Théorème des deux carrés

Référence(s) :
– Daniel Perrin - *Cours d'algèbre*, page 57

Soit $\Sigma = \{n \in \mathbb{N} | \exists a, b \in \mathbb{Z}, a^2 + b^2 = n\}$

Théorème 1

Soit p un nombre premier impair. Alors, on a :

$$p \in \Sigma \text{ si et seulement si } p \equiv 1 \ [4]$$

Étape 1

On définit une norme sur $\mathbb{Z}[i]$, l'anneau des entiers de Gauss.

On définit une "norme" sur $\mathbb{Z}[i]$: $N : \left| \begin{array}{ccc} \mathbb{Z}[i] & \longrightarrow & \mathbb{N} \\ a+ib & \longmapsto & a^2+b^2 \end{array} \right.$.
Pour $z, z' \in \mathbb{Z}[i]$, $N(zz') = zz'\overline{zz'} = N(z)N(z')$.
Ainsi, N est multiplicative sur $\mathbb{Z}[i]$.

Étape 2

$Z[i]^* = \{\pm 1, \pm i\}$

– On a : $\{\pm 1, \pm i\} \in \mathbb{Z}[i]$
– Par ailleurs, soit $z \in \mathbb{Z}[i]^*$. Alors, on a $zz^{-1} = 1$, c'est-à-dire $N(z)N(z^{-1}) = 1$. Ainsi, comme N est à valeurs dans $\mathbb{N}$, $N(z) = 1$, et si on écrit $z = a + ib$, on obtient $a^2 + b^2 = 1$, avec $a, b \in \mathbb{N}$. Nécessairement,

$$a = 0, b = \pm 1 \text{ ou } a = \pm 1, b = 0$$

Étape 3

$p \in \Sigma$ *ssi p est réductible dans $\mathbb{Z}[i]$*

$\Rightarrow$: Supposons que $p \in \Sigma$. Soient $a, b \in \mathbb{N}$ tels que $p = a^2+b^2$. Alors, $N(a+ib) = N(a-ib) = a^2+b^2 = p \neq 1$. D'après ce qui précède, $a + ib, a_i b \notin \mathbb{Z}[i]^*$. Ainsi, p est réductible dans $\mathbb{Z}[i]$.
$\Leftarrow$: Supposons que p est réductible dans $\mathbb{Z}[i]$. Alors il existe $z, z' \in \mathbb{Z}[i]$ non inversibles tels que $p = zz'$. Alors, $N(p) = p^2 = N(z)N(z')$, avec $N(z), N(z') \neq 1$. Ainsi, $p = N(z) = a^2 + b^2$, si on écrit $z = a + ib$. Donc $p \in \Sigma$

Étape 4

Preuve du théorème

Comme l'anneau $\mathbb{Z}[i]$ est euclidien, il est factoriel. Ainsi :

$$\begin{aligned} p \text{ est réductible } &\Leftrightarrow (p) \text{ est non-premier} \\ &\Leftrightarrow \mathbb{Z}[i]/(p) \text{ est non-intègre} \end{aligned}$$

Or $\mathbb{Z}[i]/(p)$ est isomorphe à $\left(\mathbb{Z}[X]/(X^2+1)\right)/(p)$, lui même isomorphe à $\mathbb{Z}[X]/(X^2+1,p)$, puis à $(\mathbb{Z}[X]/(p))/(X^2+1)$. Ainsi, $\mathbb{Z}[i]/(p)$ est isomorphe à $\mathbb{F}_p[X]/(X^2+1)$. Donc :

$$\begin{aligned} p \in \Sigma &\Leftrightarrow \mathbb{F}_p[X]/(p) \text{ non-intègre} \\ &\Leftrightarrow X^2+1 \text{ est réductible dans } \mathbb{F}_p[X] \\ &\Leftrightarrow X^2+1 \text{ admet une racine dans } \mathbb{F}_p[X] \\ &\Leftrightarrow (-1) \text{ est un carré dans } \mathbb{F}_p \\ &\Leftrightarrow \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1 \\ &\Leftrightarrow p \equiv 1\ [4] \end{aligned}$$

