Le théorème des deux carrés.

Rémi Lajugie

Définition 1 *On appelle anneau des entiers de Gauss, l'anneau* $\mathbb{Z}[i]$.

Définition 2 *On note* Σ *l'ensemble des nombres somme de deux carrés.*

Proposition 1 *Les inversibles de l'anneau* $\mathbb{Z}[i]$ *sont* $1, -1, i, -i$.

Proposition 2 *Muni du stathme* $N(z\overline{z})$, $\mathbb{Z}[i]$ *est un anneau euclidien.*

Preuve :

Soit z, t On écrit $\frac{z}{t} = x + iy$. On définit a et b les entiers les plus proches respectivement de x et de y. On a de manière évidente (comprendre ça se lit sur un dessin et on n'a pas envie de le prouver) que $|z/t - a - ib| \leq \frac{\sqrt{2}}{2} < 1$. Ainsi, on a $z = t(a + ib) + tr$ avec $N(r) < N(t)$ par multiplicativité du stathme N.

Proposition 3 *Un nombre premier est irréductible dans l'ensemble des entiers de Gauss si, et seulement si,* $p \notin \Sigma$.

Preuve :

Si p est dans Σ, $p = a^2 + b^2$ donc $p = (a + ib)(a - ib)$. Si p est irréductible dans $\mathbb{Z}[i]$ alors on écrit le diagramme suivant

$$\begin{array}{ccccc} \mathbb{Z}[i] & \xleftarrow{X^2+1} & \mathbb{Z}[X] & \xrightarrow{p\mathbb{Z}} & \mathbb{Z}/p\mathbb{Z} \\ {\scriptstyle p\mathbb{Z}[i]}\downarrow & & & & \downarrow{\scriptstyle (X^2+1)} \\ \mathbb{Z}[i]/p\mathbb{Z} & & & & \mathbb{Z}/p\mathbb{Z}[i] \end{array}$$

En écrivant les noyaux, il vient par théorème d'isomorphisme que $\mathbb{Z}/p\mathbb{Z}[i]$ est isomorphe à $\mathbb{Z}[i]/p\mathbb{Z}$.

Théorème 1 *Soit* p *un nombre premier, alors* $p \in \Sigma$ *si et seulement si* $p = 2$ *ou* $p \equiv 1[4]$.

Proposition 4 *L'ensemble des nombres sommes de deux carrés est stable par multiplication.*

Preuve : Ecrire une factorisation de deux éventuels nombres dans $\mathbb{Z}[i]$, les multiplier et obtenir la fameuse identité de Lagrange.

Théorème 2 Σ *est l'ensemble des nombres* N *tels que la valuation p-adique* $\nu_p(N) = 0[2]$ *pour* $p \equiv 3[4]$.

Preuve :

On décompose $N = \Pi_{p \in \mathcal{P}} p^{\nu_p(N)}$.

Remarquons alors que si la valuation $p - adique$ d'un nombre premier est paire, on a $p^{\nu_p(N)} = (p^{\nu_p(N)/2})^2 + 0^2$. Il vient alors par le théorème précédent et la proposition plus haut que les nombres N tels que la valuation p-adique $\nu_p(N) = 0[2]$ pour $p \equiv 3[4]$ sont dans Σ.

Réciproquement, supposons que l'une des valuations p-adiques d'un nombre premier congru à 3 modulo 4 ne soit pas paire. Quitte à mettre le plus grand nombre pair en facteur, on peut supposer $\nu_N(p) = 1$. Alors $p|N = a^2 + b^2 = (a - ib)(a + ib)$. Or p est irréductible dans l'anneau des entiers de Gauss donc $p|(a - ib)$ ou $p|(a + ib)$. Par exemple, si $p|a + ib$, on déduit que, comme p est entier, $p|a$ et $p|b$ (identifier les parties réelles et imaginaires pour s'en convaincre). Donc $p|a - ib$ donc $p^2|a^2 + b^2$, ce qui est contradictoire avec ce que nous avions supposé.

Références

— Perrin.
— Artin.