DÉVELOPPEMENT 8

ENTIERS DE GAUSS ET THÉORÈME DES DEUX CARRÉS

On considère l'anneau des entiers de Gauss $\mathbb{Z}[i]$ des nombres complexes de la forme $u+iv$ avec $(u,v) \in \mathbb{Z}^2$ et on pose

$$\varphi : \mathbb{Z}[i] \to \mathbb{N}, a \mapsto a\overline{a}.$$

Lemme. — $\mathcal{U}(\mathbb{Z}[i]) = \{-1, 1, -i, i\}$

Démonstration. — Si $a \in \mathbb{Z}[i]$ est inversible alors $ab = 1$ avec $b \in \mathbb{Z}[i]$ et la multiplicativité de φ donne $\varphi(a)\varphi(b) = 1$. Ainsi, l'entier $\varphi(a)$ est positif et inversible dans $\mathbb{Z}$ donc $\varphi(a) = 1$. Réciproquement, si $\varphi(a) = 1$ alors $a\overline{a} = 1$ et $\overline{a} \in \mathbb{Z}[i]$ est l'inverse de a. Les éléments inversibles de $\mathbb{Z}[i]$ sont donc les $a \in \mathbb{Z}[i]$ vérifiant $\varphi(a) = 1$. Si on écrit $a = u + iv$ avec $(u,v) \in \mathbb{Z}^2$, on obtient $u^2 + v^2 = 1$. Il s'ensuit que les éléments inversibles de $\mathbb{Z}[i]$ sont ± 1 et $\pm i$. □

Proposition. — *$\mathbb{Z}[i]$ est un anneau euclidien.*

Démonstration. — Soit $(a,b) \in \mathbb{Z}[i] \times \mathbb{Z}[i]^*$ et considérons le nombre complexe $\frac{a}{b} = x + iy$ avec $(x,y) \in \mathbb{R}^2$; on note u l'entier le plus proche de x, v l'entier le plus proche de y et $q = u + iv$, alors

$$\left|\frac{a}{b} - q\right|^2 = (u-x)^2 + (v-y)^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 < 1.$$

Il s'ensuit que $|a - bq|^2 < |q|^2$. Posons $r = a - bq$ alors $r \in \mathbb{Z}[i]$ puisque $a, b, q \in \mathbb{Z}[i]$ et on a $|r|^2 < |q|^2$ *i.e.* $\varphi(r) < \varphi(q)$. On a donc déterminé $(q,r) \in \mathbb{Z}[i]^2$ tels que $a = bq + r$ et $\varphi(r) < \varphi(q)$. □

Lemme. — *Si $\varphi(a)$ est un nombre premier alors a est irréductible dans $\mathbb{Z}[i]$.*

Démonstration. — Soit $a \in \mathbb{Z}[i]$ tel que $\varphi(a)$ soit premier et supposons que l'on puisse écrire $a = bc$ avec $b, c \in \mathbb{Z}[i]$. Alors $\varphi(a) = \varphi(b)\varphi(c)$ d'où $\varphi(b) = 1$ ou $\varphi(c) = 1$ *i.e.* b et c est inversible. □

Lemme. — *-1 est un carré modulo p si et seulement si $p \equiv 1 \pmod 4$.*

Démonstration. — Si $-1 = x^2$ dans $\mathbb{Z}/p\mathbb{Z}$ alors, puisque le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est d'ordre $p-1$, on a $x^{p-1} = 1$ *i.e.* $(-1)^{\frac{p-1}{2}} = 1$ donc $\frac{p-1}{2}$ est pair ce qui signifie $p \equiv 1 \pmod 4$. Réciproquement, sur le corps $\mathbb{Z}/p\mathbb{Z}$, l'équation $x^{\frac{p-1}{2}} = 1$ a au plus $\frac{p-1}{2}$ solutions or $(\mathbb{Z}/p\mathbb{Z})^*$ contient $p - 1 > \frac{p-1}{2}$ éléments donc il existe $x \neq 0$ tel que $y = x^{\frac{p-1}{2}} \neq 1$. Alors $y^2 = x^{p-1} = 1$ donc $(y+1)(y-1) = 0$ or $y \neq 1$ *i.e.* $y = -1$. Puisque $p \equiv 1 \pmod 4$, on peut écrire $\frac{p-1}{2} = 2k$ de sorte que

$$(x^k)^2 = x^{2k} = x^{\frac{p-1}{2}} = y = -1$$

i.e. -1 est un carré modulo p. □

Proposition. — *Soit p un nombre premier, on a équivalence entre*

(i) *p est irréductible dans $\mathbb{Z}[i]$,*

(ii) $p \equiv 3 \pmod 4$,

(iii) *p n'est pas somme de deux carrés.*

Démonstration. — Supposons p irréductible dans $\mathbb{Z}[i]$ et $p \not\equiv 3 \pmod 4$ alors -1 est un carré modulo p *i.e.* il existe $x \in \mathbb{Z}$ tel que $x^2 \equiv -1 \pmod p$. Il s'ensuit que p divise $x^2 + 1 = (x + i)(x - i)$ dans $\mathbb{Z}$ donc dans $\mathbb{Z}[i]$ et l'hypothèse sur p montre que p divise $x + i$ ou $x - i$, ce qui est absurde puisque $\frac{x+i}{p}$ et $\frac{x-i}{p}$ ne sont pas dans $\mathbb{Z}[i]$.

Supposons que l'on puisse écrire $p = u^2 + v^2$ avec $(u, v) \in \mathbb{Z}^2$. Un carré est congru à 0 ou 1 modulo 4 donc une somme de deux carrés est congrue à 0, 1 ou 2 et il est donc impossible que $p \equiv 3 \pmod 4$.

Écrivons $p = ab$ avec $a, b \in \mathbb{Z}[i]$ alors $p^2 = \varphi(p) = \varphi(a)\varphi(b)$. Puisque p n'est pas somme de deux carrés, il n'existe pas d'élément $c = \alpha + i\beta \in \mathbb{Z}[i]$ tel que $p = \varphi(c) = \alpha^2 + \beta^2$ et *a fortiori* on a $\varphi(a) \neq 0$ et $\varphi(b) \neq 0$. Comme p est premier, il s'ensuit que $\varphi(a) = 1$ ou $\varphi(b) = 1$ *i.e.* a ou b est inversible dans $\mathbb{Z}[i]$ et p est irréductible dans $\mathbb{Z}[i]$. □

Leçons concernées

03 Sous-groupes discrets de $\mathbb{R}^n$. Réseaux

09 Congruences dans $\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$. Applications

Références

S. Francinou, H. Gianella et S. Nicolas, *Oraux X-ENS, algèbre 1*, Cassini, 2001.

X. Gourdon, *Algèbre*, Ellipses, 1994.

Sébastien Pellerin