
Théorème des deux carrés de Fermat

Proposition — $\mathbb{Z}[i]^\times = \{\pm 1; \pm i\}$.

DÉMONSTRATION

Soit $z = a + ib \in \mathbb{Z}[i]$.

Si z est inversible, il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$. Alors

$$N(zz') = N(z)N(z') = 1$$

c'est-à-dire que $N(z) = z\bar{z}$ est un inversible de $\mathbb{Z}$.

Par positivité de $N(z)$, on a

$$N(z) = a^2 + b^2 = 1.$$

Donc

$$\begin{cases} a = 0 \\ b = \pm 1 \end{cases} \quad \text{ou} \quad \begin{cases} a = \pm 1 \\ b = 0 \end{cases}.$$

Réciproquement, il est direct que $\{\pm 1; \pm i\} \subset \mathbb{Z}[i]^\times$.

□

Proposition — *L'anneau $\mathbb{Z}[i]$ est euclidien.*

DÉMONSTRATION

Soient $z = a + ib \in \mathbb{Z}[i]$ et $t = c + id \in \mathbb{Z}[i] - \{0\}$.

On a

$$\frac{z}{t} = \frac{a + ib}{c + id} = \frac{ac - bd}{c^2 + d^2} + i \frac{ad + bc}{b^2 + d^2}.$$

On choisit $x, y \in \mathbb{Z}$ tel que

$$\left| \frac{ac - bd}{c^2 + d^2} - x \right| \leq \frac{1}{2} \quad \text{et} \quad \left| \frac{ad + bc}{b^2 + d^2} - y \right| \leq \frac{1}{2}.$$

Alors

$$\begin{aligned}\left|\frac{z}{t} - (x + iy)\right|^2 &= \Re\left(\frac{z}{t} - (x + iy)\right)^2 + \Im\left(\frac{z}{t} - (x + iy)\right)^2 \\ &\leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1.\end{aligned}$$

D'où

$$z = t(x + iy) + (z - t(x + iy)) \text{ et } N(z - t(x + iy)) < N(t)$$

Ainsi $\mathbb{Z}[i]$ est euclidien pour le stathme N . □

Lemme — Soient A un anneau et $a, b \in A$.

Alors $(A/(a))/(\bar{b}) \simeq A/(a, b) \simeq (A/(b))/(\bar{a})$.

DÉMONSTRATION

Il suffit de démontrer le premier isomorphisme. Le deuxième est alors direct par symétrie.

On note respectivement $\pi_a : A \rightarrow A/(a)$ et $\pi_{ab} : A \rightarrow A/(a, b)$ les injections canoniques de A dans ses quotients par les idéaux (a) et (a, b) .

Comme $(a) \subset (a, b)$, par la propriété universelle des quotients, il existe un morphisme d'anneaux $\overline{\pi_{ab}} : A/(a) \rightarrow A/(a, b)$ tel que

$$\overline{\pi_{ab}} \circ \pi_a = \pi_{ab}.$$

D'après le premier théorème d'isomorphisme, on en déduit que

$$\text{Im } \overline{\pi_{ab}} \simeq (A/(a))/\ker \overline{\pi_{ab}}.$$

Or

$$\text{Im } \overline{\pi_{ab}} = \text{Im } \pi_{ab} = A/(a, b)$$

et

$$\bar{x} \in \ker \overline{\pi_{ab}} \Leftrightarrow \pi_{a,b}(x) = 0 \Leftrightarrow x \in (a, b) \Leftrightarrow \bar{x} \in (\bar{b}).$$

En effet

$$\begin{aligned}x = au + bv &\Rightarrow \bar{x} = \bar{b} \cdot \bar{v} \\ \bar{x} = \bar{b} \cdot \bar{v} &\Rightarrow \bar{x} = bv + (a) \Rightarrow \exists u \in A, x = au + bv\end{aligned}$$

Donc

$$A/(a, b) \simeq (A/(a))/(\bar{b}).$$

□

Théorème

Soit p premier.

p est somme de deux carrés ssi $p = 2$ ou $p \equiv 1 \pmod{4}$.

DÉMONSTRATION

On procède par équivalence

$$\begin{aligned} p \text{ est somme de 2 carrés} &\Leftrightarrow \exists x, y \in \mathbb{Z}, p = x^2 + y^2 \\ &\Leftrightarrow \exists z \in \mathbb{Z}[i], p = N(z) = z\bar{z} \\ &\Leftrightarrow p \in \mathbb{Z}[i] \text{ est non irréductible} \\ &\Leftrightarrow p \in \mathbb{Z}[i] \text{ est non premier car } \mathbb{Z}[i] \text{ est principal} \\ &\Leftrightarrow \mathbb{Z}[i]/(p) \simeq (\mathbb{Z}[X]/(X^2 + 1))/(p) \text{ est non intègre} \\ &\Leftrightarrow (\mathbb{Z}[X]/(p))/(X^2 + 1) \text{ est non intègre} \\ &\Leftrightarrow X^2 + 1 \in \mathbb{F}_p[X] \text{ est non irréductible car } \mathbb{F}_p[X] \text{ est principal} \\ &\Leftrightarrow X^2 + 1 \text{ admet une racine dans } \mathbb{F}_p \\ &\Leftrightarrow -1 \text{ est un carré dans } \mathbb{F}_p \\ &\Leftrightarrow p = 2 \text{ ou } p \equiv 1 \pmod{4}. \quad \square \end{aligned}$$