leçons:
121 : Nombres premiers.
122 : Anneaux principaux
126 : Exemples d'équations diophantiennes

Sommes de deux carrés

46

Références:
Perrin "Cours d'algèbre"

Thm: 1) $\mathbb{Z}[i]$ est principal

2) Les irréductibles de $\mathbb{Z}[i]$ sont (à un inversible près):

- les $p \in \mathbb{Z}$ premiers tels que $p \equiv 3\ [4]$
- les $a+ib \in \mathbb{Z}[i]$ tels que a^2+b^2 est premier

3) Application : Soit $p \in \mathbb{Z}$ premier, p s'écrit comme somme de deux carrés entiers ssi $(p=2)$ ou $p \equiv 1\ [4]$

On note $\Sigma = \{n \in \mathbb{N} \mid \exists a,b \in \mathbb{N} \quad n = a^2+b^2\}$

preuve:

① On pose $N : \begin{cases} \mathbb{Z}[i] \to \mathbb{N} \\ a+ib \mapsto a^2+b^2 \end{cases}$. MQ $\mathbb{Z}[i]$ est un anneau euclidien pour N:

Soit $(x,y) \in \mathbb{Z}[i]^2, y \neq 0$. On écrit $\frac{x}{y} = u+iv \in \mathbb{C}$.

$\exists (a,b) \in \mathbb{Z}^2 \mid |a-u| \leq \frac{1}{2}$ et $|b-v| \leq \frac{1}{2}$

Alors $\left|\frac{x}{y} - (a+ib)\right|^2 \leq \frac{1}{2}$

$|x - y(a+ib)|^2 \leq \frac{|y|^2}{2}$

ie $N(x - y(a+ib)) \leq \frac{N(y)}{2} < N(y)$. $\mathbb{Z}[i]$ est euclidien donc principal □

② MQ $\mathbb{Z}[i]^\times = \{1,-1,i,-i\} = \{z \in \mathbb{Z}[i] \mid N(z) = 1\}$

$z \in \mathbb{Z}[i]^\times \Rightarrow N(z) = 1 \Rightarrow z \in \{1,-1,i,-i\} \Rightarrow z \in \mathbb{Z}[i]^\times$ □

③ MQ si $p \in \mathbb{Z}$ est premier dans $\mathbb{Z}$, alors p irréductible dans $\mathbb{Z}[i] \iff p \equiv 3\ [4]$

p irréductible dans $\mathbb{Z}[i] \iff p$ premier dans $\mathbb{Z}[i]$ (par ①)

$\iff \mathbb{Z}[i]/(p)$ est intègre

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

p irréductible dans $\mathbb{Z}[i] \iff \mathbb{Z}/p\mathbb{Z}[X]/(X^2+1)$ intègre

$\iff (X^2+1)$ premier dans $\mathbb{Z}/p\mathbb{Z}[X]$

$\iff (X^2+1)$ irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$

$\iff -1$ n'est pas un carré modulo p

$\iff (-1)^{\frac{p-1}{2}} \equiv -1\ [p]$

$\iff p \equiv 3\ [4]$

Rq: ce raisonnement est valable pour $p \geq 3$. Pour $p=2$, on a $2 = (1+i)(1-i)$

④ Classification des irréductibles :

- Soit $x \in \mathbb{Z}[i]$ irréductible. Soit $p \in \mathbb{Z}$ un diviseur premier de $N(x)$ dans $\mathbb{Z}$.

1er cas : p irréductible dans $\mathbb{Z}[i]$ (ie $p \equiv 3\ [4]$)

$p \mid N(x) = x\bar{x}$ donc $p \mid x$ ou $p \mid \bar{x}$ car p premier dans $\mathbb{Z}[i]$

donc $p = x$ dans $\mathbb{Z}[i]/\mathbb{Z}[i]^\times$ ou $p = \bar{x}$ dans $\mathbb{Z}[i]/\mathbb{Z}[i]^\times$

donc $p = x$ dans $\mathbb{Z}[i]/\mathbb{Z}[i]^\times$

2e cas : p réductible dans $\mathbb{Z}[i]$

Soit $u \in \mathbb{Z}[i]$ un facteur irréductible (premier !) de p et écrivons $p = uv$ avec $u, v \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^\times$.

$p^2 = N(p) = N(u)N(v)$ donc $N(u) = p = N(v)$ (car $N(u) \geq 2$, $N(v) \geq 2$)

On en déduit, au passage, que si p est réductible, $p \in \Sigma$. La réciproque est claire.

