2.17 Un anneau principal non euclidien

Référence : D. Perrin, *Cours d'algèbre*, Ellipses, 1996.

Leçons concernées : 122.

On cherche à montrer qu'un certain anneau est principal mais non euclidien. Pour cela on commence par énoncer une condition nécessaire lorsqu'un anneau A est euclidien.

Proposition 1. *Soit A un anneau euclidien pour le stathme v. Alors il existe $x \in A$ non inversible tel que la restriction à $A^\times \cup \{0\}$ de la projection canonique $A \to A/(x)$ soit surjective.*

Démonstration. Si A est un corps $x = 0$ convient. Sinon on choisit $x \in A$ non nul non inversible tel que $v(x)$ soit minimal (c'est possible puisque $v : A \to \mathbb{N}$). Si $a \in A$, alors $a = xq + r$ avec $r = 0$ ou $v(r) < v(x)$, ainsi $a + (x) = r + (x)$. Si $r \neq 0$, alors puisque $v(r) < v(x)$, r est inversible. Ainsi, $a + (x) = r + (x)$ où $r \in A^\times \cup \{0\}$, d'où le résultat. $\square$

Proposition 2. *L'anneau $A = \mathbb{Z}\left[\dfrac{1+i\sqrt{19}}{2}\right]$ n'est pas euclidien.*

Démonstration. Étape 1 : on pose $\alpha = \frac{1+i\sqrt{19}}{2}$ qui est racine de $X^2 - X + 5$ puisque $\overline{\alpha} = \frac{1-i\sqrt{19}}{2}$ et donc $\alpha + \overline{\alpha} = 1$ et $\alpha\overline{\alpha} = 5$. On a alors

$$A = \mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}\}$$

qui est intègre comme sous-anneau de $\mathbb{C}$. Avec $\overline{\alpha} = 1 - \alpha$ on sait que A est stable par conjugaison et on considère alors, pour $z = a + b\alpha$, $N(z) = z\overline{z} = a^2 + ab + 5b^2 \in \mathbb{N}$. On remarque que $N(zz') = N(z)N(z')$ et $N(z) > 0$ si $z \neq 0$.

Étape 2 : on détermine alors $A^\times$ le groupe des inversibles de A. Soit $z \in A^\times$, alors $N(zz^{-1}) = N(1) = 1 = N(z)N(z^{-1})$ et donc puisque N est à valeurs dans N, $N(z) = 1$. Ainsi, si $z = a + b\alpha$, $a^2 + ab + 5b^2 = 1$. Or

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

et donc $1 = a^2 + ab + 5b^2 \geqslant 4b^2$, ainsi $b = 0$ et donc $a = \pm 1$. On conclut que $A^\times = \{-1, 1\}$.

Étape 3 : on suppose enfin par l'absurde que A est euclidien. D'après la proposition précédente, il existe $x \in A$ tel que $A/(x)$ soit un corps à 2 ou 3 éléments. On a alors l'existence d'un morphisme d'anneaux $\varphi : \mathbb{Z}[\alpha] \to k$ où $k = \mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$. On remarque qu'alors φ restreint à $\mathbb{Z}$ est la projection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$. On pose $\beta = \varphi(\alpha)$ qui est racine de $X^2 - X + 5$ dans k par propriété de morphisme d'anneaux de φ. Or, $X^2 - X + 5 = X^2 + X + 1$ dans $\mathbb{Z}/2\mathbb{Z}$ qui n'a pas de racines et $X^2 - X + 5 = X^2 - X - 1$ dans $\mathbb{Z}/3\mathbb{Z}$ qui n'admet pas non plus de racines : on a trouvé une absurdité. $\square$

On montre maintenant que A est principal au moyen du lemme suivant.

Lemme 3. *Soient $a, b \in A\backslash\{0\}$, alors il existe $q, r \in A$ tels que :*

(i) $r = 0$ *ou* $N(r) < N(b)$

(ii) $a = bq + r$ *ou* $2a = bq + r$

Démonstration. On considère $x = \frac{a}{b} = \frac{a\bar{b}}{b\bar{b}} \in \mathbb{C}$ que l'on écrit $x = u + v\alpha$ avec $u, v \in \mathbb{Q}$. On note $n = \lfloor v \rfloor$.

1) Si $v \notin]n + \frac{1}{3}, n + \frac{2}{3}[$, on pose s, t les entiers les plus proches de u et v respectivement. On a alors $|s - u| \leqslant \frac{1}{2}$, $|t - v| \leqslant \frac{1}{3}$. On pose $q = s + t\alpha \in A$ et on a

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

et donc $r = a - bq = b(x - q)$ convient.

2) Sinon, on a $2x = 2u + 2v\alpha$, et $2v \in]2n + \frac{2}{3}, 2n + 1 + \frac{1}{3}[$ et ainsi si $m = \lfloor 2v \rfloor$, $2v \notin]m + \frac{1}{3}, m + \frac{2}{3}[$ et on conclut avec le cas précédent.

□

Proposition 4. *L'anneau A est principal.*

Démonstration. On montre d'abord que l'idéal (2) est maximal dans A. En effet on a par division euclidienne,

$$A \cong \mathbb{Z}[T]/(T^2 - T + 5)$$

et ainsi[1]

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

et ce dernier est un corps puisque $T^2 + T + 1$ est irréductible sur $\mathbb{F}_2$.

Soit maintenant I un idéal non nul de A et $a \in I$ non nul tel que $N(a)$ soit minimal. Si $I = (a)$ on a terminé, sinon soit $x \in I\backslash(a)$. On applique alors le lemme précédent à x et a.

(i) Ou bien $x = aq + r$ avec $r = 0$ ou $N(r) < N(a)$, or $r \in I$, donc $r = 0$, ainsi $x \in (a)$, c'est impossible.

(ii) Ou bien $2x = aq + r$ avec $r = 0$ ou $N(r) < N(a)$ et de même $r = 0$ donc $2x = aq$. On a alors $aq \in (2)$ maximal donc premier, ainsi $a \in (2)$ ou $q \in (2)$. Si $q \in (2)$, alors $q = 2q'$ et donc $x = aq' \in (a)$ ce qui est impossible. Ainsi $a \in (2)$ et $q \notin (2)$, et donc $a = 2a'$ et $x = a'q$. Puisque (2) est maximal et ne contient pas q, $(2, q) = A$ et donc $1 = 2\lambda + q\mu$ avec $\lambda, \mu \in A$ et ainsi $a' = 2\lambda a' + \mu q a' = \lambda a + \mu x \in I$ car $a, x \in I$. On obtient une absurdité par minimalité de a.

□

Commentaire : c'est sûrement trop long : admettre le lemme, qui est technique et assez classique.

1. Une justification d'un résultat analogue est faite dans le développement "Théorème des deux carrés".