Développement : Théorème des deux carrés

Leçons : 120, 121, 122.

Théorème. *Soit* $\Sigma = \{n \in \mathbb{N}, \exists (a,b) \in \mathbb{N}^2, n = a^2 + b^2\}$. *Soit* $p \geq 3$ *premier. Alors* $p \in \Sigma \Leftrightarrow p \equiv 1 \mod 4$.

Démonstration.
Étape 1 : Inversibles de $\mathbb{Z}[i]$.
Pour tout $z \in \mathbb{Z}[i]$, on définit $N(z) = |z|^2 \in \mathbb{N}$. Soit $z \in \mathbb{Z}[i]^\times$.
Alors $1 = N(1) = N(zz^{-1}) = N(z)N(z^{-1})$, donc $N(z) = N(z^{-1}) = 1$. Comme $N(a+ib) = a^2 + b^2$, on a donc $a = \pm 1$ et $b = 0$ ou $a = 0$ et $b = \pm 1$. Donc $z \in \{\pm 1, \pm i\}$. Réciproquement, ces éléments sont inversibles. Donc $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Étape 2 : $p \in \Sigma \Leftrightarrow p$ est réductible dans $\mathbb{Z}[i]$.
$\boxed{\Rightarrow}$: Si $p \in \Sigma$, p peut s'écrire $p = a^2 + b^2 = (a+ib)(a-ib)$, et $N(a+ib) = N(a-ib) = p > 1$ donc $a+ib, a-ib$ non inversibles. Ainsi p est réductible.
$\boxed{\Leftarrow}$: Si p est réductible, $p = zz'$ avec z, z' non inversibles. On a $p^2 = N(p) = N(z)N(z')$ avec $N(z), N(z') > 1$, ainsi comme p premier, $p = N(z) = N(z') = a^2 + b^2$ si $z = a + ib$.

Étape 3 : Preuve du théorème.
$\mathbb{Z}[i]$ est euclidien, donc factoriel. Ainsi, p réductible équivaut à p non premier, ou encore $\mathbb{Z}[i]/(p)$ non intègre. On a de plus $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$. On note $\pi_{X^2+1} : \mathbb{Z}[X] \to \mathbb{Z}[X]/(X^2+1)$ et $\pi_{\overline{p}} = \Big(\mathbb{Z}[X]/(X^2+1)\Big)/(\overline{p})$ les projections canoniques (où $\overline{\cdot}$ désigne la classe modulo X^2+1). Alors $\ker(\pi_{\overline{p}} \circ \pi_{X^2+1}) = \{Q \in \mathbb{Z}[X], \exists U \in \mathbb{Z}[X], \overline{Q} = \overline{pU}\} = \{Q \in \mathbb{Z}[X], \exists U, V \in \mathbb{Z}[X], Q = pU + V(X^2+1)\} = (p, X^2+1)\mathbb{Z}[X]$. Ainsi $\pi_{\overline{p}} \circ \pi_{X^2+1}$ se factorise en un isomorphisme $\mathbb{Z}[X]/(p, X^2+1) \to \Big(\mathbb{Z}[X]/(X^2+1)\Big)/(\overline{p})$. On montre de même qu'on a les isomorphismes : $\mathbb{Z}[i]/(p) \simeq \Big(\mathbb{Z}[X]/(X^2+1)\Big)/(\overline{p}) \simeq \mathbb{Z}[X]/(p, X^2+1) \simeq (\mathbb{Z}[X]/(p))/(X^2+1) \simeq (\mathbb{Z}/p\mathbb{Z}[X])/(X^2+1)$.
Ainsi, p réductible ssi $\mathbb{F}_p[X]/(X^2+1)$ non intègre, ssi X^2+1 est réductible (et donc a une racine) dans $\mathbb{F}_p[X]$, ssi -1 est un carré dans $\mathbb{F}_p$, ssi $p \equiv 1 \mod 4$. □

Corollaire. *Soit* $n \geq 2$, *de décomposition en facteurs premiers* $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$. *Alors* $n \in \Sigma \Leftrightarrow v_p(n)$ *pair pour tout* $p \equiv 3 \mod 4$.

Démonstration.
Étape 1 : Σ est stable par multiplication.
Soient $a^2+b^2, c^2+d^2 \in \Sigma$. Alors $(a^2+b^2)(c^2+d^2) = (a+ib)(a-ib)(c+id)(c-id)$
$= (ac - bd + i(bc+ad))(ac - bd - i(bc+ad)) = (ac-bd)^2 + (bc+ad)^2 \in \Sigma$.

Étape 2 : Preuve du corollaire.
$\boxed{\Rightarrow}$: comme un carré est toujours dans Σ, c'est vrai d'après ce qui précède.
$\boxed{\Leftarrow}$: Soit $n = a^2 + b^2 \in \Sigma$, soient $d = a \wedge b, a' = \frac{a}{d}, b' = \frac{b}{d}$: ainsi $a' \wedge b' = 1$ et $n = d^2(a'^2 + b'^2)$.
Soit p diviseur premier impair de $a'^2 + b'^2 = (a' + ib')(a' - ib')$. Par l'absurde, si p irréductible dans $\mathbb{Z}[i]$, on a par Euclide $p|(a'+ib')$ ou $p|(a'-ib')$. Mais par passage au conjugué, si p divise l'un, il divise l'autre, il divise donc les deux. Ainsi par somme et différence, $p|2a'$ et $p|2ib'$ dans $\mathbb{Z}[i]$. En prenant la norme, il vient $p^2|4a'^2, p^2|4b'^2$ et p impair donc par Gauss, $p|a', p|b'$, contradiction. Donc p est réductible, $p = xy$ avec $x, y \in \mathbb{Z}[i]$ non inversibles. Il vient $p^2 = N(x)N(y)$ avec $N(x), N(y) \neq 1$ donc $N(x) = N(y) = p$ car p premier. Ainsi $p \in \Sigma$ et $p \equiv 1 \mod 4$. Les facteurs premiers congrus à 3 modulo 4 sont donc "dans le d^2", donc d'exposant pair. □

Références

D. Perrin, Cours d'algèbre, Ellipses, p. 57.

Notes personnelles

Version de Florian Lemonnier. Attention, la justification de l'échange des passages au quotient est à faire parfaitement, bien qu'elle soit admise dans Perrin.