Développement 41. Un exemple d'anneau principal non euclidien

On souhaite montrer que l'anneau $\mathbf{Z}[\alpha]$ avec $a \coloneqq \frac{1}{2}(1+i\sqrt{19})$ n'est pas euclidien bien qu'il soit principal. On introduit la norme $N\colon \mathbf{Z}[\alpha] \longrightarrow \mathbf{N}$ définie par l'égalité

$$N(z) = z\overline{z} = a^2 + ab + 5b^2, \qquad z = a + b\alpha \in \mathbf{Z}[\alpha].$$

Cette application est multiplicative. Remarquons également que le nombre complexe α est annulé par le polynôme $X^2 - X + 5 \in \mathbf{Z}[X]$.

Lemme 1. Soit A un anneau euclidien. Alors il existe un élément $x \in A \setminus A^\times$ tel que la restriction $A^\times \cup \{0\} \longrightarrow A/\langle x\rangle$ de la projection canonique soit surjective.

Preuve Lorsque l'anneau A est un corps, le neutre $x = 0$ convient. On suppose désormais que l'anneau A n'est pas un corps. Soit $x \in A \setminus (A^\times \cup \{0\})$ un élément de valuation $\nu(x)$ minimale parmi les éléments non inversibles et non nuls. Montrons alors la surjectivité souhaitée. Soit $\overline{a} \in A/\langle x\rangle$. On écrit $a = xq + r$ la division euclidienne de l'élément a par l'élément x. Alors l'élément r est envoyé sur la classe $\overline{a}$ par la projection. Par ailleurs, comme $\nu(r) < \nu(x)$, le choix de l'élément x impose que $r \in A^\times \cup \{0\}$. ◁

Proposition 2. L'anneau $\mathbf{Z}[\alpha]$ n'est pas euclidien.

Preuve Calculons le groupe $\mathbf{Z}[\alpha]^\times$ des inversibles. Soit $z = a+b\alpha \in \mathbf{Z}[\alpha]^\times$ un élément. Le multiplicativité de la norme permet d'écrire $1 = N(z)N(z^{-1})$, donc $N(z) \in \mathbf{Z}^\times$, c'est-à-dire $N(z) = 1$. Par ailleurs, une identité remarquable donne

$$a^2 + ab + b^2 \geqslant a^2 - |ab| + b^2 > a^2 - 2\,|ab| + b^2 = (|a| - |b|)^2 \geqslant 0,$$

ce qui donne

$$a^2 + ab + 5b^2 \geqslant 4b^2.$$

Avec ce qui précède, on en déduit que $1 \geqslant 4b^2$, donc $b = 0$. Ainsi il ne reste plus que l'égalité $a^2 = 1$ ce qui fournit $a = \pm 1$. On obtient alors $\mathbf{Z}[\alpha]^\times = \{\pm 1\}$.

Concluons. On raisonne par l'absurde et on suppose donc que l'anneau $\mathbf{Z}[\alpha]$ est euclidien. Par le lemme 1, on peut trouver un élément $x \in \mathbf{Z}[\alpha] \setminus \{\pm 1\}$ tel que la projection $\{0, \pm 1\} \longrightarrow \mathbf{Z}[\alpha]/\langle x\rangle$ soit surjective. Le quotient $\mathbf{Z}[\alpha]/\langle x\rangle$ est donc un corps K à deux ou trois éléments. En considérant le morphisme composé surjectif

$$\varphi\colon \mathbf{Z}[\alpha] \twoheadrightarrow \mathbf{Z}[\alpha]/\langle x\rangle \xrightarrow{\sim} K,$$

L'élément $\beta \coloneqq \varphi(\alpha) \in K$ vérifie alors $\beta^2 - \beta + 5 = \varphi(\alpha^2 - \alpha + 5) = 0$.

- Lorsque $K = \mathbf{F}_2$, le polynôme $X^2 + X + 1$ n'a pas de racines dans $\mathbf{F}_2$.
- Lorsque $K = \mathbf{F}_3$, le polynôme $X^2 - X - 1$ n'a pas de racines dans $\mathbf{F}_3$.

Ceci conduit donc à une absurdité dans les deux cas. ◁

Lemme 3. Soient $a, b \in \mathbf{Z}[\alpha] \setminus \{0\}$ deux éléments non nuls. Alors il existe deux éléments $q, r \in \mathbf{Z}[\alpha]$ vérifiant les points suivants :

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

Preuve Considérons le nombre $x \coloneqq a/b \in \mathbf{Q}[\alpha]$ que l'on écrit sous la forme $x = u+v\alpha$ avec $u, v \in \mathbf{Q}$. On pose $n \coloneqq \lfloor v \rfloor$ de telle sorte que $n \leqslant v < n + 1$.

