# L'anneau $\mathbb{Z}[i]$ et le théorème des deux carrés

Riffaut Antonin

2013-2014

On considère l'anneau $\mathbb{Z}[i] = \{a + ib\,;\, a, b \in \mathbb{Z}\}$, appelé *anneau des entiers de Gauss*. On munit $\mathbb{Z}[i]$ de l'application « norme » :

$$N : \left\{ \begin{array}{ccc} \mathbb{Z}[i] & \longrightarrow & \mathbb{N} \\ z = a + ib & \longmapsto & z\overline{z} = a^2 + b^2. \end{array} \right.$$

On rappelle que $N$ est multiplicative et munit $\mathbb{Z}[i]$ d'une structure d'anneau euclidien. D'autre part, les éléments inversibles de $\mathbb{Z}[i]$ sont ceux de norme 1, à savoir 1, $-1$, $i$ et $-i$.

Notons $\Sigma$ l'ensemble des entiers naturels qui s'écrivent comme somme de deux carrés :

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

Le problème est de déterminer $\Sigma$. Le théorème des deux carrés donne une condition nécessaire et suffisante pour qu'un nombre premier impair $p$ donné appartienne à $\Sigma$ :

**Théorème 1.** *Soit $p$ un nombre premier impair. Alors $p \in \Sigma$ si et seulement si $p \equiv 1 \mod 4$.*

La démonstration du théorème s'appuie sur le lemme suivant :

**Lemme 2.** *Soit $p$ un nombre premier impair. Alors $p \in \Sigma$ si et seulement si $p$ n'est pas irréductible dans $\mathbb{Z}[i]$.*

*Démonstration.* ($\Rightarrow$) Si $p \in \Sigma$, $p = a^2 + b^2$ avec $a, b \in \mathbb{Z}$. Dans $\mathbb{Z}[i]$, on a $p = (a+ib)(a-ib)$ ; $a$ et $b$ étant non nuls (puisque $p$ n'est pas un carré parfait), $a + ib$ et $a - ib$ ne sont pas inversibles, donc $p$ n'est pas irréductible.

($\Leftarrow$) Réciproquement, supposons que $p$ ne soit pas irréductible : $p = zz'$ avec $z, z' \in \mathbb{Z}[i]$ non inversibles. En passant à la norme, on obtient $p^2 = N(z)N(z')$. Or $N(z) \neq 1$ et $N(z') \neq 1$, puisque $z$ et $z'$ ne sont pas inversibles, d'où $N(z) = p$, et ainsi $p \in \Sigma$ (si $z = a+ib$, $p = N(z) = a^2 + b^2$). ■

*Démonstration du théorème.* Comme $\mathbb{Z}[i]$ est factoriel, $p$ n'est pas irréductible dans $\mathbb{Z}[i]$ si et seulement si l'idéal $(p) \subset \mathbb{Z}[i]$ n'est pas premier, ce qui équivaut encore à dire que $\mathbb{Z}[i]/(p)$ n'est pas intègre. On exploite alors l'isomorphisme

$$\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2 + 1),$$

d'où il s'ensuit que

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

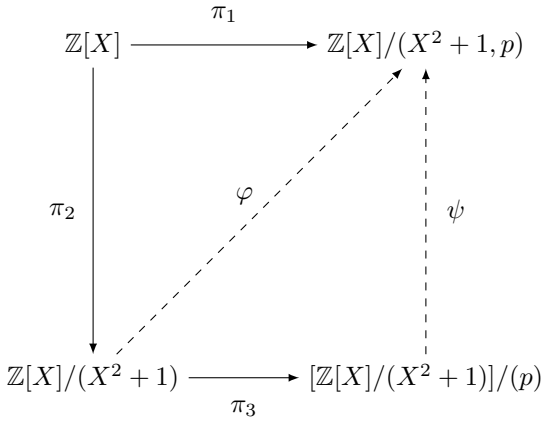
1. voir la justification ci-après

et donc $\mathbb{Z}[i]/(p)$ n'est pas intègre si et seulement si $X^2+1$ n'est pas irréductible dans $\mathbb{F}_p[X]$, ce qui revient à dire qu'il possède une racine dans $\mathbb{F}_p$ (puisqu'il est de degré 2). En résumé, $p \in \Sigma$ si et seulement si $-1$ est un carré dans $\mathbb{F}_p$. Or

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \mod 4, \\ -1 & \text{sinon.} \end{cases}$$

Autrement dit, $-1$ est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv 1 \mod 4$, ce qui constitue le résultat attendu.

