VM
26/04/15
1

121, 122, 126

Théorème des deux carrés

Réf : Perrin

Théorème : i) $\mathbb{Z}[i]$ est euclidien pour le stathme $N(a+ib) = a^2+b^2$.

ii) $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

iii) p nombre premier

p est la somme de deux carrés ssi $p = 2$ ou $p \equiv 1 \pmod 4$.

dém : i) Soit $z \in \mathbb{Z}[i]$. Soit $t \in \mathbb{Z}[i] \setminus \{0\}$.

$\frac{z}{t} \in \mathbb{C}$ donc $\exists x, y \in \mathbb{R}$ tq $\frac{z}{t} = x+iy$.

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

Soit $r = z - t(a+ib)$.

Alors $r \in \mathbb{Z}[i]$ et

$$N(r) = |r|^2 = |z - t(a+ib)|^2 = |t|^2 \left|\frac{z}{t} - (a+ib)\right|^2$$

$$= |t|^2 \left[(x-a)^2 + (y-b)^2\right] \leq \frac{|t|^2}{2} = \frac{N(t)}{2} < N(t).$$

Donc N est un stathme et $\mathbb{Z}[i]$ est euclidien.

ii) Montrons tout d'abord que $z \in \mathbb{Z}[i]^\times$ ssi $N(z) = 1$.

Si $z \in \mathbb{Z}[i]^\times$, alors $\exists z'$ tel que $zz' = 1$.

On $N(zz') = |zz'|^2 = |z|^2 |z'|^2 = N(z) N(z')$

$N(z) \in \mathbb{N}$ et divise 1, donc $N(z) = 1$.

Si $N(z) = 1$, alors $|z|^2 = z\bar{z} = N(z) = 1$ donc $z \in \mathbb{Z}[i]^\times$

(car si $z \in \mathbb{Z}[i]$, $\bar{z} \in \mathbb{Z}[i]$).

Soit $z = a+ib \in \mathbb{Z}[i]$ tel que $N(z) = 1$. $N(z) = a^2+b^2$ donc

$a^2+b^2 = 1 \Rightarrow$ $a = \pm 1$ et $b = 0$ (ou) $a = 0$ et $b = \pm 1$ $\Rightarrow z \in \{\pm 1, \pm i\}$.

Donc $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

iii) On note $\mathcal{C} = \{ p \text{ premier somme de deux carrés} \}$.

Soit p premier.

Lemme 1 : $p \in \mathcal{C}$ ssi p n'est pas irréductible dans $\mathbb{Z}[i]$.

Dém : Si $p \in \mathcal{C}$, il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2 = (a-ib)(a+ib)$.

Soit $z = a+ib$. $N(z) = z\bar{z} = p$, donc $z \notin \mathbb{Z}[i]^\times$

et $\bar{z} \notin \mathbb{Z}[i]^\times$: p est réductible dans $\mathbb{Z}[i]$.

Soit p premier tel qu'il existe $z, z' \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^\times$ tels que

$p = zz'$. On a $p^2 = N(p) = N(z)\,N(z')$.

On $N(z) > 1$ et $N(z') > 1$, et $N(z)$ divise p^2.

Donc $N(z) = a^2+b^2 = p$.

□

Soit p premier.

Ainsi, $p \in \mathcal{C}$ ssi p n'est pas irréductible dans $\mathbb{Z}[i]$

ssi $p\mathbb{Z}[i]$ n'est pas premier

ssi $\mathbb{Z}[i]/(p)$ n'est pas intègre.

Etudions $\mathbb{Z}[i]/(p)$. $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$.

Lemme 2 : A anneau commutatif. I, J idéaux de A.

$\pi_I : A \to A/I$

$\pi_J : A \to A/J$.

Alors $\dfrac{(A/I)}{\pi_I(J)} \simeq \dfrac{A}{(I+J)} \simeq \dfrac{(A/J)}{\pi_J(I)}$.

D'après le Lemme 2,

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

Donc $p \in \mathcal{C}$ ssi $\mathbb{F}_p[X]/(X^2+1)$ n'est pas intègre.

ssi X^2+1 n'est pas irréductible sur $\mathbb{F}_p$

ssi X^2+1 a une racine dans $\mathbb{F}_p$

ssi -1 est un carré dans $\mathbb{F}_p$

ssi $p=2$ ou $p \equiv 1 \pmod 4$.

---

dém (lemme 2) :

$$A \xrightarrow{\pi_I} A/I \xrightarrow{\pi} A/I/\pi_I(J)$$

$\pi \circ \pi_I$ est surjectif.

Montrons que $\ker(\pi \circ \pi_I) = I+J$.

$\supset$: $x \in I+J$: $x = \underbrace{y}_{\in I} + \underbrace{z}_{\in J}$: $\pi_I(x) = 0 + \underbrace{\pi_I(z)}_{\in \pi_I(J)}$

$\pi \circ \pi_I(x) = 0$.

$\subset$: Si $x \in \ker(\pi \circ \pi_I)$: $\pi \circ \pi_I(x) = 0$

donc $\pi_I(x) \in \pi_I(J)$: $\exists j \in J$ tel que

$\pi_I(x-j) = 0 \Rightarrow x-j \in I$

$\exists i \in I$ tel que $x = i+j$.

Donc $A/(I+J) \simeq (A/I)/\pi_I(J)$.

$q = p^n$, p premier impair.

Rappel : L'ensemble des carrés de $(\mathbb{F}_q)^\times$ est de cardinal $\frac{q-1}{2}$.

↳ noté $\mathbb{F}_q^{\times 2}$

$$x \in \mathbb{F}_q^{\times 2} \Leftrightarrow x^{\frac{q-1}{2}} = 1.$$

En effet, si x est un carré, $\exists y$ tq $x = y^2$ donc

$x^{\frac{q-1}{2}} = (y^2)^{\frac{q-1}{2}} = y^{q-1} = 1$. Comme $X^{\frac{q-1}{2}} - 1$ a

au plus $\frac{q-1}{2}$ racines dans $\mathbb{F}_q$, on les a toutes.

-1 est un carré dans $\mathbb{F}_q$ ssi $(-1)^{\frac{q-1}{2}} = 1$

ssi 4 divise $q-1$.