- On suppose que $v \notin]n + 1/3, n + 2/3[$. Soient $s, t \in \mathbf{Z}$ les entiers le plus proches des rationnels u et v. On peut écrire $|s - u| \leqslant 1/2$ et $|t - v| \leqslant 1/3$ où la dernière inégalité est vraie en vertu de notre hypothèse. En posant

  $$q \coloneqq s + t\alpha \in \mathbf{Z}[\alpha] \qquad \text{et} \qquad r \coloneqq a - bq = b(x - q) \in \mathbf{Z}[\alpha].$$

  Alors $a = bq + r$. Par ailleurs, on peut écrire

  $$N(x - q) = (s - u)^2 + (s - u)(t - v) + 5(t - v)^2 \leqslant \frac{1}{4} + \frac{1}{4}\frac{1}{3} + \frac{5}{9} = \frac{35}{36} < 1$$

  de telle sorte que $N(r) = N(b)N(x - q) < N(b)$.
- On suppose que $v \in]n + 1/3, n + 2/3[$. Alors $2v \in]2n + 2/3, 2n + 1 + 1/3[$. On en déduit $m \coloneqq \lfloor 2v \rfloor = 2n + 1$. Mais alors, la dernière inclusion se réécrit

  $$2v \in]m - 1 + 2/3, m + 1/3[=]m - 1/3, m + 1/3[,$$

  donc $2v \notin]m + 1/3, m + 2/3[$. Comme $2x = 2u + 2v\alpha$ avec $2x = 2a/b$, il reste alors à appliquer le cas précédent aux éléments $2a$ et b. ◁

Proposition 4. L'anneau $\mathbf{Z}[\alpha]$ est principal.

Preuve Montrons d'abord que l'idéal $\langle 2\rangle$ est maximal. En vertu du théorème d'isomorphisme et comme $\mathbf{Z}[\alpha] \simeq \mathbf{Z}[X]/\langle X^2 - X + 5\rangle$, il existe un isomorphisme

$$\frac{\mathbf{Z}[\alpha]}{\langle 2\rangle} \simeq \frac{\mathbf{Z}[X]}{\langle 2, X^2 - X + 5\rangle} \simeq \frac{\mathbf{F}_2[X]}{\langle X^2 + X + 1\rangle}.$$

Sur le corps $\mathbf{F}_2$, le polynôme X^2+X+1 n'admet pas de racines ce qui le fait irréductible. Ainsi l'idéal $\langle 2\rangle$ est maximal.

Concluons. Soit $I \subset \mathbf{Z}[\alpha]$ un idéal non nul. Soit $a \in I \setminus \{0\}$ un élément de norme minimale parmi les éléments non nuls de l'idéal I. On souhaite montrer que $I = \langle a\rangle$. On raisonne par l'absurde et on suppose qu'il existe un élément $x \in I \setminus \langle a\rangle$. Avec le lemme 3, on distingue deux cas qui vont mener à une contradiction.

- On suppose la relation $x = aq + r$. Comme $r \in I$ et $N(r) < N(a)$, le choix de l'élément a implique $r = 0$ ce qui aboutit à la contradiction $x \in \langle a\rangle$.
- On suppose maintenant le relation $2x = aq + r$. De même, on trouve $r = 0$, c'est-à-dire $2x = aq$. L'idéal $\langle 2\rangle$ étant maximal, il est premier ce qui nous donne l'alternative $a \in \langle 2\rangle$ ou $q \in \langle 2\rangle$. Comme $x \notin \langle a\rangle$, le second cas ne peut se produire. On obtient donc $q \notin \langle 2\rangle$ et $a \in \langle 2\rangle$. On écrit alors $a = 2a'$ avec $a' \in \mathbf{Z}[\alpha]$ de telle sorte que $x = a'q$. Montrons que $a' \in I$. Comme l'idéal $\langle 2\rangle$ est maximal et ne contient pas l'élément q, l'idéal $\langle 2, q\rangle$ est l'anneau $\mathbf{Z}[\alpha]$ tout entier, donc on peut trouver deux éléments $\lambda, \mu \in \mathbf{Z}[\alpha]$ tels que $2\lambda + q\mu = 1$. En multipliant par l'élément a', on obtient alors $a' = 2\lambda a' + q\mu a' = \lambda a + \mu x \in I$. Finalement, comme $N(a') < 2N(a') = N(a)$, donc $a' = 0$, donc $a = 0$: absurde ! ◁

[1] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1996.