Pour conclure, justifions les isomorphismes précédents. Pour ce faire, considérons le diagramme suivant :




où $\pi_1$, $\pi_2$ et $\pi_3$ désignent les morphismes de projection respectifs. On utilise ensuite le premier théorème d'isomorphisme, d'abord appliqué à $\pi_1$ : comme $(X^2+1) \subset \ker \pi_1 = (X^2+1,p)$, alors $\pi_1$ se factorise par $\mathbb{Z}[X]/(X^2+1)$ : il existe un morphisme $\varphi : \mathbb{Z}[X]/(X^2+1) \longrightarrow \mathbb{Z}[X]/(X^2+1,p)$ tel que $\pi_1 = \varphi \circ \pi_2$. D'autre part, $(p) \subset \ker \varphi = \pi_2(\ker(\pi_1)) = (p)$, donc de nouveau par le premier théorème d'isomorphisme, $\varphi$ se factorise par $[\mathbb{Z}[X]/(X^2+1)]/(p)$ : il existe un morphisme $\psi : [\mathbb{Z}[X]/(X^2+1)]/(p) \longrightarrow \mathbb{Z}[X]/(X^2+1,p)$ tel que $\varphi = \psi \circ \pi_3$. Finalement, comme $\pi_1$ est surjectif, alors $\varphi$ puis $\psi$ le sont également ; d'autre part, $\ker(\psi) = \pi_3(\ker(\varphi)) = (0)$ : $\psi$ est par conséquent un isomorphisme, ce qui prouve que $\mathbb{Z}[X]/(X^2+1,p) \simeq [\mathbb{Z}[X]/(X^2+1)]/(p)$. Le même raisonnement aboutit à $\mathbb{Z}[X]/(X^2+1,p) \simeq [\mathbb{Z}[X]/(p)]/(X^2+1)$, d'où les isomorphismes recherchés. ■

*Remarque.* Le nombre premier 2 appartient également à $\Sigma$, puisque $2 = 1^2+1^2$. En conséquence, tout nombre premier $p$ non congru à 3 modulo 4 s'écrit comme somme de deux carrés.

Nous sommes à présent en mesure de déterminer complètement $\Sigma$. Pour ce faire, commençons par un lemme :

**Lemme 3.** *Si $m, n \in \Sigma$, alors $mn \in \Sigma$.*

*Démonstration.* Si $m, n \in \Sigma$, on écrit $m = a^2+b^2$ et $n = c^2+d^2$ avec $a, b, c, d \in \mathbb{Z}$. Dans $\mathbb{Z}[i]$, on a $m = N(a+ib)$ et $n = N(c+id)$, d'où $mn = N(z)$ avec $z = (a+ib)(c+id)$, ce qui se traduit par $mn \in \Sigma$. ■

On en déduit le corollaire suivant :

**Corollaire 4.** *Soit $n \in \mathbb{N}^*$. On décompose $n$ en produit de facteurs premiers :*

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}, \quad v_p(n) \geq 0$$

*(où on a noté $\mathcal{P}$ l'ensemble des nombres premiers). Alors $n \in \Sigma$ si et seulement si pour tout $p \in \mathcal{P}$ tel que $p \equiv 3 \mod 4$, $v_p(n)$ est pair.*

*Démonstration.* ($\Leftarrow$) Si, pour tout $p \in \mathcal{P}$ tel que $p \equiv 3 \mod 4$, $v_p(n)$ est pair, on écrit

$$n = \left( \prod_{p \in \mathcal{P},\, p \equiv 3(4)} p^{\frac{v_p(n)}{2}} \right)^2 . \left( \prod_{p \in \mathcal{P},\, p \not\equiv 3(4)} p^{v_p(n)} \right).$$

Le membre de gauche est un carré parfait, donc appartient à $\Sigma$ ; le membre de droite appartient à $\Sigma$ en vertu du théorème des deux carrés et du lemme précédent. En conséquence, $n \in \Sigma$.

($\Rightarrow$) Réciproquement, supposons que $n \in \Sigma$. Écrivons $n = a^2 + b^2$ avec $a, b \in \mathbb{Z}$. Soit $d = \text{pgcd}(a, b)$. Alors $d^2 | a^2$, $d^2 | b^2$, et a fortiori $d^2 | n$. On peut ainsi se ramener au cas où $a$ et $b$ sont premiers entre eux, quitte à considérer $\frac{n}{d^2} = \left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2$, sachant que la parité des valuations $p$-adiques de $\frac{n}{d^2}$ sont identiques à celles de $n$, pour tout $p \in \mathcal{P}$.

Dans ce cas, soit $p \in \mathcal{P}$ tel que $p | n$. Alors $n = a^2 + b^2 \equiv 0 \mod p$. $p$ ne divise pas $a$, car sinon $p$ diviserait $b^2 = n - a^2$ donc $p$ diviserait $b$, ce qui est exclu puisqu'on a supposé que $a$ et $b$ sont premiers entre eux. On en déduit que $b^2$ est inversible modulo $p$, puis que $(ab^{-1})^2 \equiv -1 \mod p$, ce qui implique que $-1$ est un carré dans $\mathbb{F}_p$, et par conséquent que $p = 2$ ou $p \equiv 1 \mod 4$. Autrement dit, les valuations $p$-adiques de $n$ sont nulles pour tout nombre premier $p \equiv 3 \mod 4$, ce qui conclut la démonstration. ■

## Références

[Per] Daniel Perrin, *Cours d'algèbre.*