27. Théorème des deux carrés

[Per96, §II.6, p56–58]

ÉNONCÉ

On note $\mathbb{Z}[i] = \{a + ib \,|\, a, b \in \mathbb{Z}\}$ l'ensemble des entiers de Gauss.
On définit $\Sigma = \left\{n \in \mathbb{N} \,|\, \exists a, b \in \mathbb{N} \,|\, n = a^2 + b^2\right\}$.

Lemme. *Σ est stable par produit.*

Lemme. *Si $p \in \mathcal{P}$, alors $p \in \Sigma \iff p \equiv 1, 2 \mod 4$.*

Théorème. [Théorème des deux carrés de Fermat]
$n \in \Sigma$ si et seulement si pour tout $p \in \mathcal{P}$ tel que $p \mid n$ et $p \mid 3 \mod 4$, alors $2 \mid v_p(n)$.

DÉVELOPPEMENT

- Commençons par le premier lemme.
  Remarquons que $n \in \Sigma$ si et seulement s'il existe $z \in \mathbb{Z}[i]$ tel que $n = N(z)$. Soient donc $n, n' \in \Sigma$ et $z = a + ib, z' = c + id \in \mathbb{Z}[i]$ tels que $n = N(z)$ et $n' = N(z')$. Alors $nn' = N(zz') \in \Sigma$.
  Notons par ailleurs qu'alors : $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$.

- Ce premier lemme invite à s'intéresser aux nombres premiers appartenant à Σ.
  C'est l'objet du second. On sait que $2 \in \Sigma$. Supposons donc p premier impair.

  Si $p = a^2 + b^2$, alors a ou b (strictement) est impair, et alors $p \equiv (2k + 1)^2 \equiv 1 \mod 4$.

  Réciproquement, remarquons que $p \in \Sigma$ si et seulement si p est non irréductible dans $\mathbb{Z}[i]$. En effet, si $p = a^2 + b^2 \in \Sigma$, alors $a, b \neq 0$ et $p = (a + ib)(a - ib)$ avec $a \pm ib \notin \mathbb{Z}[i]^\times$.
  Si maintenant $p = zz'$ avec z, z' non inversibles, alors nécessairement $N(z) = N(z') = p$, donc $p \in \Sigma$.
  On veut donc montrer que p est non irréductible dans $\mathbb{Z}[i]$ principal, c'est-à-dire que $(p) = p\mathbb{Z}[i]$ est non premier, ou encore que $\mathbb{Z}[i]/(p)$ est non intègre.

  Or on a que $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2 + 1)$, et alors :

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

  Donc dire que (p) est non premier, c'est dire $X^2 + 1$ n'est pas irréductible sur $\mathbb{F}_p$, donc admet une racine dans $\mathbb{F}_p$, ou encore que $-1 \in (\mathbb{F}_p^*)^2$, ce qui équivaut à $(-1)^{\frac{p-1}{2}} = 1$, et donc à $p \equiv 1 \mod 4$.

- Venons-en alors au théorème.
  Ecrivons $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$. Si $v_p(n)$ est pair pour tout $p \in \mathcal{P}$ tel $p \mid 3 \mod 4$, alors $n \in \Sigma$ en utilisant les deux lemmes et puisque tout carré est dans $\mathcal{P}$.

  Réciproquement, soit $p \equiv 3 \mod 4$. On sait que p est irréductible dans $\mathbb{Z}[i]$, donc si p divise $n = a^2 + b^2 = (a + ib)(a - ib)$, on a que p divise par exemple $a + ib$, ce qui implique que $p \mid a$ et $p \mid b$, ou encore $p^2 \mid n$. On procède de même avec $n' = n/p^2$ tant que $p \mid n'$, et on obtient que $v_p(n)$ est pair.

COMMENTAIRES

On a utilisé le résultat (qu'il peut être intéressant de réécrire en fin de développement s'il reste un peu de place au tableau) :

Proposition. *Soit A un anneau commutatif et I, J des idéaux de A. Alors :*

$$(A/I)/\pi_I(J) \simeq A/(I + J) \simeq (A/J)/\pi_J(I)$$

où π_I et π_J sont les projections de A dans A/I et A/J.

Pour la preuve de ce résultat, on montre facilement que $p \circ \pi_I$ où $p : A/I \longrightarrow (A/I)/\pi_I(J)$ est surjectif de noyau $I + J$. D'où le résultat.