Définition 1.1 (Anneau euclidien). — Un anneau A intègre est dit euclidien s'il existe une application $\theta : A \to \mathbb{N}$ (appelée stathme) telle que :

$$\forall (a,b) \in A \times A \setminus \{0\},\ \exists q, r \in A, \quad a = bq + r \quad \text{avec} \quad \theta(r) < \theta(b)$$

Exemples 1.2. —

(a) $\mathbb{Z}$ est euclidien pour $\theta(n) = |n|$

(b) $\mathbb{R}[X]$ et $\mathbb{C}[X]$ sont euclidiens pour $\theta(P) = \begin{cases} \deg(P) + 1 & \text{si } P \neq 0 \\ 0 & \text{sinon} \end{cases}$

(c) $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ avec $\theta(z) = |z|^2$

(d) $\mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2} \mid a, b \in \mathbb{Z}\}$ avec $\theta(z) = |z|^2$

Preuve

Les points (a) et (b) sont faciles à vérifier. Nous montrons (d), et laissons le soin à l'étudiant d'adapter cette preuve pour (c). Comme $\mathbb{Z}[i\sqrt{2}]$ est un sous-anneau de $\mathbb{C}$, il est donc commutatif, unitaire ($1 = 1 + 0 \times i \times \sqrt{2}$) et intègre.

Pour $z = a + ib\sqrt{2}$, on pose $\theta(z) = |z|^2 = a^2 + 2b^2$. Il est clair que $\theta : \mathbb{Z}[i\sqrt{2}] \to \mathbb{N}$ et que θ est une application multiplicative :

$$\forall z, w \in \mathbb{Z}[i\sqrt{2}], \quad \theta(zw) = \theta(z)\theta(w)$$

Soit $z, w \in \mathbb{Z}[i\sqrt{2}]$ avec $w \neq 0$. Montrons qu'il existe $q, r \in \mathbb{Z}[i\sqrt{2}]$ tels que $z = qw + r$ avec $\theta(r) < \theta(w)$. Cette dernière inégalité est équivalente à :

$$\left| \frac{z}{w} - q \right|^2 < 1$$

Le quotient z/w peut s'écrire $\frac{z}{w} = u + iv\sqrt{2},\ u, v \in \mathbb{Q}$. Il existe $x \in \mathbb{Z}$ tel que $|u - x| < \frac{1}{2}$:

$$x = \begin{cases} \lfloor u \rfloor & \text{si } \lfloor u \rfloor \leq u \leq \lfloor u \rfloor + \frac{1}{2} \\ \lfloor u \rfloor + 1 & \text{si } \lfloor u \rfloor + \frac{1}{2} \leq u < \lfloor u \rfloor + 1 \end{cases}$$

De même, il existe $y \in \mathbb{Z}$ tel que $|v - y| < \frac{1}{2}$. Posons alors $q = x + iy\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$. On a :

$$\theta\left(\frac{z}{w} - q\right) = \left|(u - x) + i(v - y)\sqrt{2}\right|^2 = (u - x)^2 + 2(v - y)^2 \leq \frac{3}{4} < 1$$

Posons $r = z - wq$. Alors $z = wq + r$ et :

$$\theta(r) = \theta(w)\theta\left(\frac{z}{w} - q\right) < \theta(w)$$