Corollaire 1

Soit $n \in \mathbb{N}^*, n = \prod_{p\in\mathcal{P}} p^{\nu_p(n)}$. Alors

$$n \in \Sigma \Leftrightarrow (\forall p \in \mathcal{P}, p \equiv 3\ [4] \rightarrow \nu_p(n) \equiv 0\ [2])$$

L'ensemble Σ est multiplicatif : Soient $n = N(z), n' = N(z') \in \Sigma$. Alors

$$nn' = N(zz') \in \Sigma$$

.

$\underline{\Leftarrow :}$ On écrit :

$$n = \underbrace{\left(\prod_{p\equiv 3\ [4]} p^{\frac{\nu_p(n)}{2}}\right)^2}_{\in\Sigma} \left(\prod_{p\equiv 1\ [4]} \underbrace{p}_{\in\Sigma}{}^{\nu_p(n)}\right) \in \Sigma$$

$\underline{\Rightarrow :}$ Soit $n = a^2+b^2 \in \Sigma$. Soit $p \in \mathcal{P}$, tel que $p \equiv 3\ [4]$. Montrons par récurrence forte sur $\nu_p(n)$ que $\nu_p(n)$ est pair.

- Si $\nu_p(n) = 0$, c'est bon.
- Si $\nu_p(n)\ in\mathbb{N}^*$, on a : $p|n = a^2+b^2 = (a+ib)(a-ib)$. Or $p \not\equiv 1\ [4]$ donc d'après ce qui précède, p est irréductible dans $\mathbb{Z}[i]$ donc $p|a+ib$ (par exemple). Or $p \in \mathbb{N}$, donc $p|a$ et $p|b$ et donc $p^2|n$. On a $\nu_p(n/p^2) = \nu_p(n) - 2$, or par hypothèse de récurrence, $\nu_p(n/p^2)$ est pair donc $\nu_p(n)$ est pair.

Compléments

- $\mathbb{Z}[i]$ **est euclidien :** Soient $z, t \in \mathbb{Z}[i] \setminus \{0\}$. On considère $\frac{z}{t} \in \mathbb{C}$, et on note $\frac{z}{t} = x+iy$. Soit $q = a+ib$ avec a, b les entiers les plus proches de x et y. Alors :

$$|\frac{z}{t} - q| \leqslant \frac{\sqrt{2}}{2} < 1$$

On pose $r = z - qt \in \mathbb{Z}[i]$. On a : $r = t\left(\frac{z}{t} - q\right)$ donc $|r| = |t||z/t - q| < |t|$. Ainsi,

$$z = qt + r \text{ avec } N(r) < N(t)$$

- **Équivalences entre les anneaux :**
Soient $\pi_1 : \mathbb{Z}[X] \to \mathbb{Z}[X]/(X^2+1)$ et $\pi_2 : \mathbb{Z}[X]/(X^2+1) \to (\mathbb{Z}[X]/(X^2+1))/(p)$ les projections canoniques. Alors :

$$\begin{aligned} \ker(\pi_2 \circ \pi_1) &= \{f \in \mathbb{Z}[X] | \exists u \in \mathbb{Z}[X], \bar{f} = \bar{p}\bar{u}\} \\ &= \{f \in \mathbb{Z}[X] | \exists u, v \in \mathbb{Z}[X], f = pu + (X^2+1)\} \\ &= (p, X^2+1) \end{aligned}$$

D'où le résultat. De la même façon, on montre :

$$Z[X]/(p, X^2+1) \sim (\mathbb{Z}[X]/(p))/(\overline{X^2+1}) \sim \mathbb{F}_p[X]/(X^2+1)$$