$\mathbb{Z}[i]$ et le théorème des deux carrés de Fermat

Références : Perrin p. 57 mais ce n'est pas de la tarte

Leçons :

Prérequis On note $\Sigma = \{ n \in \mathbb{N},\ \exists a,b \in \mathbb{N},\ a^2+b^2 = n \}$. On note aussi

$N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$ "norme" multiplicative (donc Σ stable par $\times$) qui

$z = a+ib \longmapsto z\bar{z} = a^2+b^2$

fait de $\mathbb{Z}[i]$ un anneau euclidien, dont les inversibles sont $\{\pm 1, \pm i\}$.

Théorème :

1) Soit $p \in \mathbb{N}$ premier. On a :

$p \in \Sigma \iff p$ n'est pas irréductible dans $\mathbb{Z}[i] \iff p = 2$ ou $p \equiv 1\ [4]$

2) Soit $n \in \mathbb{N}^*$, $n \neq 1$. On écrit $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$.

$n \in \Sigma \iff \forall p \equiv 3\ [4],\ v_p(n)$ est pair.

Démonstration :

1) $p \notin \Sigma \iff p$ non irréd dans $\mathbb{Z}[i]$:

$\boxed{\Rightarrow}$ $p = a^2+b^2 = (a-ib)(a+ib)$ avec $a,b \neq 0$ et $a+ib,\ a-ib \notin \mathbb{Z}[i]^*$

$\boxed{\Leftarrow}$ $p = zz'$ avec $z, z' \notin \{\pm 1, \pm i\}$. Alors $p^2 = N(p) = \underbrace{N(z)}_{\neq 1}\underbrace{N(z')}_{\neq 1}$ donc $p = N(z)$, donc $p \in \Sigma$.

$p \in \Sigma \iff p = 2$ ou $p \equiv 1\ [4]$:

$\boxed{\Rightarrow}$ $a^2+b^2 \equiv 0, 1$ ou $2\ [4]$ donc $p \in \Sigma \Rightarrow p = 2$ ou $p \equiv 1\ [4]$

$\boxed{\Leftarrow}$ $p = 2 = 1^2+1^2 \in \Sigma$. ~~Supposons $p > 2$ et~~ p

Observons que :

p n'est pas irréductible dans $\mathbb{Z}[i] \iff \mathbb{Z}[i]/(p)$ est non intègre

Or, $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$: $\mathrm{ev}_i : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[i]$, $\ker \mathrm{ev}_i = (X^2+1)$

$P \longmapsto P(i)$

On voudrait montrer que :

$$\mathbb{Z}[i]/(p) \overset{①}{\simeq} \mathbb{Z}[X]/(X^2+1,p) \overset{②}{\simeq} \left(\mathbb{Z}[X]/(p)\right)/(X^2+1) \overset{③}{\simeq} \mathbb{F}_p[X]/(X^2+1)$$

③ : $\mathbb{Z}[X]/(p) = \mathbb{F}_p[X]$ car c'est la réduction des coeff modulo p.

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

$$\begin{array}{ccc} \mathbb{Z}[X] & \xrightarrow{\pi_1} & \mathbb{Z}[X]/(X^2+1,p) \\ \pi_2 \downarrow & \overset{\varphi}{\nearrow} & \uparrow \psi \\ \mathbb{Z}[X]/(X^2+1) & \xrightarrow{\pi_3} & \left(\mathbb{Z}[X]/(X^2+1)\right)/(p) \\ (\mathbb{Z}[i]) & & \left(\mathbb{Z}[i]/(p)\right) \end{array}$$

π_i surjectifs

- Or $(X^2+1) \subset \ker \pi_1 = (X^2+1,p)$ donc par la propriété universelle du groupe quotient, $\exists \varphi$ tq $\pi_1 = \varphi \circ \pi_2$
- $\ker \varphi = \pi_2(\ker \pi_1) = (p) \supset (p)$ donc $\exists \psi$ injectif tq $\psi = \pi_3 \circ \varphi \circ \pi_3^{-1}$.
  puis π_i surjectif $\Rightarrow \varphi$ surjectif $\Rightarrow \psi$ surjectif.

idem par (2).

Finalement, on a :

$p \in \Sigma \iff \mathbb{F}_p[X]/(X^2+1)$ n'est pas intègre

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

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

$\iff \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$

$\iff p \equiv 1 \ [4]$.

2) $\boxed{\Leftarrow}$ $n = \underbrace{\left(\prod_{\substack{p \in \mathcal{P} \\ p \equiv 3[4]}} p^{v_p(n)/2}\right)^2}_{\in \Sigma'} \underbrace{\left(\prod_{\substack{p \in \mathcal{P} \\ p \equiv 1[4]}} p^{v_p(n)}\right)}_{\in \Sigma' \text{ car } p \equiv 1[4]} \in \Sigma'$

$\boxed{\Rightarrow}$ Notons $\mathcal{P}_n$: " $n \in \Sigma$ et $p \equiv 3[4] \Rightarrow v_p(n)$ est pair "

$\underline{\mathcal{P}_0}$: $v_p(0) = 0 \quad \forall p \in \mathcal{P}$.

$\underline{\mathcal{P}_0, \dots, \mathcal{P}_{n-1}}$: soit $p \equiv 3[4] \iff p$ irréd dans $\mathbb{Z}[i]$

$p \mid n \Rightarrow p \mid a^2+b^2 = (a-ib)(a+ib) \Rightarrow p \mid a+ib$ (ex) $\Rightarrow p \mid a$ et $p \mid b$

Donc $p^2 \mid n$. On écrit $a = pa'$ et $b = pb'$: $\frac{n}{p^2} = a'^2 + b'^2 \in \Sigma'$

HR : $v_p\left(\frac{n}{p^2}\right)$ est pair donc $v_p(n) = v_p\left(\frac{n}{p^2}\right) + 2$ l'est aussi. ∎