Développement : Un anneau principal non euclidien

Leçons : 122.

Théorème. *Soit* $\omega = \dfrac{1+i\sqrt{19}}{2}$. $\mathbb{Z}[\omega]$ *est principal mais non euclidien.*

Démonstration. On pose $A = \mathbb{Z}[\omega]$.
Étape 1 : Généralités sur l'anneau A.
On a $\omega^2 = -\frac{9}{2} + i\frac{\sqrt{19}}{2} = -5 + \omega$, ainsi $A = \{a + b\omega, (a,b) \in \mathbb{Z}^2\}$. On en déduit que A est un sous-anneau de $\mathbb{C}$.
De plus, $\overline{\omega} = 1 - \omega$ donc A est stable par conjugaison. A est intègre car $\mathbb{C}$ est intègre.
Déterminons les inversibles de A. On pose, pour $z \in A, N(z) = z\overline{z} = |z|^2$.
Comme $\omega + \overline{\omega} = 1$ et $\omega\overline{\omega} = \frac{1}{4} + \frac{19}{4} = 5$, on a $N(a+b\omega) = (a+b\omega)(a+b\overline{\omega}) = a^2 + ab + 5b^2 \in \mathbb{N}$, et on a aussi en passant à la forme canonique $N(z) = \left(a + \dfrac{b}{2}\right)^2 + \dfrac{19b^2}{4}$ $(*)$.
Soient $z, z' \in A$. On a $N(zz') = N(z)N(z')$ d'où si $z|z'$ dans A, on a aussi $N(z)|N(z')$ dans $\mathbb{N}$. Ainsi, si $z = a + b\omega$ inversible dans A, z divise 1 donc $N(z)$ divise $N(1) = 1$ donc $N(z) = 1$. Réciproquement, si $N(z) = 1$, on a $z\overline{z} = 1$ et comme $\overline{z} \in A$, z est inversible d'inverse $\overline{z}$. Si $N(z) = 1$, on a d'après $(*)$ que $b = 0$ d'où $1 = N(z) = a^2 + ab + 5b^2 = a^2$, ainsi $a = \pm 1$. Comme $N(\pm 1) = 1$, on a les inversibles : $A^\times = \{-1, 1\}$.

Étape 2 : A n'est pas euclidien.
Par l'absurde, supposons A euclidien, soit $\varphi : A\backslash\{0\} \to \mathbb{N}$ un stathme associé.
Soit $X = \{\varphi(z), z \in A\backslash\{-1,0,1\}\}$. On a $\varphi(\omega) \in X$ donc X partie non vide de $\mathbb{N}$, elle admet donc un plus petit élément m. Soit $u \in A\backslash\{-1,0,1\}$ tel que $\varphi(u) = m$. On a $u \neq 0$ et u non inversible donc $N(u) \geq 2$.
Soit $z \in A\backslash\{-1,0,1\}$. Il existe $q, r \in A$ tels que $z = uq + r$ et $r = 0$ ou $\varphi(r) < \varphi(u)$. Par définition de u, $\varphi(r) \notin X$ donc $r \in \{-1,0,1\}$. On a donc trois possibilités : $z = uq - 1, z = uq$ ou $z = uq + 1$, par suite u divise $z-1, z$ ou $z+1$. On appelle $P(z)$ cette propriété.

On applique $P(z)$ à $z = 2$: ainsi u divise 1, 2 ou 3. Si u divise 1, alors u inversible, impossible. On note $u = a + b\omega$.
- Supposons que u divise 2 : alors $N(u)$ divise $N(2) = 4$ donc $N(u) = 2$ ou 4.
- Supposons que u divise 3 : alors $N(u)$ divise $N(3) = 9$ donc $N(u) = 3$ ou 9.

En appliquant maintenant $P(z)$ à $z = \omega$, on a u divise $\omega - 1, \omega$ ou $\omega + 1$. Donc $N(u)$ divise $N(\omega - 1) = 5, N(\omega) = 5$ ou $N(\omega + 1) = 7$, contradiction avec $N(u) \in \{2,3,4,9\}$. Donc A n'est pas euclidien.

Étape 3 : A est principal.
Soit I idéal de A non réduit à $\{0\}$. Soit $T = \{N(x), x \in I\backslash\{0\}\}$, c'est une partie non vide de $\mathbb{N}$ qui possède donc un plus petit élément $k \in \mathbb{N}^*$, soit $y \in I$ tel que $N(y) = k$. Soit $x \in I\backslash\{0\}$. On a dans $\mathbb{C}$, $z := \dfrac{x}{y} = \dfrac{x\overline{y}}{N(y)} = \dfrac{\alpha + \beta\omega}{\gamma}$
où on peut supposer $\alpha, \beta, \gamma \in \mathbb{Z}$ premiers entre eux dans leur ensemble et $\gamma > 0$.
- Si $\gamma = 2$: alors α ou β est impair. Soit $u = \alpha + \beta\overline{\omega}$, ainsi $z = \overline{u}/2$. Alors $N(u) = \alpha^2 + \alpha\beta + 5\beta^2$ est impair : soit $v \in \mathbb{N}$ tel que $N(u) = 2v + 1$, alors $zu - v = \frac{1}{2}N(u) - v) = \frac{1}{2}$.
- Si $\gamma \geq 3$: par Bézout, il existe $m, n, q \in \mathbb{Z}$ tels que $n\alpha + (m+n)\beta - q\gamma = 1$.
  Soit p un des entiers les plus proches de $\frac{m\alpha - 5n\beta}{\gamma}$. Soient $u = m + n\omega, v = p + q\omega$. On a
  $$zu - v = \frac{\alpha + \beta\omega}{\gamma}(m + n\omega) - (p + q\omega) = \frac{m\alpha + m\beta\omega + \alpha n\omega + \beta n(-5 + \omega)}{\gamma} - (p + q\omega)$$
  $$= \frac{m\alpha - 5n\beta}{\gamma} - p + \frac{\beta(m+n) + \alpha n - q\gamma}{\gamma}\omega = r + \frac{\omega}{\gamma} \text{ avec } r \in \mathbb{Q}, |r| \leq \tfrac{1}{2}.$$
  Alors $N(zu - v) = r^2 + r\frac{\omega + \overline{\omega}}{\gamma} + \frac{\omega\overline{\omega}}{\gamma^2} = r^2 + \frac{r}{\gamma} + \frac{5}{\gamma^2} \leq \frac{1}{4} + \frac{1}{6} + \frac{5}{9} = \frac{35}{36} < 1$.
  Et $zu - v \neq 0$ sinon $\omega = -r\gamma \in \mathbb{R}$, ce qui est faux.

On a donc $u, v \in A$ tq $zu - v \neq 0, N(zu - v) < 1$. On a $ux - vy = y(zu - v) \neq 0$ et $N(ux - vy) < N(y)$, contradiction avec la définition de y car $ux - vy \in I\backslash\{0\}$. Ainsi $\gamma < 2$ donc $\gamma = 1$ et $z = \alpha + \beta\omega \in A$, donc $x = yz \in yA$ et comme $y \in I, I = yA$ et A est principal. □

Références

B. Hauchecorne, Les contre-exemples en mathématiques, Ellipses, p. 49.