

# Théorème des deux carrés.

Ref: Perrin 127

121

122

120

Notations: On introduit:  $\mathbb{Z} = \{n \in \mathbb{N}, n = a^2 + b^2, (a, b) \in \mathbb{N}^2\}$ .

$\mathbb{Z}[i] = \{a + ib, (a, b) \in \mathbb{Z}^2\}$  sous anneau de  $\mathbb{C}$  (intégral)

$N: \mathbb{Z}[i] \rightarrow \mathbb{N}$

$z = (a + ib) \mapsto z\bar{z} = a^2 + b^2$ .

est multiplicative  $N(zz') = N(z)N(z')$

1) Lemme 1:  $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ .

2) Lemme 2:  $\mathbb{Z}$  est stable par  $\times$

3) Lemme 3:  $\mathbb{Z}[i]$  est euclidien donc principal

4) Lemme 4:  $(p \in \mathbb{Z})$  si  $(p$  pas irréductible dans  $\mathbb{Z}[i])$  pour  $p \in \mathcal{P}$ .

Théorème: Soit  $p \in \mathcal{P}$ ,  $(p \in \mathbb{Z}) \Leftrightarrow p=2$  ou  $p \equiv 1[4]$ .

1) Soit  $z \in \mathbb{Z}[i]^*$ ,  $z\bar{z} = 1$  donc  $\underbrace{N(z)}_{\in \mathbb{N}} \underbrace{N(\bar{z})}_{\in \mathbb{N}} = 1$  donc  $N(z) = N(\bar{z}) = 1$ .

Si  $z = a + ib$ , alors  $a^2 + b^2 = 1$  donc  $\begin{cases} a=0 \\ b=\pm 1 \end{cases}$  ou  $\begin{cases} a=\pm 1 \\ b=0 \end{cases}$  donc  $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$

On vérifie l'inclusion réciproque.

2)  $n \in \mathbb{Z}$  si  $\exists z \in \mathbb{Z}[i] \text{ tq } n = N(z)$

Donc pour  $(n, n') \in \mathbb{Z}^2$  tq  $n = N(z)$  et  $n' = N(z')$ ,  $nn' = N(zz')$

Si  $z = a + ib$  et  $z' = c + id$ ,

on a  $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$ .

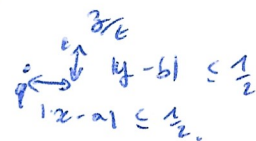
3) Soient  $(z, t) \in (\mathbb{Z}[i] \setminus \{0\})^2$

On veut faire la D.E. de  $z$  par  $t$ .

$z/t \in \mathbb{C}$ , on l'approxime par  $q \in \mathbb{Z}[i]$ : si  $z/t = x + iy$ ,  $q = a + ib$

où  $a$  et  $b$  sont les entiers les plus proches de  $x$  et  $y$ .

Ainsi,  $|z/t - q| \leq \frac{\sqrt{2}}{2} < 1$ .



On pose alors  $r = z - qt$  de sorte que  $r \in \mathbb{Z}[i]$

$r = t(z/t - q)$  d'où  $|r| = |t| |z/t - q| < |t|$ .

Donc  $N(r) < N(t)$ .

Donc  $z = qt + r$  avec  $N(r) < N(t)$ .

4)  $\Rightarrow$  Soit  $p \in \mathcal{P}$  tq  $p = a^2 + b^2$ , alors  $p = (a + ib)(a - ib)$  et  $a, b \neq 0$ .

Donc  $a + ib, a - ib \notin \mathbb{Z}[i]^*$  d'après lemme 1.

Donc  $p$  n'est pas irréductible.

$\Leftarrow$  Réciproquement, soit  $p \in \mathcal{P}$  tq  $p = z\bar{z}$  où  $z, \bar{z} \notin \{\pm 1, \pm i\}$

alors  $N(p) = N(z)N(z')$  d'après lemme 2,  
 $= p^2$

et comme  $N(z), N(z') \neq 1$ ,  $p = N(z)$   
 donc  $p \in \Sigma$ .

5) D'après lemme 3),  $\mathbb{Z}[\cdot]$  est principal, donc factoriel.

~~donc~~  $p \in \Sigma$  si  $p$  n'est pas irréductible dans  $\mathbb{Z}[\cdot]$  d'après lemme 4  
 si  $(p) = p \mathbb{Z}[\cdot]$  est non premier ~~car  $\mathbb{Z}[\cdot]$  factoriel~~  
 si  $\mathbb{Z}[\cdot]/(p)$  est non intègre.

On a l'isomorphisme  $\mathbb{Z}[\cdot] \simeq \mathbb{Z}[x]_{(x^2+1)}$

D'après le théorème d'isomorphisme :  $\mathbb{Z}[\cdot]/(p) \simeq \frac{\mathbb{Z}[x]}{(x^2+1, p)}$  

$$\simeq \frac{\mathbb{Z}[x]/(p)}{(x^2+1)}$$

$$\simeq \frac{\mathbb{F}_p[x]}{(x^2+1)}$$

Donc  $p \in \Sigma$  si  $x^2+1$  non irréductible dans  $\mathbb{F}_p[x]$

si  $x^2+1$  a une racine dans  $\mathbb{F}_p[x]$

si  $-1 \in \mathbb{F}_p^{\times 2}$

si  $p=2$  ou  $(-1) = y^2$

si  $p \equiv 1 \pmod{4}$  ou  $(-1)^{\frac{p-1}{2}} = y^{p-1} = 1$

si  $p \equiv 3 \pmod{4}$  ou  $\frac{p-1}{2}$  est pair

si  $p=2$  ou  $p \equiv 1 \pmod{4}$ .

⊗ Soient  $A$  anneau,  $I, J$  idéaux,  $A/(I, J) \simeq A/I / \pi_I(J)$

preuve :

$$\begin{array}{ccc} A & \xrightarrow{\pi} & A/I \\ \pi_I \downarrow & \searrow f & \uparrow g \\ A/I & \xrightarrow{\pi'} & A/I / \pi_I(J) = A/I / \pi_I(J) \end{array}$$

On  $x \in A$ ,  $\pi_I(x) \in A/I$  si  $0 \pi_I(x) = \pi(x)$

si  $\pi(x) = \pi(0)$

si  $x \in \ker(\pi) = (I, J)$

si  $\pi_I(x) \in \pi_I(J)$