12 Entiers de Gauss et théorème des deux carrés

On note $\mathbb{Z}[i]$ l'image de l'unique morphisme d'anneaux $\mathbb{Z}[X] \to \mathbb{C}$ qui envoie X sur i. On a immédiatement $\mathbb{Z}[i] \approx \mathbb{Z}[X]/(X^2+1)$ et $\mathbb{Z}[i] = \{a+ib, a, b \in \mathbb{Z}\}$. On l'appelle anneau des entiers de Gauss. Pour l'instant il s'agit au moins d'un anneau intègre.

Soit $N : \mathbb{Z}[i] \to \mathbb{N}$, $a+ib \mapsto a^2+b^2$.

Proposition.
– *N est multiplicative sur $\mathbb{Z}[i]$.*
– *Les inversibles de $\mathbb{Z}[i]$ sont $\{1, i, -1, -i\}$.*
– *$\mathbb{Z}[i]$ est euclidien pour le stathme N.*

Preuve.
Pour le premier point, il suffit d'écrire que $N(a+ib) = z\bar{z} = |z|^2$ où $z = a+ib$, il s'ensuit que $N(zz') = N(z)N(z')$.

Par conséquent, si z, $z' \in \mathbb{Z}[i]$ vérifient $zz' = 1$, on doit avoir $N(z)N(z') = 1$ donc $N(z) = N(z') = 1$. En écrivant $z = a+ib$, on a nécessairement $a = \pm 1$ et $b = 0$ ou l'inverse. Réciproquement, on vérifie immédiatement que ces nombres conviennent, finalement $\mathbb{Z}[i]^\times = \{1, i, -1, -i\}$.

Montrons maintenant le troisième point. Soient $z, z' \in \mathbb{Z}[i]$ avec $z' \neq 0$. Soit q un point de $\mathbb{Z}[i]$ le plus proche de $\frac{z}{z'}$ (au sens de la distance usuelle dans $\mathbb{C}$). Il est clair que q existe et $\left|\frac{z}{z'} - q\right| \leqslant \frac{\sqrt{2}}{2} < 1$ ($\frac{\sqrt{2}}{2}$ est le diamètre du domaine fondamental du réseau $\mathbb{Z}[i]$). Si on pose $r = z - z'q \in \mathbb{Z}[i]$, on a alors $z = z'q + r$ et $N(r) = |z - z'q|^2 = |z'|^2 \left|\frac{z}{z'} - q\right|^2$ d'où $N(r) < N(z')$ (y compris dans le cas où $r = 0$, mais peu importe).

□

Théorème. *Soit $p \in \mathbb{N}^*$ un nombre premier. Alors p est somme de deux carrés si et seulement si $p = 2$ ou $p = 1$ [4].*

Preuve.
Notons $\Sigma = \{a^2+b^2,\ a, b \in \mathbb{N}\}$. Il est facile de voir que les nombres de Σ sont égaux à 0, 1 ou 2 modulo 4. En particulier, la condition ci-dessus est nécessaire. Montrons maintenant qu'elle est suffisante.

Premièrement, on remarque qu'un nombre premier p est dans Σ si et seulement si p est réductible dans $\mathbb{Z}[i]$. En effet, si $p = a^2+b^2$, alors $p = (a+ib)(a-ib)$ et a et b sont non nuls donc $a+ib$ et $a-ib$ sont non inversibles, p est donc réductible dans $\mathbb{Z}[i]$. Réciproquement,

si $p = zz'$ avec $z,\ z' \in \mathbb{Z}[i]^\times$, alors $p^2 = N(z)N(z')$ avec $N(z),\ N(z') \neq 1$, si bien que $N(z) = N(z') = p$. p est donc somme de deux carrés.

$Z[i]$ est un anneau euclidien et en particulier factoriel, les irréductibles de $\mathbb{Z}[i]$ sont donc ses éléments premiers. Dire que p est un élément premier de $\mathbb{Z}[i]$ revient à dire (par définition) que l'anneau $\mathbb{Z}[i]/(p)$ est intègre. On a par des identifications classiques $\mathbb{Z}[i]/(p) \approx \mathbb{F}_p[X]/(X^2+1)$. Il s'ensuit que p n'est pas premier dans $\mathbb{Z}[i]$ si et seulement si -1 est un carré dans $\mathbb{F}_p$. On sait que cela équivaut à $p = 2$ ou $p = 3$ [4].

□

THÉORÈME. *Soit $n \in \mathbb{N}^*$, alors n est somme de deux carrés si et seulement si pour tout entier p premier (de $\mathbb{Z}$) tel que $p = 3$ [4], $\nu_p(n)$ est pair.*

Preuve.
Il est clair que la condition est suffisante car Σ est stable par multiplication. En effet, si $m = N(z)$ et $m' = N(z')$ alors $mm' = N(zz')$ est somme de deux carrés.

Réciproquement, supposons que $n \in \Sigma$ et soit p un entier premier égal à 3 modulo 4. D'après ce qu'on a vu dans la démonstration précédente, p est un élément premier de $\mathbb{Z}[i]$. Comme $n = a^2 + b^2$, on peut écrire $n = z\bar{z}$, avec $z = a + ib$. L'idéal engendré par p dans $\mathbb{Z}[i]$ étant stable par conjugaison, p divise z « autant de fois » que $\bar{z}$. Il s'ensuit que $\nu_p(n)$ est pair.

□

Leçons possibles
(**102** Sous-groupes discrets de R^n. Réseaux. Exemples.)
110 Nombres premiers. Applications.
111 Exemples d'applications des idéaux d'un anneau commutatif unitaire.
(**146** Anneaux principaux.)
114 Équations diophantiennes du premier degré $ax + by = c$. Autres exemples d'équations diophantiennes.

Références
[Sam03]