Théorème des deux carrés

Leçons 121,122,126

Théorème (Théorème des deux carrés de Fermat)

Soit l'ensemble:

$$\Sigma \;=\; \left\{n \in \mathbb{N} : \exists (a,b) \in \mathbb{N}^2 : n = a^2 + b^2\right\}$$

Soit $p \in \mathbb{N}$ premier. On a alors:

$$p \in \Sigma \;\Leftrightarrow\; p = 2 \text{ ou } p \equiv 1\ [4]$$

Voici le plan de la démonstration:

1. Montrer que $\mathbb{Z}[i]$ est euclidien et que:

$$\mathbb{Z}[i]^\times \;=\; \{-i, i, -1, 1\}$$

2. Montrer que, pour $p \in \mathbb{N}$ premier:

$$\begin{aligned} p \in \Sigma &\Leftrightarrow p \text{ n'est pas irréductible dans } \mathbb{Z}[i] \\ &\Leftrightarrow p \equiv 1\ [4] \text{ ou } p = 2 \end{aligned}$$

Démonstration. *1. Montrons que $\mathbb{Z}[i]$ est euclidien pour le stathme:*

$$\begin{array}{rccc} N: & \mathbb{Z}[i] & \longrightarrow & \mathbb{N} \\ & z & \longmapsto & z\overline{z} = |z|^2 \end{array}$$

Soient $z, t \in \mathbb{Z}[i]$ avec $t \neq 0$. $\frac{z}{t} \in \mathbb{C}$ donc il existe $(x,y) \in \mathbb{R}^2$ tel que: $\frac{z}{t} = x + iy$.

Soit alors $q \in \mathbb{Z}[i]$ tel que $q = a + ib$ avec:

$$(a,b) \in \mathbb{Z}^2 \quad et \quad |a - x| \leq \frac{1}{2}, |b - y| \leq \frac{1}{2} \tag{1}$$

Alors on a:

$$N\left(\frac{z}{t} - q\right) = |a - x|^2 + |b - y|^2 \leq \frac{1}{2} < 1$$

Posons alors $r = z - qt$. On a: $N(r) = N(z - qt) = N(t)N\left(\frac{z}{t} - q\right) < N(t)$.

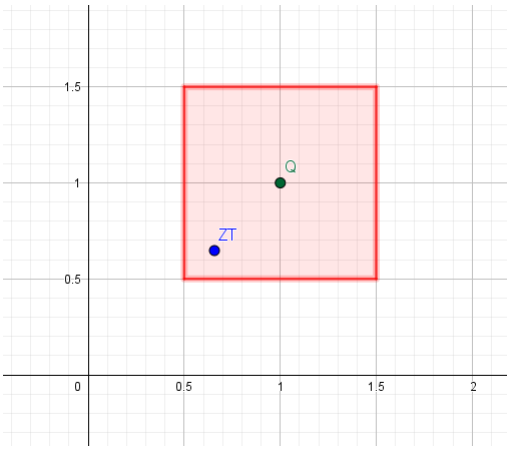

Figure 1: Illustration de la propriété (1), le carré rouge indique la zone pour laquelle q est l'élément de $\mathbb{Z}[i]$ le plus "proche". q et $\frac{z}{t}$ ont respactivement Q et ZT pour image dans le plan complexe

Ainsi, $z = qt + r$ avec $0 \leq N(r) \leq N(t)$. N est bien un stathme euclidien. Ainsi, l'anneau $\mathbb{Z}[i]$ est euclidien, donc factoriel.

Soit $z \in \mathbb{Z}[i]^\times$. Il existe $u \in \mathbb{Z}[i]$ tel que $zu = 1$. Donc $N(zu) = N(z)N(u) = 1$. Comme N est à valeurs dans $\mathbb{N}$, on a forcément $N(z) = 1$, i.e. $z \in \{-i, i, -1, 1\}$.

De plus, si $z \in \{-i, i, -1, 1\}$, alors $z \in \mathbb{Z}[i]^\times$ $z\overline{z} = 1$. Donc on a bien:

$$\mathbb{Z}[i]^\times = \{-i, i, -1, 1\}$$

2. *Soit $p \in \mathbb{N}$ un nombre premier. Montrons que:*

$$p \in \Sigma \Leftrightarrow p \text{ n'est pas irréductible dans } \mathbb{Z}[i]$$

- $\Rightarrow$: *Si $p \in \Sigma$, alors il existe $(a, b) \in \mathbb{N}^2$ tel que $p = a^2 + b^2$, avec $a, b \neq 0$ puisque $p \geq 2$ et p est premier (par exemple si $a = 0$ alors $p = b^2$ ce qui contredit la primalité de p). Donc $p = (a + ib)(a - ib)$ et $a \pm ib \notin \mathbb{Z}[i]^\times$. Donc p n'est pas irréductible dans $\mathbb{Z}[i]^\times$.*
- $\Leftarrow$ *Si p est non irréductible dans $\mathbb{Z}[i]$, alors $p = zz'$, avec $z, z' \notin \mathbb{Z}[i]^\times$. Donc on a:*

$$\begin{aligned} N(p) &= N(zz') \\ &= N(z)N(z') \\ &= p^2 \end{aligned}$$

Comme $z, z' \notin \mathbb{Z}[i]^\times$, il vient $N(z) = N(z') = p$, donc $p \in \Sigma$

On obtient ainsi:

$$\begin{aligned}
p \text{ non irréductible dans } \mathbb{Z}[i] &\Leftrightarrow \langle p\rangle \text{ n'est pas un idéal premier de } \mathbb{Z}[i] \\
&\Leftrightarrow \frac{\mathbb{Z}[i]}{\langle p\rangle} \simeq \frac{\mathbb{Z}[X]}{\langle X^2+1, p\rangle} \simeq \frac{\mathbb{F}_p[X]}{\langle X^2+1\rangle} \\
&\quad \text{n'est pas un anneau intègre} \\
&\Leftrightarrow \langle X^2+1\rangle \text{ n'est pas un idéal premier de } \mathbb{F}_p[i] \\
&\Leftrightarrow X^2+1 \text{ n'est pas irréductible dans } \mathbb{F}_p[X] \quad (2) \\
&\Leftrightarrow -1 \text{ est un carré modulo } p \quad (3) \\
&\Leftrightarrow p=2 \text{ ou } (-1)^{\frac{p-1}{2}}=1 \quad (4) \\
&\Leftrightarrow p=2 \text{ ou } \frac{p-1}{2} \text{ est pair} \\
&\Leftrightarrow p=2 \text{ ou } p\equiv 1\ [4]
\end{aligned}$$

■

Remarque(s).
1. *L'implication* (2) $\Rightarrow$ (3) *se montre en partant du fait que si* $X^2+1 \in \mathbb{F}_p[X]$ *n'est pas irréductible, comme il est de degré 2, alors il se décompose en un produit de deux facteurs de degré 1, i.e. admet au moins une racine* α*, vérifiant* $\alpha^2+1=0$ *dans* $\mathbb{F}_p=\frac{\mathbb{Z}}{p\mathbb{Z}}$*. L'implication réciproque est triviale.*
2. *L'équivalence* (3) $\Leftrightarrow$ 4 *est triviale lorsque* $p=2$ *et repose sur le symbole de Legendre (ainsi que le théorème de Lagrange pour le groupe multiplicatif* $\mathbb{F}_p^*=\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$*)*

Reférence(s). *D.Perrin, Cours d'algèbre*