\pi : A \to K$ surjectif, avec $K = \mathbb{F}_2$ ou $K = \mathbb{F}_3$. En particulier, $\beta = \pi(\alpha)$ vérifie $\beta^2 - \beta + 5 = 0$ dans K. Or on vérifie à la main que cette équation n'a pas de solution. Donc A n'est pas euclidien.

– *Étape 3 : Pseudo-division euclidienne.* Montrons que pour $a,b \in A\backslash\{0\}$, il existe $q,r \in A$ tel que $N(r) < N(b)$ et

$$a = bq + r \qquad \text{ou} \qquad 2a = bq + r.$$

Notons $x = \dfrac{a}{b} = \dfrac{a\overline{b}}{b\overline{b}} = u + v\alpha$ avec $u,v \in \mathbb{Q}$, et $n = \lfloor v \rfloor$.

⋆ 1er cas : $v \notin \left]n+\frac{1}{3}, n+\frac{2}{3}\right[$. Soient s et t les entiers les plus proches, respectivement, de u et v. On a alors

$$|s-u| \leq \frac{1}{2} \qquad \text{et} \qquad |t-v| \leq \frac{1}{3}$$

donc, en posant $q = s+t\alpha \in A$ on a

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

donc avec $r = a - bq = b(x-q)$ on a bien $N(r) < N(q)$.

⋆ 2e cas : $v \in \left[n+\frac{1}{3}, n+\frac{2}{3}\right]$ alors $2v \in \left[2n+\frac{2}{3}, 2n+1+\frac{1}{3}\right]$ donc l'entier le plus proche de $2v$ est $t = 2n+1$ et $|t-2v| \leq \dfrac{1}{3}$ et on conclut comme au cas précédent.

– *Étape 4 : (2) est un idéal maximal de A.* On a $A \simeq \mathbb{Z}[X]/(X^2-X+5)$ donc le théorème d'isomorphisme montre que

$$A/(2) \simeq \mathbb{Z}[X]/(2, X^2-X+5) \simeq \mathbb{F}_2[X]/(X^2-X+5).$$

Or $X^2 - X + 5$ est de degré 2 et n'a pas de racine dans $\mathbb{F}_2$ donc $A/(2)$ est un corps, donc (2) est un idéal maximal.

– *Étape 5 : A est principal.* Soit $I \neq \{0\}$ un idéal de A. Soit $a \in I\backslash\{0\}$ tel que $N(a)$ est minimal. Si $I \neq (a)$, soit $x \in I\backslash(a)$. On effectue la pseudo-division euclidienne de x par a :

⋆ si $x = aq + r$ avec $N(r) < N(a)$ alors, comme $r \in I$, on a $x \in (a)$: absurde.

Donc $2x = aq + r$ avec $N(r) < N(a)$ et, de même, $r = 0$ donc $2x = aq$. Comme (2) est maximal, donc premier, $a \in (2)$ ou $q \in (2)$. Si $q \in (2)$ on aurait $q = 2q'$ et donc $x \in (a)$ absurde. Donc $q \notin (2)$ et $a = 2a'$, donc $x = a'q \in (a')$. Il suffit alors de montrer que $a' \in I$, ce qui contredira la minimalité de $N(a)$. Comme $q \notin (2)$ et (2) est maximal, on a $(2, q) = A$ donc il existe $u, v \in A$ tels que $2u + qv = 1$. Donc $a' = 2ua' + qva' = ua + vx \in (I)$.

Ainsi, $I = (a)$ et A est principal. □