Théorème des deux carrés

Leçons : ***120*****, 121, 122, 126**

Théorème 1

Soit $n = \prod_{p\in\mathcal{P}} p^{v_p(n)} \in \mathbb{N}^*$. *Alors* p *s'écrit comme somme de deux carrés dans* $\mathbb{Z}$ *si et seulement si* $v_p(n)$ *est pair pour* $p \equiv 3[4]$.

Démonstration. Considérons l'anneau des entiers de Gauss

$$\mathbb{Z}[i] = \left\{a + ib, (a,b) \in \mathbb{Z}^2\right\}$$

muni de $N : z = a + ib \mapsto a^2 + b^2$. Soit $\Sigma = \left\{a^2 + b^2, (a,b) \in \mathbb{Z}^2\right\} = N(\mathbb{Z}[i])$.

- $(\mathbb{Z}[i], N)$ est un anneau euclidien. En effet, si $z, z' \in \mathbb{Z}[i]$, alors $\dfrac{z}{z'} = x + iy \in \mathbb{Q}[i]$ donc en prenant $a, b \in \mathbb{Z}$ tels que $|a-x| \leqslant \dfrac{1}{2}$ et $|b-y| \leqslant \dfrac{1}{2}$, on a en posant $q = a+ib$,

  $$\left|\frac{z}{z'} - q\right| \leqslant \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

  donc $z = qz' + r$, où $N(z) < N(z')$.

- Si $z = a + ib \in \mathbb{Z}[i]^\times$, alors il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$ donc $N(zz') = 1 = N(z)N(z')$ de sorte que $N(z) = 1 = a^2 + b^2$. Ainsi, $z = \pm 1$ ou $\pm i$ et

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

- Soit p premier dans $\mathbb{Z}$. Montrons que $p \in \Sigma \Leftrightarrow p$ n'est pas irréductible dans $\mathbb{Z}[i]$.
  En effet, d'une part, si $p = a^2 + b^2 = (a - ib)(a + ib)$, p n'est pas irréductible : on ne peut avoir $a = 0$ ou $b = 0$ puisque p est premier dans $\mathbb{Z}$, donc selon la description de $\mathbb{Z}[i]^\times$, ni $a + ib$, ni $a - ib$ ne sont des unités de $\mathbb{Z}[i]$.
  Réciproquement, si p n'est pas irréductible, on écrit $p = zz'$ avec $z, z' \notin \{\pm 1, \pm i\}$ donc $p^2 = N(p) = N(z)N(z')$ avec $N(z), N(z') \neq p$. Par conséquent, $N(z) = N(z') = p$ et $p \in \Sigma$.

- Comme $\mathbb{Z}[i]$ est principal, p est irréductible dans $\mathbb{Z}[i]$ si et seulement si $\mathbb{Z}[i]/(p)$ est intègre. Or, $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2 + 1)$ et le morphisme canonique

  $$\mathbb{Z}[X] \xrightarrow[\text{reduction mod } p]{} (\mathbb{Z}/p\mathbb{Z})[X] \to (\mathbb{Z}/p\mathbb{Z})[X]/(X^2 + 1)$$

  se factorise en $\mathbb{Z}[X]/(X^2 + 1) \to \mathbb{F}_p[X]/(X^2 + 1)$ dont on vérifie immédiatement qu'il est de noyau (p). Donc

  $$\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[X]/(X^2 + 1).$$

  Ainsi, p est irréductible dans $\mathbb{Z}[i] \Leftrightarrow X^2 + 1$ est irréductible dans $\mathbb{F}_p[X]$, c'est-à-dire s'il n'a aucune racine dans $\mathbb{F}_p[X]$, soit encore si -1 n'est pas un carré modulo p. Or, dans $\mathbb{F}_p$,

  $$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow \frac{p-1}{2} \equiv -1[2] \Leftrightarrow p \equiv 3[4].$$

  Finalement, $p \in \Sigma \Leftrightarrow p = 2$ ou $p \equiv 1[4]$.

- Pour terminer, traitons le cas général. Soit $n = \prod_{p \in \mathscr{P}} p^{v_p(n)}$. Remarquons que $\Sigma = N(\mathbb{Z}[i])$ est stable par multiplication car $\mathbb{Z}[i]$ est un anneau.
  Alors si pour tout $p \equiv 3[4]$, $v_p(n)$ est pair, on a

$$n = \left(\prod_{p \equiv 3} p^{\frac{v_p(n)}{2}}\right)^2 \times \left(\prod_{p \equiv 1 \text{ ou } p=2} p^{v_p(n)}\right)$$

  si bien que $n \in \Sigma$ en tant que produit d'éléments de Σ.
  Montrons la réciproque par récurrence sur n. Soit $n = a^2 + b^2 \in \Sigma$, et $p \equiv 3[4]$ tel que $v_p(n) > 0$. Alors $p | a^2 + b^2 = (a+ib)(a-ib)$ donc comme p est irréductible dans $\mathbb{Z}[i]$, $p|a+ib$ ou $p|a-ib$ dans $\mathbb{Z}[i]$. Dans les deux cas, comme p est entier, on a $p|a$ et $p|b$, si bien que $p^2|n$. Appliquant l'hypothèse de récurrence à $\frac{n}{p^2} = \left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2 \in \Sigma$, on obtient que $v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2$ est pair, ce qui conclut.

□

Corollaire 2

Les irréductibles de $\mathbb{Z}[i]$ sont, à association près, les premiers $p \in \mathbb{Z}$ tels que $p \equiv 3[4]$ et les entiers de Gauss $z = a + ib$ tels que $N(z)$ est un premier de $\mathbb{Z}$.

Démonstration.
- On a déjà vu que les premiers $p \in \mathbb{Z}$ tels que $p \equiv 3[4]$ sont irréductibles. Soit $z = a + ib$ tels que $p = N(z)$ est premier dans $\mathbb{Z}$. Si $z = z'z''$, alors $N(z) = N(z')N(z")$ donc $N(z') = 1$ ou $N(z") = 1$ c'est-à-dire z' ou $z'' \in \mathbb{Z}[i]^\times$.
- Réciproquement, soit $z = a + ib \in \mathbb{Z}[i]$ irréductible. Alors $N(z) = z\overline{z}$. Soit p premier dans $\mathbb{Z}$ tel que $p \mid N(z)$. Alors si $p \equiv 3[4]$, p divise z ou $\overline{z}$ dans $\mathbb{Z}[i]$ donc comme z est irréductible, $z = p$ à $\pm 1, \pm i$ près. Sinon, $p \in \Sigma$, $p = a^2 + b^2$ donc selon le premier point, $t = a + ib$ est irréductible. Selon le lemme de Gauss, t divise z ou $\overline{z}$ donc est égal à z à association près.

□

Référence : Daniel PERRIN (1996). *Cours d'algèbre*. Ellipses, pp. 56-58.