$uv = p \mid N(x) = x\bar{x}$ donc $u \mid x$ ou $u \mid \bar{x}$

donc $u = x$ dans $\mathbb{Z}[i]/\mathbb{Z}[i]^\times$ ou $u = \bar{x}$ dans $\mathbb{Z}[i]/\mathbb{Z}[i]^\times$

donc $N(x) = p$ ou $N(x) = N(\bar{u}) = N(u) = p$

donc $N(x) = p$

- Soit $x \in \mathbb{Z}[i]$ réductible. Alors $x = uv$ avec $u, v \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^\times$

$N(x) = N(u)N(v)$ avec $N(u) \geq 2$, $N(v) \geq 2$ donc $N(x)$ n'est pas premier.

Avec ③ la réciproque est achevée.

⑤ Soit $\Sigma = \{n \in \mathbb{N} \mid \exists a, b \in \mathbb{N}\ n = a^2 + b^2\}$. Soit $n = \prod_{p \in \mathcal{P}} p^{v_p(n)} \in \mathbb{N}$

MQ $n \in \Sigma \iff \forall p \in \mathcal{P}, p \geq 3, \quad p \equiv 3\ [4] \Rightarrow v_p(n)$ pair

- La réciproque est claire car Σ est stable par multiplication ($n \in \Sigma \iff \exists z \in \mathbb{Z}[i]\ n = N(z)$ et $N(z)N(z') = N(zz')$)

- Sens direct : par récurrence. Soit $p \in \mathcal{P}$ tq $p \equiv 3\ [4]$ et $n \in \Sigma$.

(H_d) : si $v_p(n) \leq d$, alors $v_p(n)$ est pair

  - (H_0) est vraie
  - Supposons $v_p(n) \geq 1$: $p \mid n = a^2 + b^2 = (a+ib)(a-ib)$

donc $p \mid a+ib$ ou $p \mid a-ib$ (car p premier dans $\mathbb{Z}[i]$)

donc $p \mid a$ et $p \mid b$ (car $p \in \mathbb{Z}$)

donc si l'on pose $a = \tilde{a}p$ et $b = \tilde{b}p$, on a $n = p^2(\tilde{a}^2 + \tilde{b}^2)$

donc $p^2 \mid n$ et $\frac{n}{p^2} \in \Sigma$

On en déduit que $v_p(n) = 1$ est impossible, que (H_1) est vraie

et comme $v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2$, l'hypothèse de récurrence s'applique

et $v_p\left(n/p^2\right)$ est pair ☐ (où l'hypothèse de récurrence est $(H_{v_p(n)-2})$)

Complément sur les anneaux quotients

Soit $\left|\begin{array}{l} A \text{ un anneau} \\ I, J \text{ deux idéaux de } A \end{array}\right.$

On note $\pi_I : A \to A/_I$ et $\pi_J : A \mapsto A/_J$ les projections canoniques.

MQ $\quad (A/_I)/_{\pi_I(J)} \simeq A/(I,J) \simeq (A/_J)/_{\pi_J(I)}$ (isomorphismes d'anneaux)

Remarque : Formellement, on devrait écrire $\pi_I(J+I)$ (mais c'est le même ensemble) pour que $I+J$ contienne I et donc que $\pi_I(I+J)$ soit un idéal de $A/_I$.

preuve : On pose $\varphi : \begin{cases} A \longrightarrow (A/_I)/_{\pi_I(J)} \\ x \longmapsto c(\bar{x}) \end{cases}$ $\quad \varphi$ est un morphisme d'anneaux surjectif

où $\left|\begin{array}{l} \bar{x} \text{ est la classe de } x \text{ dans } A/_I \text{ (ie } \bar{x} = \pi_I(x)) \\ c(y) \text{ est la classe de } y \in A/_I \text{ dans } (A/_I)/_{\pi_I(J)} \end{array}\right.$

- Soit $x \in I$.

  $\varphi(x) = c(\bar{x}) = c(0) = 0$

  Soit $x \in J$.

  $\varphi(x) = c(x+I)$ et $x+I \in \pi_I(J)$ donc $\varphi(x) = 0$

  D'où $(I,J) \subset \operatorname{Ker} \varphi$

- Réciproque :

  Soit $x \in \operatorname{Ker}\varphi$.

  $\varphi(x) = c(x+I) = 0$

  Donc $x+I \in \pi_I(J)$

  $\exists y \in J \quad x+I = y+I$

  D'où $x \in I+J = (I,J)$