

Références :

Cours d'algèbre, Daniel Perrin

Déf. On définit l'ensemble des **entiers de Gauss** comme

$$\mathbb{Z}[i] = \{a + ib \in \mathbb{C} : a, b \in \mathbb{Z}\}.$$

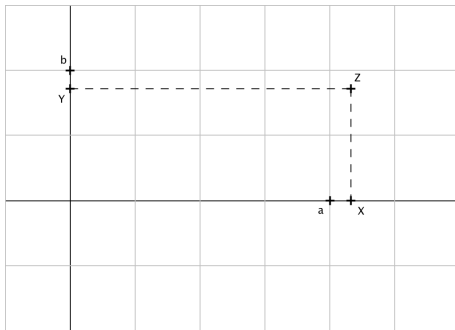
Lemme. $\mathbb{Z}[i]$ est un anneau euclidien et $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

Démonstration.

- Posons

$$\begin{aligned} N : \mathbb{Z}[i] &\longrightarrow \mathbb{N} \\ z = a + ib &\longmapsto a^2 + b^2 \end{aligned}$$

Soit $z, t \in \mathbb{Z}[i]$, on a $\frac{z}{t} = x + iy \in \mathbb{C}$.



Il existe $a, b \in \mathbb{Z}$ tels que $|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$.

Posons $q = a + ib \in \mathbb{Z}[i]$ et $r = z - qt$. On veut $N(r) < N(t)$. On a

donc

$$\begin{aligned} |r| &= |z - qt| \\ &= \left| t \left(\frac{z}{t} - q \right) \right| \\ &= |t| |x + iy - (a + ib)| \\ &= |t| ((x - a)^2 + (y - b)^2) \\ &\leq \frac{|t|}{2} \\ &< |t| \end{aligned}$$

On obtient donc bien, en passant au carré, $N(r) = |r|^2 < |t|^2 = N(t)$. Ainsi, N est un stathme. On a donc bien montré que $\mathbb{Z}[i]$ est un anneau euclidien.

- Soit $z = a + ib \in \mathbb{Z}[i]^*$. Il existe donc $z' \in \mathbb{Z}[i]^*$ tel que $zz' = 1$. On a donc $N(z)N(z') = 1$. Or $N(z)$ et $N(z')$ sont des éléments de $\mathbb{N}$. On obtient $N(z) = N(z') = 1$. Ainsi, il est nécessaire d'avoir $a^2 + b^2 = 1$. Les seules solutions entières de cette équation sont $a = \pm 1$ et $b = 0$ ou $a = 0$ et $b = \pm 1$, d'où le résultat. □

Lemme. Soit p un nombre premier. p est somme de deux carrés si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.

Démonstration. • Supposons que $p = a^2 + b^2$, on a alors $p = (a + ib)(a - ib)$ avec a et b non nuls. Ainsi, $a + ib$ et $a - ib$ ne sont pas des éléments inversibles. Ainsi, p n'est pas irréductible.

- Supposons que $p = zz'$ avec $z, z' \notin \mathbb{Z}[i]^*$ ($z = a + ib$). On a $N(p) = N(z)N(z') = p^2$ et comme $N(z)$ et $N(z')$ sont différents de 1, on a nécessairement $p = N(z)$ et donc $p = a^2 + b^2$. □

Théo. Soit p premier. p est somme de deux carrés si et seulement si $p \equiv 1 \pmod{4}$.

Démonstration.

- Montrons que p est somme de deux carrés si et seulement si -1 est un carré dans $\mathbb{F}_p^*$.

On sait que $\mathbb{Z}[i]$ est factoriel donc

$$p \text{ irréductible dans } \mathbb{Z}[i] \Leftrightarrow (p) \text{ est premier} \Leftrightarrow \mathbb{Z}[i]/(p) \text{ est intègre.}$$

On a aussi la série d'isomorphismes suivant :

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

(pour ce qui est des morphismes, pour montrer $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[X]/(X^2 + 1, p)$ on pose

$$\begin{aligned} \psi : \mathbb{Z}[X] &\longrightarrow \mathbb{Z}[i]/(p) \\ Q &\longmapsto \overline{Q(i)} \end{aligned}$$

et on obtient le résultat par théorème de factorisation)

On a donc

$$\begin{aligned} p \text{ somme de deux carrés} &\Leftrightarrow p \text{ non irréductible dans } \mathbb{Z}[i]. \\ &\Leftrightarrow \mathbb{F}_p[X]/(X^2 + 1) \text{ non intègre} \\ &\Leftrightarrow X^2 + 1 \text{ non irréductible dans } \mathbb{F}_p[X] \\ &\Leftrightarrow -1 \text{ est un carré dans } \mathbb{F}_p^* \end{aligned}$$

- Montrons maintenant le théorème.

- Si $p = 2$ alors $-1 = 1 = 1^2$. Ainsi -1 est un carré dans $\mathbb{F}_2^*$ et on a le résultat.
- Si $p > 2$, montrons que -1 est un carré dans $\mathbb{F}_p^*$ si et seulement si $x^{\frac{p-1}{2}} = 1$.

Montrons donc

$$\{x \in \mathbb{F}_p^* : x \text{ est un carré de } \mathbb{F}_p^*\} = \{x \in \mathbb{F}_p^* : x^{\frac{p-1}{2}} = 1\}.$$

Soit $x = y^2$ avec $y \in \mathbb{F}_p^*$. On a alors

$$x^{\frac{p-1}{2}} = y^{p-1} = 1.$$

Ainsi, on a

$$\{x \in \mathbb{F}_p^* : x \text{ est un carré de } \mathbb{F}_p^*\} \subset \{x \in \mathbb{F}_p^* : x^{\frac{p-1}{2}} = 1\}.$$

On sait aussi que

$$|\{x \in \mathbb{F}_p^* : x^{\frac{p-1}{2}} = 1\}| \leq \frac{p-1}{2}.$$

Montrons maintenant que

$$|\{x \in \mathbb{F}_p^* : x \text{ est un carré de } \mathbb{F}_p^*\}| = \frac{p-1}{2}.$$

On définit l'application

$$\begin{aligned} \phi : \mathbb{F}_p^* &\longrightarrow \mathbb{F}_p^* \\ x &\longmapsto x^2 \end{aligned}$$

On a donc que $Im(\phi) = \{x \in \mathbb{F}_p^* : x \text{ est un carré de } \mathbb{F}_p^*\}$ et $Ker(\phi) = \{\pm 1\}$. On obtient donc $|Im(\phi)| = \frac{|\mathbb{F}_p^*|}{|Ker(\phi)|} = \frac{p-1}{2}$. Ainsi, les deux ensembles étudiés sont de même cardinal et sont donc égaux.

On a donc

$$\begin{aligned} -1 \text{ est un carré dans } \mathbb{F}_p^* &\Leftrightarrow (-1)^{\frac{p-1}{2}} = 1. \\ &\Leftrightarrow \exists k \in \mathbb{Z}, \frac{p-1}{2} = 2k \\ &\Leftrightarrow \exists k \in \mathbb{Z}, p = 4k + 1 \\ &\Leftrightarrow p \equiv 1[4] \end{aligned}$$

□

Leçons possibles : 121 - 122 - 126